

Oracle[®] Fabric Interconnect
Security Guide



VIRTUAL
NETWORKING

Part No.: E50940-02
September 2014

Copyright © 2013, 2014, 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 which 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, 2014, 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.



Adobe PostScript

Contents

Oracle Fabric Interconnect and XgOS Security 1

System Overview 2

Security Principles 3

Security Guidelines 4

 Console Security 4

 CLI User Accounts 4

 ▼ Add a User and Assign Appropriate Privilege 5

 ▼ Disable or Enable Root Login Over SSH 5

 CLI User Account Password Criteria 6

 ▼ Set High User Password Strength 6

Monitor Log Files 7

Access Control Lists 7

Network Access Controls 8

 SNMP Configuration 8

 ▼ Change the SNMP Read Community String 8

ProWatch Remote Monitoring 9

 ▼ Show the Current ProWatch Phone Home Status 9

 ▼ Enable ProWatch Phone Home 9

 ▼ Disable Phone Home Automatic Transmission and Send Data Manually

10

- ▼ Disable or Enable Phone Home Feature to Remove Private IP Addresses 10
- ▼ Disable ProWatch Phone Home 11

Oracle Fabric Interconnect and XgOS Security

Oracle Fabric Interconnect and XgOS employ network virtualization to enable flexible connections from servers to networks and storage. The Oracle Fabric Interconnect replaces the need for server network adapters with virtual network interface cards (vNICs) and virtual host bus adapters (vHBAs) that can be configured in real-time. Applications and OSs see these virtual resources exactly as they would their physical counterparts. The result is an architecture that is much faster, easier to manage, and far more cost-effective.

This guide is intended for experienced network administrators and provides both general guidelines and specific instructions to enhance security.

- [“System Overview” on page 2](#)
- [“Security Principles” on page 3](#)
- [“Security Guidelines” on page 4](#)
- [“Access Control Lists” on page 7](#)
- [“Network Access Controls” on page 8](#)
- [“ProWatch Remote Monitoring” on page 9](#)

This guide does not provide security guidance for Oracle Fabric Manager or Oracle SDN Controller. For security information on these products, refer to:

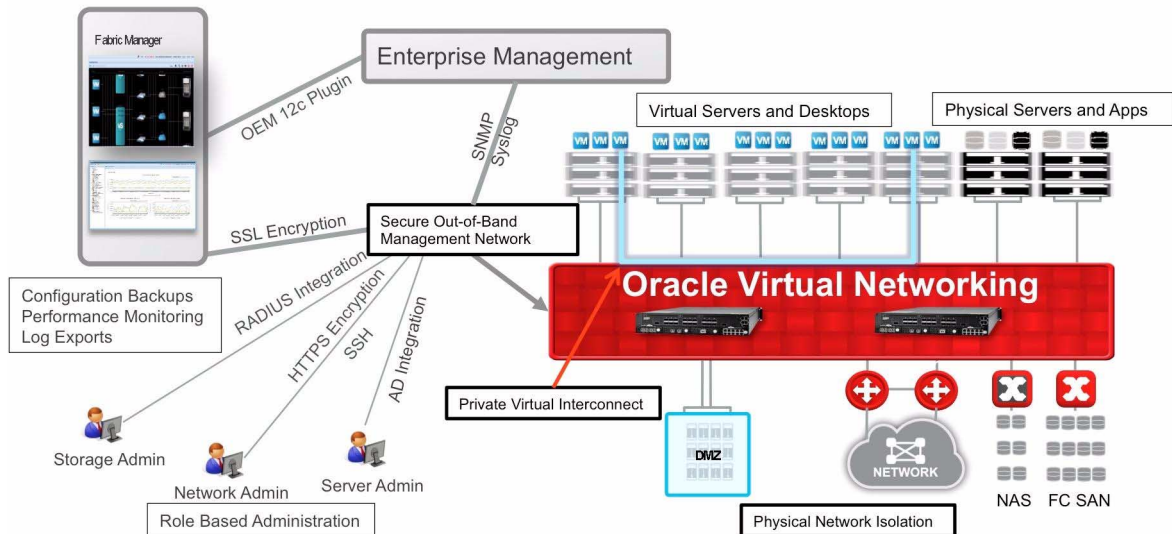
- *Oracle Fabric Manager Security Guide*
- *Oracle SDN Controller Security Guide*

System Overview

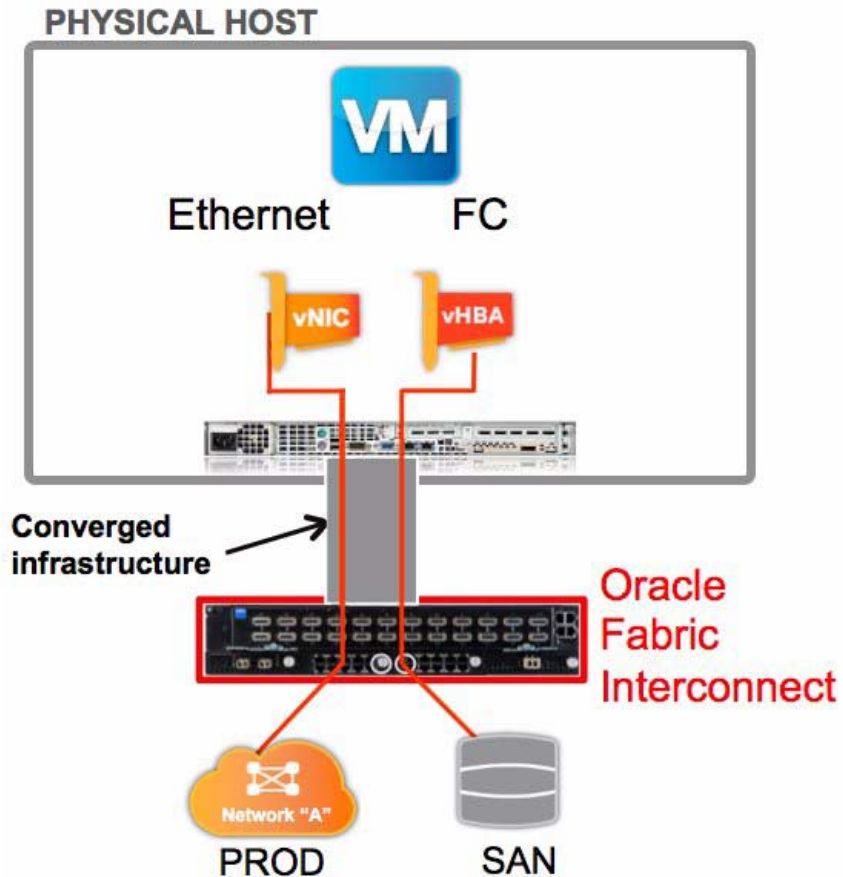
The Fabric Interconnect manages traffic from host servers to Ethernet or Fibre Channel interfaces using high-speed, low-latency InfiniBand network connections. The Fabric Interconnect uses XgOS and is available in 4U, 15-slot and 2U, 4-slot models. For security configurations, both Fabric Interconnects are considered identical.

- Oracle Fabric Interconnect F1-15
- Oracle Fabric Interconnect F1-4

The following is an overview of virtual networking with the Fabric Interconnects.



The following illustrates the relationship between the Fabric Interconnect and other components in the data center.



Security Principles

The following principles are fundamental to using the Fabric Interconnect securely.

1. **Keep up to date on the latest security and software update information.**

Oracle continually improves its software and documentation. Check product and release notes often for updates at: http://docs.oracle.com/cd/E38500_01/

2. **Keep XgOS software and patches up to date.**

3. Monitor system activity.

See “Monitor Log Files” on page 7 and refer to the *Oracle Fabric Manager Security Guide*.

4. Ensure the hardware is in a locked environment.

Security Guidelines

The following topics describe security guidelines for the Fabric Interconnect CLI.

Console Security

Access to the Fabric Interconnect command line interface is provided exclusively over encrypted Secure Shell connections. Telnet is not supported.

For example, connect to the Fabric Interconnect command line interface as user `admin`.

```
ssh -l admin ip-address
```

Additionally, a serial port interface is available to allow initial configuration of network parameters or maintenance access. Do not use the serial port interface unless required. Connect to the serial interface only through private management devices and with authorized personnel.

CLI User Accounts

The Identity Management System (IMS) service authenticates users and grants them suitable privileges according to assigned user roles when users access the Fabric Interconnect. The IMS service can be one of the following:

- Oracle XgOS local system, which is always present.
- Microsoft Active Directory (AD).
- Remote Authentication Dial In User Service (RADIUS).

Only the local XgOS identity management features are described in this guide. Refer to the CLI user’s guide for details on using Active Directory or RADIUS authentication services.

The system is delivered with two default management accounts. The password strength controls do not apply to these accounts. Enforce complex passwords for these accounts through policy.

- `root` – Allows complete administrative access to the underlying Linux based XgOS. This access is intended for Oracle certified personnel only. Changes to the XgOS configurations by the customer are not supported by Oracle.
- `admin` – Allows administrative access to the CLI management tools and security including the ability to create new user accounts.

To avoid the shared use of accounts and passwords, provide each Fabric Interconnect CLI user with a unique username and password and assign the proper role to match the user’s tasks.

Available roles for the Fabric Interconnect CLI users include:

- `Administrator` – Allows configuration, editing, and management of all objects in Oracle’s Fabric Directors (full administrative responsibilities).
- `Network` – Allows configuration, editing, and management of all objects related to vNIC configuration, Ethernet I/O cards and ports, network QoS parameters, ACLs, and server profiles.
- `Operator` – Allows read-only access including all show commands.
- `Server` – Allows all operations related to a server’s physical connection, compute-resource configuration, and management.
- `Storage` – Allows vHBA configuration and management, Fibre Channel I/O module and ports, LUN masks, persistent mappings, and SAN QoS.

Note – Always assign users the least privileges required for their tasks.

▼ Add a User and Assign Appropriate Privilege

Administrator privileges are required to add users.

- **Add a user and assign the storage management role, type.**

```
add user frank
set user frank -role=storage
```

▼ Disable or Enable Root Login Over SSH

Administrator privileges are required to disable or enable root login over ssh.

- Type either of these commands:

```
set system root-ssh-login disable
set system root-ssh-login enable
```

CLI User Account Password Criteria

Fabric Interconnect local users are prompted for a password for authentication. Through XgOS you must set the password strength by specifying criteria with the `set system password-strength` command. The available criteria is as follows:

- `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 Fabric Interconnect passwords.
- `min-upper-case` – Sets the minimum number of uppercase letters required for Fabric Interconnect passwords.

Note – Configure user password strength criteria to adhere to your organizational security policy.

The criteria set with the `set system password-strength` command affects nondefault local user accounts only. This criteria does not affect login passwords for the following:

- Oracle Fabric Manager
- Windows Active Directory
- Any Identity Management System
- Default `root` or `admin` passwords

▼ Set High User Password Strength

In this example, the password for nondefault local user accounts must be at least 8 characters with at least 3 lower case, 2 numbers, 2 special characters, and 1 uppercase.

- Type:

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

Monitor Log Files

Log files are stored in the `/log` directory. A variety of subsystems have separate log file entries, including: `dmesg`, `apache`, `syslog`, `cli`, `xms`, and others.

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

1. Show CLI login activity.

```
# more /log/cli.log
```

2. Show daily boot messages.

```
# more /log/dmesg
```

Access Control Lists

Access control lists (ACLs) classify packets. The classification result can be applied to quality-of-service (QoS) application flows (mark, police) or to network-access control (deny, allow). Strict ACL configurations are critical for enhancing security. Consider the following examples:

- **Prioritizing outbound traffic by marking fields in the IP header** – Enables upstream routers to handle this marked (set) traffic in a specific way.
For example, any RTP VoIP traffic within a certain port range could have its IP TOS bit set to a value of 5. Any packet that satisfies these conditions will have its IP header field set by the I/O card.
- **Intentionally dropping packets during a denial-of-service (DoS) attack** – All traffic is blocked from specific IP or MAC addresses.
For example, an ACL could block any traffic heading in an egress direction (server to network) with a specified IP or MAC address.

Refer to the *XgOS User's Guide* for instructions on how to create and enforce ACLs.

Network Access Controls

The Fabric Interconnect advertises the following ports:

- **Port 22 ssh** – CLI management.
- **Port 80 http** – Unencrypted Oracle Fabric Manager client access.
- **Port 443 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

XgOS supports SNMPv1, v2, and v3. `get`, `getnext`, and `getbulk` operations are supported. `set` operations are not supported. Community strings are read only. The default `read-community` string is `public`.

Note – Change the default `read-community` string to prevent unauthorized monitoring of the systems.

Note – Always use SNMPv3 and use the correct authentication protocol.

▼ Change the SNMP Read Community String

- **Type:**

```
set snmp -read-community=string
```

ProWatch Remote Monitoring

Note – If you require high security, do not enable this feature. This feature is disabled by default.

The ProWatch feature automatically sends scheduled transmissions of the contents of log files and the output of the `show tech-support` command to Oracle Technical Support. This information enables Oracle Technical Support to proactively look for and diagnose potential problems without requiring you to collect data, package it, and transmit it to Oracle.

The information collected is from the `show tech-support` command and system logs only. No sensitive customer data is gathered and transmitted to Oracle. To ensure that private information is kept safe, the Oracle ProWatch feature provides ways to:

1. Send a copy of the information to an internal website for auditing purposes.
2. Remove private data, such as IP addresses, from the data.

Also, the data is transmitted encrypted so that it cannot be easily read.

ProWatch is disabled by default. If it is against your local policy to allow ProWatch to connect to Oracle, do not enable this feature.

▼ Show the Current ProWatch Phone Home Status

- Type:

```
show system phone-home
```

▼ Enable ProWatch Phone Home

Enabling Phone Home enables automatic data transmission.

- Type:

```
set system phone-home enable
```

▼ Disable Phone Home Automatic Transmission and Send Data Manually

With this feature, you decide when you want to send Phone Home data.

Note – The automatic and manual transmission commands are different. The manual transmission commands for Phone Home do not use the `set` command keyword.

1. Disable automatic Phone Home transmissions.

```
set system phone-home disable
```

2. Send Phone Home data manually.

```
system phone-home
```

```
This will send quite a large amount of data to Xsigo Systems. It
requires that the I/O Director has access to the internet for an
HTTP transfer (perhaps through a proxy if necessary). Do you really
want to send the data (y/n)? y
```

Or, use the `-noconfirm` option to skip requiring y/n input.

```
system phone-home -noconfirm
```

▼ Disable or Enable Phone Home Feature to Remove Private IP Addresses

Note – This feature is enabled by default.

1. To disable removing private IP addresses.

```
set system phone-home -strip-private=false
```

2. To enable removing private IP addresses.

```
set system phone-home -strip-private=true
```

Or,

```
set system phone-home -strip-private=default
```

▼ Disable ProWatch Phone Home

- Type:

```
set system phone-home disable
```

