Netra Modular System Security Guide

Part No: E59326-01
August 2015

Netra Modular System Security Guide

Part No: E59326-01

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: E59326-01

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 au support électronique

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

Security Overview

Oracle's Netra Modular System is a preintegrated, precabled platform that can be completely virtualized to reduce costs and deployment time in your data center. The modular system includes the hardware that you specified and is assembled at the factory and shipped to you.

These topics describe security concepts and features for the modular system:

- "Basic Security Principles" on page 7
- "Advanced Security Considerations" on page 7
- "Security Features" on page 8

Basic Security Principles

Follow these basic security principles for all modular system software and hardware:

- Authentication – Authentication is how a user is identified, typically through confidential information such as user name and password, or shared keys. Authentication ensures that users of hardware or software are who they say they are. By default, local user names and passwords are used for authentication. Shared key-based authentication is also available.
- Accounting and Auditing – Accounting and auditing maintain a record of a user's activity on the system. The modular system software and hardware features allow administrators to monitor login activity and maintain hardware inventories:
  - User logins are monitored through system logs. System administrator and service accounts have access to commands that used incorrectly could cause harm and data loss.
  - Hardware assets are tracked through serial numbers. Oracle part numbers are electronically recorded on all cards, modules, and motherboards, and can be used for inventory purposes.

Advanced Security Considerations

In addition to the basic security principles, the modular system addresses survivability and defense in depth. The modular system delivers a well-integrated set of security capabilities to satisfy important security requirements and concerns. The following sections describe these principles:

- Survivability of Mission-Critical Workloads – Organizations that select hardware and software platforms for mission-critical workloads can be assured that the modular system can prevent or minimize the damage caused from accidental and malicious actions taken by internal users or external parties. As part of the Oracle Maximum Availability Architecture best practices, the following practices increase survivability:
  - Ensuring that the components used have been designed, engineered, and tested to work well together in support of secure deployment architectures. The modular system supports secure isolation, access control, quality of service, and secure management.
  - Reducing the default attack surface of its constituent products helps minimize the overall exposure of the machine.
  - Protecting the machine, including its operational and management interfaces, using a complement of open and vetted protocols, and APIs capable of supporting traditional security goals of strong authentication, access control, confidentiality, integrity, and availability.
  - Verifying that software and hardware contain features that keep the service available even when failures occur. These capabilities help in cases where attackers attempt to disable one or more individual components in the system.
- Defense in Depth to Secure the Operating Environment – The modular system employs multiple, independent, and mutually-reinforcing security controls to help create a secure operating environment for workloads and data. The modular system supports the principle of defense in depth as follows:
  - Offering a strong complement of protections to secure information in transit, in use, and at rest. Security controls are available at the server and network layers. Each layer's unique security controls can be integrated with the others to enable the creation of strong, layered security architectures.
  - Supporting the use of well-defined and open standards, protocols, and interfaces. The modular system can be integrated into existing security policies, architectures, practices, and standards.

Security Features

The modular system hardware and software are hardened. Oracle also provides recommended secure configurations for services such as NTP and SSH. In addition, the modular system's architecture provides security capabilities to the core components. These security capabilities are most often applied by organizations that are deploying a layered security strategy. The capabilities are grouped into the following categories:

- "Network Traffic Isolation" on page 9
- "Oracle ILOM for Secure Management" on page 9

Network Traffic Isolation

If you want to consolidate IT infrastructure, implement shared service architectures, and deliver secure multitenant services, consider isolating the network traffic. The modular system provides the flexibility to implement the isolation policies and strategies based on needs.

At the physical network level, client access is isolated from device management and inter-device communication. Client and management network traffic are isolated on separate networks. Client access is provided over a redundant 10 Gbps Ethernet network that ensures reliable, high-speed access to services running on the system. Management access is provided over a physically separate 1 Gbps Ethernet network. This provides a separation between operational and management networks.

Organizations can choose to further segregate network traffic over the client access Ethernet network by configuring virtual LANs (VLANs). VLANs segregate network traffic based on their requirements. Oracle recommends the use of encrypted protocols over VLANs to assure the confidentiality and integrity of communications.

Oracle ILOM for Secure Management

Collections of security controls and capabilities are necessary to properly secure individual applications and services. It is equally important to have comprehensive management capabilities to sustain the security of the deployed services and systems. The modular system uses the security management capabilities of Oracle ILOM.

Oracle ILOM is an SP embedded in the modular system's compute nodes. Oracle ILOM is used to perform out-of-band management activities, such as the following:

- Provide secure access to perform secure lights-out management of the database and storage servers. Access includes web-based access protected by SSL, command-line access using Secure Shell, and IPMI v2.0 and SNMPv3 protocols.
- Separate duty requirements using a role-based access control model. Individual users are assigned to specific roles that limit the functions that can be performed.
- Provide an audit record of all logins and configuration changes. Each audit log entry lists the user performing the action, and a timestamp. The audit record enables organizations to detect unauthorized activity or changes, and attribute those actions back to specific users.

For more information about Oracle ILOM security, refer to the *Oracle ILOM Security Guide* at `http://www.oracle.com/goto/ILOM/docs`.

Planning a Secure Environment

Put security guidelines in place before the arrival of the Netra Modular System. After the system in installed, periodically review and adjust security guidelines to stay current with the security requirements of your organization.

These topics provide security guidelines for the installation of the Netra Modular System:

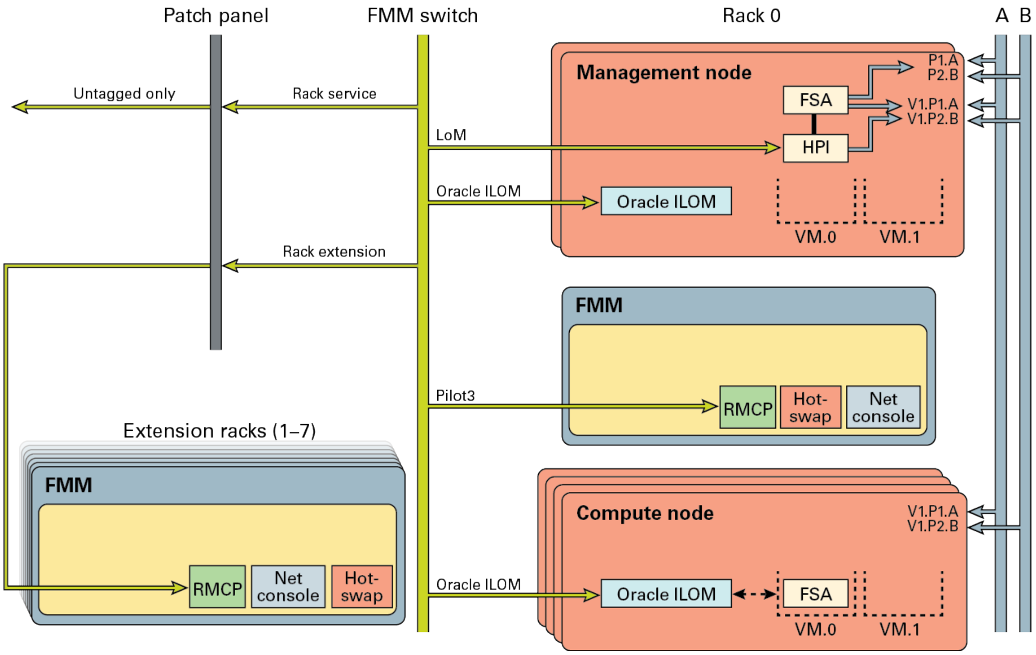
- “Default Network” on page 11
- “User Accounts” on page 12
- “Default Security Settings” on page 12

Contact your IT Security Officer for additional security requirements that pertain to your system and specific environment.

Default Network

The following figure and descriptions explain the default network for the Netra Modular System.

- The System/Telemetry Network (light green network) includes the management node's LoM port on VLAN 4090 through the FMM switch.
- The Telemetry ILOM Network on an internal VLAN 4094 with FMM includes compute nodes Oracle ILOM, and network nodes Oracle ILOM through the FMM switch.
- The patch panel extends the Telemetry Network to racks 1-7. A multi-rack configuration supports the same subnets and VLAN with a different rack ID
- The VLAN(1) provides other services to the Telemetry Network through proper authentication.
- The Data Networks (A &B) provide in-band access to the FSA node.
- The HA application can manage the racks through the modular system's exposed interfaces (JMX, C- API, and so on).



User Accounts

This table lists the default users and passwords for the modular system components. Change all default passwords after you install the Netra Modular System.

Component	User Name and Password
Ethernet switches	`root/changeme` **Note -** Secure the `enable mode password` and `secret` values for the `admin` user.
Management and compute nodes	`root/changeme`

Default Security Settings

The modular system is installed with many default security settings. Whenever possible and practical, configure secure default settings. Refer to the default settings in your version of Oracle ILOM at `http://www.oracle.com/goto/ILOM/docs`.

Securing the Hardware

Physical isolation and access control are the foundation on which you build the security architecture. Ensuring that the physical system is installed in a secure environment protects the system against unauthorized access. Likewise, recording all serial numbers helps prevent the use of unauthorized hardware components.

These sections provide general hardware security guidelines for the modular system.

- "Access Restrictions" on page 13
- "Serial Numbers" on page 14
- "Hard Drives" on page 14

Access Restrictions

- Install systems and related equipment in a locked, restricted-access room.
- If equipment is installed in a rack with a locking door, always lock the rack door until you have to service the components within the rack. Locking the doors also restricts access to hot-plug or hot-swap devices.
- Store all spare replacement parts in a locked cabinet. Restrict access to the locked cabinet to authorized personnel.
- Periodically, verify the status and integrity of the locks on the rack and the spares cabinet to guard against, or detect, tampering or doors being accidentally left unlocked.
- Store cabinet keys in a secure location with limited access.
- Restrict access to USB consoles. Devices such as system controllers, PDUs, and network switches can have USB connections. Physical access is a more secure method of accessing a component since it is not susceptible to network-based attacks.
- Connect the console to an external KVM to enable remote console access. KVM devices often support two-factor authentication, centralized access control, and auditing. For more information about the security guidelines and best practices for KVMs, refer to the documentation that came with the KVM device.

Serial Numbers

Prevent the use of unauthorized hardware components by carefully recording all serial numbers as components are received and taken into inventory. Before any component is installed or used, confirm its authenticity by comparing its serial number against what was recorded when the component was received. Follow these practices to secure hardware:

- Keep a record of the serial numbers of all your hardware.
- Security-mark all significant items of computer hardware, such as replacement parts. Use special ultraviolet pens or embossed labels.
- 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.

Wireless radio frequency identification (RFID) readers can further simplify asset tracking. Refer to the Oracle white paper, *How to Track Your Oracle Sun System Assets by Using RFID*, at `http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o11-001-rfid-oracle-214567.pdf`.

Hard Drives

Hard drives are often used to store sensitive information. To protect this information from unauthorized disclosure, sanitize hard drives prior to reusing, decommissioning, or disposing of them.

- Refer to your data protection policies to determine the most appropriate method to sanitize hard drives.
- If required, take advantage of Oracle's Customer Data and Device Retention Service.

  `http://www.oracle.com/us/support/library/data-retention-ds-405152.pdf`

Securing the Software

Most hardware security is implemented through software measures. These sections provide general software security guidelines for the Netra Modular System.

▼ Prevent Unauthorized Access (Oracle Linux)

- **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`.

▼ Prevent Unauthorized Access (Oracle ILOM)

- **Use Oracle ILOM commands to restrict access to the Oracle ILOM firmware, change the factory-set password, limit the use of the root superuser account, and secure the private network to the SP.**

  Refer to your version of the *Oracle ILOM Security Guide* at `http://www.oracle.com/goto/ILOM/docs`.

▼ Prevent Unauthorized Access (Oracle VM Server With Oracle Linux)

- **Use Oracle Linux commands to restrict access to the Oracle VM Server software, use security features, and protect applications.**

  Refer to the *Oracle VM Security Guide for Release 3.3* at `http://docs.oracle.com/cd/E50245_01/E50254/html/index.html`.

Oracle Hardware Management Pack Security

Oracle Hardware Management Pack features two components: an SNMP monitoring agent and a family of cross-operating system command-line interface tools (CLI Tools) for managing your system.

- Hardware Management Agent SNMP Plugins – SNMP is a standard protocol that monitors or manages a system. With the Hardware Management Agent SNMP Plugins, you can use SNMP to monitor Oracle systems in your data center with the advantage of not having to connect to two management points: the host and Oracle ILOM. This functionality enables you to use a single IP address (the host's IP address) to monitor multiple systems.

  The SNMP Plugins run on the host OS of Oracle systems. The SNMP Plugin extends the native SNMP agent in the host OS to provide additional Oracle MIB capabilities. Oracle Hardware Management Pack itself does not contain an SNMP agent. For Oracle Linux, a module is added to the `net-snmp` agent. For Microsoft Windows, the plugin extends the native SNMP service. Any security settings related to SNMP for the Oracle Hardware Management Pack are determined by the settings of the native SNMP agent or service, and not by the plugin.

  Note that SNMPv1 and SNMPv2c provide no encryption and use community strings as a form of authentication. SNMPv3 is more secure and is the recommended version to use because it employs encryption to provide a secure channel, as well as individual user names and passwords.
- Oracle Hardware Management Pack documentation – For security guidelines that are specific to Oracle Hardware Management Pack, refer to the *Oracle Hardware Management Pack (HMP) Security Guide* at `http://www.oracle.com/goto/OHMP/docs`.

Locating Related Security Guides

Security Guides

These guides describe policies and procedures to keep related products secure:

- *Oracle Server X5-2 Security Guide*
- *Oracle Switch ES2-72 and Oracle Switch ES2-64 Security Guide*
- *Oracle Linux Security Guide for Release 6* at `http://docs.oracle.com/cd/E37670_01/E36387/html/index.html`
- *Oracle ILOM Security Guide* at `http://www.oracle.com/goto/ILOM/docs`
- *Oracle VM Security Guide for Release 3.3* at `http://docs.oracle.com/cd/E50245_01/E50254/html/index.html`
- *Oracle Hardware Management Pack (HMP) Security Guide* at `http://www.oracle.com/goto/OHMP/docs`