Netra 模块化系统安全指南

文件号码 E68381-01
2015 年 8 月

ORACLE

文件号码 E68381-01

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

安全概览

Oracle Netra 模块化系统是一款预先集成和预先布线的平台，可以完全虚拟化，从而降低了数据中心的成本和部署时间。该模块化系统包括您指定的硬件并在出厂时已装配好，一同发送给您。

以下主题介绍了有关模块化系统的安全概念和功能：

基本安全原则

对于所有模块化系统软件和硬件，均应遵循以下基本安全准则：

- 验证 – 验证就是识别用户的身份，通常是通过用户名和密码或共享密钥等保密信息来进行。验证可确保硬件或软件的用户与其表明的身份相符。默认情况下，使用本地用户名和密码进行验证。也可以使用基于共享密钥的验证。
- 记帐和审计 – 记帐和审计用于维护用户在系统中执行的活动的记录。利用模块化系统相关软件和硬件功能，管理员可以监视登录活动并维护硬件清单：
  - 可通过系统日志监视用户登录。系统管理员和服务帐户有权访问由于误用而导致损坏和数据丢失的命令。
  - 通过序列号跟踪硬件资产。Oracle 部件号以电子方式记录在所有卡、模块和主板上，并可用于盘点目的。

高级安全注意事项

除了基本安全原则外，模块化系统还需要具有持续有效性和深度防御功能。模块化系统提供了一系列良好集成的安全功能，能够满足重要安全要求和关注事项。以下各节介绍了这些原则：

- 任务关键型工作负载的持续有效性 – 为任务关键型工作负载选择硬件和软件平台的组织可以确信，模块化系统能够防止内部用户或外部各方由于意外操作和恶意操作而造

成的损坏或将其降至最低。作为“Oracle 最高可用性体系结构”最佳做法的一部分，以下做法可提高持续有效性：

- 确保所用组件已经过设计、制造和测试，能够很好地支持安全部署体系结构。模块化系统支持安全隔离、访问控制、服务质量和安全管理。
- 降低其组成产品的默认攻击面，有助于将计算机的整体风险降至最低。
- 使用开放但经过审查的完整协议以及能够支持传统安全目标（强验证、访问控制、保密性、完整性和可用性）的 API 保护计算机（包括其运行的管理接口）。
- 确认软件和硬件都包含即使在出现故障时仍能保持服务可用的功能。在攻击者尝试禁用系统中一个或多个单独组件时，这些功能非常有用。

- 用于保护操作环境的深度防御 – 模块化系统采用了多种独立且又相互增强的安全控件，从而有助于为工作负载和数据创建一个安全的操作环境。模块化系统支持深度防御原则，如下所述：
  - 提供强有力的补充保护，从而确保信息在传输、使用和闲置时的安全。在服务器和网络层提供安全控件。每层的独特安全控件都可以与其他层的安全控件集成，从而能够创建强有力的分层安全体系结构。
  - 支持使用定义明确的开放标准、协议和接口。模块化系统可以与现有的安全策略、体系结构、做法和标准集成。

安全功能

模块化系统硬件和软件都进行了强化。Oracle 还针对 NTP 和 SSH 之类的服务提供了建议的安全配置。此外，模块化系统的体系结构还为核心组件提供了安全功能。部署分层安全策略的组织最经常应用这些安全功能。这些功能分为以下几种类别：

- “网络通信隔离” [8]
- “Oracle ILOM 安全管理” [9]

网络通信隔离

如果要整合 IT 基础结构，应实施共享服务体系结构、提供安全的多租户服务，并考虑隔离网络通信。模块化系统提供了灵活性，可以根据需要实施隔离策略和战略。

在物理网络级别，将客户机访问与设备管理和设备间通信隔离。将客户机网络通信与管理网络通信隔离在单独的网络中。通过冗余 10 Gbps 以太网网络提供客户机访问，确保对系统上运行的服务进行高速可靠的访问。通过物理上独立的 1 Gbps 以太网网络提供管理访问。这样能够将运行网络和管理网络分隔开。

通过配置虚拟 LAN (virtual LAN, VLAN)，组织可以选择进一步隔离客户机访问以太网网络上的网络通信。VLAN 根据其要求隔离网络通信。Oracle 建议在 VLAN 上使用加密的协议，以确保通信的保密性和完整性。

Oracle ILOM 安全管理

需要使用安全控件和功能集合才能适当保护各个应用程序和服务。通过综合管理功能来维护已部署服务和系统的安全也同样重要。模块化系统使用 Oracle ILOM 的安全管理功能。

Oracle ILOM 是一个嵌入在模块化系统计算节点中的 SP。Oracle ILOM 用于执行带外管理活动，如下所述：

- 提供安全访问，以执行对数据库和存储服务器的安全快速远程管理。访问包括受 SSL 保护的基于 Web 的访问、使用安全 Shell 的命令行访问以及 IPMI v2.0 和 SNMPv3 协议。
- 使用基于角色的访问控制模型分离职责要求。为各个用户分配特定角色以限制可执行的功能。
- 提供有关所有登录和配置更改事项的审计记录。每个审计日志条目都会列出执行操作的用户和时间戳。利用审计记录，组织能够检测未授权的活动或更改，并把这些操作归还给特定用户。

有关 Oracle ILOM 安全的更多信息，请参阅《*Oracle ILOM* 安全指南》，网址为 http://www.oracle.com/goto/ILOM/docs。

规划安全环境

安全准则应在 Netra 模块化系统到位之前制定就绪。系统安装之后，应定期审核和调整安全准则，以便与组织当前的安全要求保持同步。

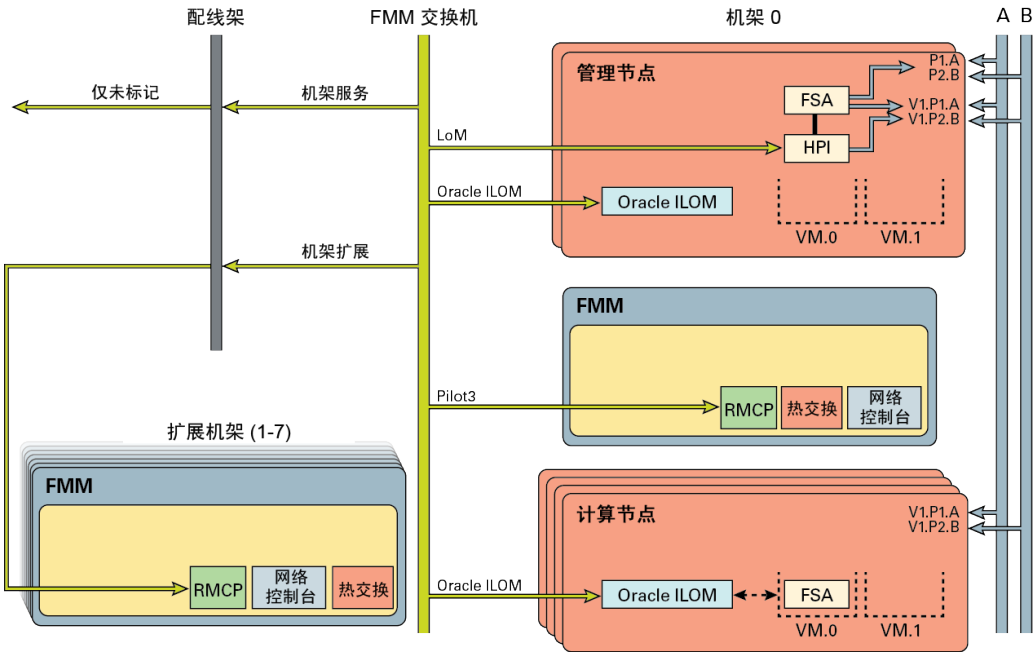
以下主题提供了有关安装 Netra 模块化系统的安全准则：

有关您所用系统和特定环境的其他安全要求，请联系您的 IT 安全主管。

默认网络

下图及描述介绍了 Netra 模块化系统的默认网络。

- 系统/遥测网络（浅绿色网络）在 VLAN 4090 上包括管理节点的 LoM 端口（通过 FMM 交换机）。
- 位于内部 VLAN 4094（带有 FMM）中的遥测 ILOM 网络包括计算节点 Oracle ILOM 和网络节点 Oracle ILOM（通过 FMM 交换机）。
- 配线架将遥测网络扩展到机架 1-7。多机架配置支持相同的子网以及具有不同机架 ID 的 VLAN
- VLAN(1) 通过合适的验证为遥测网络提供其他服务。
- 数据网络（A 和 B）提供对 FSA 节点的带内访问。
- HA 应用程序可通过模块化系统的公开接口（JMX、C- API 等）管理机架。



用户帐户

此表列出了模块化系统组件的默认用户和密码。安装 Netra 模块化系统之后，请更改所有默认密码。

组件	用户名和密码
以太网交换机	`root/changeme` 注 - 保护 `admin` 用户的 `enable mode password` 和 `secret` 值。
管理节点和计算节点	`root/changeme`

默认安全设置

模块化系统安装有多种默认安全设置。只要有可能并可行，就配置安全的默认设置。请参阅您的 Oracle ILOM 版本中的默认设置，网址为 http://www.oracle.com/goto/ILOM/docs。

保护硬件

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。确保物理系统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模块化系统的一般硬件安全准则。

访问限制

- 将系统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。
- 定期检验机架和备用机柜上锁的状况和完整性，以防止或发现擅自换锁或者门意外未上锁等情况。
- 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、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仔细记录所有序列号，从而防止未经授权使用该组件。在安装或使用任何组件之前，一定将其序列号与收到该组件时记录的序列号进行比较，确保其真实性。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项（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。 请参阅 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》），网址为 http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o11-001-rfid-oracle-214567.pdf。

硬盘驱动器

硬盘驱动器通常用来存储敏感信息。为防止未经授权泄露这些信息，在重新使用、停止使用或处置硬盘驱动器之前，要对其进行净化处理。

- 请参考您的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

保护软件

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 Netra 模块化系统的一般软件安全准则。

▼ 防止未经授权的访问 (Oracle Linux)

- 使用 Oracle Linux OS 命令限制对软件的访问、强化 OS、使用安全功能以及保护应用程序。

  请参阅《*Oracle Linux Security Guide for Release 6*》（《Oracle Linux 发行版 6 安全指南》），网址为 `http://docs.oracle.com/cd/E37670_01/E36387/html/index.html`。

▼ 防止未经授权的访问 (Oracle ILOM)

- 使用 Oracle ILOM 命令限制对 Oracle ILOM 固件的访问、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 SP 的专用网络。

  请参阅您的《*Oracle ILOM* 安全指南》版本，网址为 `http://www.oracle.com/goto/ILOM/docs`。

▼ 防止未经授权的访问（Oracle VM Server With Oracle Linux）

- 使用 Oracle Linux 命令限制对 Oracle VM Server 软件的访问、使用安全功能以及保护应用程序。

  请参阅《*Oracle VM Security Guide for Release 3.3*》（《Oracle VM 发行版 3.3 安全指南》），网址为 `http://docs.oracle.com/cd/E50245_01/E50254/html/index.html`。

Oracle Hardware Management Pack 安全性

Oracle Hardware Management Pack 采用两种组件（即 SNMP 监视代理和一系列跨操作系统的命令行界面工具 (CLI Tools)）来管理您的系统。

- Hardware Management Agent SNMP Plugins – SNMP 是一个用于监视或管理系统的标准协议。通过 Hardware Management Agent SNMP Plugins，您可以使用 SNMP 来监视数据中心中的 Oracle 系统，其优点是不必连接到两个管理点：主机和 Oracle ILOM。通过此功能，可以使用单个 IP 地址（主机的 IP 地址）来监视多个系统。

  SNMP Plugins 在 Oracle 系统的主机 OS 上运行。SNMP Plugin 可扩展主机 OS 中的本机 SNMP 代理，以提供其他 Oracle MIB 功能。Oracle Hardware Management Pack 本身不包含 SNMP 代理。对于 Oracle Linux，模块将添加到 `net-snmp` 代理。对于 Microsoft Windows，该插件可扩展本机 SNMP 服务。与 Oracle Hardware Management Pack 的 SNMP 相关的任何安全性设置均由本机 SNMP 代理或服务的设置（而不是插件）来决定。

  请注意，SNMPv1 和 SNMPv2c 不提供加密，并且使用团体字符串作为验证形式。相比之下，SNMPv3 更为安全，是建议使用的版本，因为它使用加密来提供安全的通道并使用单独的用户名和密码。
- Oracle Hardware Management Pack 文档 – 有关特定于 Oracle Hardware Management Pack 的安全准则，请参阅《*Oracle Hardware Management Pack (HMP)* 安全指南》，网址为 `http://www.oracle.com/goto/OHMP/docs`。

查找相关安全指南

安全指南

这些指南介绍了用于确保相关产品安全的策略和过程：

- 《Oracle Server X5-2 Security Guide》
- 《Oracle Switch ES2-72 and Oracle Switch ES2-64 Security Guide》
- 《*Oracle Linux Security Guide for Release 6*》（《Oracle Linux 发行版 6 安全指南》），网址为 `http://docs.oracle.com/cd/E37670_01/E36387/html/index.html`
- 《*Oracle ILOM* 安全指南》，网址为 `http://www.oracle.com/goto/ILOM/docs`
- 《*Oracle VM Security Guide for Release 3.3*》（《Oracle VM 发行版 3.3 安全指南》），网址为 `http://docs.oracle.com/cd/E50245_01/E50254/html/index.html`
- 《*Oracle Hardware Management Pack (HMP)* 安全指南》，网址为 `http://www.oracle.com/goto/OHMP/docs`