Oracle® Fabric OS 1.0.2 Security Guide

Part No: E66327-02
November 2016

Oracle Fabric OS 1.0.2 Security Guide

Part No: E66327-02

Copyright © 2016, 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 documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then 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 about 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 unless otherwise set forth in an applicable agreement between you and Oracle. 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, except as set forth in an applicable agreement between you and Oracle.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Référence: E66327-02

Copyright © 2016, 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 stipulation expresse de votre contrat de licence ou de la loi, vous ne pouvez pas copier, reproduire, traduire, diffuser, modifier, accorder de licence, 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 livré sous licence au Gouvernement des Etats-Unis, ou à quiconque qui aurait souscrit la licence de ce logiciel 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, sauf mention contraire stipulée dans un contrat entre vous et Oracle. 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, sauf mention contraire stipulée dans un contrat entre vous et Oracle.

Accessibilité de la documentation

Pour plus d'informations sur l'engagement d'Oracle pour l'accessibilité à la documentation, visitez le site Web Oracle Accessibility Program, à l'adresse `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Accès aux services de support Oracle

Les clients Oracle qui ont souscrit un contrat de support ont accès au support électronique via My Oracle Support. Pour plus d'informations, visitez le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` ou le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` si vous êtes malentendant.

Contents

Oracle Fabric OS Security 7
Security Principles 7
Keep Software and Updates Up to Date 7
Restrict Network Access to Critical Services 7
Follow the Principle of Least Privilege 8
Monitor System Activity 8
Keep Up to Date on Latest Security Information 8
User Security 8
User Accounts 8
User Account Password Criteria 9
▼ Set High User Password Strength 9
▼ Add a User and Assign Appropriate Privilege 10
Block Access by Unlisted Users 11
Network Access Controls 11
SNMP Configuration 11
System Activity Monitoring 11

Oracle Fabric OS Security

This document provides general security guidelines for the Oracle Fabric OS 1.0.2. This information is intended for experienced network administrators and provides both general guidelines and specific instructions to enhance security.

See these guides for security guidance for the other related products:

- *Oracle Fabric Manager 5.0.2 Security Guide*
- *Oracle EDR InfiniBand Switch and Virtualized I/O Systems Hardware Security Guide*

These topics explain the security guidelines for Oracle Fabric OS 1.0.2.

- "Security Principles" on page 7
- "User Security" on page 8
- "Network Access Controls" on page 11
- "System Activity Monitoring" on page 11

Security Principles

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

Keep Software and Updates Up to Date

Stay current with the version of the Oracle Fabric OS that you run. You can find current versions of the software to download at My Oracle Support (`https://support.oracle.com`).

Restrict Network Access to Critical Services

Keep the Oracle Fabric OS on devices that are on a secure management network. The devices 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. The Oracle Fabric OS has various roles that can be granted to users. These roles grant different types and amounts of privilege.

Monitor System Activity

Monitor system activity to determine how well the Oracle Fabric OS is operating and whether it is logging any unusual activity.

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, refer to `http://www.us-cert.gov`.
- Run the most current version of Oracle Virtual Networking software and refer to its documentation.

User Security

The following topics describe security guidelines that you should follow for the Oracle Fabric OS.

User Accounts

The system is delivered with two default management accounts. Enforce complex passwords for these accounts through policy.

- `root` – Allows complete administrative access to the underlying Linux-based Oracle Fabric OS. Security credentials are controlled by Oracle Enterprise Linux 6.7 (UEK 4).
- `admin` – Allows administrative access to the Oracle Fabric OS management tools and security, including the ability to create new user accounts. These uses have access to the chassis configuration, but they cannot reconfigure Linux settings. The Oracle Fabric OS supports password hardening though the `set system password` command. Use the procedure below to prevent an attacker from creating users on the system in a way that exploits these accounts

To avoid the shared use of accounts and passwords, provide each Oracle Fabric OS user with a unique user name and password, and assign the proper role to match the user's tasks.

The Oracle Fabric OS users are not allowed to modify anything at the Linux level. Five types of roles are supported for Oracle Fabric OS users:

- Administrator – Superuser. Allows creation, editing, and management of the Oracle Fabric OS.
- Network – Allows creation, editing, and deletion of server profiles, vNICs, Ethernet cards and ports, and network QoS.
- Operator – Allows read-only access, including all `show` commands.
- Server – Allows creation, editing, and deletion of server profiles, as well as the ability to operate the physical server.
- Storage – Allows creation, editing, and deletion of server profiles for vHBAs, and FC I/O cards and ports.

Note - Always assign users the least privilege required for their tasks.

User Account Password Criteria

Users are prompted for a password for authentication. Before you create user passwords, set the password strength by specifying criteria with the `set system password-strength` command in the Oracle Fabric OS. Use the following criteria:

- `min-length` – Sets the minimum number of characters allowed for the password string.
- `min-lower-case` – Sets the minimum number of lowercase letters required for passwords.
- `min-number` – Sets the minimum number of numbers required for passwords.
- `min-special` – Sets the minimum number of special characters required for passwords.
- `min-upper-case` – Sets the minimum number of uppercase letters required for passwords.

Note - When you install the system, determine the password strength criteria before you create user passwords. Configure user password strength to adhere to your organizational security policy.

▼ Set High User Password Strength

In this example, the password for non default local user accounts must be at least eight characters with at least three lower case, two numbers, two special characters, and one uppercase.

1. **Log in to the Oracle Fabric OS.**

   Refer to "Log In to Oracle Fabric OS (SSH)" in *Oracle Fabric OS 1.0.2 Administration Guide*.

2. **Set the password strength.**

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

   For more information on using the Oracle Fabric OS to set a strong password, refer to "Set System Password Strength" in *Oracle Fabric OS 1.0.2 Administration Guide* or "set system" in *Oracle Fabric OS 1.0.2 Command Reference*.

Add a User and Assign Appropriate Privilege

You must have administrator privileges to add users and assign roles.

For more information on adding users, refer to "View Privileges for a User" in *Oracle Fabric OS 1.0.2 Administration Guide* or "user" in *Oracle Fabric OS 1.0.2 Command Reference*.

1. **Log in to the Oracle Fabric Manager GUI.**

   Refer to "Log In to Oracle Fabric Manager (GUI)" in *Oracle Fabric OS 1.0.2 Administration Guide*.

2. **In the GUI, add a user and assign a role to the user.**

   Refer to "Assign a Role to a User" in *Oracle Fabric Manager 5.0.2 Administration Guide*. For a list of roles, refer to "Users and Roles" in *Oracle Fabric OS 1.0.2 Administration Guide*.

3. **In the Oracle Fabric Manager GUI or the Oracle Fabric OS, verify that the user was configured correctly.**

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

4. **In the Oracle Fabric OS, test the new user account.**

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

Block Access by Unlisted Users

By default, unlisted users are not allowed to access Oracle Fabric OS. A listed user has a user role defined in Oracle Fabric OS, in addition to the underlying user account. 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 OS and be given the operator role (read-only access). When unlisted users are blocked, an unlisted user's host authentication can succeed, but Oracle Fabric OS will deny that user access, causing it to appear that the authentication failed.

To verify this level of security, ensure that access by unlisted users is disabled.

Network Access Controls

The fabric advertises the following ports:

- **Port 22 ssh** – CLI management.
- **Port 8080 http** – Unencrypted Oracle Fabric Manager client access.
- **Port 7443 https** – Encrypted Oracle Fabric Manager client access.
- **Port 161 SNMP** – SNMP monitoring.
- **Port 6522** – Enables Oracle Fabric Manager to discover the Fabric Interconnects.

SNMP Configuration

The Oracle Fabric OS supports SNMP v3. Always use SNMP v3 and use the correct authentication protocol.

System Activity Monitoring

Log files are stored in the `/log` directory. A variety of subsystems have separate log file entries, including `dmesg`.

Standard `syslog` messages go to the `user.log` file, where log rotation and auto-archive occurs for up to 10 gzipped files:

Note - Monitor log files regularly and archive them to facilitate security reviews in case of a security breach.

---

1. **Show CLI login activity.**

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

2. **Show daily boot messages.**

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

For detailed information about log files, refer to "Troubleshoot With System Log Files" in *Oracle Fabric OS 1.0.2 Administration Guide*.