Oracle® Fabric Manager 5.0.2 安全指南

文件号码 **E79492-02**
2016 年 11 月

ORACLE

文件号码 E79492-02

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

Oracle Fabric Manager 安全

本文档提供了 Oracle Fabric Manager（从版本 5.0.0 开始）的一般安全准则。此信息旨在帮助保护 Oracle Fabric Manager 软件。

Oracle Fabric Manager 概述

Oracle Fabric Manager 是 Oracle 推出的一种多设备管理系统，其作用是保管并管理 Oracle 网状结构网络设备（一台或多台 Oracle InfiniBand Switch IS2-46、Oracle 网状结构网络互联设备或 Oracle SDN Controller）和 Oracle 虚拟 I/O。Oracle Fabric Manager 产品是一种服务器/客户机模型，支持在网状结构网络设备、模块、服务器或虚拟机级配置并管理虚拟资源。

Oracle Fabric Manager 是运行在远程服务器上的一个基于浏览器的管理系统。Oracle Fabric Manager 远程服务器可对 Oracle Fabric Manager 界面上的配置和管理任务进行转换，然后将信息转发给由 Oracle Fabric Manager 管理的网状结构网络设备。

一般安全原则

以下主题介绍了安全使用任何应用程序需要遵循的基本原则。

使软件保持最新

使运行的 Oracle Fabric Manager 版本保持最新。您可以在以下网址查找软件的最新版本进行下载：http://support.oracle.com。

限制对关键服务的网络访问

Oracle Fabric Manager 使用以下端口：

端口	说明
8880 或 8443 (HTTPS)	供最终用户连接到 Oracle Fabric Manager。 或者，也可以使这些端口保持关闭，但是应打开 RDP 会话并使用本地浏览器，以增强安全性。
443	供 Oracle Fabric Manager 建立连接以配置网状结构网络互联设备和 OSDN Controller。
6522	供 Oracle Fabric Manager 建立连接以搜索网状结构网络互联设备和 OSDN Controller。
7443	供 Oracle Fabric Manager 建立连接以配置 Oracle InfiniBand 交换机。
7777	供 Oracle Fabric Manager 建立连接以搜索 Oracle InfiniBand 交换机。
22	供 Oracle Fabric Manager 在所有类型的设备上下载日志以及导出和导入备份文件

将 Oracle Fabric Manager 和它控制的设备放置在安全的管理网络上。它们不应该面向 Internet。

遵循最小特权原则

授予用户或管理员完成任务所需的最小特权。Oracle Fabric Manager 具有可以授予用户的各种角色。这些角色可以授予不同类型和数量的特权。

使用 "Security Manager"（安全管理器）功能，这些功能可以从界面的导航面板中获得，用于为 Oracle Fabric Manager 配置用户角色。"Security Manager"（安全管理器）功能还允许您在特定网络域中配置网状结构网络设备。有关使用 "Security Manager"（安全管理器）的详细信息，请参阅*Oracle Fabric Manager 5.0.2* 管理指南。

监视系统活动

监视系统活动以确定 Oracle Fabric Manager 的运行情况以及是否正在记录任何异常活动。检查以下日志文件，其中包含有关 Oracle Fabric Manager 的信息：

Windows 服务器	Linux 服务器	Oracle Solaris 服务器
director-<name>.log	director-<name>.log	director-<name>.log
xmsaudit.log.1	xmsaudit.log.1	xmsaudit.log.1
xms-ha.log.1	xms-ha.log.1	xms-ha.log.1
xmsjobs.log.1	xmsjobs.log.1	xmsjobs.log.1
xms.log.1	xms.log.1	xms.log.1
xms-schedule.log.1	xms-schedule.log.1	xms-schedule.log.1
xms-stderr.log	tomcat.log	tomcat.log
xms-stdout.log	catalina.out	catalina.out
commons-daemon.log		catalina.pid

密切关注最新安全信息

可以从多个来源获取安全信息。

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

访问

只能从 DMZ 后面的专用网络对 Oracle Fabric Manager 进行 Web 访问。

考虑禁止对 Oracle Fabric Manager 的本地访问。一种方法是使用防火墙阻止 Oracle Fabric Manager 端口。要连接到 Oracle Fabric Manager，必须首先执行远程桌面协议以连接到主机，然后使用 localhost 连接到 Oracle Fabric Manager。

确保 Oracle Fabric Manager 仅使用专用安全网络与网状结构网络设备（例如网状结构网络互联设备或 Oracle SDN Controller）通信。

▼ 检查文件权限

在安装 Oracle Fabric Manager 软件后检查文件权限。使用以下过程检查Linux 或 Oracle Solaris 的文件权限。

1. **在安装 Oracle Fabric Manager 之前，创建名为 `xsigo` 的用户。**
   创建包含以下行的 `~xsigo/.profile` 文件：

   ```
   umask 077
   ```

   通过输入以下命令并验证输出是否为 `077` 来验证此配置文件是否已生效。

   ```
   # su xsigo
   # umask
   0077
   ```

2. **安装 Oracle Fabric Manager。**
   请参阅《Oracle Fabric Manager 5.0.2 安装指南》 中的 “安装软件”。

3. **安装后，检查产品文件的权限级别，确定是否有任何文件是全局可读或全局可写的。**
   以下 Linux 命令不应检索任何文件：

   ```
   find /opt/xsigo/xms/ -perm -o=r
   find /opt/xsigo/xms/ -perm -o=w
   ```

4. **修复发现的任何文件的权限。**

▼ 控制对默认帐户的访问

Oracle Fabric Manager 附带了两个自动获得授权的用户：

- `root`（在 Windows 中为 `administrator`）
- `ofmadmin`

防止攻击者利用这些帐户在系统上创建用户。

1. **为系统建立安全的集中化验证。**

2. **安装 Oracle Fabric Manager 后，立即创建名为 `ofmadmin` 的用户并为该帐户指定随机密码。**
   有关更多信息，请参阅《Oracle Fabric Manager 5.0.2 管理指南》 中的 “将角色分配给用户”。

SSL 证书

为 Oracle Fabric Manager 安装正确签名的 SSL 证书。有关更多详细信息，请参阅《Oracle Fabric Manager 5.0.2 安装指南》 中的 “配置 Oracle Fabric Manager 的证书”。

▼ 阻止未列出的用户进行访问

默认情况下，不允许未列出的用户访问 Oracle Fabric Manager。对于列出的用户，除了在主机 OS 中具有底层用户帐户之外，还在 Oracle Fabric Manager 中为其定义了用户角色。如果更改了设置，允许未列出的用户访问，那么以下用户将能够登录 Oracle Fabric Manager 并将获得操作员角色（实际拥有只读访问权限）：具有可以向主机验证身份的帐户。如果阻止未列出的用户，则未列出用户的主机验证可以成功，但 Oracle Fabric Manager 将拒绝该用户访问，看起来就像验证失败一样。

要验证此级别的安全性，请检查是否已禁止未列出用户的访问。

1. **单击 Fabric Manager "Maintenance"（维护）图标**
2. **找到 "Allow Unlisted Users"（允许未列出的用户）选项。**
   如果此选项的旁边显示复选标记，则去掉该复选标记以禁止访问。

Oracle Fabric Manager 插件的安全

可以向 Oracle Fabric Manager 添加各种插件模块。决定安装并使用任何插件模块时，同样请考虑一般安全注意事项。

此外，还需要遵循特定于每个插件的安全准则。“Oracle Fabric Monitor 的安全” [11]中提供了一些插件模块的安全信息。

Oracle Fabric Monitor 的安全

如果您将 Oracle Fabric Monitor 插件模块与 Oracle Fabric Manager 结合使用，则除了遵循 Oracle Fabric Manager 的一般安全做法之外，还需要遵循以下准则。

一般性准则

- 数据库应位于管理网络上并且应位于 DMZ 后面。
- 保留数据库的备份。

MySQL

保护此插件模块中包含的 MySQL 功能的安全。请参阅 `http://dev.mysql.com/doc/refman/5.7/en/security-guidelines.html`

PostGres

保护此插件模块中包含的 postgres 功能的安全。请参阅包含的 postgres 版本的安全准则，网址为：http://www.postgresql.org/docs/。