

# **Sun Blade 6000 Virtualized 40 GbE Network Express Module**

## **Security Guide**

September 2011

Part No.: E24668-01

Copyright © 2011, Oracle and/or its affiliates. All rights reserved.

Author: Tanli Chang

Contributor: Ajoy Siddabathuni

This document provides guidelines for securing the Sun Blade 6000 Virtualized 40 GbE Network Express Module and systems assisted with it.

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.

This documentation is in prerelease status and is intended for demonstration and preliminary use only. It may not be specific to the hardware on which you are using the software. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to this documentation and will not be responsible for any loss, costs, or damages incurred due to the use of this documentation.

The information contained in this document is for informational sharing purposes only and should be considered in your capacity as a customer advisory board member or pursuant to your beta trial agreement only. It is not a commitment to deliver any material, code, or functionality, and should not be

relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle Software License and Service Agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced, or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

Copyright © 2011, 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.

# Contents

## Table of Contents

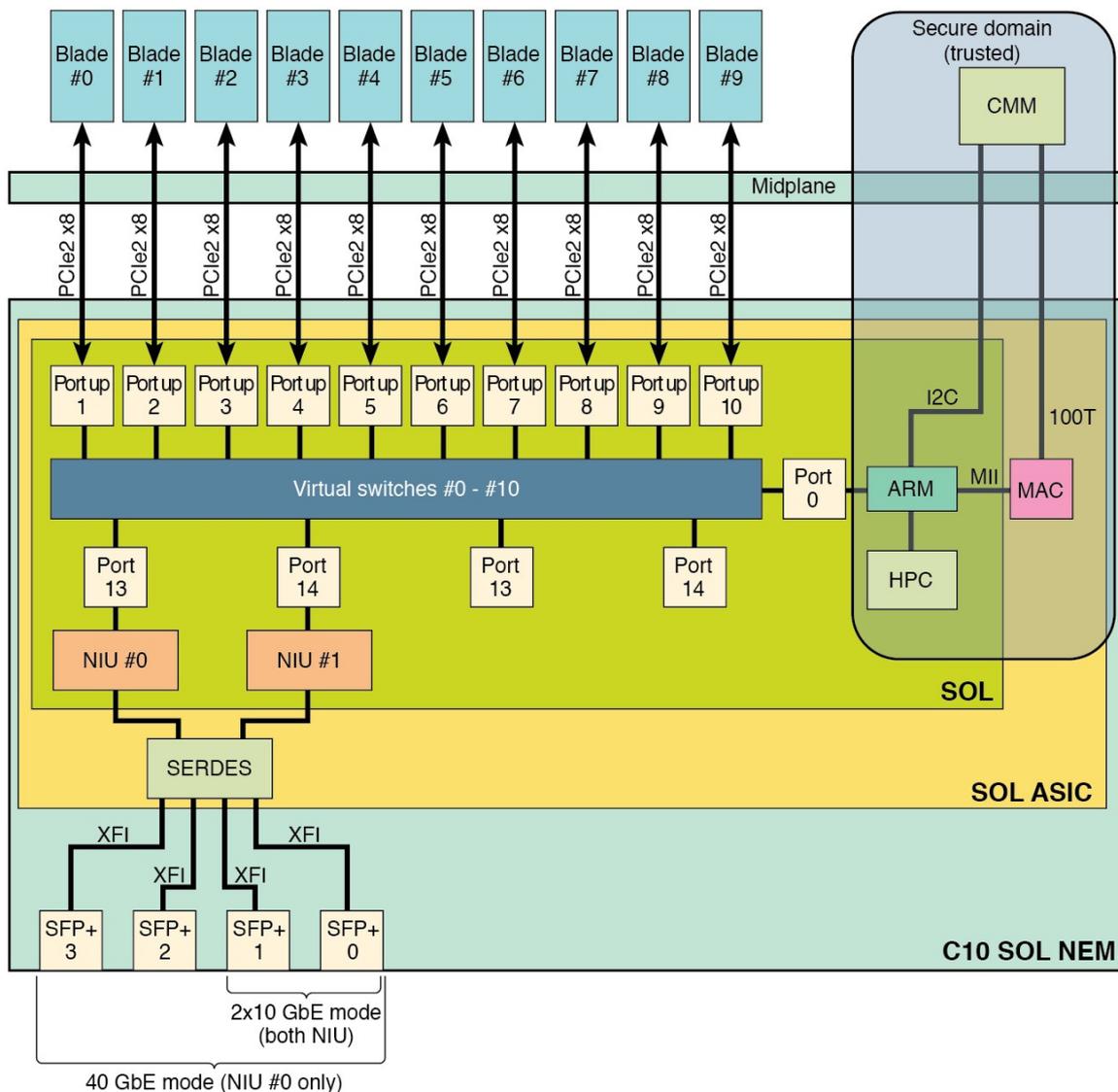
<a href="#">Part 1: Overview</a>	<a href="#">4</a>
<a href="#">Product Overview</a>	<a href="#">4</a>
<a href="#">General Security Principles</a>	<a href="#">5</a>
<a href="#">Keep Software Up To Date</a>	<a href="#">5</a>
<a href="#">Monitor System Activity</a>	<a href="#">6</a>
<a href="#">Keep Up To Date on Latest Security Information</a>	<a href="#">6</a>
<a href="#">Part 2: Secure Installation and Configuration</a>	<a href="#">6</a>
<a href="#">Installation Overview</a>	<a href="#">6</a>
<a href="#">Installing Firmware</a>	<a href="#">6</a>
<a href="#">Installing Drivers</a>	<a href="#">6</a>
<a href="#">Part 3: Security Features</a>	<a href="#">7</a>
<a href="#">AAA</a>	<a href="#">7</a>
<a href="#">Bandwidth Allocation</a>	<a href="#">7</a>
<a href="#">VLAN Membership</a>	<a href="#">7</a>
<a href="#">SRIOV Modes</a>	<a href="#">7</a>
<a href="#">Promiscuous Mode</a>	<a href="#">7</a>
<a href="#">Link Management</a>	<a href="#">8</a>
<a href="#">Trunking/Link Aggregation Management</a>	<a href="#">8</a>
<a href="#">Logging Information</a>	<a href="#">8</a>
<a href="#">NEM Configuration</a>	<a href="#">8</a>
<a href="#">Firmware/EEPROM Upgrades</a>	<a href="#">8</a>
<a href="#">Part 4: Security Considerations for Developers</a>	<a href="#">8</a>

# Part 1: Overview

This section provides an overview of the product and explains the general principles of security.

## Product Overview

Oracle’s Sun Blade 6000 Virtualized 40 GbE Network Express Module (NEM) is a multi-purpose connectivity module for the Sun Blade 6000 modular system. The NEM provides network and storage connectivity between the blades in a Sun Blade 6000 modular system chassis and external devices. The NEM supports connection to external devices through 40 GbE small form-factor pluggable (SFP+) ports and 10/100/1000 TPE ports. Also, the NEM supports Sun ASIC Dual 10GbE Network Interface Card (NIC) virtualization.



The system diagram shows the general system security domains. The chassis management module (CMM) and NEM-EPs firmware are part of the secure domain. Only system administrators are allowed to access the CMM externally. The blades are connected to the Virtualized NICs via the PCI-E spigots.

It is important to understand that having access to the blades does not compromise the security of the NEM in general. The NEM is designed to run under a variety of operating systems (including VMs) on the blades and in general blades are protected from each other. Blades do not have direct access to the NEM-EPS firmware.

All policies that need to be set up in the NEM are only accessible via the CMM. Following are some of the policies that can be set up via the NEM-EPS only with access to the CMM:

- Bandwidth allocation
- VLAN membership
- SRIOV modes
- Promiscuous mode
- Link management
- Trunking/Link aggregation management
- Logging information
- NEM configuration
- Firmware/EEPROM upgrades

## General Security Principles

The following principles are fundamental to using any NEM securely.

### ***Keep Software Up To Date***

One of the principles of good security practice is to keep all software versions and patches up to date. The list of software is as follows:

- Solaris sxge driver
- Linux sxge/sxgevf driver
- VMWare and Windows drivers

The following software components are only accessible to system administrators having access to the CMM.

- NEM firmware
- EEPROM image

### **Monitor System Activity**

1. CMM has message log to log system activity. NEM firmware upgrade activity will be included in system log.
2. The sxge driver has support for:
  - kstat, netstat, dladm, pcitool, ethtool
  - log/message (can be turned on or off)

### **Keep Up To Date on Latest Security Information**

Oracle continually improves its software and documentation. Check product release notes often for updates.

[\*Sun Blade 6000 Virtualized 40 GbE Network Express Module Product Notes\*](#)

## **Part 2: Secure Installation and Configuration**

### **Installation Overview**

The NEM is shipped with all firmware installed. It does not require any installation or configuration. All software update components such as patches and new firmware releases must be downloaded from Oracle web download site after logging in using service contract information and credentials.

Note that NEM-EPS firmware is only upgradeable via the CMM.

To install new firmware and drivers, refer to:

[\*Sun Blade 6000 Virtualized 40 GbE Network Express Module Product Notes\*](#)

### **Installing Firmware**

For detailed instructions, refer to:

[\*Sun Blade 6000 Virtualized 40 GbE Network Express Module User's Guide\*](#)

### **Installing Drivers**

Please refer to:

[\*Sun Blade 6000 Virtualized 40 GbE Network Express Module User's Guide\*](#)

## Part 3: Security Features

Users cannot access NEM directly. All the requests are by proxy through the CMM ILOM.

### AAA

The critical security features provided by ILOM are as follows:

- Authentication: ensuring that only authorized individuals get access to the system and data.
- Authorization: access control to system privileges and data. This builds on authentication to ensure that individuals only get appropriate access.
- Audit: allows administrators to detect attempted breaches of the authentication mechanisms and attempted or successful breaches of access control.

ILOM information is located in the *Oracle Integrated Lights Out Manager 3.0* documentation collection at:

[Integrated Lights Out Manager \(ILOM\) 3.0](#)

NEM security features are only accessible via the CMM ILOM.

### Bandwidth Allocation

Each blade is initially allocated 10% bandwidth per port. Administrators who have access to NEM-EPS (through CMM) can change the settings. Any excess bandwidth is available to blades as best effort.

### VLAN Membership

VLAN memberships are only managed via the NEM-EPS (via CMM). Blades that are not part of a VLAN will not receive packets on that VLAN-ID.

### SRIOV Modes

PCI functions visible from the blade (per port) are configured via the NEM-EPS. Only blades set up to be in SR-IOV mode can run VFs and VMs to share the Virtualized-IO domains per port.

### Promiscuous Mode

Blades can be allowed to see all traffic from the network ports only if configured on the NEM-EPS

## **Link Management**

Blades can be forced to see a Virtualized NIC as up, down, or auto (auto being the actual physical link status).

## **Trunking/Link Aggregation Management**

Trunking/Link aggregation is having the ability to see both ports on the NEM as one logical trunk (for load sharing and failover purposes). These capabilities can only be set up via the NEM-EPS.

## **Logging Information**

All logging information is only available via the NEM-EPS

## **NEM Configuration**

Custom configurations can be saved, and settings can be reset to factory defaults.

## **Firmware/EEPROM Upgrades**

Upgrades are only allowed via the CMM.

For more information refer to:

[\*Sun Blade 6000 Virtualized 40 GbE Network Express Module User's Guide\*](#)

## **Part 4: Security Considerations for Developers**

All software and firmware running on Oracle's Sun Blade 6000 Virtualized Network Express Module (NEM) are provided by Oracle. Customers cannot develop their own software to run on the NEM.