Oracle® SDN Controller

Security Guide

Part No.: E50941-01
December 2013

Please
Recycle

Contents

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.

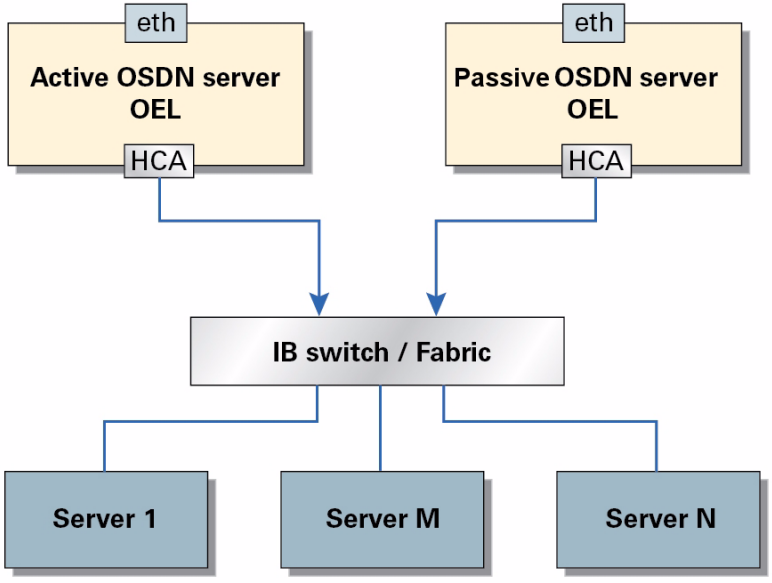
This guide does not cover Oracle Linux, Oracle Fabric Manager, or Oracle Fabric Interconnects and XgOS. For security information on these products, refer to:

- *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
```