

Oracle® Fabric OS 1.0.2 安全指南



文件号码 E74811-02
2016 年 11 月

文件号码 E74811-02

版权所有 © 2016, 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, 则适用以下注意事项:

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。除非您与 Oracle 签订的相应协议另行规定, 否则对于第三方内容、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保证, 亦不对其承担任何责任。除非您和 Oracle 签订的相应协议另行规定, 否则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。

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

Oracle Fabric OS 安全	7
安全原则	7
保持软件和更新为最新版本	7
限制对关键服务的网络访问	7
遵循最小特权原则	7
监视系统活动	8
密切关注最新安全信息	8
用户安全性	8
用户帐户	8
用户帐户密码条件	9
▼ 设置高用户密码强度	9
▼ 添加用户并分配适当特权	9
阻止未列出用户的访问	10
网络访问控制	10
SNMP 配置	10
系统活动监视	11

Oracle Fabric OS 安全

本文档提供了有关 Oracle Fabric OS 1.0.2 的一般安全准则。这些内容适用于有经验的网络管理员，其中介绍了用于增强安全性的一般准则和具体说明。

请参阅以下指南来获取其他相关产品的安全指导：

- [Oracle Fabric Manager 5.0.2 安全指南](#)
- [Oracle EDR InfiniBand 交换机和虚拟化 I/O 系统硬件安全指南](#)

以下主题阐述了 Oracle Fabric OS 1.0.2 的安全准则。

- “安全原则” [7]
- “用户安全性” [8]
- “网络访问控制” [10]
- “系统活动监视” [11]

安全原则

以下主题介绍了安全使用任何应用程序所需的基本原则。

保持软件和更新为最新版本

使运行的 Oracle Fabric OS 的版本保持最新。可在以下网址查找要下载的最新软件版本：[My Oracle Support \(https://support.oracle.com\)](https://support.oracle.com)。

限制对关键服务的网络访问

将 Oracle Fabric OS 放在位于安全管理网络上的设备上。该设备不应面向 Internet。

遵循最小特权原则

授予用户或管理员完成要执行的任务所需的最小特权。Oracle Fabric OS 具有可为用户授予的各种角色。这些角色可以授予不同类型和数量的特权。

监视系统活动

监视系统活动以确定 Oracle Fabric OS 的运行情况以及是否正在记录任何异常活动。

密切关注最新安全信息

可以访问安全信息的多个源：

- 有关各种软件产品的安全信息和警报，请参阅 <http://www.us-cert.gov>。
- 运行 Oracle 虚拟网络软件的最新版本并参阅其文档。

用户安全性

以下主题介绍对于 Oracle Fabric OS 应遵循的安全准则。

用户帐户

该系统附带两个默认管理帐户。通过策略对这些帐户执行复杂密码。

- root—允许对底层基于 Linux 的 Oracle Fabric OS 进行完全管理访问。安全凭证由 Oracle Enterprise Linux 6.7 (UEK 4) 控制。
- admin—允许对 Oracle Fabric OS 管理工具和安全进行管理访问，包括创建新用户帐户的能力。这些用户可以访问机箱配置，但是他们不能重新配置 Linux 设置。Oracle Fabric OS 支持通过 `set system password` 命令进行密码强化。使用下面的过程阻止攻击者采用利用这些帐户的方式在系统上创建用户

为避免共用帐户和密码，我们为每个 Oracle Fabric OS 用户都提供了一个唯一的用户名和密码，并指定了与用户任务相匹配的相应角色。

不允许 Oracle Fabric OS 用户在 Linux 级别修改任何数据。Oracle Fabric OS 用户支持五种类型的角色：

- 管理员—超级用户。允许创建、编辑和管理 Oracle Fabric OS。
- 网络—允许创建、编辑和删除服务器配置文件、vNIC、以太网卡和端口以及网络 QoS。
- 操作员—允许只读访问，包括所有 `show` 命令。
- 服务器—允许创建、编辑和删除服务器配置文件以及操作物理服务器的能力。
- 存储—允许创建、编辑和删除 vHBA、光纤通道 I/O 卡和端口的服务器配置文件。

注 - 始终为用户分配其任务所需的最小特权。

用户帐户密码条件

系统将提示用户输入密码以进行验证。创建用户密码之前，在 Oracle Fabric OS 中通过 `set system password-strength` 命令指定条件来设置密码强度。使用以下条件：

- `min-length`—设置允许密码字符串包含的最少字符数量。
- `min-lower-case`—设置密码所需的小写字母的最少数量。
- `min-number`—设置密码所需的数字的最少数量。
- `min-special`—设置密码所需的特殊字符的最少数量。
- `min-upper-case`—设置密码所需的大写字母的最少数量。

注 - 安装系统时，在创建用户密码之前，先确定密码强度条件。将用户密码强度配置为遵循组织安全策略。

▼ 设置高用户密码强度

在本示例中，非默认本地用户帐户的密码必须至少有 8 个字符，其中含 3 个小写字母、2 个数字、2 个特殊字符和 1 个大写字母。

1. 登录到 Oracle Fabric OS。

请参阅 [《Oracle Fabric OS 1.0.2 管理指南》](#) 中的“登录到 Oracle Fabric OS (SSH)”。

2. 设置密码强度。

```
[OFOS] set system password-strength -min-length=8 -min-lower-case=3 -min-number=2 -min-special=2 -min-upper-case=1
```

有关使用 Oracle Fabric OS 设置强密码的更多信息，请参阅 [《Oracle Fabric OS 1.0.2 管理指南》](#) 中的“设置系统密码强度”或 [《Oracle Fabric OS 1.0.2 命令参考》](#) 中的“`set system`”。

▼ 添加用户并分配适当特权

必须具有管理员特权才能添加用户和分配角色。

有关添加用户的更多信息，请参阅 [《Oracle Fabric OS 1.0.2 管理指南》](#) 中的“查看用户的特权”或 [《Oracle Fabric OS 1.0.2 命令参考》](#) 中的“`user`”。

1. 登录到 Oracle Fabric Manager GUI。

请参阅 [《Oracle Fabric OS 1.0.2 管理指南》](#) 中的“登录到 Oracle Fabric Manager (GUI)”。

2. 在 GUI 中，添加用户并向该用户分配角色。

请参阅《Oracle Fabric Manager 5.0.2 管理指南》中的“将角色分配给用户”。有关角色列表，请参阅《Oracle Fabric OS 1.0.2 管理指南》中的“用户和角色”。

3. 在 Oracle Fabric Manager GUI 或 Oracle Fabric OS 中，验证用户配置是否正确。

```
[OFOS] show user frank
name          role          descr
-----
frank          administrators
1 record displayed
```

4. 在 Oracle Fabric OS 中，测试新用户帐户。

```
[OFOS] quit
Connection to 192.168.8.133 closed.
$ ssh frank@192.168.8.133
Password:
[OFOS] pwd
/home/frank
```

阻止未列出用户的访问

默认情况下，不允许未列出的用户访问 Oracle Fabric OS。除了底层用户帐户，列出的用户还具有 Oracle Fabric OS 中定义的用户角色。更改某项设置来允许未列出的用户时，如果某个用户具有能够对主机进行验证的帐户，则该用户将能够登录到 Oracle Fabric OS 并被授予操作员角色（只读访问）。阻止未列出的用户时，某个未列出用户的主机验证可能成功，但是 Oracle Fabric OS 将拒绝该用户访问，导致该用户看起来身份验证失败。

要验证此级别的安全性，请确保禁止未列出用户的访问。

网络访问控制

网状结构网络公布以下端口：

- 端口 22 **ssh**—CLI 管理。
- 端口 8080 **http**—未加密的 Oracle Fabric Manager 客户机访问权限。
- 端口 7443 **https**—加密 Oracle Fabric Manager 客户机访问。
- 端口 161 **SNMP**—SNMP 监视。
- 端口 6522—允许 Oracle Fabric Manager 搜索网状结构网络互联设备。

SNMP 配置

Oracle Fabric OS 支持 SNMP v3。始终使用 SNMP v3 并使用正确的验证协议。

系统活动监视

日志文件存储在 /log 目录中。各种子系统具有单独的日志文件条目，包括 dmesg。

标准 syslog 消息放入 user.log 文件，达到 10 个使用 gzip 压缩的文件时进行日志滚动和自动归档：

注 - 定期监视日志文件并对其进行归档，以便利用安全审核来避免安全违规情况。

1. 显示 CLI 登录活动。

```
[OFOS] more /log/cli.log
```

2. 显示每日引导消息。

```
[OFOS] more /log/dmesg
```

有关日志文件的详细信息，请参阅 [《Oracle Fabric OS 1.0.2 管理指南》](#) 中的“使用系统日志文件进行故障排除”。

