

SuperCluster 系统

安全指南

版权所有 © 2011, 2013, Oracle 和/或其附属公司。保留所有权利。

本软件和相关文档是根据许可证协议提供的，该许可证协议中规定了关于使用和公开本软件和相关文档的各种限制，并受知识产权法的保护。除非在许可证协议中明确许可或适用法律明确授权，否则不得以任何形式、任何方式使用、拷贝、复制、翻译、广播、修改、授权、传播、分发、展示、执行、发布或显示本软件和相关文档的任何部分。除非法律要求实现互操作，否则严禁对本软件进行逆向工程设计、反汇编或反编译。

此文档所含信息可能随时被修改，恕不另行通知，我们不保证该信息没有错误。如果贵方发现任何问题，请书面通知我们。

如果将本软件或相关文档交付给美国政府，或者交付给以美国政府名义获得许可证的任何机构，必须符合以下规定：

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.

本软件或硬件是为了在各种信息管理应用领域内的一般使用而开发的。它不应被应用于任何存在危险或潜在危险的应用领域，也不是为此而开发的，其中包括可能会产生人身伤害的应用领域。如果在危险应用领域内使用本软件或硬件，贵方应负责采取所有适当的防范措施，包括备份、冗余和其它确保安全使用本软件或硬件的措施。对于因在危险应用领域内使用本软件或硬件所造成的一切损失或损害，Oracle Corporation 及其附属公司概不负责。

Oracle 和 Java 是 Oracle 和/或其附属公司的注册商标。其他名称可能是各自所有者的商标。

Intel 和 Intel Xeon 是 Intel Corporation 的商标或注册商标。所有 SPARC 商标均是 SPARC International, Inc 的商标或注册商标，并应按照规定许可证的规定使用。AMD、Opteron、AMD 徽标以及 AMD Opteron 徽标是 Advanced Micro Devices 的商标或注册商标。UNIX 是 The Open Group 的注册商标。

本软件或硬件以及文档可能提供了访问第三方内容、产品和服务的方式或有关这些内容、产品和服务的信息。对于第三方内容、产品和服务，Oracle Corporation 及其附属公司明确表示不承担任何种类的担保，亦不对其承担任何责任。对于因访问或使用第三方内容、产品或服务所造成的任何损失、成本或损害，Oracle Corporation 及其附属公司概不负责。

目录

1. SuperCluster 系统安全指南	5
了解安全原则	5
规划安全环境	6
硬件安全	6
软件安全	6
固件安全	7
Oracle ILOM 固件	7
维护安全环境	7
硬件控制	7
资产跟踪	7
软件和固件	7
本地和远程访问	8
数据安全	8
网络安全	8
相关安全指南	9

1

... 第 1 章

SuperCluster 系统安全指南

本文档提供常规安全准则以帮助您保护 Oracle 硬件产品，如服务器、网络交换机、网络接口卡等。

本章包含以下几节：

- “了解安全原则”— [5]
- “规划安全环境”— [6]
- “维护安全环境”— [7]
- “相关安全指南”— [9]

了解安全原则

有四个基本安全原则：访问、验证、授权和记帐。

• 访问

物理和软件控制是保护硬件或数据免遭入侵所必需的。

- 对于硬件，访问限制通常是指物理访问限制。
- 对于软件，则通过物理和虚拟方法来限制访问。
- 除非通过 Oracle 更新过程，否则无法更改固件。

• 验证

所有平台操作系统都提供可设置的验证功能，以确保用户为他们所声明的身份。

验证通过诸如胸卡和密码之类的措施提供不同程度的安全性。

• 授权

授权使公司职员只能使用他们经过培训并有资格使用的硬件和软件。为实现此目的，系统管理员将创建包含读/写/执行权限的系统，以控制用户对命令、磁盘空间、设备和应用程序的访问。

• 记帐

Oracle 软件和硬件功能允许客户 IT 部门监视登录活动和维护硬件库存。

- 可通过系统日志监视用户登录。尤其是系统管理员和服务帐户可以访问许多功能强大的命令，应当通过系统日志进行仔细监视。日志通常会被维护较长的一段时间，因此，当日志文件超出合理大小时，有必要根据客户公司政策定期弃用一些日志文件。

- 通常通过序列号跟踪客户 IT 资产。Oracle 部件号以电子方式记录在所有卡、模块和主板上，并可用于库存目的。

规划安全环境

在安装和配置服务器及相关设备之前和期间内，请遵循以下注意事项。

硬件安全

保护物理硬件的方式非常简单：限制对硬件的接近并记录序列号。

- 限制接近
 - 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。
 - 热插拔或热交换设备可以轻松地移除，特别需要限制人员的接近。
 - 在带锁的机柜中存储备用现场可更换单元 (Field-Replaceable Unit, FRU) 或客户可更换单元 (Customer-Replaceable Unit, CRU)。仅限经授权的人员接近带锁机柜。
- 记录序列号
 - 对计算机硬件的所有重要物项（如 FRU）添加安全标记。使用特殊的紫外线笔或压纹标签。
 - 记录所有硬件的序列号。
 - 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。

软件安全

大多数硬件安全都通过软件方法实现。

- 安装新系统时，更改所有默认密码。大多数类型的设备都使用默认密码（如 `changeme`），这些密码广为人知，从而有可能导致对设备进行未经授权的访问。此外，默认情况下，一些设备（如网络交换机）可能有多个用户帐户。请确保更改所有帐户密码。
- 限制 `root` 超级用户帐户的使用。而是应尽可能使用 Oracle Integrated Lights Out Manager (Oracle ILOM) 帐户（如 `ilom-operator` 和 `ilom-admin`）。
- 对服务处理器使用专用网络，从而将其与常规网络隔离。
- 在 Oracle Solaris 安装过程中，将提示您为系统创建用户帐户和密码，以及 `root` 用户密码。在此过程中，`root` 用户是您承担的一个角色。如果您要更改此帐户的设置，可以删除 `root` 用户帐户，并将 `root` 角色提供给拥有较少特权的用户。
- 保护对 USB 控制台的访问。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，这些连接可以提供比 SSH 连接更强大的访问功能。
- 请参阅软件随附的文档以启用可用于该软件的任何安全功能。
- 可以使用 WAN Boot 或 iSCSI Boot 安全地引导服务器。有关信息，请参阅相应 Oracle Solaris 发行版的《Oracle Solaris 安装指南：基于网络的安装》一书。

Oracle Solaris 安全准则文档提供有关以下内容的信息：

- 如何强化 Oracle Solaris
- 配置系统时如何使用 Oracle Solaris 安全功能
- 将应用程序和用户添加到系统时如何安全操作
- 如何保护基于网络的应用程序

可在以下位置找到 Oracle Solaris 安全准则文档：

- http://www.oracle.com/technetwork/indexes/documentation/index.html#sys_sw

固件安全

普通用户帐户无法编辑 OpenBoot PROM (OBP) 或其他 Oracle 固件。Oracle Solaris 操作系统使用受控固件更新过程来防止进行未经授权的固件修改。只有超级用户可以使用该更新过程。

有关设置 OBP 安全变量的信息，请参阅《*OpenBoot 4.x Command Reference Manual*》，网址为：

- <http://download.oracle.com/docs/cd/E19455-01/816-1177-10/cfg-var.html#pgfid-17069>

Oracle ILOM 固件

Oracle Integrated Lights Out Manager (Oracle ILOM) 是预先安装在某些 SPARC 服务器上的系统管理固件。借助 Oracle ILOM，可以有效管理和监视系统中安装的组件。您使用 Oracle ILOM 的方式将影响系统的安全性。要了解有关设置密码、管理用户以及应用与安全相关的功能（包括安全 Shell (Secure Shell, SSH)、安全套接字层 (Secure Socket Layer, SSL) 和 RADIUS 验证）时如何使用该固件的更多信息，请参阅 Oracle ILOM 文档：

- <http://www.oracle.com/pls/topic/lookup?ctx=E19860-01>

维护安全环境

Oracle 硬件和软件提供了许多用于控制硬件和跟踪资产的安全功能。

硬件控制

某些 Oracle 系统可设置为通过软件命令打开和关闭。此外，某些系统机柜的配电设备 (Power Distribution Unit, PDU) 也可以通过软件命令远程启用和禁用。这些命令的授权通常在系统配置期间设置，并且通常仅限系统管理员和服务人员使用这些命令。有关详细信息，请参阅系统或机柜文档。

资产跟踪

Oracle 序列号嵌入在选件卡和系统主板上的固件中。可以通过局域网连接读取这些序列号以进行库存跟踪。

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>

软件和固件

- 始终在设备上安装软件或固件的最新发行版本。一些设备（如网络交换机）包含固件，可能需要修补程序和固件更新。
- 为您的软件安装任何必要的安全修补程序。

本地和远程访问

请遵循以下准则以确保对系统的本地和远程访问的安全性：

- 创建标题以指出禁止未经授权的访问。
- 在适用的情况下使用访问控制列表。
- 设置扩展会话的超时时间，并设置特权级别。
- 针对交换机的本地和远程访问，使用验证、授权和记帐 (Authentication, Authorization, and Accounting, AAA) 功能。
- 如果可能，使用 RADIUS 和 TACACS+ 安全协议：
 - RADIUS (Remote Authentication Dial In User Service，远程验证拨入用户服务) 是一种客户机/服务器协议，可保护网络免受未经授权的访问。
 - TACACS+ (Terminal Access Controller Access-Control System，终端访问控制器访问控制系统) 是一种协议，它允许远程访问服务器与验证服务器通信，以确定用户是否有权访问网络。
- 对入侵检测系统 (Intrusion Detection System, IDS) 访问使用交换机的端口镜像功能。
- 实施端口安全，以基于 MAC 地址限制访问。对所有端口禁用自动中继。
- 使用 SSH 而非 Telnet 限制只有特定的 IP 地址才可以进行远程配置。Telnet 以明文形式传递用户名和密码，可能使 LAN 段上的每个人都能看到登录凭据。为 SSH 设置强密码。
- 全面设置 {SuperCluster 系统 后，作为一种系统安全措施，安装人员将禁用所有 SSH 密钥，并且还将使所有密码过期。如果不希望禁用 SSH 密钥或使密码过期，请在 SuperCluster 系统 安装结束时与安装人员讨论此问题。
- SNMP 的早期版本不安全（以未加密的文本形式传输验证数据）。只有 SNMP 的版本 3 可以提供安全传输。
- 某些产品出厂时便将 PUBLIC 设置为默认 SNMP 团体字符串。攻击者可以查询团体以绘制非常完整的网络图，并可能修改管理信息库 (Management Information Base, MIB) 值。如果 SNMP 是必需的，请将默认的 SNMP 团体字符串改为加强的团体字符串。
- 启用日志记录并向专用安全日志主机发送日志。
- 使用 NTP 和时间戳配置日志记录以包含准确的时间信息。
- 查看日志以发现可能的事件，并根据安全策略将其归档。
- 如果系统控制器使用浏览器界面，请确保在使用后注销。

数据安全

请遵循以下准则以最大限度地确保数据安全：

- 使用外部硬盘驱动器、笔式驱动器或记忆棒等设备备份重要数据。将备份的数据存储在另一个不在现场的安全位置。
- 使用数据加密软件确保硬盘驱动器上的机密信息安全。
- 处置旧硬盘驱动器时，请物理销毁该驱动器或彻底清除该驱动器上的所有数据。删除所有文件或重新格式化驱动器将仅删除驱动器上的地址表 - 删除文件或重新格式化驱动器后，仍然可以恢复驱动器中的信息。（使用磁盘擦除软件彻底清除驱动器上的所有数据。）

网络安全

请遵循以下准则以最大限度地确保网络安全：

- 大多数交换机允许您定义虚拟局域网 (Virtual Local Area Network, VLAN)。如果您使用交换机定义 VLAN，请将系统的敏感群集与网络的其余部分隔离。这样可以降低用户访问这些客户机和服务器上信息的可能性。

- 带外管理交换机（与数据通信隔开）。如果带外管理不可行，则专门使用一个单独的 VLAN 号进行带内管理。
- 确保 Infiniband 主机安全。Infiniband 光纤网络的安全程度取决于其安全程度最低的 Infiniband 主机。
- 请注意，分区不会保护 Infiniband 光纤网络。分区只会使主机上各虚拟机之间的 Infiniband 通信相互隔离。
- 脱机维护交换机配置文件，并且仅限授权的管理员访问。该配置文件应包含每个设置的描述性注释。
- 如果可能，使用静态 VLAN 配置。
- 禁用未使用的交换机端口，并为其指定未使用的 VLAN 号。
- 为中继端口指定唯一本机 VLAN 号。
- 将可通过中继传输的 VLAN 仅限于绝对必需的那些 VLAN。
- 如果可能，禁用 VLAN 中继协议 (VLAN Trunking Protocol, VTP)。否则，为 VTP 设置以下内容：管理域、密码和删除。然后将 VTP 设置为透明模式。
- 禁用不必要的网络服务，如 TCP 小型服务器或 HTTP。启用必要的网络服务并以安全方式配置这些服务。
- 不同的交换机将提供不同级别的端口安全功能。如果您的交换机具有以下端口安全功能，请使用这些功能：
 - MAC 绑定 (MAC Locking)：这涉及将一个或多个连接设备的介质访问控制 (Media Access Control, MAC) 地址绑定到交换机上的物理端口。如果将交换机端口绑定到特定的 MAC 地址，超级用户将无法利用非法接入点在您的网络中创建后门。
 - MAC 锁定 (MAC Lockout)：这将禁止指定的 MAC 地址连接到交换机。
 - MAC 学习 (MAC Learning)：使用有关每个交换机端口的直接连接的知识，以便交换机可以基于当前连接设置安全性。

相关安全指南

SuperCluster 系统中使用的软件和硬件组件还可能有特定于产品的安全指南。下面列出了 SuperCluster 系统中使用的组件以及特定于产品的安全指南所在的位置（如果这些组件的安全指南可用）：

- SPARC T4-4 服务器：

http://www.oracle.com/pls/topic/lookup?ctx=E23411_01

- SPARC T5-8 服务器：

http://www.oracle.com/pls/topic/lookup?ctx=E35078_01

- Sun ZFS Storage 7320 设备：

http://www.oracle.com/pls/topic/lookup?ctx=ZFS_Storage_7x20_2011.1

- Sun Datacenter InfiniBand Switch 36 交换机：

<http://www.oracle.com/pls/topic/lookup?ctx=E19197-01>

- Exadata 存储服务器：安装在 Exadata 存储服务器上 /opt/oracle/cell/doc} 目录中的文档
- Oracle Solaris 操作系统：

http://www.oracle.com/technetwork/documentation/index.html#sys_sw

