# SPARC M8 和 SPARC M7 服务器安全指南

文件号码 **E63777-02**
2017 年 9 月

ORACLE

**文件号码 E63777-02**



**文档可访问性**

有关 Oracle 对可访问性的承诺，请访问 Oracle Accessibility Program 网站 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc。

**获得 Oracle 支持**

购买了支持服务的 Oracle 客户可通过 My Oracle Support 获得电子支持。有关信息，请访问 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info；如果您听力受损，请访问 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs。

# 目录

# 了解硬件安全

应该将安全体系结构建立在物理隔离和访问控制的基础之上。确保物理服务器安装在安全的环境中，防止其遭受未经授权的访问。同样，记录所有序列号也有助于防止未经授权使用硬件组件。

以下几节提供了有关这些服务器的一般硬件安全准则。



## 限制人员接近

- 将服务器和相关设备安装在带锁并限制随意出入的房间内。
- 如果设备安装在带有门锁的机架中，则除非必须在机架内维修组件，否则应始终锁上机架门。锁上机架门还可以限制人员接近热插拔或热交换设备。
- 在带锁的机柜内存储所有备用的替换部件。仅限经授权的人员接近带锁机柜。
- 定期检验机架或备用机柜上锁的状况和完整性，防止或洞察锁受损或门无意中未上锁等情况。
- 将机柜钥匙保存在不得随意接近的安全位置。
- 限制人员接近 USB 控制台。系统控制器、配电设备 (power distribution unit, PDU) 和网络交换机之类的设备都可能有 USB 连接。由于物理访问不容易遭受网络攻击，因此是一种较安全的组件访问方法。
- 将控制台连接到外部 KVM 以实现远程控制台访问。KVM 设备通常支持双重验证、集中访问控制和审计。有关 KVM 的安全准则和最佳实践的更多信息，请参阅 KVM 设备随附的文档。

## 序列号

收到硬件组件并将其入库时，请仔细记录所有序列号，以防未经授权使用这些组件。在安装或使用任何组件之前，务必将其序列号与收到该组件时记录的序列号进行比较，以确保其真实可靠。遵循以下做法来保护硬件：

- 记录所有硬件的序列号。
- 为计算机硬件的所有重要物品（如更换部件）添加安全标记。使用特殊的紫外线笔或压纹标签。
- 将硬件激活密钥和许可证保存在一个安全位置，在系统出现紧急状况时系统管理员可以轻松访问该位置。打印的文档可能是证明所有权的唯一证据。

无线射频识别 (Radio Frequency Identification, RFID) 读取器可以进一步简化资产跟踪。可从以下位置获取 Oracle 白皮书《*How to Track Your Oracle Sun System Assets by Using RFID*》（《如何使用 RFID 跟踪 Oracle Sun 系统资产》）：

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

# 硬盘驱动器

硬盘驱动器（硬盘驱动器和固态驱动器）通常用来存储敏感信息。要防止这些信息遭受未经授权的披露，在重新使用、停止使用或处置硬盘驱动器之前，应该对其进行净化处理。

- 使用 Oracle Solaris `format`(1M) 命令等磁盘擦除工具彻底删除硬盘驱动器上的所有数据。
- 组织应当参考其数据保护策略来确定最合适的硬盘驱动器净化方法。
- 如果需要，可以利用 Oracle 的客户数据和设备保留服务。

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

# 了解软件安全

大多数硬件安全都通过软件方法实现。以下几节提供了有关这些服务器的一般软件安全准则。



## ▼ 防止未经授权的访问 (Oracle Solaris OS)

- **使用 Oracle Solaris OS 命令限制对 Oracle Solaris 软件的访问、强化 OS、使用安全功能以及保护应用程序。**
  从以下网址获取您使用的版本所对应的《*Oracle Solaris* 安全准则》文档：
  - `http://www.oracle.com/goto/solaris11/docs`
  - `http://www.oracle.com/goto/solaris10/docs`

## ▼ 防止未经授权的访问 (Oracle ILOM)

1. **使用 Oracle ILOM 命令限制对 Oracle ILOM 软件的访问、更改出厂设置的密码、限制 root 超级用户帐户的使用以及保护连接到服务处理器的专用网络。**
   从以下网址获取《*Oracle ILOM* 安全指南》：
   `http://www.oracle.com/goto/ilom/docs`

2. **如果可能，使用特定于平台的 Oracle ILOM 命令创建具有应用到特定物理域的角色的用户帐户，以此保护各个域。**
   将用户角色分配给物理域后，该域的功能会镜像这些为平台分配的用户角色，但是它们仅限于使用对指定组件执行的命令。

---

**注 -** 只能为单个物理域分配管理员 (a)、控制台 (c) 和重置 (r) 用户角色。

---

可从以下网址获取《*SPARC M8* 和 *SPARC M7* 服务器管理指南》：

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

## ▼ 防止未经授权的访问 (Oracle VM Server for SPARC)

- **使用 Oracle VM for SPARC 命令限制对 Oracle VM for SPARC 软件的访问。**
  从以下网址获取《*Oracle VM for SPARC Security Guide*》：http://www.oracle.com/goto/vm-sparc/docs。

# 限制访问 (OBP)

这些主题介绍了如何在 OBP 提示符下限制访问。



有关设置 OpenBoot 安全变量的信息，请参阅 OpenBoot 文档，网址为：

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

## ▼ 实现密码保护

- **如果您尚未设置密码，则执行此步骤。**

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

密码可以是一到八个字符。如果输入的字符超过八个，将仅使用前八个字符。接受所有可输出的字符。不接受控制字符。

---

**注 -** 将密码设置为零个字符会关闭安全性并视同 `security-mode` 参数设置为 none。但是，不会更改此设置。

---

## ▼ 启用安全模式

1. **将 `security-mode` 参数设置为 `full` 或 `command`。**

   设置为 `full` 时，必须提供密码才能执行包括正常操作（如 `boot`）在内的任何操作。设置为 `command` 时，`boot` 或 `go` 命令不需要密码，但所有其他命令都需要密码。出于业务持续性考虑，请将 `security-mode` 参数设置为 `command`，如以下示例所示。

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

2. **获取安全模式提示符。**

   如上所述设置安全模式后，可使用以下两种方式之一获取安全模式提示符。

   - **使用 `logout` 和 `login` 命令。**

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

     要退出安全模式，请使用 `logout` 和 `login` 名称。

   - **使用 `reset-all` 命令。**

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

     此命令可以重置系统。系统重新启动时，OpenBoot 转至安全模式提示符。要重新登录到命令提示符（或者从安全模式中注销），请使用 `logout` 和 `login` 名称，然后输入密码，如上所述。

## ▼ 禁用安全模式

1. **将 `security-mode` 参数设置为 `none`。**

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

2. **通过在两次密码提示后都按回车键将密码设置为零长度。**

## ▼ 检查失败的登录 (OBP)

1. **确定是否有人尝试使用 `security-#badlogins` 参数访问 OpenBoot 环境且访问失败，如以下示例所示。**

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

如果此命令返回任何大于 Ø 的值，则记录了访问 OpenBoot 环境失败的尝试。

2. **通过键入以下内容重置该参数：**

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

### ▼ 提供打开电源横幅

虽然横幅不是直接预防或检测控件，但会出于以下原因使用它：

- 通报所有权。
- 警告用户注意服务器的使用限制。
- 指示将对 OpenBoot 参数的访问和修改限制为经授权的人员。

- **使用以下命令启用定制警告消息。**

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

横幅消息最多可以为 68 个字符。接受所有可输出的字符。

## Oracle 系统固件

Oracle 系统固件使用受控更新过程防止未经授权的修改。只有超级用户或具有相应授权的已验证身份的用户才可以使用该更新过程。

有关如何获取最新更新或修补程序的信息，请参阅以下网址的产品说明：

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

## 安全 WAN Boot

WAN Boot 支持多种安全级别。可以组合使用 WAN Boot 中支持的安全功能来满足网络需求。虽然较安全的配置需要额外的管理，但是却可以较大程度地保护您的系统数据。

- 有关 Oracle Solaris 10 OS，请参阅《*Oracle Solaris* 安装指南：基于网络的安装》一书中关于保护 WAN Boot 安装配置的信息。

  请参见 http://www.oracle.com/goto/solaris10/docs
- 有关 Oracle Solaris 11 OS，请参阅《*Securing the Network in Oracle Solaris*》。

请参见 http://www.oracle.com/goto/solaris11/docs