Oracle® Fabric Manager

Security Guide

Part No.: E49555-01
December 2013

Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related software documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

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.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Copyright © 2013, Oracle et/ou ses affiliés. Tous droits réservés.

Ce logiciel et la documentation qui l'accompagne sont protégés par les lois sur la propriété intellectuelle. Ils sont concédés sous licence et soumis à des restrictions d'utilisation et de divulgation. Sauf disposition de votre contrat de licence ou de la loi, vous ne pouvez pas copier, reproduire, traduire, diffuser, modifier, breveter, transmettre, distribuer, exposer, exécuter, publier ou afficher le logiciel, même partiellement, sous quelque forme et par quelque procédé que ce soit. Par ailleurs, il est interdit de procéder à toute ingénierie inverse du logiciel, de le désassembler ou de le décompiler, excepté à des fins d'interopérabilité avec des logiciels tiers ou tel que prescrit par la loi.

Les informations fournies dans ce document sont susceptibles de modification sans préavis. Par ailleurs, Oracle Corporation ne garantit pas qu'elles soient exemptes d'erreurs et vous invite, le cas échéant, à lui en faire part par écrit.

Si ce logiciel, ou la documentation qui l'accompagne, est concédé sous licence au Gouvernement des Etats-Unis, ou à toute entité qui délivre la licence de ce logiciel ou l'utilise pour le compte du Gouvernement des Etats-Unis, la notice suivante s'applique :

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.

Ce logiciel ou matériel a été développé pour un usage général dans le cadre d'applications de gestion des informations. Ce logiciel ou matériel n'est pas conçu ni n'est destiné à être utilisé dans des applications à risque, notamment dans des applications pouvant causer des dommages corporels. Si vous utilisez ce logiciel ou matériel dans le cadre d'applications dangereuses, il est de votre responsabilité de prendre toutes les mesures de secours, de sauvegarde, de redondance et autres mesures nécessaires à son utilisation dans des conditions optimales de sécurité. Oracle Corporation et ses affiliés déclinent toute responsabilité quant aux dommages causés par l'utilisation de ce logiciel ou matériel pour ce type d'applications.

Oracle et Java sont des marques déposées d'Oracle Corporation et/ou de ses affiliés.Tout autre nom mentionné peut correspondre à des marques appartenant à d'autres propriétaires qu'Oracle.

Intel et Intel Xeon sont des marques ou des marques déposées d'Intel Corporation. Toutes les marques SPARC sont utilisées sous licence et sont des marques ou des marques déposées de SPARC International, Inc. AMD, Opteron, le logo AMD et le logo AMD Opteron sont des marques ou des marques déposées d'Advanced Micro Devices. UNIX est une marque déposée d'The Open Group.

Ce logiciel ou matériel et la documentation qui l'accompagne peuvent fournir des informations ou des liens donnant accès à des contenus, des produits et des services émanant de tiers. Oracle Corporation et ses affiliés déclinent toute responsabilité ou garantie expresse quant aux contenus, produits ou services émanant de tiers. En aucun cas, Oracle Corporation et ses affiliés ne sauraient être tenus pour responsables des pertes subies, des coûts occasionnés ou des dommages causés par l'accès à des contenus, produits ou services tiers, ou à leur utilisation.

Please
Recycle

Adobe PostScript

Contents

Oracle Fabric Manager Security 1

Oracle Fabric Manager Overview 1

General Security Principles 2

Keep Software Up To Date 2

Restrict Network Access to Critical Services 2

Follow the Principle of Least Privilege 2

Monitor System Activity 3

Keep Up To Date on Latest Security Information 4

Access 4

▼ Review File Permissions 4

▼ Control Access to Default Accounts 5

SSL Certificate 5

▼ Block Access by Unlisted Users 6

Security for Oracle Fabric Manager Plug-Ins 6

Security for Oracle Fabric Performance Monitoring 7

Security for Oracle Fabric Manager VMware Integrator 8

Oracle Fabric Manager Security

This document provides general security guidelines for Oracle Fabric Manager 4.2.0. This guide is intended to help you ensure security when using this software.

The following sections are in this chapter:

- "Oracle Fabric Manager Overview" on page 1
- "General Security Principles" on page 2
- "Access" on page 4
- "Review File Permissions" on page 4
- "Control Access to Default Accounts" on page 5
- "SSL Certificate" on page 5
- "Block Access by Unlisted Users" on page 6
- "Security for Oracle Fabric Manager Plug-Ins" on page 6
- "Security for Oracle Fabric Performance Monitoring" on page 7
- "Security for Oracle Fabric Manager VMware Integrator" on page 8

Oracle Fabric Manager Overview

Oracle Fabric Manager is a multidevice management system created by Oracle to inventory and manage Oracle Fabric Devices (one or more Oracle Fabric Interconnects and/or Oracle SDN Controllers) and Oracle virtual I/O

Oracle Fabric Manager product is a browser-based web application that supports configuring and managing virtual resources at Fabric Device, module, and server or virtual machine level. The Oracle Fabric Manager server accepts user configuration and management tasks from its interface, and relays that information to the underlying Fabric Devices.

General Security Principles

These topics describe the fundamental principles that are required to use any application securely.

Keep Software Up To Date

Stay current with the version of Oracle Fabric Manager that you run. You can find current versions of the software for download at http://support.oracle.com.

Restrict Network Access to Critical Services

Oracle Fabric Manager uses the following ports:

- Ports 8880 and 8443 must be open for incoming traffic. If not, remote access to Oracle Fabric Manager will not be permitted.
- Ports 22, 80, 443, and 6522 must be open for outgoing traffic to support communication with other Oracle Fabric Devices.

Keep Oracle Fabric Manager and the devices it controls on a secure management network. They should not be internet facing.

Follow the Principle of Least Privilege

Grant the user or administrator the least privilege that is required to accomplish the task to be performed. Oracle Fabric Manager has various roles that can be granted to users. These roles grant varying types and amounts of privilege.

Use the Security Manager functions, which are available in the navigation panel of the interface, to configure user roles for Oracle Fabric Manager. The Security Manager functions also allow you to configure Fabric Devices in specific network domains. For details on using Security Manager, refer to the *Oracle Fabric Manager User Guide*.

Monitor System Activity

Monitor system activity to determine how well Oracle Fabric Manager is operating and whether it is logging any unusual activity. Check the following log files that contain information about Oracle Fabric Manager:

- For a Microsoft Windows server:
  - `director-`*`name`*`.log`
  - `commons-daemon.log`
  - `xmscli`
  - `xmx-stderr.log`
  - `xms-stdout.log`
  - `xms-ha.log.1`
  - `xmsjobs.log.1`
  - `xms.log.1`
  - `xms-schedule.log.1`
  - `xmsaudit.log.1`
- For a Linux server:
  - `director-`*`name`*`.log`
  - `catalina.out`
  - `catalina.pid`
  - `tomcat.log`
  - `xmsaudit.log.1`
  - `xms-ha.log.1`
  - `xmsjobs.log.1`
  - `xms.log.1`
  - `xms-schedule.log.1`
- For an Oracle Solaris server:
  - `director-`*`name`*`.log`
  - `catalina.out`
  - `tomcat.log`
  - `xmsaudit.log.1`
  - `xms-ha.log.1`
  - `xmsjobs.log.1`
  - `xms.log.1`
  - `xms-schedule.log.1`

Keep Up To Date on Latest Security Information

You can access several sources of security information.

- For security information and alerts for a large variety of software products see http://www.us-cert.gov.
- Run the most current version of Oracle Virtual Networking software and refer to its documentation.

Access

Only allow access to Oracle Fabric Manager from a private network, behind the DMZ.

Consider going further by preventing local access. One method is to use a firewall to block the Oracle Fabric Manager ports. Then, to connect to Oracle Fabric Manager, first do RDP (Remote Desktop Protocol) onto the host and then use "localhost" to connect to Oracle Fabric Manager.

Make sure that Oracle Fabric Manager only uses a private secure network to communicate with Fabric Devices, such as a Fabric Interconnect or an Oracle SDN Controller.

▼ Review File Permissions

Check the file permissions after you install Oracle Fabric Manager software. In Linux or Oracle Solaris you can do so with the following steps.

1. **Before you install Oracle Fabric Manager, create a user named** `xsigo`**.**

   Create a `~xsigo/.profile` file that includes this line:

   ```
   umask 077
   ```

   Verify that this profile has taken effect by entering these commands and seeing if the output is `077`.

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

2. **Install Oracle Fabric Manager.**

   Refer to the *Oracle Fabric Manager User Guide*.

3. **After installation, review the permission level of the product's files to find if any are world readable or world writable.**

   No files should be found by these Linux commands:

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

   Fix the permissions of any files that are identified.

▼ Control Access to Default Accounts

Oracle Fabric Manager comes with two users automatically authorized:

- `root` (or `administrator` in WIndows)
- `ofmadmin` (`xsigoadmin` in earlier releases)

Prevent an attacker from creating users on the system in a way that exploits these accounts.

1. **Establish secure centralized authentication for the system.**
2. **Immediately after installing Oracle Fabric Manager, make a user named** `ofmadmin` **and give that account a random password.**

   Refer to "Working With User Roles" in the *Oracle Fabric Manager User Guide*.

SSL Certificate

Install a properly signed SSL Certificate for Oracle Fabric Manager. For further details, refer to "Configuring a Certificate for Fabric Manager" in the *Oracle Fabric Manager User Guide*.

▼ Block Access by Unlisted Users

By default, no unlisted users are allowed to access Oracle Fabric Manager. A listed user has a user role defined in Oracle Fabric Manager in addition to the underlying user account in the host OS. If a setting is changed to allow unlisted users, then a user with an account that can authenticate to the host will be able to log in to Oracle Fabric Manager and be given the operator role (effectively read only access). When unlisted users are blocked, then an unlisted user's host authentication can succeed, but Oracle Fabric Manager will deny that user access, causing it to look like authentication failed.

You can check that access by unlisted users is disabled to verify this level of security

1. **Select the Fabric Manager Maintenance icon, which resembles a screwdriver.**

   A menu of options drops down.

2. **Find the Allow Unlisted Users option.**

   If a check mark appears next to that option, remove the check mark to disable access.

Security for Oracle Fabric Manager Plug-Ins

A variety of plug-in modules can be added to Oracle Fabric Manager. Take the same general security considerations into account when you decide to install and use any plug-in module.

In addition, follow the security guidelines specific to each plug in. Security information for some of the plug-in modules is included in these topics:

- "Security for Oracle Fabric Performance Monitoring" on page 7
- "Security for Oracle Fabric Manager VMware Integrator" on page 8

Security for Oracle Fabric Performance Monitoring

If you use the Oracle Fabric Performance Monitoring plug-in module with Oracle Fabric Manager, follow these guidelines, in addition to the general security practices for Oracle Fabric Manager.

- Secure the `postgres` functions included in this plug-in module. Refer to security guidelines for the included version of `postgres` at:

  `http://www.postgresql.org`

- The database should not be open to the internet, and should be behind the DMZ.
- Treat the `postgres` user carefully. Keep the user password secret or have only the superuser be the `postgres` user.
- Configure the `pg_hba.conf` file to open traffic only to limited sources. For both Oracle Fabric Manager boxes, provide open access to the outside world only to the `xmspm` database by the `xsigo` user.

Note – The database name (`xmspm`), user name (`xsigo`), and the IP addresses are specified during setup of Oracle Performance Monitoring. The IP addresses represent two Oracle Fabric Manager instances for a high availability configuration.

```
# TYPE    DATABASE     USER      ADDRESS          METHOD
...
  host    xmspm        xsigo     192.168.0.3/1    md5
  host    xmspm        xsigo     192.168.0.4/1    md5
```

Note – You must restart `postgres` for the `pg_hba.conf` changes to take affect.

- Keep backups of the `postgres` database.

Security for Oracle Fabric Manager VMware Integrator

If you use the Oracle Fabric Manager VMware Integrator plug-in module with Oracle Fabric Manager, follow these guidelines, in addition to the general security practices for Oracle Fabric Manager.

- Install VMware vCenter Server in a secure way. Refer to the *VMware vSphere 4.1 Security Hardening Guide* at: `http://www.vmware.com`
- Set parameters required for basic Microsoft Windows hardening.
- Create a separate vCenter user (for example, `ofm`) and use this user only for the Oracle Fabric Manager plug-in connection. Doing so makes it clear who is making changes in vCenter.