Oracle® ILOM 安全指南（固件发行版 3.0、3.1 和 3.2）

文件号码 E40361-04
2015 年 10 月

ORACLE

文件号码 E40361-04

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

使用本文档

- **概述** – 提供了关于 Oracle ILOM 安全任务准则的 Web 和 CLI 信息。请将本指南与 Oracle ILOM 文档库中的其他指南结合使用。
- **目标读者** – 技术人员、系统管理员、获得授权的 Oracle 服务提供商以及有系统硬件管理经验的用户。
- **必备知识** – 配置和管理 Oracle 服务器的经验。

产品文档库

可从以下网址获得有关该产品及相关产品的文档和资源：http://www.oracle.com/goto/ilom/docs。

反馈

可以通过以下网址提供有关本文档的反馈：http://www.oracle.com/goto/docfeedback

每个 Oracle ILOM 固件发行版的安全功能

使用下表确定开始提供某种 Oracle ILOM 安全功能的固件发行版。

在哪些固件版本中可用	安全功能	有关详细信息，请参见：
所有	验证和授权	■ “保护 Oracle ILOM 用户访问” [21]
所有	专用安全管理连接	■ “保护物理管理连接” [13] ■ “维护安全管理连接” [47]
所有	预先配置的加密网络端口	■ “预先配置的服务和网络端口” [17]
所有	IPMI 2.0 安全管理	■ “配置 IPMI 管理访问以实现最高级别的安全性” [42]
所有	安全 Shell 密钥加密配置	■ 使用服务器端密钥加密 SSH 连接 [39] ■ 将 SSH 密钥附加到用户帐户以实现自动 CLI 验证 [39]
所有	SNMP 3.0 安全管理	■ “配置 SNMP 管理访问以实现最高级别的安全性” [40]
所有	SSL 协议和证书	■ 将定制 SSL 证书和私钥上载到 Oracle ILOM [33] ■ 使用 OpenSSL 获取 SSL 证书和私钥 [32] ■ 启用最强的 SSL 和 TLS 加密属性 [34]
所有	远程控制台加密和安全协议	■ “安全地使用远程 KVMS” [50]
3.0.4 及更高版本	KVMS 主机锁定配置	■ 退出 KVMS 会话时锁定主机访问 [28]
3.0.4 及更高版本	会话超时配置	■ 设置非活动 Web 会话的超时间隔 [36] ■ 设置非活动 CLI 会话的超时间隔 [37]
3.0.12 及更高版本	本地主机互连验证会话	■ “首选的验证主机互连访问” [48]
3.0.8 及更高版本	登录标题配置	使用登录标题保护系统访问（3.0.8 及更高版本） [30]
3.0.8 到 3.1.2	WS-Management 安全访问	■ “配置 WS-Management 访问以实现最高级别的安全性” [44]
3.1.0 及更高版本	单独的审计日志	■ “监视审计事件以发现未经授权的访问” [54]
3.1.0 及更高版本	亲临现场安全检查	■ “出于安全考虑亲临现场重置 `root` 帐户的默认密码” [53]
3.2.4 及更高版本	IPMI 1.5 可配置属性	■ “配置 IPMI 管理访问以实现最高级别的安全性” [42]
3.2.4 及更高版本	TLS 协议版本 1.1 和 1.2	■ 启用最强的 SSL 和 TLS 加密属性 [34]
3.2.4 及更高版本	KVMS 会话计数	■ 限制 Remote System Console Plus（3.2.4 或更高版本）可查看的 KVMS 会话 [29]
3.2.4 及更高版本	符合 FIPS 的加密支持	■ “选择是否在部署时配置 FIPS 模式” [14] ■ “启用 FIPS 模式时不受支持的功能” [16] ■ “保护用户访问的部署后注意事项” [52]

在哪些固件版本中可用	安全功能	有关详细信息，请参见：
3.2.5 及更高版本	SSH 服务器状态和弱加密	■ SSH 服务器状态和弱加密的管理（3.2.5 及更高版本） [37]
3.2.5 及更高版本	本地用户帐户的密码策略	■ 为所有本地用户设置密码策略限制（3.2.5 及更高版本） [25]

其他安全信息

有关保护 Oracle ILOM 的更多信息，请参见本指南中的以下各节：

- Oracle ILOM 的安全最佳做法核对表
- Oracle ILOM 的部署安全最佳做法
- Oracle ILOM 的部署后安全最佳做法

Oracle ILOM 的安全最佳做法核对表

Oracle Integrated Lights Out Manager (ILOM) 是预先安装在所有 Oracle 服务器和大多数旧式 Sun 服务器中的服务处理器 (service processor, SP)。系统管理员使用 Oracle ILOM 的用户界面执行远程服务器管理任务，以及实时服务器运行状况监视操作。

为了确保为您的环境实施适用于 Oracle ILOM 的最佳安全做法，系统管理员应执行以下核对表中建议的安全任务：

- “服务器部署的安全核对表” [11]
- “服务器部署后的安全核对表” [12]

相关信息

- Oracle ILOM 的部署安全最佳做法
- Oracle ILOM 的部署后安全最佳做法
- 每个 Oracle ILOM 固件发行版的安全功能 [9]

服务器部署的安全核对表

为了确定规划新服务器部署时的最佳 Oracle ILOM 安全做法，系统管理员应执行下面表 1 “核对表 – 在服务器部署时配置 Oracle ILOM 安全 ”中建议的安全任务列表。

表 1　　核对表 – 在服务器部署时配置 Oracle ILOM 安全

✓	安全任务	适用的固件版本	有关详细信息，请参见：
	建立与 Oracle ILOM 的安全专用管理连接。	所有固件版本	■ “保护物理管理连接” [13]
	部署期间或部署后决定是需要符合 FIPS 140-2 安全标准，还是根本不需要。	固件版本 3.2.4 及更高版本	■ “选择是否在部署时配置 FIPS 模式” [14] ■ “启用 FIPS 模式时不受支持的功能” [16]
	为所有本地用户帐户设置密码策略	固件版本 3.2.5 及更高版本	■ 为所有本地用户设置密码策略限制（3.2.5 及更高版本） [25]
	修改为预先配置的管理员 `root` 帐户提供的默认密码。	所有固件版本	■ “避免创建共享用户帐户” [21] ■ 首次登录时修改 `root` 帐户的默认密码 [26]
	决定预先配置的 Oracle ILOM 服务及其开放网络端口是否适用于您的目标环境。	所有固件版本	■ “保护服务和开放网络端口” [17]

✓	安全任务	适用的固件版本	有关详细信息，请参见：
	配置用户对 Oracle ILOM 的访问。	所有固件版本	■ “保护 Oracle ILOM 用户访问” [21] ■ 使用基于角色的特权创建本地用户帐户 [27]
	决定在退出远程 KVMS 会话时是否应该锁定对主机操作系统的访问。	固件版本 3.0.4 及更高版本	■ 退出 KVMS 会话时锁定主机访问 [28]
	决定是否限制其他 SP 用户查看从 SP 启动的远程 KVMS 会话。	固件版本 3.2.4 及更高版本	■ 限制 Remote System Console Plus（3.2.4 或更高版本）可查看的 KVMS 会话 [29]
	决定是在用户登录期间还是在用户登录之后立即显示安全标题消息。	固件版本 3.0.8 及更高版本	■ 使用登录标题保护系统访问（3.0.8 及更高版本） [30]
	确保为所有 Oracle ILOM 用户界面设置最大安全属性。	所有固件版本	■ “配置 Oracle ILOM 界面以实现最高级别的安全性” [31]

服务器部署后的安全核对表

为了确定维护环境中现有服务器的最佳 Oracle ILOM 安全做法，系统管理员应执行下面表 2 “核对表 – 服务器部署后维护 Oracle ILOM 安全 ”中建议的安全任务列表。

表 2　　核对表 – 服务器部署后维护 Oracle ILOM 安全

✓	安全任务	适用的固件版本	有关详细信息，请参见：
	维护与 Oracle ILOM 的安全管理连接	所有固件版本	■ “避免未经验证的主机 KCS 设备访问” [47] ■ “首选的验证主机互连访问” [48] ■ “使用 IPMI 2.0 加密保护通道” [49]
	确保从 Oracle ILOM 安全启动远程 KVMS 和串行基于文本的会话。	所有固件版本	■ “KVMS 远程通信和加密” [50] ■ “针对远程 KVMS 共享访问实施保护” [51] ■ “针对主机串行控制台共享访问实施保护” [51]
	维护并跟踪用户对 Oracle ILOM 的访问。	所有固件版本	■ “保护用户访问的部署后注意事项” [52]
	重置预先配置的管理员 `root` 帐户的丢失密码所需的安全操作。	固件版本 3.1 及更高版本	■ “出于安全考虑亲临现场重置 `root` 帐户的默认密码” [53]
	服务器部署后必须在 Oracle ILOM 中修改 FIPS 140-2 符合性模式时所需的安全操作。	固件版本 3.2.4 及更高版本	■ 部署后修改 FIPS 模式 [55] ■ “启用 FIPS 模式时不受支持的功能” [16]
	确保服务器上的软件和固件均为最新。	所有固件版本	■ “更新至最新的软件和固件” [57]

Oracle ILOM 的部署安全最佳做法

使用以下主题决定服务器部署时要实施的最佳 Oracle ILOM 安全做法。

相关信息

- Oracle ILOM 的安全最佳做法核对表。
- Oracle ILOM 的部署后安全最佳做法
- 每个 Oracle ILOM 固件发行版的安全功能 [9]

保护物理管理连接

Oracle ILOM 是带外 (out-of-band, OOB) 管理工具，使用专用管理通道维护和监视 Oracle 服务器。与具有带内管理工具的服务器不同，Oracle 服务器具有内置的远程管理功能，使系统管理员能够通过服务处理器上单独的专用网络连接器安全访问 Oracle ILOM。尽管 Oracle ILOM 的管理功能为系统管理员提供了监视和管理 Oracle 服务器的特定功能，但 Oracle ILOM 的设计目的并不是成为通用的计算引擎或者通过不安全、不可信的网络连接进行访问。

无论通过本地串行端口、专用网络管理端口还是标准数据网络端口与 Oracle ILOM 建立物理管理连接，服务器或机箱监视模块 (chassis monitoring module, CMM) 上的此物理端口始终连接到内部的可信网络或者专用的安全管理或专用网络至关重要。有关与 Oracle ILOM 建立物理管理连接的其他准则，请参见下表。

与 Oracle ILOM 的物理端口管理连接	支持的 Oracle 硬件	管理连接安全准则
专用连接	■ 服务器（端口：NET MGT）	对服务处理器 (service processor, SP) 使用专用内部网络，以将其与常规数据网络通信隔离。

与 Oracle ILOM 的物理端口管理连接	支持的 Oracle 硬件	管理连接安全准则
	■ CMM（端口：NET MGT）	有关与 Oracle ILOM 建立专用网络管理连接的更多详细信息，请参见 ■ 《*Oracle ILOM* 配置和维护管理员指南 *(3.2.x)*》中的“专用网络管理连接”
本地连接	■ 服务器（端口：SER MGT） ■ CMM（端口：SER MGT）	使用本地串行管理连接直接从物理服务器或 CMM 访问 Oracle ILOM。 有关与 Oracle ILOM 建立本地串行管理连接的更多详细信息，请参见： ■ 《*Oracle ILOM* 配置和维护管理员指南 *(3.2.x)*》中的“与 Oracle ILOM 的本地串行网络管理连接”
边带连接	服务器（端口：NET0、NET1、NET2、NET3）	有必要通过避免使用两个单独的网络连接来简化电缆管理和网络配置时，使用共享以太网数据网络访问服务处理器 (service processor, SP)。 有关与 Oracle ILOM 建立边带管理连接的更多详细信息，请参见 ■ 《*Oracle ILOM* 配置和维护管理员指南 *(3.2.x)*》中的“边带管理连接” 注 - 大多数 Oracle 服务器都支持边带管理。

注 - 为了使系统免受安全攻击，**切勿将 Oracle ILOM SP 连接到公共网络**，例如 Internet。应确保 Oracle ILOM SP 管理通信始终位于单独的管理网络上并仅授予系统管理员访问权限。

选择是否在部署时配置 FIPS 模式

自 Oracle ILOM 固件发行版 3.2.4 起，Oracle ILOM CLI 和 Web 界面提供了可配置模式以实现联邦信息处理标准 (Federal Information Processing Standards, FIPS) 1 级符合性。启用了此模式时，Oracle 使用符合 FIPS 140-2 安全标准的加密算法保护系统的敏感或重要数据。

部署固件版本为 3.2.4 或更高版本的服务器的系统管理员应在配置其他 Oracle ILOM 属性之前决定是否配置 FIPS 模式。默认情况下，Oracle ILOM 在出厂时会禁用 FIPS 符合性模式。更改 FIPS 符合性模式将导致所有配置数据都重置为其出厂默认值。

要在部署期间启用 FIPS 符合性模式（在配置 Oracle ILOM 属性之前），请参见部署期间启用 FIPS 模式 [15]。如果在 Oracle ILOM 中设置了用户定义的配置属性并且需要修改 FIPS 属性，请参见“部署后修改 FIPS 模式的操作” [55]。

▼ 部署期间启用 FIPS 模式

注 - Oracle ILOM 中的 FIPS 符合性模式由 State 和 Status 属性表示。State 属性表示 Oracle ILOM 中的已配置模式，而 Status 属性表示 Oracle ILOM 中的操作模式。如果更改 FIPS State 属性，则在下一次 Oracle ILOM 重新引导之前，更改不会影响操作模式（FIPS Status 属性）。

开始之前

- 默认情况下，FIPS State 和 Status 属性在出厂时为禁用状态。
- 启用了 FIPS 时（已配置且可以正常运行），Oracle ILOM 中的一些功能不受支持。有关启用 FIPS 后不受支持功能的列表，请参见表 3 “启用 FIPS 模式时 Oracle ILOM 中不受支持的功能”。
- 需要具有 Admin (a) 角色才能修改 FIPS State 属性。
- 自固件 3.2.4 或更高版本起，Oracle LOM 提供了用于实现 FIPS 符合性的可配置属性。在固件发行版 3.2.4 之前，Oracle ILOM 不提供用于实现 FIPS 符合性的可配置属性。
- 在 Oracle ILOM 中修改 FIPS 模式的 State 和 Status 属性时，所有用户定义的配置设置都会重置为其出厂默认值。

1. 在 Oracle ILOM Web 界面中，单击 "ILOM Administration" -> "Management Access" -> "FIPS"。

2. 在 "FIPS" 页面中，执行以下操作：

   a. 选中 "FIPS State" 复选框以启用配置的 FIPS 属性。

   b. 单击 "Save" 应用更改。

   有关其他配置详细信息，请单击 "FIPS" Web 页上的 `More details...` 链接。

3. 要在 Oracle ILOM 中更改 FIPS 操作模式状态，请执行以下步骤以重新引导 Oracle ILOM。

   a. 在 Web 界面中，单击 "ILOM Administration" -> "Maintenance" -> "SP Reset"。

   b. 在 "SP Reset" 页面中，单击 "SP Reset" 按钮。

   重新引导 Oracle ILOM 时，将发生以下情况：

   - 在系统上应用上次配置的 FIPS State（已启用）。
   - 在 Oracle ILOM 中之前配置的所有用户定义的配置设置都会重置为其出厂默认值。
   - 更新 FIPS Status 属性以反映 Oracle ILOM 中当前启用的操作状态。

有关 FIPS Status 消息的完整列表和描述，请单击 "FIPS" 页面上的 `More details` 链接。

- FIPS 护盾图标显示在 Web 界面的主工具栏区域中。
- CLI 和 Web 界面禁用或删除了所有不受支持的 FIPS 功能。

  有关不受支持的 FIPS 功能的完整列表和描述，请单击 "FIPS" 页面上的 `More details` 链接。

相关信息

- “启用 FIPS 模式时不受支持的功能” [16]
- “部署后修改 FIPS 模式的操作” [55]
- 《*Oracle ILOM* 配置和维护管理员指南 *(3.2.x)*》中的“配置 FIPS 模式属性”。

启用 FIPS 模式时不受支持的功能

在 Oracle ILOM 中启用 FIPS 符合性时，Oracle ILOM 中以下不符合 FIPS 140-2 的功能不受支持。

表 3 启用 FIPS 模式时 Oracle ILOM 中不受支持的功能

不受支持的 FIPS 模式功能	说明
IPMI 1.5	当 FIPS 模式启用并在系统中运行时，会从 Oracle ILOM CLI 和 Web 界面中删除 IPMI 1.5 配置属性。将在 Oracle ILOM 中自动启用 IPMI 2.0 服务。IPMI 2.0 同时支持符合以及不符合 FIPS 的模式。
Oracle ILOM 系统远程控制台的固件兼容性	Oracle ILOM 中的 FIPS 模式阻止较早的 Oracle ILOM Remote System Console 固件版本与较新的 Oracle ILOM Remote System Console 固件版本兼容。 例如，Oracle ILOM Remote System Console 客户机固件版本 3.2.4 可以向后兼容 Oracle ILOM Remote System Console 固件版本 3.2.3 及更低版本。然而，Oracle ILOM Remote System Console 客户机固件版本 3.2.2 及更低版本不可以向前兼容 Oracle ILOM Remote System Console 固件版本 3.2.4 及更高版本。 注 - 此固件兼容性限制不适用于 Oracle ILOM Remote System Console Plus。Oracle ILOM Remote System Console Plus 在较新的服务处理器系统（例如 SPARC T5 及之后的系统或 Oracle Server x4-4、x4-8 及之后的系统）上提供。Oracle ILOM Remote System Console 在较早的服务处理器系统（例如 SPARC T3 和 T4 以及 Sun Server x4-2/2L/2B 及更早的系统）上提供。
轻量目录访问协议 (Lightweight Directory Access Protocol, LDAP)	当 FIPS 模式启用并在系统中运行时，会从 Oracle ILOM CLI 和 Web 界面中自动删除 Oracle ILOM 的 LDAP 配置属性。 注 - 符合和不符合 FIPS 的模式都支持以下远程验证服务：Active Directory 和 LDAP/SSL。
远程验证拨入用户服务 (Remote Authentication Dial-In User Service, RADIUS)	当 FIPS 模式启用并在系统中运行时，会从 Oracle ILOM CLI 和 Web 界面中自动删除 Oracle ILOM 的 RADIUS 配置属性。 注 - 符合和不符合 FIPS 的模式都支持以下远程验证服务：Active Directory 和 LDAP/SSL。
简单网络管理协议 (Simple Network Management Protocol, SNMP) DES 和 MD5	当 FIPS 模式启用并在系统中运行时，Oracle ILOM CLI 或 Web 界面不支持 DES 隐私协议和 MD5 验证协议的 SNMP 配置属性。

保护服务和开放网络端口

要确保在 Oracle ILOM 中正确配置服务及其相应的网络端口，请参阅以下主题：

预先配置的服务和网络端口

Oracle ILOM 预配置了许多服务，这些服务默认情况下处于启用状态。这样可以简单、直接地完成 Oracle ILOM 的部署。然而，服务器上的每个开放服务网络端口都可能成为恶意用户的攻击点。因此，务必了解初始 Oracle ILOM 设置及其用途并选择部署的系统实际需要的服务。为了实现最高级别的安全性，请仅启用所需的 Oracle ILOM 服务。

下表列出了 Oracle ILOM 默认情况下启用的服务。

表 4 默认启用的服务和端口

服务	端口
HTTP 重定向到 HTTPS	80
HTTPS	443
IPMI	623
用于 Oracle ILOM Remote Console 的远程 KVMS	5120, 5121, 5122, 5123, 5555, 5556, 7578, 7579
用于 Oracle ILOM Remote Console Plus 的远程 KVMS	5120, 5555
服务标签	6481
SNMP	161
单点登录	11626
SSH	22

下表说明了 Oracle ILOM 默认情况下禁用的服务。

表 5 默认禁用的服务和端口

服务	端口
HTTP	80

不需要的服务和开放端口的管理

可以选择禁用所有 Oracle ILOM 服务，这样会关闭这些服务各自的开放网络端口。尽管大多数服务默认情况下处于启用状态，但是您可能希望禁用某些功能或更改默认设置，

以提高 Oracle ILOM 环境的安全级别。任何 Oracle ILOM 服务都可以禁用，但是会失去相应的功能。一般而言，仅在部署的环境启用绝对必要的那些服务。必须将失去的功能与减少启用的网络服务所带来的安全性益处进行权衡。

下表说明启用或禁用各个服务的影响。

表 6 禁用服务的影响

服务	说明	启用/禁用服务的结果
HTTP	用于访问 Oracle ILOM Web 界面的非加密协议	与加密的 HTTP (HTTPS) 相比，启用此服务时性能更佳。然而，使用此协议可能会导致在不加密的情况下通过 Internet 发送敏感信息。
HTTPS	用于访问 Oracle ILOM Web 界面的加密协议	启用此服务可在 Web 浏览器和 Oracle ILOM 之间提供安全的通信。然而，由于它需要在 Oracle ILOM 上开放网络端口，因此增加了受到攻击（如拒绝服务）的可能性。
Servicetag	用于识别服务器和支持服务请求的 Oracle 搜索协议	如果禁用此服务，将导致 Oracle Enterprise Manager Ops Center 无法搜索 Oracle ILOM，并且将无法集成到其他 Oracle 自动化服务解决方案中。 只能在 Oracle ILOM CLI 中配置 Servicetag 状态。例如，要修改 servicetag 状态属性，请键入： `set /SP/services/servicetag state=`*enabled*|*disabled*
IPMI	标准管理协议	如果禁用此服务，则可能无法通过 Oracle Enterprise Manager Ops Center 和第三方软件的某些 Oracle 管理连接器来管理系统。
SNMP	标准管理协议，用于监视 Oracle ILOM 的运行状况和监视收到的陷阱通知	如果禁用此服务，则可能无法通过 Oracle Enterprise Manager Ops Center 和第三方软件的某些 Oracle 管理连接器来管理系统。
KVMS	用于提供远程键盘、视频、鼠标和存储的一组协议	如果禁用此服务，将导致主机控制台和远程存储功能不可用，从而导致其无法使用 Oracle ILOM Remote System Console（或 Oracle ILOM Remote System Console Plus）和 Storage Redirection CLI 应用程序。
SSH	用于访问远程 shell 的安全协议	如果禁用此服务，将无法通过网络进行命令行访问，并且可能会导致 Oracle Enterprise Manager Ops Center 无法搜索 Oracle ILOM。
SSO	单点登录功能，用于减少用户必须输入用户名和密码的次数	如果禁用此服务，则在启动 KVMS 时需要重新输入密码，而且在从机箱监视模块 (chassis monitoring module, CMM) 深入到刀片 SP 时无需重新输入密码。

有关启用和禁用各个网络服务的信息，请参见下面的“配置服务和网络端口” [18]主题。

配置服务和网络端口

有关如何在 Oracle ILOM 中配置管理服务及其相应网络端口的说明，请参见以下过程。

您可以使用 Oracle ILOM 命令行界面 (command-line interface, CLI) 或 Web 界面禁用或启用各项服务及其相应的网络端口。本节中的过程提供适用于所有 Oracle ILOM 固件发行版的基于 Web 的导航说明。有关配置属性的 CLI 说明或更多详细信息，请参阅每个过程后面“相关信息”部分中列出的相应文档。

▼ 修改协议管理服务状态和端口

开始之前

- 查看下表以确定 Oracle ILOM 中默认情况下启用或禁用哪些协议服务和网络端口。
  - 表 4 “默认启用的服务和端口”
  - 表 5 “默认禁用的服务和端口”
- 需要在 Oracle ILOM 中具有 Admin (a) 角色，才能修改协议服务的 State 属性。

执行以下步骤以修改网络服务的 State 属性。

1. 在 Oracle ILOM Web 界面中，导航到 "Management Access" 服务。
   例如，在以下界面中：
   - 3.0.x Web 界面，单击 "Configuration" -> "System Management Access"。
   - 3.1 和更高版本的 Web 界面，单击 "ILOM Administration" -> "Management Access"。
2. 单击下面列出的相应 "Management Access" -> 服务选项卡：

"Management Access" ->	说明
Web Server	使用 "Web Server" 页面管理 HTTP 和 HTTPS 协议管理访问的服务状态和端口分配。
IPMI	使用 "IPMI" 页面管理 IPMI 协议管理访问的服务状态和端口属性。
SNMP	使用 "SNMP" 页面管理 SNMP 管理访问的服务状态和端口属性。
SSH	使用 "SSH" 页面管理安全 shell 管理访问的服务状态属性。

3. 修改 "Management Access" -> 服务页面上的 State 属性，然后单击 "Save" 应用更改。
   请注意，禁用协议服务的 State 属性会导致关闭相应的协议服务网络端口，并阻止将该协议服务用于 Oracle ILOM。

相关信息

- 《*Oracle ILOM* 配置和维护管理员指南（固件 *3.2.x*）》中的“管理服务和网络默认属性”
- 《*Oracle ILOM 3.1* 配置和维护指南》中的“管理服务和网络默认属性”
- 《*Oracle ILOM 3.0* 日常管理 – *CLI* 过程指南》中的“配置网络设置”
- 《*Oracle ILOM 3.0* 日常管理 – *Web* 过程指南》中的“配置网络设置”

▼ 修改 KVMS 服务状态和端口

开始之前
- Oracle ILOM 中默认情况下启用 KVMS 服务的 State 属性。有关与 KVMS 服务关联的开放网络端口的列表，请参见表 4 “默认启用的服务和端口”。
- 需要具有 Admin (a) 角色，才能在 Oracle ILOM 中修改 KVMS 的 State 属性。

1. 在 Oracle ILOM Web 界面中导航到 "KVMS" 选项卡。

   例如，在以下界面中：

   - 3.0.x Web 界面，单击 "Remote Control" -> "KVMS"。
   - 3.1 和更高版本的 Web 界面，单击 "Remote Console" -> "KVMS"。

2. 在 "KVMS" 选项卡中，修改 KVMS 的 State 属性，然后单击 "Save" 应用更改。

   请注意，禁用 State 属性会导致关闭相应的开放 KVMS 服务网络端口；从而阻止使用：a) 远程主机控制台，以及 b) Oracle ILOM Remote Console 和 Oracle ILOM Remote Storage CLI；或者 Oracle ILOM Remote Console Plus。

相关信息

- 《*Oracle ILOM* 配置和维护管理员指南（固件 *3.2.x*）》中的“配置本地客户机的 KVMS 设置”。
- 《*Oracle ILOM 3.1* 配置和维护指南》中的“配置本地客户机的 KVMS 设置”
- 《*Oracle ILOM 3.0* 远程重定向控制台 – *Web* 和 *CLI* 指南》中的“初始设置任务”

▼ 修改单点登录服务状态和端口

开始之前
- Oracle ILOM 中默认情况下启用单点登录 (Single Sign-On, SSO) 服务的 State 属性和相应网络端口 (1126)。
- 需要在 Oracle ILOM 中具有 Admin (a) 角色，才能修改 SSO 服务的 State 属性。

1. 在 Oracle ILOM Web 界面中导航到 "User Account" 选项卡。

   例如，在以下界面中：

   - 3.0.x Web 界面，单击 "User Management" -> "User Account"。
   - 3.1 和更高版本的 Web 界面，单击 "ILOM Administration" -> "User Account"。

2. 在 "User Account" 页面中，修改 SSO 的 State 属性，然后单击 "Save" 应用更改。

   请注意，禁用 Oracle ILOM 中 SSO 的 State 属性会导致：a) 关闭开放 SSO 网络端口；b) 启动 KVMS 控制台时提示用户重新输入密码；和 c) 允许 CMM 用户无需重新输入密码即可导航到刀片服务器 SP。

相关信息

- 《*Oracle ILOM* 配置和维护管理员指南（固件 *3.2.x*）》中的“单点登录服务”
- 《*Oracle ILOM 3.1* 配置和维护指南》中的“单点登录服务”
- 《*Oracle ILOM 3.0* 日常管理 – *CLI* 过程指南》中的“配置单点登录”
- 《*Oracle ILOM 3.0* 日常管理 – *Web* 过程指南》中的“配置单点登录”

保护 Oracle ILOM 用户访问

要在 Oracle ILOM 中保护用户访问，请参阅以下主题：

避免创建共享用户帐户

可以通过避免创建共享帐户来维护安全的环境。共享帐户是指共享给定用户帐户密码的用户帐户。处理用户帐户的最佳方法是为有权访问 Oracle ILOM 的每个用户创建唯一密码，而不是创建共享帐户。确保每个用户帐户和密码组合只有一个用户知悉。

注 - Oracle ILOM 最多支持 10 个本地用户帐户。如果您需要允许更多用户访问 Oracle ILOM，您可以配置目录服务（如 LDAP 或 Active Directory）以使用集中数据库支持更多帐户。有关更多详细信息，请参见“远程验证服务和安全等级” [24]。

使用唯一密码建立各个用户帐户之后，系统管理员应确保将一个唯一的密码分配给预先配置的管理员 `root` 帐户。否则，如果没有唯一密码，则预先配置的管理员 `root` 帐户会被视为共享帐户。要确保未经授权的用户无法使用预先配置的管理员 `root` 帐户，您必须修改密码或从 Oracle ILOM 中删除预先配置的 `root` 帐户。有关预先配置的管理员 `root` 帐户的更多详细信息，请参见首次登录时修改 `root` 帐户的默认密码 [26]。

有关使用唯一密码建立安全帐户的更多指导，请参阅“管理用户帐户和密码的安全准则” [22]。

有关用户帐户配置信息，请参见“配置用户访问以实现最高级别的安全性” [25]。

基于角色的特权分配

所有 Oracle ILOM 用户帐户都分配有一组基于角色的特权。利用这些基于角色的特权可以访问 Oracle ILOM 中的不同功能。可以配置用户帐户，以便用户可以监视系统，但是无法对配置进行任何更改。或者，您可以允许用户修改大多数配置选项，但不能创建和修改用户帐户。还可以限制哪些用户可以控制服务器电源，哪些用户可以访问远程控制台。务必了解特权级别并为组织中的用户指定适当的特权级别。

下表定义了您可以分配给单个 Oracle ILOM 用户帐户的特权列表。

表 7　　用户帐户特权描述

角色	说明
Admin (a)	允许用户更改所有 Oracle ILOM 配置选项，但由其他特权（如 User Management）明确授权的那些配置选项除外。
User Management (u)	允许用户添加和删除用户、更改用户密码和配置验证服务。具有此角色的用户可以创建具有所有特权的另一用户帐户，因此在所有用户角色中，此角色具有最高特权级别。
Console (c)	允许用户远程访问主机控制台。此远程控制台访问权限可能允许用户访问 BIOS 或 OpenBoot PROM (OBP)，这使用户能够通过更改引导行为来获取对系统的访问权限。
Reset and Host Control (r)	允许用户控制主机电源和重置 Oracle ILOM。
Read-only (o)	允许用户对 Oracle ILOM 用户界面进行只读访问。所有用户都具有此访问权限，此访问权限使用户可以读取日志和环境信息以及查看配置设置。

有关创建本地用户帐户并分配基于角色的特权的更多信息，请参见使用基于角色的特权创建本地用户帐户 [27]。

管理用户帐户和密码的安全准则

管理 Oracle ILOM 用户帐户和密码时，请考虑下列安全准则：

- “用户帐户管理准则” [22]
- “密码管理准则” [23]

用户帐户管理准则

用户帐户管理准则	说明
切勿提倡共享用户帐户	务必为每个 Oracle ILOM 用户创建单独的帐户。 Oracle ILOM 最多支持 10 个本地用户帐户。如果您管理的是大型站点，需要的用户帐户超过 10 个，应考虑使用第三方用户验证服务，例如 LDAP 或 Active Directory。 有关通过外部验证服务在 Oracle ILOM 实施用户验证的更多信息，请参见“远程验证服务和安全等级” [24]。

用户帐户管理准则	说明
为本地用户帐户选择符合要求的名称	为本地 Oracle ILOM 用户帐户选择用户名时，用户名必须： ■ 长度为 4 到 16 个字符（第一个字符必须为字母）。 ■ 在组织中必须唯一 ■ 不包含空格、句点 (.) 或冒号 (:)
为本地用户帐户选择符合要求的密码	为本地 Oracle ILOM 用户帐户选择密码时，密码必须： ■ 始终为长度不超过 16 个字符的高安全性密码 ■ 既包含小写字符又包含大写字符，还包含一个或两个特殊字符以创建复杂的高安全性密码 ■ 不包含空格、句点 (.) 或冒号 (:) ■ 符合公司的密码管理策略 有关 Oracle ILOM 中密码管理的更多详细信息，请参见“管理用户帐户和密码的安全准则” [22]。
基于工作职责限制用户帐户特权（最小特权原则）	最小特权原则是指出于安全考虑，应该向用户授予履行其职责所需的最小特权。授予用户过多的职责、角色等（特别是在组织成立早期）可能会导致系统遭到滥用。定期查看用户特权，以确保仅授予与每个用户的当前工作职责相关的特权。 Oracle ILOM 提供了控制每个用户的用户特权的功能。确保根据工作职责为每个用户帐户指定适当的用户角色权限。 有关如何使用基于角色的特权创建用户帐户的详细信息，请参见：使用基于角色的特权创建本地用户帐户 [27]

密码管理准则

密码管理准则	说明
初次登录之后立即更改默认 `root` 密码 (`changeme`)	为了允许首次登录和访问 Oracle ILOM，随系统提供了本地管理员 `root` 帐户。要构建安全的环境，必须在初次登录 Oracle ILOM 之后更改提供的管理员密码 (`changeme`)。 如果可以对管理员 `root` 帐户进行未经授权的访问，则表明用户可以不受限制地访问 Oracle ILOM 的所有功能。因此，指定安全强度高的密码至关重要。
定期更改所有 Oracle ILOM 帐户的密码	为了防止恶意行为和确保密码符合当前的密码策略，应定期更改所有 Oracle ILOM 密码。
强制实施用于创建复杂的高安全性密码的常见做法	强制实施用于创建复杂的高安全性密码的以下常见做法： ■ 不要创建长度少于 16 个字符的密码。 ■ 不要创建包含用户名、员工姓名或家庭成员姓名的密码。 ■ 不要选择易于猜测的密码。 ■ 不要创建包含连续数字字符串（例如 12345）的密码。 ■ 创建的密码不得包含通过简单的 Internet 搜索便可轻松发现的单词或字符串。 ■ 不要允许用户在多个系统中重复使用相同的密码。 ■ 不要允许用户重复使用旧密码。 ■ 为了实现最高级别的安全性，您应当使用以下语法在 CLI 中始终屏蔽新的密码输入： **`set [`***SP|CMM***`]/users/root password=`**[不要键入密码，请按 *Enter* 键] - 或者 - **`set [`***SP|CMM***`]/users/newuser password=`**[不要键入密码，请按 *Enter* 键]

密码管理准则	说明
	CLI 会提示输入新的密码值，并且会屏蔽密码以防被看见。
为本地用户设置密码策略限制 （自固件 3.2.5 及更高版本起可用）	为所有本地用户帐户强制实施密码策略。有关更多详细信息，请参见为所有本地用户设置密码策略限制（3.2.5 及更高版本） [25]
咨询 IT 安全专员以了解密码管理策略	请咨询 IT 安全专员，确保符合公司的密码管理要求和策略。

远程验证服务和安全等级

可以将 Oracle ILOM 配置为使用外部集中用户存储库，而无需配置每个 Oracle ILOM 实例上的本地用户。这样可以更方便地集中创建和修改用户凭证以及允许用户访问许多不同的系统。

在选择和配置验证服务之前，请了解这些服务的工作原理以及需要如何配置各个服务。除了验证之外，支持的每个服务还允许配置授权规则来定义如何为给定远程用户指定 Oracle ILOM 用户特权。确保指定正确的用户角色或特权。

下表介绍了 Oracle ILOM 支持的用户验证服务。

表 8　　远程验证服务和安全等级

服务名称	安全等级	信息
Active Directory	高	■ 默认情况下，此服务是安全的。 ■ 使用严格的认证模式需要证书服务器，但是可以多添加一层保护。
轻量目录访问协议/安全套接字层 (Lightweight Directory Access Protocol/Secure Socket Layer, LDAP/SSL)	高	■ 默认情况下，此服务是安全的。 ■ 使用严格的认证模式需要证书服务器，但是可以多添加一层保护。
传统 LDAP	低	■ 可以在没有可疑恶意用户的专用安全网络上使用此服务。
远程验证拨入用户服务 (Remote Authentication Dial In User Service, RADIUS)	低	■ 可以在没有可疑恶意用户的专用安全网络上使用此服务。

安全等级高的服务可以在安全要求非常高的环境中使用，因为这些服务由证书和其他形式的保护通道的强加密来保护。安全等级低的服务默认情况下处于禁用状态。仅在您了解并接受此低安全等级的限制之后才能启用这些安全等级低的服务。

有关远程验证服务配置的详细信息，请参阅下面相应的 Oracle ILOM 文档：

- 《*Oracle ILOM* 配置和维护管理员指南（固件 *3.2.x*）》中的“设置和维护用户帐户”
- 《Oracle ILOM 3.1 配置和维护指南》中的“设置和维护用户帐户”

- 《*Oracle ILOM 3.0* 日常管理 – *CLI* 过程指南》中的“管理用户帐户”
- 《*Oracle ILOM 3.0* 日常管理 – *Web* 过程指南》中的“管理用户帐户”

配置用户访问以实现最高级别的安全性

有关如何以最佳方式配置 Oracle ILOM 的用户访问以实现最高级别的安全性，请参阅以下主题。

您可以使用命令行界面 (command-line interface, CLI) 或 Web 界面在 Oracle ILOM 中配置用户访问属性。本节中的过程提供适用于所有 Oracle ILOM 固件发行版的基于 Web 的导航说明。有关配置属性的 CLI 说明或更多详细信息，请参阅每个过程后面“相关信息”部分中列出的相应文档。

▼ 为所有本地用户设置密码策略限制（3.2.5 及更高版本）

自固件发行版 3.2.5 起，Oracle ILOM 为所有本地用户帐户强制实施密码策略。该密码策略附带了一组默认的密码策略限制。系统管理员可以选择原样使用默认属性或者修改它们以满足其密码策略要求。

注 - 修改密码策略属性应当在创建本地用户帐户之前进行。如果在配置本地用户帐户之后修改密码策略属性，则 Oracle ILOM 将自动执行以下操作：1) 删除所有本地用户帐户的配置 2) 恢复随系统初始提供的默认 root 帐户。

开始之前

- 需要具有 Admin (a) 角色才能配置密码策略属性。
- 密码策略仅应用于本地用户帐户。它对远程用户验证服务帐户（例如 LDAP 或 Active Directory）没有影响。
- 在保存对密码策略属性的更改时，将发生以下操作：
  - 从 Oracle ILOM 中删除所有本地用户帐户配置。
  - 将恢复随系统提供的默认本地用户帐户 (root)。
  - 在 root 初次登录时，会提示 root 用户更改 root 帐户密码。

使用以下基于 Web 的说明为所有本地用户设置密码策略：

注 - 有关 CLI 密码策略说明，请单击本过程的“相关信息”部分中列出的 Oracle ILOM 管理指南参考。

1. 要查看 Oracle ILOM 中当前的密码策略限制，请单击 "ILOM Administration" > "User Management" > "Password Policy"。
2. 要修改密码策略限制，请单击 "Password Policy" 页面上的 "More Details..." 链接以获得更多说明。
3. 要保存更改，请单击 "Save"。

相关信息

- “Modify Password Policy Restrictions for Local Users” in 《Oracle ILOM Administrator’s Guide for Configuration and Maintenance Firmware Release 3.2.x》

▼ 首次登录时修改 root 帐户的默认密码

为了允许首次登录和访问 Oracle ILOM，随系统提供了预先配置的管理员 root 帐户及默认密码 (changme)。为了阻止未经授权访问 Oracle ILOM，必须在首次登录时更改随预先配置的 root 帐户提供的默认密码 (changeme)。否则，该预先配置的 root 帐户和默认密码 (changeme) 将充当共享帐户，使所有用户都具有管理员访问权限。

使用以下基于 Web 的说明修改随预先配置的管理员 root 帐户提供的默认密码 (changeme)。

注 - 如果您不具有预先配置的 root 帐户的访问权限，但是您需要访问 Oracle ILOM 管理员功能，则联系您的系统管理员以获取具有管理员特权的用户帐户。

开始之前

- 请参见“管理用户帐户和密码的安全准则” [22]。

  注 - 为了阻止未经授权访问 Oracle ILOM 功能，向 root 帐户分配安全强度高的密码非常重要。高安全性密码应包含大写和小写字符的组合，并且至少有一个特殊字符，例如 % 或 $。

- 在 Oracle ILOM 中需要具有 User Management (u) 角色才能修改本地用户帐户密码。

1. 在 Oracle ILOM Web 界面中导航到 "User Account" 页面。
   例如，在以下界面中：

- 3.0.x Web 界面，单击 "User Management" -> "User Accounts"。
- 3.1 和更高版本的 Web 界面，单击 "User Management" -> "User Accounts"。

2. 在 "User Account" 页面中，单击 **root** 帐户的 "Edit"。
此时将显示 "Edit: User Root" 对话框。

3. 在 "Edit: User Root" 对话框中，执行以下操作：

   - 在 "New Password" 文本框中输入一个唯一的密码，然后在 "Confirm New Password" 文本框中重新输入相同的密码。
   - 单击 "Save" 应用更改。

相关信息

- 《*Oracle ILOM* 配置和维护管理员指南（固件 *3.2.x*）》中的“配置本地用户帐户”。
- 《*Oracle ILOM 3.1* 配置和维护指南》中的“配置本地用户帐户”
- 《*Oracle ILOM 3.0* 日常管理 – *CLI* 过程指南》中的“修改用户帐户”
- 《*Oracle ILOM 3.0* 日常管理 – *Web* 过程指南》中的“修改用户帐户”
- “出于安全考虑亲临现场重置 root 帐户的默认密码” [53]

▼ 使用基于角色的特权创建本地用户帐户

开始之前 Oracle ILOM 在一个 SP 或机箱监视模块 (chassis monitoring module, CMM) 中最多支持创建和存储 10 个本地用户帐户。Oracle ILOM 用户分配有一组特权，允许他们使用为他们配置的帐户所允许的功能。

注 - 另外，系统管理员还可以配置 Oracle ILOM 以通过远程验证服务支持更多的用户帐户。对于远程验证服务配置，登录名、密码和特权均从外部用户存储库派生而来。有关更多详细信息，请参见“远程验证服务和安全等级” [24]。

有关使用基于角色的访问特权配置本地用户帐户的基于 Web 的说明，请参见以下说明。

开始之前

- 请参见“管理用户帐户和密码的安全准则” [22]。
- 查看表 7 “用户帐户特权描述” Oracle ILOM 支持的 Web 浏览器。
- 需要在 Oracle ILOM 中具有 User Management (u) 角色才能创建具有特权的本地用户帐户。

1. 在 Oracle ILOM Web 界面中导航到 "User Account" 页面。

例如，在以下界面中：

- 3.0.x Web 界面，单击 "User Management" -> "User Accounts"。
- 3.1 和更高版本的 Web 界面，单击 "User Management" -> "User Accounts"。

2. 在 "User Account" 页面中，单击 "Add"。
   此时将显示 "Add User" 对话框。
3. 在 "Add User" 对话框中，执行以下操作：
   a. 在 "User Name" 文本框中指定用户的名称。
   b. 在 "Roles" 下拉列表中，选择相应的用户角色配置文件（Administrator、Operator 或 Advanced）。
   c. 在 "New Password" 文本框中输入一个唯一的密码，然后在 "Confirm New Password" 文本框中重新输入相同的密码。
   d. 单击 "Save" 应用更改。

相关信息

- 《*Oracle ILOM* 配置和维护管理员指南（固件 *3.2.x*）》中的“创建用户帐户和分配用户角色”
- 《*Oracle ILOM 3.1* 配置和维护指南》中的“创建用户帐户和分配用户角色”
- 《*Oracle ILOM 3.0* 日常管理 – *CLI* 过程指南》中的“添加用户帐户和分配角色”
- 《*Oracle ILOM 3.0* 日常管理 – *Web* 过程指南》中的“添加用户帐户和分配角色”

▼ 退出 KVMS 会话时锁定主机访问

由于使用远程 KVMS 时会将主机控制台视为共享网络资源，因此，如果一个用户登录主机控制台后，未从主机操作系统注销即关闭了 Oracle ILOM Remote System Console、Remote System Console Plus 或 CLI Storage Redirection 应用程序，使用远程 KVMS 连接到同一控制台的另一用户将能够使用先前验证的操作系统会话。因此，Oracle ILOM 提供了在远程 KVMS 会话断开连接时自动锁定主机操作系统的功能。为了实现最高级别的安全性，请在 Oracle ILOM 中启用或配置此功能。

要在终止 KVMS 会话后锁定远程主机桌面，请参见以下基于 Web 的说明。有关如何启用主机锁定功能的信息，请参见《*Oracle ILOM* 配置和维护管理员指南（固件 *3.2.x*）》。

开始之前

- 需要具有 Console (c) 角色才能在 Oracle ILOM 中修改主机锁定模式属性。
- 需要具有固件 3.0.4 或更高版本才能在 Oracle ILOM 中使用主机锁定模式功能。
- 默认情况下禁用主机锁定模式功能。

1. 在 Oracle ILOM Web 界面中导航到 "KVMS" 页面。
   例如，在以下界面中：
   - 3.0.x Web 界面，单击 "Remote Console" -> "KVMS"。
   - 3.1 和更高版本的 Web 界面，单击 "Remote Control" -> "KVMS"。
2. 在 "KVMS" 页面的 "Host Lock Settings" 部分中，执行以下操作之一：
   - 指定一种锁定模式（Windows、Custom 或 Disabled）。
   - 单击 "Save" 应用更改。

相关信息

- 《*Oracle ILOM* 配置和维护管理员指南（固件 *3.2.x*）》中的“锁定主机桌面”
- 《*Oracle ILOM 3.1* 配置和维护》中的“锁定主机桌面”
- 《*Oracle ILOM 3.0* 远程重定向控制台 – *CLI* 和 *Web* 指南》中的“KVMS 锁定”

▼ 限制 Remote System Console Plus（3.2.4 或更高版本）可查看的 KVMS 会话

自固件发行版 3.2.4 起，主 Remote System Console Plus 用户可以通过将 "Maximum Client Session Count" 限制为一 (1) 个会话查看者来阻止 SP 上其他登录的会话用户查看视频重定向会话期间输入的机密数据。默认情况下，Oracle ILOM Remote System Console Plus 的 "Maximum Client Session Count" 属性设置为四个会话查看者。

要修改 Oracle ILOM Remote System Console Plus 的 "Maximum Client Session Count" 属性，请参见以下基于 Web 的说明。

开始之前

- 自固件发行版 3.2.4 起，为 Oracle ILOM Remote System Console Plus 提供了 KVMS "Maximum Client Session Count" 属性。

  注 - KVMS "Maximum Client Session Count" 属性在支持 Oracle ILOM 远程控制台的系统上不可配置。

- Oracle ILOM Remote System Console Plus 仅适用于自固件发行版 3.2.1 起新发行的 SP 系统。

- 需要在 Oracle ILOM 中具有 Console (c) 角色才能修改 KVMS "Maximum Client Session Count" 属性。
- 在 Oracle ILOM 中重置 "Maximum Client Session Count" 属性时，将终止 SP 上所有活动的 Oracle ILOM Remote System Console Plus 视频会话。
- 默认情况下，最多可以针对每个 SP 从 Oracle ILOM 的 "Redirection" 页面启动 4 个 Remote System Console Plus 视频重定向会话。

1. 在 Oracle ILOM Web 界面中通过单击 "Remote Console" -> "KVMS" 导航到 "KVMS" 页面。
2. 在 "KVMS" 页面中，修改 "Maximum Client Session Count" 属性（可接受的值：*4*（默认值）|*1*|*2*|*3*）。
3. 单击 "Save" 应用更改。

相关信息

- 《*Oracle ILOM* 配置和维护管理员指南（固件 *3.2.x*）》中的“远程设备重定向属性”

▼ 使用登录标题保护系统访问（3.0.8 及更高版本）

自固件发行版 3.0.8 起，Oracle ILOM 允许系统管理员在所有用户登录到 Oracle ILOM CLI 和 Web 界面时向他们显示标题消息。使用登录标题可以帮助阻止远程设备未经授权进行系统访问，并向授权和合法用户说明其合理使用系统的责任。

您实施的标题消息应根据信息安全策略进行编写。有关编写消息的更多准则，请咨询您的站点管理员或安全专员。

要在所有用户登录时或登录后向他们显示标题消息，请参见以下基于 Web 的说明。

开始之前
- 需要具有 Admin (a) 角色才能创建标题消息。
- 自 Oracle ILOM 固件发行版 3.0.8 起，才可以配置标题消息。
- 管理员可以将标题消息配置为显示在 "Login" 页面上，或者显示在用户登录到 Oracle ILOM 后立即出现的对话框中。

1. 在 Oracle ILOM Web 界面中导航到 "Banner Message" 页面。

   例如，在以下界面中：

   - 3.0.x Web 界面，单击 "System Information" -> "Banner Messages"。
   - 3.1 和更高版本的 Web 界面，单击 "ILOM Administration" -> "Management Access" -> "Banner Messages"。

2. 在 "Banner Message" 页面中，单击 *More Details...* 链接以决定如何配置标题消息。

有关 CLI 说明，请参阅本过程的“相关信息”部分中列出的适用的 *Oracle ILOM* 管理指南。

3. 单击 "Save" 以应用所做的更改。

相关信息

- “Management of Banner Messages at Log-In” in 《Oracle ILOM Administrator’s Guide for Configuration and Maintenance Firmware Release 3.2.x》
- 《*Oracle ILOM* 配置和维护管理员指南（固件 *3.2.x*）》中的“标题消息的管理”
- 《*Oracle ILOM 3.1* 配置和维护指南》中的“标题消息配置属性”
- 《*Oracle ILOM 3.0* 日常管理 – *CLI* 过程指南》中的“显示标题消息”
- 《*Oracle ILOM 3.0* 日常管理 – *Web* 过程指南》中的“显示标题消息”

配置 Oracle ILOM 界面以实现最高级别的安全性

要配置 Oracle ILOM 界面以实现最高级别的安全性，请参阅以下主题：

- “配置 Web 界面以实现最高级别的安全性” [31]
- “配置 CLI 以实现最高级别的安全性” [37]
- “配置 SNMP 管理访问以实现最高级别的安全性” [40]
- “配置 IPMI 管理访问以实现最高级别的安全性” [42]
- “配置 WS-Management 访问以实现最高级别的安全性” [44]

配置 Web 界面以实现最高级别的安全性

有关如何以最佳方式配置 Oracle ILOM Web 界面以实现最高级别的安全性，请参阅以下主题。

注 - 您可以使用命令行界面 (command-line interface, CLI) 或 Web 界面在 Oracle ILOM 中配置 Web 管理界面属性。本节中的过程提供适用于所有 Oracle ILOM 固件发行版的基于 Web 的导航说明。有关配置属性的 CLI 说明或更多详细信息，请参阅每个过程后面“相关信息”部分中列出的相应文档。

- “使用可信的 SSL 证书和私钥提高安全性” [32]
- 启用最强的 SSL 和 TLS 加密属性 [34]
- 设置非活动 Web 会话的超时间隔 [36]

使用可信的 SSL 证书和私钥提高安全性

安全套接字层 (Secure Socket Layer, SSL) 证书用于对网络通信进行加密和确保服务器或客户机的真实性。Oracle ILOM 包含一个自签名 SSL 证书，有了它，无需上载证书即可直接使用 HTTP over SSL 协议。首次连接到 Oracle ILOM Web 界面时，系统会通知用户即将使用自签名证书，并询问是否接受使用该证书。如果使用提供的证书，Web 浏览器和 Oracle ILOM 之间的所有通信都将完全加密。

然而，还可以创建并上载可信证书以提高安全性。可信证书是指证书是通过受信任证书授权机构授予的。使用已知证书颁发机构授予的可信证书可以确保 Oracle ILOM Web 服务器的真实性。使用不可信（自签名）证书可能会遭受中间人 (man-in-the-middle, MITM) 攻击。

要获取并上载临时自签名或证书颁发机构签名的证书，请参阅以下过程。

- 使用 OpenSSL 获取 SSL 证书和私钥 [32]
- 将定制 SSL 证书和私钥上载到 Oracle ILOM [33]

▼ 使用 OpenSSL 获取 SSL 证书和私钥

此过程是如何使用 OpenSSL 工具包创建 SSL 证书和私钥的简要说明。

注 - Oracle ILOM 不要求您使用 OpenSSL 生成 SSL 证书。在此过程中 OpenSSL 仅用于演示目的。其他工具也可用于生成 SSL 证书。

您需要使用临时自签名证书还是证书颁发机构签名的证书应该由您的站点管理员或安全专员确定。在您需要获取 SSL 证书（临时自签名或证书颁发机构签名）时，可以遵循下面这些示例 OpenSSL 命令行说明。

注 - 如果需要其他 OpenSSL 说明来生成 SSL 证书，请参见 OpenSSL 工具包随附的用户文档。

---

1. **创建用于存储证书和私钥的网络共享或本地目录。**

2. **要使用 OpenSSL 工具包生成新的 RSA 私钥，请键入：**

   ```
   openssl genrsa -out <foo>.key 2048
   ```

   其中 *<foo>* 为私钥的名称。

   注 - 此私钥是以 PEM 格式存储的 2048 位的 RSA 密钥，因此它可以作为 ASCII 文本读取。

   ---

3. **要使用 OpenSSL 工具包生成证书签名请求 (certificate signing request, CSR)，请键入：**

```
openssl req -new -key <foo>.key -out <foo>.csr
```

其中 *<foo>* 为证书签名请求的名称。

注 - 在 CSR 生成期间，系统将显示多条信息以给出提示。

<foo>.csr 文件现在应显示在您当前的工作目录中。

4. 要生成 SSL 证书，请执行以下操作之一：

   - 生成临时自签名证书（有效期 365 天）。

     自签名 SSL 证书基于 server.key 私钥和 server.csr 文件生成。

     使用 OpenSSL 工具包，键入：

     ```
     openssl x509 -req -days 365 -in <foo>.csr
     -signkey <foo>.key -out <foo>.cert
     ```

     其中，*<foo>* 为分配给私钥 (.key) 或证书 (.cert) 的名称。

注 - 此临时证书在客户机浏览器中将生成一个错误，指出签名证书颁发机构未知或者不可信。如果此错误不可接受，则应该请求证书颁发机构向您颁发一个签名的证书。

   - 从证书颁发机构提供商获取官方签名的证书。

     将您的证书签名请求 (*<foo>*.csr) 提交至 SSL 证书颁发机构提供商。大多数证书颁发机构提供商都要求您剪切并粘贴 Web 应用程序屏幕中的 CSR 输出。通常需要七个工作日才能收到您的签名证书。

5. 将新的 SSL 证书和私钥上载到 Oracle ILOM。

   请参见以下说明：将定制 SSL 证书和私钥上载到 Oracle ILOM [33]。

▼ 将定制 SSL 证书和私钥上载到 Oracle ILOM

开始之前

- 需要具有 Admin (a) 角色才能在 Oracle ILOM 中修改 Web 服务器属性。
- 获取新的（临时自签名或证书颁发机构签名）HTTPS 证书和私钥。有关使用 OpenSSL 工具包的说明，请参见使用 OpenSSL 获取 SSL 证书和私钥 [32]。
- 确保您可以通过网络或本地文件系统访问新的 HTTPS 证书和私钥。

1. 在 Oracle ILOM Web 界面中导航到 "SSL Certificate" 页面。

   例如，在以下界面中：

- 3.0.x Web 界面，单击 "Configuration" -> "System Management Access" -> "SSL Certificate"。
- 3.1 和更高版本的 Web 界面，单击 "ILOM Administration" -> "Management Access" -> "SSL Certificate"。

2. 在 "SSL Server" 页面中，执行以下操作：

   a. 单击 "Load Certificate" 按钮以上载文件传输方法属性中指定的定制证书文件。

   b. 单击 "Load Custom Private Key" 按钮以上载文件传输方法属性中指定的定制私钥文件。

   c. 单击 "Save" 应用更改。

相关信息

- 《*Oracle ILOM* 配置和维护管理员指南（固件 *3.2.x*）》中的“SSL 证书和私钥配置属性”
- 《*Oracle ILOM 3.1* 配置和维护指南》中的“SSL 证书和私钥配置属性”
- 《*Oracle ILOM 3.0* 日常管理 – *CLI* 过程指南》中的“上载 SSL 证书”
- 《*Oracle ILOM 3.0* 日常管理 – *Web* 过程指南》中的“上载 SSL 证书”

▼ 启用最强的 SSL 和 TLS 加密属性

Oracle ILOM 支持具有最强加密的最强安全套接字层加密（SSLv3 和 TLS v1.0、v1.1 和 v1.2）协议。但是在某些情况下，可能需要启用 SSLv2 或弱加密来支持使用较早的 Web 浏览器。

使用此过程在 Oracle ILOM 中设置 SSL 和 TLS 属性以满足您的安全策略要求。

注 - 自固件发行版 3.1.0 起，提供了对 SSL 和 TLSv1.0 的支持。自固件发行版 3.2.4 起，Oracle ILOM 提供了对 TLS v1.1 和 v1.2 的支持。

开始之前

- 需要具有 Admin (a) 角色才能在 Oracle ILOM 中修改 Web 服务器属性。
- Oracle ILOM 中 TLS 属性的默认设置取决于服务器上当前安装的固件版本。

固件	TLS 默认设置
3.1.x、3.2.1.x、3.2.2.x 和 3.2.3.x	启用 TLS v1.0

固件	TLS 默认设置
3.2.4 及更高版本	启用 TLS v1.0、v1.1 和 v1.2

- 对于早于 3.2.4 的 Oracle ILOM 固件发行版，默认情况下会启用 SSLv3 属性。

注 - 由于 SSLv3 暴露了一个安全漏洞，在有修补程序可用之前应当禁用 SSLv3。有关更多详细信息，请参阅 Oracle：MOS SSLv3 漏洞文章。

- 对于 Oracle ILOM 固件发行版 3.2.4.x 和更高版本，默认 SSLv3 设置取决于服务器型号和所安装的 3.2.4.x 固件版本。

服务器型号	固件	SSLv3 默认设置
SPARC T3、T4、 T5、M5、M6	3.2.4.1	禁用 SSLv 3
X4-2 X4-2L X4-2B	3.2.4.20 (x4-2) 3.2.4.22 (x4-2L) 3.2.24.24 (X4-2B)	启用 SSLv3 有关更多详细信息，请参阅 MOS SSLv3 漏洞文章。
X4-4 X4-8	3.2.4.18	启用 SSLv3 有关更多详细信息，请参阅 MOS SSLv3 漏洞文章。
X5-2 X5-2L	3.2.4.10 (x5-2) 3.2.4.12 (x5-2L)	禁用 SSLv3

- 在 Oracle ILOM 中，SSLv2 和弱加密属性默认处于禁用状态

要在 Oracle ILOM 中查看或修改 SSL 或 TLS Web 服务器安全属性，请参阅以下基于 Web 的说明。

1. 在 Oracle ILOM Web 界面中，单击 "ILOM Administration" -> "Management Access" -> "Web Server"。
2. 在 "Web Server" 页面中，查看或修改 SSL、TLS 或弱加密的 Web 安全属性。
3. 单击 "Save" 应用更改。

相关信息

- 《*Oracle ILOM* 配置和维护管理员指南（固件 *3.2.x*）》中的“Web 服务器配置属性”
- 《*Oracle ILOM 3.1* 配置和维护指南》中的“Web 服务器配置属性”

▼ 设置非活动 Web 会话的超时间隔

Oracle ILOM Web 会话超时间隔保障忘记注销的 Web 访问用户的安全。Web 会话超时间隔确定 HTTP 或 HTTPS Web 会话处于非活动状态多少分钟后自动注销。此功能可降低未经授权的用户找到已与 Oracle ILOM 建立已验证 Web 会话的无人看管计算机的风险。

要查看或修改为 HTTP 和 HTTPS 会话设置的 Web 会话超时间隔，请参见以下基于 Web 的说明。

开始之前

- 为 HTTP 和 HTTPS 连接设置的默认 Web 会话超时间隔为 15 分钟。

注 - 降低会话超时可能会导致用户因会话过期而必须更频繁地重新输入其用户名和密码。但是，降低会话超时将会缩短无人看管的已验证 Web 会话保持活动状态的时间。

- 需要具有 Admin (a) 角色才能修改 Web 服务器属性
- HTTP 和 HTTPS 会话超时间隔属性仅可以在 Oracle ILOM 中针对运行固件发行版 3.0.4 或更高版本的服务器 SP 进行配置。

1. 导航到 "Web Server" 页面。

   例如，在以下界面中：

   - 3.0.x Web 界面，单击 "Configuration" -> "System Management Access" -> "Web Server"。
   - 3.1 和更高版本的 Web 界面，单击 "ILOM Administration" -> "Management Access" -> "Web Server"。

2. 在 "Web Server" 页面中，执行以下操作：

   a. 导航到 HTTP 或 HTTP 会话超时属性。

   b. 输入一个介于 1-720 分钟之间的数字，指定 Web 会话处于非活动状态多少分钟后自动注销。

   c. 单击 "Save" 应用更改。

相关信息

- 《*Oracle ILOM* 配置和维护管理员指南（固件 *3.2.x*）》中的“Web 服务器配置属性”
- 《*Oracle ILOM 3.1* 配置和维护指南》中的“Web 服务器配置属性”

- 《*Oracle ILOM 3.0* 日常管理 – *Web* 过程指南》中的“设置会话超时”

配置 CLI 以实现最高级别的安全性

有关如何以最佳方式配置 Oracle ILOM 命令行界面 (command-line interface, CLI) 以实现最高级别的安全性，请参阅以下主题。

您可以使用命令行界面 (command-line interface, CLI) 或 Web 界面在 Oracle ILOM 中配置 CLI 管理属性。本节中的过程提供适用于所有 Oracle ILOM 固件发行版的基于 Web 的导航说明。有关配置属性的 CLI 说明或更多详细信息，请参阅每个过程后面“相关信息”部分中列出的相应文档。

▼ SSH 服务器状态和弱加密的管理（3.2.5 及更高版本）

自固件发行版 3.2.5 起，可以在 Oracle ILOM CLI 和 Web 界面中配置 SSH 服务器状态属性和弱加密属性。为了实现最高级别的安全性，SSH 服务器状态属性处于启用状态，弱加密属性处于禁用状态。要修改这些 SSH 管理访问属性，请参见以下基于 Web 的说明。

1. 在 Oracle ILOM Web 界面中，单击 "ILOM Administration" -> "Management Access" -> "SSH Server"。
2. 在 "SSH Server" 页面中，单击 *More Details...* 链接以获得更多说明。
3. 单击 "Save" 以应用所做的更改。

相关信息

- 《*Oracle ILOM* 配置和维护管理员指南（固件 *3.2.x*）》中的“SSH 服务器状态和弱加密的管理”

▼ 设置非活动 CLI 会话的超时间隔

Oracle ILOM CLI 支持用于关闭非活动 CLI 会话的可配置的会话超时间隔，用户可以通过使用安全 Shell (Secure Shell, SSH) 协议连接到 Oracle ILOM 来访问 CLI，也可以使用串行连接来访问 CLI。配置后，此功能可降低未经授权的用户找到已与 Oracle ILOM 建立已验证 CLI 会话的无人看管计算机的风险。

为了实现最高级别的安全性，您应该在共享控制台上使用 Oracle ILOM CLI 的任何环境中都配置 CLI 会话超时间隔。理想的情况下，您应该将 CLI 会话超时间隔设置为 15 分钟或更短的时间。

要查看或修改非活动 Oracle ILOM CLI 会话的超时间隔属性设置，请参见以下基于 Web 的说明。

开始之前

- 需要具有 Admin (a) 角色才能修改 CLI 属性。
- 为 SSH 连接设置的默认 CLI 会话超时间隔处于禁用状态并设置为 0（零）分钟。

注 - 当将 CLI 超时间隔设置为 0（零）时，Oracle ILOM 将不管会话保持闲置状态多长时间都不关闭非活动的 CLI 会话。

- CLI 会话超时间隔属性仅可以在 Oracle ILOM 中针对运行固件发行版 3.0.4 或更高版本的服务器 SP 进行配置。

1. 在 Oracle ILOM Web 界面中导航到 "CLI" 页面。

   例如，在以下界面中：

   - 3.0.x Web 界面，单击 "Configuration" -> "System Management Access" -> "CLI"。
   - 3.1 和更高版本的 Web 界面，单击 "ILOM Administration" -> "Management Access" -> "CLI"。

2. 在 "CLI" 页面中，通过执行以下操作来设置 CLI 会话超时间隔。

   a. 选中 "Enable" 复选框。

   b. 输入一个介于 1-1440 分钟之间的数字，指定命令行会话处于非活动状态多少分钟后自动注销。

   c. 单击 "Save" 应用更改。

相关信息

- 《*Oracle ILOM* 配置和维护管理员指南（固件 *3.2.x*）》中的“CLI 会话超时配置属性”
- 《*Oracle ILOM 3.1* 配置和维护指南》中的“CLI 会话超时配置属性”
- 《*Oracle ILOM 3.0* 日常管理 – *CLI* 过程指南》中的“设置 CLI 会话超时”

▼ 使用服务器端密钥加密 SSH 连接

Oracle ILOM 提供了安全 Shell (Secure Shell, SSH) 服务器功能，使远程客户机能够通过命令行界面安全地连接 Oracle ILOM 并进行管理。SSH 协议使用服务器端密钥加密管理通道和保护所有通信。SSH 客户机还使用这些密钥检验 SSH 服务器的真实性。

Oracle ILOM 在首次引导出厂默认系统时生成一组唯一的 SSH 密钥。在需要新服务器端密钥时，Oracle ILOM 支持手动生成其他 SSH 服务器端密钥的功能。

要查看或手动生成 SSH 服务器端加密密钥，请参见以下基于 Web 的说明。

开始之前

- 需要具有 Admin (a) 角色才能修改 SSH 服务器属性。

1. 在 Oracle ILOM Web 界面中导航到 "SSH Server" 页面。
例如，在以下界面中：

   - 3.0.x Web 界面，单击 "System Management" -> "SSH Server"。
   - 3.1 和更高版本的 Web 界面，单击 "ILOM Administration" -> "Management Access" -> "SSH Server"。

2. 在 "SSH Server" 页面中，查看已生成的 RSA 和 DSA 密钥信息，或者执行以下操作：

   a. 单击 "Generate RSA Key" 生成新的密钥。

   b. 单击 "Generate DSA Key" 生成新的密钥。

相关信息

- 《*Oracle ILOM* 配置和维护管理员指南（固件 *3.2.x*）》中的“SSH 服务器配置属性”
- 《*Oracle ILOM 3.1* 配置和维护指南》中的“SSH 服务器配置属性”
- 《*Oracle ILOM 3.0* 日常管理 – *Web* 过程指南》中的“生成新 SSH 密钥”
- 《*Oracle ILOM 3.0* 日常管理 – *CLI* 过程指南》中的“生成新 SSH 密钥”

▼ 将 SSH 密钥附加到用户帐户以实现自动 CLI 验证

定制的已生成 SSH 密钥对（DSA 或 RSA）可以用于各个用户帐户，为此需要将公钥上载到 Oracle ILOM。这在使用无需手动干预即可执行并且不包含嵌入式明文密码的脚本时非常有用。用户可以编写从远程系统通过基于网络的 SSH 连接自动或定期执行服务处理器命令的脚本。

要上载生成的 SSH 公钥并将其附加到 Oracle ILOM 帐户，请参见以下基于 Web 的说明。

开始之前

- 使用 SSH 连接工具（例如 ssh-keygen）生成 SSH 私钥和公钥，然后将生成的 SSH 密钥文件存储在远程 SSH 系统上。
- 需要具有 User Management (u) 角色才能将 SSH 公钥附加到其他用户帐户。
- 需要具有 Read Only (o) 角色才能将 SSH 公钥附加到您自己的用户帐户。

1. 在 Oracle ILOM Web 界面中导航到 "User Account" 页面。
   例如，在以下界面中：
   - 3.0.x Web 界面，单击 "User Management" -> "User Accounts"。
   - 3.1 和更高版本的 Web 界面，单击 "ILOM Administration" -> "User Management" -> "User Accounts"。
2. 在 "User Account" 页面中，执行以下操作：
   a. 向下滚动到 "SSH Keys" 部分，然后单击 "Add"。
   b. 从 "User" 列表中选择一个用户帐户。
   c. 从列表中选择传输方法，然后指定上载 SSH 公钥所需的传输方法属性。
3. 单击 "Load" 以上载 SSH 公钥并将其附加到选定的用户帐户。

相关信息

- 《*Oracle ILOM* 配置和维护管理员指南（固件 *3.2.x*）》中的“使用本地 SSH 密钥进行 CLI 验证”
- 《*Oracle ILOM 3.1* 配置和维护指南》中的“使用本地 SSH 密钥进行 CLI 验证”
- 《*Oracle ILOM 3.0* 日常管理 – *Web* 过程指南》中的“管理用户帐户”
- 《*Oracle ILOM 3.0* 日常管理 – *CLI* 过程指南》中的“管理用户帐户”

配置 SNMP 管理访问以实现最高级别的安全性

SNMP 是用于监视或管理系统的标准协议。Oracle ILOM 提供了 SNMP 解决方案以同时用于监视和管理，但是在使用之前必须对其进行配置。在配置此服务之前，务必了解各个 SNMP 用户可配置选项在安全性方面的影响。有关更多详细信息，请参见以下信息：

- 使用 SNMPv3 加密和用户验证 [41]
- “支持可配置对象的 Sun SNMP MIB” [42]

▼ 使用 SNMPv3 加密和用户验证

SNMPv1 和 SNMPv2c 不提供加密，并且使用团体字符串 (community string) 作为验证形式。团体字符串 (community string) 通过网络以明文形式发送，并且通常在一组用户之间共享，而不是供单个用户专用。与之相反，SNMPv3 使用加密提供安全的通道和单独的用户名和密码。SNMPv3 用户密码已本地化，以便可以安全地存储在管理站上。

SNMPv1、SNMPv2c 和 SNMPv3 都受 Oracle ILOM 支持，并且可以单独地启用或禁用。此外，可以启用或禁用 "set" 以多添加一层保护。此可配置选项确定 SNMP 服务是否允许设置可配置的 SNMP MIB 属性。禁用 set 可有效地使 SNMP 服务只能用于监视。

默认情况下，禁用 SNMPv1 和 SNMPv2c。默认情况下启用 SNMPv3，但是在使用之前需要创建一个或多个 SNMP 用户。系统没有提供预配置的 SNMPv3 用户。

要在 Oracle ILOM 中配置 SNMP 管理，请参见以下基于 Web 的说明。

开始之前

- 为了实现最高级别的 SNMP 安全性，请仅将 SNMPv1 和 SNMPv2c 用于监视，在启用这些不太安全的协议时不要启用 "set"。
- SNMP set 应仅针对 SNMPv3 管理启用。默认情况下禁用 SNMP 的 Set 属性。
- SNMPv3 set 要求配置 SNMPv3 用户帐户。未提供预先配置的 SNMPv3 用户帐户。
- 默认情况下启用 SNMP 服务的 State 属性。
- 需要具有 Admin (a) 角色特权才能修改 SNMP 属性。
- 需要具有 User management (u) 特权才能添加或修改 SNMPv3 用户帐户。

1. 在 Oracle ILOM Web 界面中导航到 "SNMP" 页面。

   例如：

   - 3.0.x Web 界面，单击 "System Management Access" -> "SNMP"。
   - 3.1 和更高版本的 Web 界面，单击 "ILOM Administration" -> "Management Access" -> "SNMP"。

2. 在 "SNMP" 页面中，查看或修改 SNMP 属性，然后单击 "Save" 应用更改。

   有关更多说明，请参见本过程“相关信息”部分中列出的文档。对于运行固件版本 3.2 或更高版本的用户，请单击 "SNMP" 页面中的 `More details` 链接以获得更多信息。

相关信息

- 《*Oracle ILOM* 配置和维护管理员指南（固件 *3.2.x*）》中的“配置 SNMP 设置”
- 《*Oracle ILOM* 协议管理参考（适用于 *SNMP* 和 *IPMI*）（固件 *3.2.x*）》中的“配置 SNMP 设置”

- 《*Oracle ILOM 3.1 SNMP*、*IPMI*、*CIM* 和 *WS-Man* 协议管理参考》中的“配置 SNMP 设置”
- 《*Oracle ILOM 3.0 SNMP*、*IPMI*、*CIM* 和 *WS-Man* 协议管理参考》中的“配置 SNMP 设置”

支持可配置对象的 Sun SNMP MIB

Oracle 提供的支持可配置对象且适用 "set" 的 Sun MIB 如下所示：

- `SUN-HW-CTRL-MIB` – 此 MIB 用于配置硬件策略，如电源管理策略。
- `SUN-ILOM-CONTROL-MIB` – 此 MIB 用于配置 Oracle ILOM 功能，如创建用户和配置服务。

注 - 在满足以下条件时可以设置 MIB 对象：1) MIB 对象支持修改；2) MIB 对象的 `MAX-ACCESS` 元素设置为 `read-write`；3) 尝试执行 set 的用户有权这样做。

配置 IPMI 管理访问以实现最高级别的安全性

有关如何以最佳方式配置 Oracle ILOM IPMI 管理访问以实现最高级别的安全性，请参阅以下主题。

- 使用 IPMI v2.0 实现增强的验证和数据包加密 [42]
- “IPMI 安全准则和最佳做法” [44]
- “IPMI 2.0 验证密码组支持” [44]

▼ 使用 IPMI v2.0 实现增强的验证和数据包加密

尽管 Oracle ILOM 支持使用 IPMI v1.5 和 v2.0 进行远程管理，但是系统管理员应始终使用 IPMI v2.0 -I lanplus 界面安全地管理 Oracle 服务器。自 IPMI 版本 2.0 开始，-I lanplus 界面提供增强的验证和数据完整性检查。

自固件发行版 3.2.4 起，Oracle ILOM 提供了用于启用或禁用 IPMI v1.5 会话的可配置属性。为了实现高安全性，IPMI v1.5 属性默认处于禁用状态。当禁用 IPMI v1.5 属性时，会禁止（阻止）所有 IPMI v1.5 会话连接到 Oracle ILOM。

请参阅以下过程以查看或修改 IPMI 服务的 State 属性，或可配置的 IPMI v1.5 属性，该属性自固件发行版 3.2.4 开始提供。

开始之前

- 需要具有 Admin (a) 角色才能在 Oracle ILOM 中修改 IPMI 属性。

- 默认情况下启用 IPMI 服务的 State 属性。使用之前，必须在 Oracle ILOM 中使用正确的基于角色的特权 (Administrator, Operator) 配置用户帐户，才能执行 IPMI 管理功能。
- 对于运行 Oracle ILOM 固件 3.2.4 或更高版本的 SP，支持 IPMI v2.0 管理会话，但默认情况下不支持 IPMI v1.5 管理会话。IPMI v1.5 属性在 Oracle ILOM 中可以配置。

注 - 当 IPMI v1.5 会话在 Oracle ILOM 中处于禁用状态时，IPMItool 的用户必须使用 IPMI 2.0 -I lanplus 选项。

- 对于运行 Oracle ILOM 固件 3.2.3 或更低发行版的 SP，Oracle ILOM 支持 IPMI v2.0 和 v1.5 管理会话。IPMI v1.5 属性在 Oracle ILOM 中不可配置。

注 - IPMI v1.5 会话不支持增强的验证和数据包加密。对于增强的验证和 IPMI 数据包加密，您必须使用 IPMI v2.0。

---

1. 在 Oracle ILOM Web 界面中导航到 "IPMI" 页面。

   例如，在以下界面中：

   - 3.0 Web 界面，单击 "Configuration" -> "System Management Access" -> "IPMI"。
   - 3.1 和更高版本的 Web 界面，单击 "ILOM Administration" -> "Management Access" -> "IPMI"。

2. 在 "IPMI" 页面中，查看或配置相应的 IPMI 属性，然后单击 "Save" 应用更改。

   有关更多的 IPMI 配置说明，请参阅下面“相关信息”部分列出的相应文档。

相关信息

- 《*Oracle ILOM* 协议管理参考（适用于 *SNMP* 和 *IPMI*）（固件 *3.2.x*）》中的“使用 IPMI 进行服务器管理”
- 《*Oracle ILOM 3.1 SNMP*、*IPMI*、*CIM*、*WS-MAN* 协议管理参考》中的“使用 IPMI 进行服务器管理”
- 《*Oracle ILOM 3.0 SNMP*、*IPMI*、*CIM*、*WS-MAN* 协议管理参考》中的“使用 IPMI 进行服务器管理”
- “IPMI 安全准则和最佳做法” [44]
- “IPMI 2.0 验证密码组支持” [44]

IPMI 安全准则和最佳做法

为了确保建立的 IPMI 系统管理会话是安全的并且不易受到网络攻击，系统管理员应该：

- 切勿使用 IPMI 版本 1.5 建立 IPMI 远程管理会话（`-I lan` IPMItool 界面）。使用命令行实用程序（例如 IPMItool）时，应明确使用 IPMI 版本 2.0（`-I lanplus` IPMItool 界面）。
- 定期更改 IPMI 密码。确保正确管理 Oracle ILOM 用户帐户的生命周期。

  有关更多详细信息，请参见“保护 Oracle ILOM 用户访问” [21]。
- 限制从外部进行网络访问。使用专用的以太网管理通道与 Oracle ILOM 进行通信。

  有关更多详细信息，请参见“保护物理管理连接” [13]。
- 与 IT 安全专员合作，围绕服务器管理和 IPMI 安全制定一组最佳做法和策略。

IPMI 2.0 验证密码组支持

密码组为 IPMI 版本 2.0 中的验证、机密性和完整性检查提供支持。这些密码组使用 RMCP+ 验证密钥交换协议，如 IPMI 2.0 规范中所述。

Oracle ILOM 支持使用以下密码组密钥算法在客户机和服务器之间建立安全的 IPMI 2.0 会话。

- **密码组 2** – 密码组 2 使用验证和完整性算法。
- **密码组 3** – 密码组 3 使用全部三种算法，即验证、机密性和完整性算法。

注 - 为了确保对所有 IPMI 2.0 通信进行加密，Oracle ILOM 不支持 IPMI 2.0 加密类型 0（不加密的运行模式）。

配置 WS-Management 访问以实现最高级别的安全性

从固件发行版 3.0.8 到固件发行版 3.1.2，Oracle ILOM 提供了标准的 Web 服务界面来监视服务器的运行状况并使用名为 Ws-Management (Ws-Man) 的协议提供清单信息。

Oracle ILOM Ws-Man 接口还允许对主机进行对等控制和重置 Oracle ILOM SP 本身。Ws-Man 是基于简单对象访问协议 (Simple Object Access Protocol, SOAP) 的协议，并且利用 HTTP(S) 协议。Oracle ILOM Ws-Man 接口可以使用 HTTP 或 HTTPS 作为传输机制。如果使用 HTTPS，则通道使用 SSL 证书进行加密。有关使用 SSL 证书的安全优势以及自签名证书和可信证书之间差异的信息，请参见“使用可信的 SSL 证书和私钥提高安全性” [32]。

仅在使用 SSL 证书时才能使用此 Web 服务界面。为了实现最高级别的安全性，请使用 HTTPS 作为传输机制。有关配置 Web 服务器属性的更多信息，请参见“配置 Web 界面以实现最高级别的安全性” [31]。

Oracle ILOM 的部署后安全最佳做法

使用以下主题决定服务器部署后要实施的最佳 Oracle ILOM 安全做法。

相关信息

- Oracle ILOM 的部署安全最佳做法
- Oracle ILOM 的安全最佳做法核对表

维护安全管理连接

维护与 Oracle ILOM 的安全管理连接时，请考虑以下信息。

避免未经验证的主机 KCS 设备访问

Oracle 服务器支持在主机和 Oracle ILOM 之间建立标准的低速连接，称为键盘控制器样式 (Keyboard Controller Style, KCS) 接口。此受支持的 KCS 接口完全符合智能平台管理接口 (Intelligent Platform Management Interface, IPMI) 版本 2.0 规范，同样无法禁用。

尽管 KCS 设备访问是从主机配置 Oracle ILOM 的简便方法，但是此类型的访问也带来了安全风险，因为任何对物理 KCS 设备具有内核或驱动程序访问权限的操作系统用户

无需验证即可修改 Oracle ILOM 设置。通常，只有 `root` 或管理员用户才可以访问 KCS 设备。然而，可以将大多数操作系统配置为提供对 KCS 设备的更广泛访问。

例如，具有 KCS 访问权限的操作系统用户可以执行以下操作：

- 添加或创建 Oracle ILOM 用户。
- 更改用户密码。
- 以 ILOM 管理员身份访问 Oracle ILOM CLI。
- 访问日志和硬件信息。

通常，此设备在 Linux 或 Oracle Solaris 上称为 `/dev/kcs0` 或 `/dev/bmc`，在 Microsoft Windows 上称为 `ipmidrv.sys` 或 `imbdrv.sys`。必须使用主机操作系统中包含的适当访问控制机制严格控制对此设备（也称为底板管理控制器 (Baseboard Management Controller, BMC) 驱动程序或 IPMI 驱动程序）的访问。

可以考虑将 Oracle ILOM 互连接口用作使用主机 IPMI KCS 设备配置 Oracle ILOM 设置的备用方法。有关更多详细信息，请参见“首选的验证主机互连访问” [48]。

有关如何控制或保护对于 KCS 设备等硬件设备的访问的更多信息，请参见主机操作系统随附的文档。

首选的验证主机互连访问

作为 KCS 接口的速度更快的替代连接，主机操作系统上的客户机可以通过内部高速互连与 Oracle ILOM 进行通信。此互连通过内部 Ethernet-over-USB 连接实现，并且运行 IP 堆栈。系统为 Oracle ILOM 提供了一个不可路由的内部 IP 地址，主机上的客户机可以使用该 IP 地址连接到 Oracle ILOM。

KCS 接口依赖于受保护的硬件设备访问，与之不同，LAN 互连默认情况下可供所有操作系统用户使用。因此，通过 LAN 互连连接到 Oracle ILOM 需要验证，就像通过网络连接到 Oracle ILOM 管理端口一样。

此外，主机可通过 LAN 互连使用在管理网络上公开的所有服务或协议。可以使用主机上的 Web 浏览器访问 Oracle ILOM Web 界面或使用安全 Shell 客户机连接到 Oracle ILOM 命令行界面。在任何情况下，必须提供有效的用户名和密码才能使用 LAN 互连。

默认情况下，禁用 LAN 互连。在禁用时，不会在主机操作系统中显示以太网设备，该通道不存在。Oracle Hardware Management Pack 帮助置备和配置 LAN 互连。

有关通过安全的专用主机互连连接管理 Oracle ILOM 的信息，请参见以下主题之一：

- 对于固件发行版 3.2 或更高版本，请参见《*Oracle ILOM* 配置和维护管理员指南（固件 *3.2x*）》中的“专用互连 SP 管理连接”
- 对于固件发行版 3.1.x，请参见《*Oracle ILOM 3.1* 配置和维护指南》中的“专用互连 SP 管理连接”

- 对于固件发行版 3.0.12 到 3.0.16，请参见《*Oracle ILOM 3.0 Web* 过程指南》中的“配置本地主机互连”。

使用 IPMI 2.0 加密保护通道

智能平台管理接口 (Intelligent Platform Management Interface, IPMI) 版本 2.0 支持一种加密的网络协议，称为远程管理和控制协议+ (Remote Management and Control Protocol+, RMCP+)。此协议使用基于密钥的对称型质询响应机制对通道进行加密。此机制确保不会通过网络发送未加密的敏感数据，并且需要用户密码才能对通信进行加密和解密。为了确保对所有 IPMI 2.0 通信进行加密，Oracle ILOM 不支持 IPMI 2.0 加密类型 0（不加密）运行模式。

如果使用 IPMItool，请使用 `-I lanplus` 标志指明必须建立加密的 RMCP+ 会话。

有关更多信息，请参见 `ipmitool` 文档。

注 - 自固件发行版 3.2.4 起，Oracle ILOM 针对 IPMI 1.5 提供了一个可配置的属性。默认情况下禁用该 IPMI 1.5 属性。有关更多详细信息，请参见使用 IPMI v2.0 实现增强的验证和数据包加密 [42]。

使用安全协议进行远程管理

Oracle ILOM 支持多种不同的远程管理协议。在某些情况下，同时支持相同协议的加密版本和未加密版本。出于安全考虑，如果可以，您应该始终使用最安全的可用协议。有关受支持的加密和未加密协议的列表，请参见下表。

表 9　支持的安全协议

类别	安全/已加密	未加密
Web 浏览器访问	HTTPS	HTTP
命令行访问	SSH	都不支持
IPMI 访问	IPMI v2.0	IPMI v1.5
协议访问	SNMPv3	SNMPv1/v2c

建立安全的可信网络管理连接

带有 Oracle ILOM 的所有 Oracle 服务器都具有用于通过网络连接到 Oracle ILOM 的专用管理端口。使用专用管理端口可以提供一个专用的安全管理网络。一些系统还支持边带管理，该功能允许通过标准服务器数据端口访问主机和 Oracle ILOM。如果使用边带管理，则无需建立两个单独的网络连接，从而简化了电缆管理和网络配置。然而，

这也意味着如果专用或边带管理端口未连接到可信网络，则可能会通过不可信网络发送 Oracle ILOM 通信。

要为 Oracle ILOM 维护最安全可靠的环境，服务器上的专用网络管理端口或边带管理端口必须始终连接到内部的可信网络或专用的安全管理/专用网络。

建立安全的本地串行管理连接

您可以通过位于服务器上的物理串行管理端口在本地将终端服务器或转储终端连接到 Oracle ILOM。为了保证与 Oracle ILOM 建立的本地管理连接的安全性，如果终端设备已连接到内部或专用网络，则应避免将该设备连接到本地串行管理端口。

安全地使用远程 KVMS

Oracle ILOM 提供了将主机服务器的键盘、视频和鼠标远程重定向到远程客户机的功能，还提供了挂载远程存储的功能。这些功能统称为远程 KVMS。借助远程 KVMS，您可以在客户机上运行称为 Oracle ILOM Remote Console、Remote Console Plus 和 Storage Redirection CLI 的 Java 应用程序通过图形控制台监视服务器上的主机操作系统。

为了确保从 Oracle ILOM 安全启动远程 KVMS 和串行基于文本的会话，请考虑以下措施：

- “KVMS 远程通信和加密” [50]
- “针对远程 KVMS 共享访问实施保护” [51]
- “针对主机串行控制台共享访问实施保护” [51]

KVMS 远程通信和加密

Oracle ILOM Remote System Console、Remote System Console Plus 和 CLI Storage Redirection 应用程序使用一系列网络协议与 Oracle ILOM 进行远程通信。使用这些 Java 应用程序，您可以控制主机键盘和鼠标以及在远程服务器上挂载本地存储设备（如 CD 或 DVD 驱动器）。

下表更详细地说明了通过网络传输远程 KVMS 信息的方式。

表 10 KVMS 功能和加密

KVMS 功能	加密或未加密	描述
鼠标重定向	加密	您鼠标的坐标通过网络安全地发送到 Oracle ILOM。
键盘重定向	加密	您在客户机上键入的任何字符都使用加密的协议传输到 Oracle ILOM。

KVMS 功能	加密或未加密	描述
视频重定向	加密	视频数据通过加密的协议在 Java 客户机和 Oracle ILOM 之间传输。
存储重定向	未加密	在存储设备中读取和写入的数据在不加密的情况下通过网络传输到 Oracle ILOM。

有关远程 KVMS 启用的网络端口列表，请参见表 4 “默认启用的服务和端口”。

针对远程 KVMS 共享访问实施保护

远程 KVMS 视频控制台重定向的内容与通过连接到服务器的物理监视器查看时看到的内容相同。尽管可以有多个远程客户机与 Oracle ILOM 建立 KVMS 会话，但是每个会话将显示完全相同的视频，因为一个服务器通常只有一个视频输出。

同样，您在一个远程 KVMS 会话的屏幕上键入的任何内容都将显示给连接到同一计算机的其他 KVMS 用户。最重要的是，如果一个用户以特权用户的身份在 Oracle ILOM Remote Console、Remote Console Plus 和 Storage Redirection CLI 应用程序中登录到主机操作系统，所有其他 KVMS 用户都能够共享此已验证会话。因此，一定要知道远程 KVMS 功能允许建立共享连接。

要针对终止远程 KVMS 重定向会话后保持闲置状态的已验证操作系统会话实施保护，您应该：

- 将 Oracle ILOM 配置为在终止远程 KVMS 重定向会话时自动锁定主机操作系统。
  有关说明，请参见退出 KVMS 会话时锁定主机访问 [28]。
- 在主机操作系统中设置超时间隔以自动关闭无人看管的已验证用户会话。
  有关说明，请参阅您主机操作系统的用户文档。

如果您是 Oracle ILOM Remote System Console Plus 用户并需要限制从 Oracle ILOM 启动的可查看 KVMS 会话的数量，请参见限制 Remote System Console Plus（3.2.4 或更高版本）可查看的 KVMS 会话 [29]。

针对主机串行控制台共享访问实施保护

大多数操作系统的主机控制台还可以通过基于文本的串行控制台访问。此控制台可通过在 Oracle ILOM CLI 的命令行中运行 `start /HOST/console` 命令来访问。与图形控制台类似，所有 Oracle ILOM 用户只能使用一个串行控制台。因此，可以将其视为共享资源。如果一个用户从串行控制台登录到主机操作系统，然后未注销即终止了控制台重定向，那么串行控制台的另一用户可以访问先前验证的操作系统会话。

在终止控制台重定向会话时，Oracle ILOM 会向主机操作系统发送数据传输请求 (Data Transfer Request, DTR) 信号。许多操作系统在收到此信号时自动注销用户。然而，不是所有操作系统都支持此功能：

- Oracle Linux 5 支持 DTR 信号，并且该功能默认情况下处于启用状态。
- Oracle Linux 6 支持 DTR，但是必须手动启用该功能。
- Oracle Solaris 不支持 DTR 信号。为了降低安全风险，用户可以在主机操作系统中配置会话超时。

有关针对终止主机串行重定向会话后保持闲置状态的已验证操作系统会话实施保护的准则，请参见下文：

- 确定主机操作系统是否支持 DTR 信号功能，如果支持，则确保默认情况下启用该功能。

  有关 DTR 信号的信息，请参阅您主机操作系统的用户文档。
- 在主机操作系统中配置会话超时间隔。

  有关如何在主机操作系统中设置会话超时间隔的信息，请参阅您主机操作系统的用户文档。
- 实施安全策略以确保用户不会将远程串行主机控制台置于无人看管的状态。当不再使用会话时，用户应当始终注销所有远程主机控制台会话。

保护用户访问的部署后注意事项

为了确保可以一直保持安全的用户访问，请考虑以下措施：

- “强制实施密码管理” [52]
- “出于安全考虑亲临现场重置 root 帐户的默认密码” [53]
- “监视审计事件以发现未经授权的访问” [54]

强制实施密码管理

您需要定期更改所有 Oracle ILOM 密码。这样可以防止恶意行为，并且可以确保密码符合当前的密码策略。

通常，用户自行更改其密码，但是，具有用户管理特权的系统管理员可以修改与其他用户帐户关联的密码。

要更改与 Oracle ILOM 用户帐户关联的密码，请参见以下基于 Web 的说明。

注 - 有关用户管理配置属性的 CLI 说明或其他详细信息，请参见以下过程中提供的“相关信息”部分列出的文档。

▼ 修改本地用户帐户密码

开始之前

- 请参见“管理用户帐户和密码的安全准则” [22]。
- 需要具有 User Management (u) 角色才能修改与其他用户帐户关联的密码或特权。
- Operator (o) 角色允许用户修改其自己帐户的密码。

1. 在 Oracle ILOM Web 界面中导航到 "User Account" 页面。
   例如，在以下界面中：
   - 3.0.x Web 界面，单击 "User Management" -> "User Accounts"。
   - 3.1 和更高版本的 Web 界面，单击 "User Management" -> "User Accounts"。
2. 在 "User Account" 页面中，单击要修改帐户的 "Edit"。
   此时将显示 "Edit: User Name" 对话框。
3. 在 "Edit: User Name" 对话框中，执行以下操作：
   - 在 "New Password" 文本框中输入一个唯一的密码，然后在 "Confirm New Password" 文本框中重新输入相同的密码。
   - 单击 "Save" 应用更改。

相关信息

- 为所有本地用户设置密码策略限制（3.2.5 及更高版本） [25]
- 《*Oracle ILOM* 配置和维护管理员指南（固件 *3.2.x*）》中的“配置本地用户帐户”。
- 《*Oracle ILOM 3.1* 配置和维护指南》中的“配置本地用户帐户”
- 《*Oracle ILOM 3.0* 日常管理 – *CLI* 过程指南》中的“修改用户帐户”
- 《*Oracle ILOM 3.0* 日常管理 – *Web* 过程指南》中的“修改用户帐户”

出于安全考虑亲临现场重置 `root` 帐户的默认密码

如果 Oracle ILOM 的 `root` 用户密码丢失，可以将其重置。要重置 `root` 密码，需要使用串行端口连接到 Oracle ILOM。尽管大多数情况下连接到 Oracle ILOM 串行端口需要实际接触系统，但是串行控制台可以连接到终端服务器。使用终端服务器，可以通过网络有效地访问物理串行端口。

为了防止使用终端服务器时通过网络重置 `root` 密码，大多数服务器都提供了亲临现场检查功能。此功能要求用户按服务器上的一个按钮，以证明自己在实际接触服务器。为了实现最高级别的安全性，请确保在 Oracle ILOM 串行端口连接到终端服务器时启用亲临现场检查功能。

要查看或修改亲临现场检查功能，请参见以下基于 Web 的说明。

注 - 有关 root 帐户属性的 CLI 说明或其他详细信息，请参见以下过程中提供的“相关信息”部分列出的文档。

▼ 设置亲临现场检查

开始之前

- Oracle ILOM 默认情况下启用亲临现场检查模式。
- 需要具有固件版本 3.1 或更高版本才能在 Oracle ILOM 中使用亲临现场检查模式。

1. 在 Oracle ILOM Web 界面中，单击 "ILOM Administration" -> "Identification"
2. 在 "Identification" 页面中，导航到 "Physical Presence Check" 属性，然后执行以下操作之一：

   - 选中 "Physical Presence" 复选框以启用。处于启用状态时，必须按物理系统上的 "Locator" 按钮才能恢复默认的 Oracle ILOM 密码。
     – 或者 –
   - 清除 "Physical Presence" 复选框以禁用。处于禁用状态时，可以重置默认的 Oracle ILOM 管理员密码，而无需按物理系统上的 "Locator" 按钮。

3. 单击 "Save" 应用更改。

相关信息

- 《*Oracle ILOM* 配置和维护管理员指南（固件 *3.2.x*）》中的“设备标识配置属性”
- 《*Oracle ILOM 3.1* 配置和维护指南》中的“设备标识配置属性”
- 《*Oracle ILOM* 配置和维护管理员指南（固件 *3.2.x*）》中的“root 帐户的密码恢复”。
- 《*Oracle ILOM 3.1* 配置和维护指南》中的“root 帐户的密码恢复”

监视审计事件以发现未经授权的访问

Oracle ILOM 审计日志会记录所有登录活动和配置更改。每个审计日志条目都会记下与事件相关联的用户和时间戳。如果要跟踪更改和确定是否存在未经授权的更改或对 Oracle ILOM 的未经授权的访问，审计事件可能是非常有用的工具。

要查看 Oracle ILOM 审计日志中的事件，请参见以下基于 Web 的说明。

注 - 有关审计日志的 CLI 说明或其他详细信息，请参见以下过程的“相关信息”部分中列出的文档。

▼ 查看审计日志

开始之前

- 自固件发行版 3.1 起，Oracle ILOM 中提供了审计日志。在固件发行版 3.1 之前，审计事件被捕获在 Oracle ILOM 事件日志中。
- 需要在 Oracle ILOM 中具有 Admin (a) 角色特权才能清除审计日志中的条目。

1. 在 Web 界面中，单击 "ILOM Administration" -> "Logs" -> "Audit"。
2. 在 "Audit" 日志页面中，使用控件过滤日志条目，或者清除日志中的事件。

   对于运行固件版本 3.2 或更高版本的用户，请单击 "Audit" 页面中的 `More details` 链接以获得更多信息。

相关信息

- 《*Oracle ILOM* 系统监视和诊断用户指南（固件 *3.2.x*）》中的“管理 Oracle ILOM 日志条目”
- 《*Oracle ILOM 3.1* 用户指南》中的“管理 Oracle ILOM 日志条目”

部署后修改 FIPS 模式的操作

自固件发行版 3.2.4 起，Oracle ILOM 提供了用于实现 FIPS 1 级符合性的可配置属性。默认情况下，该属性出厂时处于禁用状态。在 Oracle ILOM 中修改 FIPS 符合性的操作状态时，所有用户定义的配置属性都会重置为其出厂默认设置。为了避免丢失 Oracle ILOM 中用户定义的配置设置，应该在配置任何其他 Oracle ILOM 设置之前修改 FIPS 符合性。如果必须在部署 Oracle ILOM 配置后修改 FIPS 符合性，请参见以下说明以避免丢失用户定义的设置。

注 - Oracle 使用符合 FIPS 140-2 安全标准的加密算法保护系统的敏感或重要数据。

▼ 部署后修改 FIPS 模式

如果在执行固件更新或指定 Oracle ILOM 中用户定义的配置属性后需要修改 FIPS 模式的操作状态，请使用此过程。

注 - Oracle ILOM 中的 FIPS 符合性模式由 State 和 Status 属性表示。State 属性表示 Oracle ILOM 中的已配置模式，而 Status 属性表示 Oracle ILOM 中的操作模式。如果更改 FIPS State 属性，则在下一次 Oracle ILOM 重新引导之前，更改不会影响操作模式（FIPS Status 属性）。

开始之前

- 自固件 3.2.4 或更高版本起，Oracle ILOM 提供了用于实现 FIPS 1 级符合性的可配置属性。在固件发行版 3.2.4 之前，Oracle ILOM 不提供用于实现 FIPS 1 级符合性的可配置属性。
- 启用了 FIPS 时（已配置且可以正常运行），Oracle ILOM 中的一些功能不受支持。有关启用 FIPS 后不受支持功能的列表，请参见“启用 FIPS 模式时不受支持的功能” [16]。
- 需要具有 Admin (a) 角色才能执行此过程。

1. 在 Oracle ILOM Web 界面中，备份 Oracle ILOM 配置。

   例如：

   a. 单击 "ILOM Administration" -> "Configuration Management" -> "Backup/Restore"。

   b. 在 "Backup/Restore" 页面中，单击 "More details..." 链接以获得更多说明。

   注 - 为了简化固件更新后与 Oracle ILOM 重新建立连接的过程，您应该启用保留配置的固件更新选项。

   注 - 如果您在执行第 1 步之前执行第 2 步，则需要编辑 XML 备份配置文件并删除 FIPS 设置。否则，您在备份的 Oracle ILOM XML 文件和服务器上运行的 FIPS 模式操作状态之间将具有不一致的配置，这是不允许的。

2. 如果需要固件更新，请执行以下步骤：

   a. 单击 "ILOM Administration" -> "Maintenance" -> "Firmware Update"。

   b. 在 "Firmware Update" 页面中，单击 "More details..." 链接以获得更多说明。

3. 按如下所示在 Oracle ILOM 中修改 FIPS 符合性模式：

   a. 单击 "ILOM "Administration" -> "Management Access" -> "FIPS"。

   b. 在 "FIPS" 页面中，单击 **`More details`** 链接以获得有关操作方法的说明：

      - 修改 FIPS State 配置。
      - 通过重置 SP 更新系统上的 FIPS 操作状态。

4. 按如下所示恢复备份的 Oracle ILOM 配置：

a. 单击 "ILOM Administration" -> "Configuration Management" -> "Backup/Restore"。

b. 在 "Backup/Restore" 页面中，单击 **More details** 链接以获得更多说明。

相关信息

- “选择是否在部署时配置 FIPS 模式” [14]
- “启用 FIPS 模式时不受支持的功能” [16]
- 《*Oracle ILOM* 配置和维护管理员指南（固件 *3.2.x*）》中的“配置 FIPS 模式属性”

更新至最新的软件和固件

保持服务器上的软件和固件为最新版本。

- 定期查看 My Oracle Support 上发布的更新。
- 通过始终安装最新发行的服务器可用的软件或固件版本来利用各项错误修复和增强。
- 安装所有已安装软件所需的所有必要安全修补程序。

要更新服务器上的 Oracle ILOM 固件，请参见以下说明。

▼ 更新 Oracle ILOM 固件

开始之前

- 需要在 Oracle ILOM 中具有 Admin (a) 角色才能更新 Oracle ILOM 固件。
- 向所有 Oracle ILOM 用户通知预定固件更新并请他们关闭所有客户机会话直至固件更新完成。
- 固件更新过程需要几分钟的时间才能完成，在此期间不应执行任何其他 Oracle ILOM 任务。

1. 从 My Oracle Support (MOS) Web 站点下载适用于您服务器的最新软件更新。
   如果需要，请参阅您服务器随附的文档以获得有关从 MOS 获取软件更新的说明。

   注 - MOS 上面向您的服务器发布的最新软件修补程序中包含适用于您服务器的最新 Oracle ILOM 固件版本。

2. 将固件映像放在本地或网络共享驱动器上。

3. 在 Web 界面中导航到 "Firmware Update" 页面。

例如：

- 在 3.0.x Web 界面中，单击 "Maintenance" -> "Firmware"。
- 在 3.1 或更高版本的 Web 界面中，单击 "ILOM Administration" -> "Maintenance" -> "Firmware Upgrade"。

4. 在 "Firmware Upgrade" 页面中，单击 "Enter Firmware Upgrade" 模式，然后按照提示操作。

   对于运行 Oracle ILOM 固件 3.2 或更高版本的用户，请单击 "Firmware Upgrade" 页面上的 `More details` 链接。