Oracle Dual Port QDR InfiniBand Adapter M4 Security Guide

Part No: E64149-01
June 2016

Oracle Dual Port QDR InfiniBand Adapter M4 Security Guide

Part No: E64149-01

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: E64149-01

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 Dual Port QDR InfiniBand Adapter M4 Security 7
Security Principles 7
Planning a Secure Environment 8
Hardware Security 8
Software Security 9
Oracle Solaris OS Guidelines 9
Oracle Linux OS Guidelines 9
Network Switches 10
Oracle Firmware Security 10
Oracle ILOM Firmware 10
VLAN Security 11
Infiniband Security 11
User Accounts 11
System Logs 12
Maintaining a Secure Environment 12
Hardware Power Control 12
Asset Tracking 12
Updates for Software and Firmware 13
Network Access 13
Data Protection 13
Log Security 14

Oracle Dual Port QDR InfiniBand Adapter M4 Security

This document provides general security guidelines for the Oracle Dual Port QDR InfiniBand Adapter M4. This guide is intended for experienced network administrators and provides both general guidelines and specific instructions to enhance security.

This document covers the following topics:

- "Security Principles" on page 7
- "Planning a Secure Environment" on page 8
- "Maintaining a Secure Environment" on page 12

Security Principles

There are four basic security principles: access, authentication, authorization, and accounting.

- Access

  Physical and software controls protect your hardware or data from intrusion.

  - For hardware, access limits usually mean physical access limits.
  - For software, access is limited through both physical and virtual means.
  - Firmware cannot be changed except through the Oracle update process.
- Authentication

  Set up the authorization features such as a password system in your platform operating systems to ensure that users are who they say they are. Ensure that your personnel use employee badges properly to enter the computer room.
- Authorization

  Allow personnel to work only with hardware and software that they are trained and qualified to use. Set up a system of Read/Write/Execute permissions to control user access to commands, disk space, devices, and applications.
- Accounting

  Use Oracle software and hardware features to monitor login activity and maintain hardware inventories.

- Use system logs to monitor user logins. Monitor system administrator and service accounts in particular because these accounts can access powerful commands.
- Use component serial numbers to track system assets. Oracle part numbers are electronically recorded on cards, modules, and motherboards.

Planning a Secure Environment

Use the following notes for the installation and configuration of a server and related equipment.

- "Hardware Security" on page 8
- "Software Security" on page 9
- "Oracle Solaris OS Guidelines" on page 9
- "Oracle Linux OS Guidelines" on page 9
- "Network Switches" on page 10
- "Oracle Firmware Security" on page 10
- "Oracle ILOM Firmware" on page 10
- "VLAN Security" on page 11
- "Infiniband Security" on page 11
- "User Accounts" on page 11
- "System Logs" on page 12

Hardware Security

Physical hardware can be secured fairly simply: limit access to the hardware and record serial numbers.

- Restrict access
  - Install servers and related equipment in a locked, restricted access room.
  - If equipment is installed in a rack with a locking door, keep the door locked except when you have to service components in the rack.
  - Restrict access to USB consoles, which can provide more powerful access than SSH connections. Devices such as system controllers, power distribution units (PDUs), and network switches can have USB connections.
  - Restrict access to hot-plug or hot-swap devices in particular because they can be easily removed.
  - Store spare field-replaceable units (FRUs) and customer-replaceable units (CRUs) in a locked cabinet. Restrict access to the locked cabinet to authorized personnel.
- Record serial numbers
  - Security-mark all significant items of computer hardware such as FRUs. Use special ultraviolet pens or embossed labels.

- Keep a record of the serial numbers of all your hardware.
- Keep hardware activation keys and licenses in a secure location that is easily accessible to the system manager in system emergencies. The printed documents might be your only proof of ownership.

Software Security

Most hardware and software security is implemented through software measures.

- Refer to the documentation that came with your software to enable any security features available for the software.
- Implement port security to limit access based upon MAC addresses. Disable auto-trunking on all ports.
- Use a dedicated network for service processors to separate them from the general network.
- You can boot a system securely over a wide area network (WAN) or a storage area network (SAN). For information about using WAN Boot or iSCSI Boot for secure booting, refer to the Oracle Solaris Installation Guide: Network-Based Installations book for your Oracle Solaris operating system release.
- Change all default passwords when installing a new system. Most types of equipment use default passwords, such as changeme, that are widely known and would allow unauthorized access to the equipment.
- Change every password on network switches which might have multiple user accounts and passwords by default.

Oracle Solaris OS Guidelines

Refer to Oracle Solaris Security Guidelines documents for information on:

- How to harden Oracle Solaris
- How to use Oracle Solaris security features when configuring your systems
- How to operate securely when you add applications and users to a system
- How to protect network-based applications

  Oracle Solaris Security Guidelines documents can be found at http://www.oracle.com/technetwork/indexes/documentation/index.html#sys_sw

Oracle Linux OS Guidelines

Use Oracle Linux OS commands to restrict access to the software, harden the OS, use security features, and protect applications. Refer to the Oracle Linux Security Guide for Release 6 at http://docs.oracle.com/cd/E37670_01/E36387/html/index.html.

Network Switches

Different switches offer different levels of port security features. Refer to the switch documentation to learn how to do the following:

- Use authentication, authorization, and accounting features for local and remote access to the switch.
- Manage switches out-of-band (separated from data traffic). If out-of-band management is not feasible, then dedicate a separate VLAN number for in-band management.
- Use the port mirroring capability of the network switch for intrusion detection system (IDS) access.
- Maintain a switch configuration file off-line and limit access only to authorized administrators. The configuration file should contain descriptive comments for each setting.
- Use these port security features if they are available on your switch:
  - MAC Locking involves tying a Media Access Control (MAC) address of one or more connected devices to a physical port on a switch. If you lock a switch port to a particular MAC address, superusers cannot create backdoors into your network with rogue access points.
  - MAC Lockout disables a specified MAC address from connecting to a switch.
  - MAC Learning uses the knowledge about each switch port's direct connections so the network switch can set security based on current connections.

Oracle Firmware Security

Use the superuser account to set up and update the OpenBoot PROM (OBP) or other Oracle firmware. Ordinary user accounts allow users to view but not edit firmware. The Oracle Solaris OS firmware update process prevents unauthorized firmware modifications.

For information for setting OBP security variables, refer to the OpenBoot 4.x Command Reference Manual at http://download.oracle.com/docs/cd/E19455-01/816-1177-10/cfg-var.html#pgfId-17069

Oracle ILOM Firmware

You can actively secure, manage, and monitor system components through Oracle Integrated Lights Out Manager (Oracle ILOM) management firmware which is preinstalled on some SPARC servers.

Refer to Oracle ILOM documentation to understand more about setting up passwords, managing users, and applying security-related features, including Secure Shell (SSH), Secure Socket Layer (SSL), and RADIUS authentication: http://docs.oracle.com/cd/E37444_01/index.html

VLAN Security

If you set up a virtual local area network (VLAN), remember that VLANs share bandwidth on a network and require additional security measures.

- Define virtual local area networks (VLANs) to separate sensitive clusters of systems from the rest of the network. This decreases the likelihood that users will gain access to information on these clients and servers.
- Assign a unique native VLAN number to trunk ports.
- Limit the VLANs that can be transported over a trunk to only those that are strictly required.
- Disable VLAN Trunking Protocol (VTP), if possible. Otherwise, set the following for VTP: management domain, password and pruning. Then set VTP into transparent mode.

Infiniband Security

Infiniband (IB) security is a function of the IB Fabric and the Subnet Manager (SM) running in the IB fabric. Keep all IB hosts attached to IB fabric secure. An IB fabric is as secure as the least secure IB host attached to it. Attackers having root access to a host can bring the whole IB fabric down. (Physical access is also important in this regard - an attacker able to connect his own host to an IB switch may be able to compromise security of IB fabric.)

When an Oracle Dual Port EDR InfiniBand Adapter or an Oracle Dual Port QDR InfiniBand Adapter M4 is used in a virtualized environment, pay special attention to the security of the physical domain because a compromised physical domain would lead to all virtual machines being exposed and vulnerable.

For more information about securing InfiniBand and supported switches, which also run the SM, see the InfiniBand Switch Security Guide for the applicable switch:

- For Sun Datacenter InfiniBand Switch 36, see the Sun Datacenter InfiniBand Switch 36 Hardware Security Guide at: http://docs.oracle.com/cd/E36265_01/
- For Sun Network QDR InfiniBand Gateway Switch, see the Sun Network QDR InfiniBand Gateway Switch Hardware Security Guide at: http://docs.oracle.com/cd/E36256_01/
- For the IB switch and SM on an Oracle Virtual Network InfiniBand switch, see: http://docs.oracle.com/cd/E38500_01/

User Accounts

- Set up RADIUS and TACACS+ access protocols if possible: RADIUS (Remote Authentication Dial In User Service) is a client/server protocol that secures networks against unauthorized access.

TACACS+ (Terminal Access Controller Access-Control System) is a protocol that permits a remote access server to communicate with an authentication server to determine if a user has access to the network.

- Limit use of superuser account (root). It has special privileges, which, if misused, can adversely affect security. Instead, use other, lower privileged, user accounts whenever possible. That applies to host operating system (Solaris, Linux), as well as Oracle ILOM.
- Use access control lists where appropriate.
- Set time-outs for extended sessions.
- Set privilege levels.
- Create a system banner to remind the user that unauthorized access is prohibited.

System Logs

- Enable logging and send logs to a dedicated secure log host.
- Configure logging to include accurate time information, using NTP and timestamps.

Maintaining a Secure Environment

After the initial installation and setup, use Oracle hardware and software security features to continue controlling hardware and tracking system assets.

Hardware Power Control

You can use software to turn on and off power to some Oracle systems. The power distribution units (PDUs) for some system cabinets can be enabled and disabled remotely. Authorization for these commands is typically set up during system configuration and is usually limited to system administrators and service personnel. Refer to your system or cabinet documentation for further information.

Asset Tracking

Use serial numbers to track inventory. Oracle embeds serial numbers in firmware on option cards and system motherboards. You can read these serial numbers through local area network connections.

You can also use wireless radio frequency identification (RFID) readers to further simplify asset tracking. An Oracle white paper, How to Track Your Oracle Sun System Assets by Using

RFID is available at: http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o11-001-rfid-oracle-214567.pdf

Updates for Software and Firmware

Keep your firmware versions and related host software (driver, user space tools) current on your server equipment.

- Check regularly for updates.
- Always install the latest released version of the software or firmware.
- Install any necessary security patches for your software.
- Remember that devices such as network switches also contain firmware and might require patches and firmware updates.

Check availability of updates and patches at https://support.oracle.com

Network Access

Follow these guidelines to secure local and remote access to your systems:

- Implement port security to limit access based upon a MAC address. Disable auto-trunking on all ports.
- Limit remote configuration to specific IP addresses using SSH instead of Telnet. Telnet passes user names and passwords in clear text, potentially allowing everyone on the LAN segment to see login credentials. Set a strong password for SSH.
- Use version 3 of SNMP to provide secure transmissions. Earlier versions of SNMP are not secure and transmit authentication data in unencrypted text.
- Change the default SNMP community string to a strong community string if SNMP is necessary. Some products have PUBLIC set as the default SNMP community string. Attackers can query a community to draw a very complete network map and possibly modify management information base (MIB) values.
- Always log out after using the system controller if it uses a browser interface.
- Disable unnecessary network services, such as TCP small servers or HTTP. Enable necessary network services and configure these services securely

Data Protection

Follow these guidelines to maximize data security:

- Back up important data using devices such as external hard drives, pen drives, or memory sticks. Store the backed up data in a second, off-site, secure location.

- Use data encryption software to keep confidential information on hard drives secure.
- When disposing of an old hard drive, physically destroy the drive or completely erase all the data on the drive. Information can still be recovered from a drive after files are deleted or the drive has been reformatted. Deleting the files or reformatting the drive removes only the address tables on the drive. Use disk wiping software to completely erase all data on a drive.

Log Security

Inspect and maintain your log files on a regular schedule.

- Review logs for possible incidents and archive them in accordance with a security policy.
- Periodically retire log files when they exceed a reasonable size. Maintain copies of the retired files for possible future reference or statistical analysis.