

Oracle[®] SDN Controller
Security Guide



VIRTUAL
NETWORKING

Part No.: E50941-01
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 RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

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, 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 RIGHTS. Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

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 SDN Controller Security	1
System Overview	2
Security Principles	3
Security Guidelines	3
Console Security	3
CLI User Accounts	4
▼ Disable Root Login Over SSH	4
Monitor Log Files	5
Access Control Lists	5
Network Access Controls	6
SNMP Configuration	6
▼ Change the SNMP Read Community String	6

Oracle SDN Controller Security

Oracle SDN Controller brings high-speed Ethernet connectivity to your current IB networks. Oracle SDN Controller runs on an Oracle Linux server and provides the same features as the software stacks of the Oracle Fabric Interconnect. Oracle SDN Controller is configured and managed with Oracle Fabric Manager 4.2.0 and up, which provides a comprehensive UI for configuring PVI clouds and vNICs.

Key features include:

- Physical server auto-discovery
- I/O template, PVI cloud, and vNIC management
- Multi-tenant support
- IB topology view

This guide is intended for experienced system and network administrators.

- [“System Overview” on page 2](#)
- [“Security Principles” on page 3](#)
- [“Security Guidelines” on page 3](#)
- [“Monitor Log Files” on page 5](#)
- [“Access Control Lists” on page 5](#)
- [“Network Access Controls” on page 6](#)

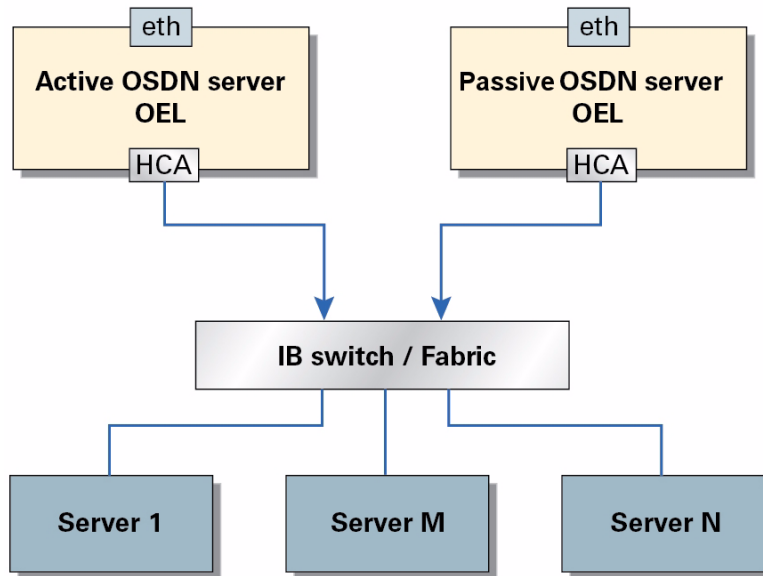
This guide does not cover Oracle Linux, Oracle Fabric Manager, or Oracle Fabric Interconnects and XgOS. For security information on these products, refer to:

- *Oracle Linux Security Guide for Release 6*
- *Oracle Fabric Interconnects and XgOS Security Guide*
- *Oracle Fabric Manager Security Guide*

System Overview

Two controllers are supported in the same subnet. One controller must be active and one controller must be passive.

The following is an overview of an Oracle SDN Controller configuration.



At startup, the controller servers are in passive mode. When a controller is made active, Oracle Fabric Manager pushes the latest configurations to that controller and periodically backs up the active controller configuration. The backups are available to send to the passive controller if the active controller goes down.

Security Principles

The following principles are fundamental to using the Oracle SDN Controller securely.

1. **For security information on system and network administration, refer to the *Oracle Linux Security Guide for Release 6* at:**
http://docs.oracle.com/cd/E37670_01/
2. **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/
3. **Keep software and patches up to date.**
4. **Monitor system activity.**
See “[Monitor Log Files](#)” on page 5 and refer to the *Oracle Fabric Manager Security Guide*.
5. **Ensure the hardware is in a locked environment.**

Security Guidelines

The following topics describe security guidelines for the Oracle SDN Controller CLI.

Console Security

Access to the Oracle SDN Controller command line interface is provided exclusively over encrypted Secure Shell connections. Telnet is not supported.

For example, connect to the Oracle SDN Controller command line interface as user `admin`.

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

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 Oracle SDN Controller. The IMS service can be one of the following:

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

Only the local Oracle identity management features are described in this guide. Refer to the documentation 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 controller. This access is intended for Oracle certified personnel only. Changes to the controller 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.

▼ Disable Root Login Over SSH

1. Login as root.

Change the default password (`root`) on initial login.

```
ssh -l root ip-address
```

2. Edit the `sshd_config` file.

Change `PermitRootLogin yes` to `PermitRootLogin no`.

```
vi /etc/ssh/sshd_config
...
PermitRootLogin no
...
```

3. Save the file.

4. Restart `sshd`.

```
# service sshd restart
```


5. Verify that you cannot login as `root` over SSH.

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 Command-Line Interface User's Guide* for instructions on how to create and enforce ACLs.

Network Access Controls

The Oracle SDN Controller 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 Oracle SDN Controllers.

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
```