Oracle SuperCluster M6-32

Security Guide

Part No.: E54095-01
October 2014

Please
Recycle

Adobe PostScript

Contents

Accessing Oracle SuperCluster M6-32 Security Resources 1

Security Task Overview 1

Security Information for SuperCluster Components 3

Understanding Oracle SuperCluster M6-32 Security Guidelines 7

Understanding Hardware Security Guidelines 7

Access Restrictions 7

Serial Numbers 8

Drives 8

SPARC M6-32 Hardware Security 9

Physical Domains 9

OBP 9

Oracle System Firmware 10

Secure WAN Boot 10

Software Security Guidelines 11

Network Security Considerations 11

Understanding Oracle SuperCluster M6-32 Security Settings and Services 15

Default Security Settings 15

Changing Passwords on Default User Accounts 16

▼ Change Passwords on Default Accounts 16

Default User Accounts and Passwords 17

▼ Change the Exadata Storage Server Passwords 18

▼ Change the Ethernet Switch Password 18

Default TCP/IP Ports and Services 19

Keeping Oracle SuperCluster M6-32 Secure 23

Managing SuperCluster Security 23

Oracle ILOM for Secure Management 23

Oracle Identity Management Suite 24

Oracle Key Manager 24

Oracle Enterprise Manager 25

Oracle Enterprise Manager Ops Center (Optional) 25

Monitoring and Auditing 26

Workload Monitoring and Auditing 26

Database Activity Monitoring and Auditing 27

Monitoring the Network 27

Software and Firmware Updating 28

Index 29

Accessing Oracle SuperCluster M6-32 Security Resources

This guide provides information about planning, configuring, and maintaining a secure environment for Oracle SuperCluster M6-32.

These topics are covered in this section:

- "Security Task Overview" on page 1
- "Security Information for SuperCluster Components" on page 3

Security Task Overview

This table provides a summary of the tasks involved in securing Oracle SuperCluster M6-32.

Use this table in conjunction with the security documents listed in "Security Information for SuperCluster Components" on page 3.

Task	Links
1. Before your system arrives, plan for a secure integration into your environment.	
a. Access security information.	"Security Information for SuperCluster Components" on page 3
b. Read these white papers:. • *Oracle SuperCluster T5-8 Platform Security Principles and Capabilities* • *Secure Database Consolidation Using the Oracle SuperCluster T5-8 Platform* These white papers describe how to deploy the system using Oracle SuperCluster's integrated security capabilities. **Note -** Even though the white papers specify SuperCluster T5-8 in the title, the concepts also apply to SuperCluster M6-32.	`http://www.oracle.com/technetwork/server-storage/sun-sparc-enterprise/documentation/o13-052-osc-t5-8-security-1989641.pdf` `http://www.oracle.com/technetwork/server-storage/sun-sparc-enterprise/documentation/o13-053-securedb-osc-t5-8-1990064.pdf`
c. Review security guidelines.	"Understanding Hardware Security Guidelines" on page 7 "Software Security Guidelines" on page 11 "Network Security Considerations" on page 11
2. While completing the *Oracle SuperCluster M6-32 Configuration Worksheet*, **select configuration options that correspond to your security policies and environment.**	
a. Before making any configuration changes, review the default security settings.	"Default Security Settings" on page 15
b. Review the preconfigured network services to ensure they will integrate securely into your network.	"Default TCP/IP Ports and Services" on page 19
3. After installation, perform immediate security measures.	
a. Secure the hardware.	"Understanding Hardware Security Guidelines" on page 7
b. Change all preconfigured passwords. **Note -** Oracle SuperCluster M6-32 uses preconfigured passwords for initial installation and deployment that are widely known.	"Changing Passwords on Default User Accounts" on page 16
4. Configure SuperCluster security features in accordance with your security architecture and policies:	

Task	Links
a. Establish and configure isolation of the hardware, workload, network traffic, database, and storage. **b. Configure the system to control access to data.** **c. Take advantage of built-in cryptographic services.** **d. Ensure quality of service for all the components.** **e. Before deploying the system in your production environment, thoroughly test the security configuration.**	**a - d** are covered in the white paper titled *Secure Database Consolidation Using the Oracle SuperCluster T5-8 Platform* available at: `http://www.oracle.com/technetwork/server-storage/sun-sparc-enterprise/documentation/o13-053-securedb-osc-t5-8-1990064.pdf` **Note -** Even though the white paper specifies SuperCluster T5-8 in the title, the concepts also apply to SuperCluster M6-32.
5. After deployment, ensure ongoing security.	
a. Use SuperCluster features to ensure optimum security for the life of the system.	"Managing SuperCluster Security" on page 23
b. Monitor and audit critical aspects of the system.	"Monitoring and Auditing" on page 26
c. Ensure that the Quarterly Full Stack Download Patches (QFSDP) are applied to the system.	"Software and Firmware Updating" on page 28

Security Information for SuperCluster Components

Indepth security information is available for each of the major Oracle SuperCluster M6-32 components.

Use these tables to locate applicable security guides and white papers.

TABLE: Hardware Security Documentation

Component	Title	Links
SPARC M6-32 servers	*SPARC M6-32 Servers Security Guide*	http://www.oracle.com/goto/M6-32/docs
Exadata storage servers	*Exadata Database Machine Security Guide*	On the Exadata storage servers, in the `/opt/oracle/cell/doc` directory
ZFS Storage Appliance	*Oracle ZFS Storage Appliance Security Guide*	http://www.oracle.com/goto/ZS3-ES/docs
InfiniBand switches	*Sun Datacenter InfiniBand Switch 36 Hardware Security Guide*	http://docs.oracle.com/cd/E36265_01
Cisco 4948 Ethernet switch	*IPv6 First-Hop Security Configuration Guide, Cisco IOS Release 15.1SG*	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/15-1sg/ip6f-15-1sg-book.html

TABLE: Software Security Documentation

Component	Title	Links
Oracle Solaris 11 OS	• *Oracle Solaris 11 Security Guidelines* • *Securing the Network in Oracle Solaris 11.1* • *Oracle Solaris 11.1 Administration: Security Services*	http://www.oracle.com/goto/Solaris11/docs
Oracle Solaris 10 OS	*Oracle Solaris 10 Security Guidelines* *Oracle Solaris Administration: Security Services*	http://www.oracle.com/goto/Solaris10/docs
Oracle Solaris Cluster	*Oracle Solaris Cluster 4.1 Security Guide*	http://docs.oracle.com/cd/E29086_01
Oracle Solaris Cluster	*Oracle Solaris Cluster 3.3 Security Guide*	http://docs.oracle.com/cd/E37745_01

TABLE: Software Security Documentation *(Continued)*

Component	Title	Links
Oracle Database (including Database Vault and Label Security)	• *Oracle Database 11g (11.2) Security* Guide • *Advanced Security Administrator's Guide* • *Database Vault Administrator's Guide* • *Label Security Administrator's Guide* • *Enterprise User Security Administrator's Guide*	http://docs.oracle.com/cd/E11882_01/nav/portal_25.htm#database_security
Oracle ILOM	*Oracle ILOM Security Guide Firmware Release 3.2.x*	http://docs.oracle.com/cd/E37444_01
Oracle VM Server for SPARC	*Oracle VM Server for SPARC 3.1 Security Guide*	http://docs.oracle.com/cd/E38405_01
Oracle Enterprise Manager Ops Center	*Oracle Enterprise Manager Ops Center Security Guide*	http://docs.oracle.com/cd/E11857_01/nav/management.htm

TABLE: Additional Security Information

Information	Links
Oracle Security and Compliance for Oracle Database	http://www.oracle.com/technetwork/database/security
Oracle SuperCluster articles and white papers	http://www.oracle.com/technetwork/server-storage/engineered-systems/supercluster-whitepapers-1965427.html
Identity management and security articles	http://www.oracle.com/technetwork/articles/idm
Oracle VM Server for SPARC technical white papers	http://www.oracle.com/technetwork/server-storage/vm/overview

Understanding Oracle SuperCluster M6-32 Security Guidelines

These sections describe Oracle SuperCluster M6-32 security guidelines and features:

- "Understanding Hardware Security Guidelines" on page 7
- "Software Security Guidelines" on page 11
- "Network Security Considerations" on page 11

Understanding Hardware Security Guidelines

These sections describe hardware security guidelines:

- "Access Restrictions" on page 7
- "Serial Numbers" on page 8
- "Drives" on page 8

Access Restrictions

- Install Oracle SuperCluster M6-32 and related equipment in a locked, restricted-access room.
- Lock the rack doors unless service is required on components within the rack. Doing so restricts access to hot-pluggable or hot-swappable devices, and to USB ports, network ports, and system consoles.
- Store spare field-replaceable units (FRUs) or customer-replaceable units (CRUs) 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, power distribution units (PDUs), and network switches can have USB connections. Restricting physical access is a more secure method of accessing a component since it is not susceptible to network-based attacks.

Serial Numbers

- Record the serial numbers of the components in Oracle SuperCluster M6-32.
- 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.
- Securely store all the information sheets that are provided with the system.

Drives

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

- Use disk-wiping tools such as the Oracle Solaris `format(1M)` command to completely erase all data from the drive.
- Organizations should refer to their 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. Refer to this document: http://www.oracle.com/us/support/library/data-retention-ds-405152.pdf

Caution – Disk-wiping software might not be able to delete some data on modern drives, due to the way that they manage data access.

SPARC M6-32 Hardware Security

All of the security principles that are outlined in the *SPARC M6-32 Servers Security Guide* apply to the SPARC M6-32 servers in SuperCluster. This security guide is available at: http://www.oracle.com/goto/M6-32/docs

Physical Domains

A physical domain (PDomain) operates like an independent server that has full hardware isolation from other PDomains in the server. A hardware or software failure on one PDomain does not affect the other PDomains on a server.

You can divide the server into two or four PDomains, depending on your application requirements. For example, you can divide the server into four PDomains, each running its own applications.

PDomain Type	Description
Bounded PDomain	A Bounded PDomain contains only one DCU and has total hardware isolation from other PDomains in the server. Bounded PDomains performance might be better when compared to PDomains.
PDomain	A PDomain can contain one or two DCUs. In a multiple DCU PDomain, processor data traffic between the DCUs is routed through the SSBs, so PDomains might have lower performance compared to a Bounded PDomain.

OBP

By default, the SPARC M6-32 OBP is not password-protected. You can enhance the security of the SPARC M6-32 by restricting access to the OBP by performing these actions:

- Implement password protection.
- Check for failed OBP logins.
- Provide an OBP power-on banner.

Oracle System Firmware

The Oracle system firmware that runs on the SPARC M6-32 servers uses a controlled update process to prevent unauthorized modifications. Only the superuser or an authenticated user with proper authorization can use the update process.

Secure WAN Boot

WAN boot supports varying levels of security. You can use a combination of the security features that are supported in WAN boot to meet the needs of your network. A more secure configuration requires more administration, but also protects your system data to a greater extent.

- For the Oracle Solaris 10 OS, refer to the information on securing WAN boot installation configuration in *Oracle Solaris Installation Guide: Network-Based Installations* at: `http://docs.oracle.com/cd/E26505_01`
- For the Oracle Solaris 11 OS, refer to Securing the *Network in Oracle Solaris 11* available at: `http://www.oracle.com/goto/Solaris11/docs`

Software Security Guidelines

- Ensure that all default passwords are changed as soon as the system is installed.
- When creating user accounts, use role-based access control (RBAC) features to disable the ability to directly log in to common OS accounts such as `root`, `grid`, and `oracle`. Instead, create individual user accounts for each administrator. After logging in with their individual account, the administrator can use `su` to run privileged commands, when required.
- Create and use Oracle ILOM user accounts for individual users to ensure a positive identification in audit trails.
- Disable unnecessary protocols and modules in the OS.
- Restrict the capability to restart the system over the network.
- Limit SSH listener ports to the management and private networks.
- Use SSH protocol 2 (SSH-2) and FIPS 140-2 approved ciphers.
- Use intrusion prevention systems on servers to monitor network traffic flowing to and from Oracle SuperCluster M6-32.
- Use host-based intrusion detection and prevention systems for increased visibility within Oracle SuperCluster M6-32. By using the fine-grained auditing capabilities of Oracle Database, host-based systems have a greater likelihood of detecting inappropriate actions and unauthorized activity.
- Use application and network-layer firewalls to protect information flowing to and from Oracle SuperCluster M6-32. Filtering network ports provides the first line of defense in preventing unauthorized access to systems and services.

  Network-level segmentation using Ethernet VLANs and host-based firewalls enforce inbound and outbound network policy at the host level. SuperCluster M6-32 includes a configured software firewall by default.
- Use encryption features such as Transparent Data Encryption (TDE) and Oracle Recovery Manager (RMAN) encryption for backups.
- Use centralized audit and log repositories to aggregate the security-relevant information for improved correlation, analysis, and reporting.

Network Security Considerations

This list provides a number of security features worth considering to enhance network security.

Caution – Ensure that you fully test these features before you deploy the system in your environment.

- Configure administrative and operational services to use encryption protocols and key lengths that align with current policies. Cryptographic services provided by Oracle SuperCluster M6-32 benefit from hardware acceleration, which improves security without impacting performance.
- Create separate software owner accounts for Oracle Grid Infrastructure and Oracle Database software installations. Use these accounts when deploying Oracle SuperCluster M6-32.
- Disable unnecessary network services, such as TCP small servers or HTTP. Enable only necessary network services, and configure these services securely.
- Create a login banner to state that unauthorized access is prohibited.
- Use access control lists to apply restrictions where appropriate.
- Set time-outs for extended sessions and set privilege levels.
- Use the port mirroring capability of the switch for intrusion detection system (IDS) access.
- Implement port security to limit access based upon a MAC address. Disable auto-trunking on all ports for any switch connected to Oracle SuperCluster M6-32.
- Limit remote configuration to specific IP addresses using SSH.
- Require users to use strong passwords by setting minimum password complexity rules and password expiration policies.
- Enable logging and send logs to a dedicated secure log host.
- Configure logging to include accurate time information, using NTP and timestamps.
- Secure the IB Switches:
  - Use network switch port security features if they are available.
  - Lock the Media Access Control (MAC) address of one or more connected devices to a physical port on a switch. If a switch port is locked to a particular MAC address, then superusers cannot create back doors into the network with rogue access points.
  - Disable a specified MAC address from connecting to a switch.
  - Manage the Ethernet switch configuration file offline and limit access to the file to only authorized administrators.
  - Use each switch port's direct connections so the switch can set security based on its current connections.
  - Use authentication, authorization, and accounting (AAA) features for local and remote access to a switch.
- Secure VLANs:

- Use a static VLAN configuration.
- Disable unused switch ports, and assign an unused VLAN number.
- 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. If disabling VTP is not possible, then set the management domain, password, and pruning for VTP. In addition, set VTP to transparent mode.

Understanding Oracle SuperCluster M6-32 Security Settings and Services

These sections describe Oracle SuperCluster M6-32 security guidelines and features:

- "Default Security Settings" on page 15
- "Changing Passwords on Default User Accounts" on page 16
- "Default TCP/IP Ports and Services" on page 19

Default Security Settings

Oracle SuperCluster M6-32 software is installed with many default security settings. Whenever possible, use the default secure settings:

- Password policies enforces a minimum password complexity.
- Failed login attempts cause a lockout after a set number of failed attempts.
- All default system accounts in the OS are locked and prohibited from logging in.
- Limited ability to use the `su` command is configured.
- Unnecessary protocols and modules are disabled from the OS kernel.
- Boot loader is password protected.
- All unnecessary system services are disabled, including `inetd` (Internet service daemon).
- Software firewall is configured on the storage cells.
- Restrictive file permissions are set on key security-related configuration files and executable files.
- SSH listen ports are restricted to management and private networks.
- SSH is limited to v2 protocol.
- Insecure SSH authentication mechanisms are disabled.
- Specific cryptographic ciphers are configured.
- The switches are separated in the system from data traffic on the network.

Changing Passwords on Default User Accounts

After Oracle SuperCluster M6-32 is installed, the system is configured with a set of user accounts and passwords. The root SSH equivalence is enabled.

These topics describe the default user accounts and passwords:

- "Change Passwords on Default Accounts" on page 16
- "Default User Accounts and Passwords" on page 17
- "Change the Exadata Storage Server Passwords" on page 18
- "Change the Ethernet Switch Password" on page 18

▼ Change Passwords on Default Accounts

Before deploying the system, perform these actions:

1. **Change all user account passwords on all components.**

   See "Default User Accounts and Passwords" on page 17.

   Ensure that you create strong passwords. Refer to the security guides for each component. The guides are listed in "Security Information for SuperCluster Components" on page 3.

   You must change Oracle Solaris passwords for each logical domain and for each zone.

2. **Limit use of the `root` superuser account.**

   Instead, create user accounts with the Oracle Solaris OS RBAC facility.

   For more information, refer to the security documentation for Oracle Solaris 11 at: `http://www.oracle.com/goto/Solaris11/docs`

Default User Accounts and Passwords

Component	User Name	Password	User Account and Password Information
SPARC M6-32 servers	• root • oracle • grid	welcome1 welcome1 welcome1	• **Oracle Solaris 11** – Refer to the security documentation for Oracle Solaris 11 at: http://www.oracle.com/goto/Solaris11/docs • **Oracle Solaris 10** – Refer to *Oracle Solaris Administration: Basic Administration* at: http://docs.oracle.com/cd/E26505_01
Exadata Storage Servers	• root • celladmin • cellmonitor	welcome1 welcome1 welcome1	See "Change the Exadata Storage Server Passwords" on page 18.
Oracle ZFS Storage ZS3-ES	• root	welcome1	Refer to the "Users" section in the *Oracle ZFS Storage Appliance Administration Guide* at: http://www.oracle.com/goto/ZS3-ES/docs
InfiniBand switches	• root • nm2user	welcome1 changeme	Refer to "Controlling the Chassis" in the *Sun Datacenter InfiniBand Switch 36 HTML Document Collection for Firmware Version 2.1* at: http://docs.oracle.com/cd/E36265_01
PDUs	• admin • root	welcome1 welcome1	Refer to "Changing Interface Settings" in the *Sun Rack II Power Distribution Units User's Guide* at: http://docs.oracle.com/cd/E19844-01
Oracle ILOM on: • SPARC M6-32 servers • Exadata Storage Servers • ZFS storage appliance	• root	welcome1	Refer to "Configuration and Maintenance" in the Oracle ILOM documentation collection, at: http://docs.oracle.com/cd/E24707_01/html/E24528
InfiniBand Oracle ILOM	• ilom-admin • ilom-operator	ilom-admin ilom-operator	Refer to the InfiniBand documentation at: http://docs.oracle.com/cd/E36265_01
Ethernet switch	• admin	welcome1	See "Change the Ethernet Switch Password" on page 18.

▼ Change the Exadata Storage Server Passwords

1. **Log into the storage server as `root` using the preconfigured password `welcome1`.**

2. **Change the password for the `root`, `celladmin`, and `cellmonitor` accounts.**

   Syntax: `passwd` *username*

   Example: **`passwd celladmin`**

   You are prompted to enter a password.

Note – The `celladmin` user runs all services on the cell. The `cellmonitor` user is used for monitoring purposes, but cannot run services on the cell.

For more information about Exadata Storage Server security, on the Exadata storage servers, go to the `/opt/oracle/cell/doc` directory and refer to these documents:

- *Exadata Database Machine Security Guide*
- "Understanding Operating System Security of Oracle Exadata Storage Servers" in the *Exadata Storage Server Software User's Guide*

▼ Change the Ethernet Switch Password

1. **Connect a serial cable from the Ethernet switch console to a laptop or similar device.**

   The default serial port speed is 9600 baud, 8 bits, no parity, 1 stop bit, and no handshake.

```
sscsw-adm0 con0 is now available
Press RETURN to get started.
```

2. **Put the switch in enable mode.**

```
sscsw-adm0> enable
```

3. **Set the password.**

```
sscsw-adm0# configure terminal
Enter configuration commands,one per line.End with CNTL/Z.
sscsw-adm0(config)# enable password *******
sscsw-adm0(config)# enable secret *******
sscsw-adm0(config)# end
sscsw-adm0# write memory
```

```
*Apr 24 14:25:05.893:%SYS-5-CONFIG_I:Configured from console by
console
Building configuration...
Compressed configuration from 2502 bytes to 1085 bytes [OK ]
```

4. **Save the configuration.**

```
sscsw-adm0# copy running-config startup-config
```

5. **Exit from the session.**

```
sscsw-adm0# exit
```

6. **Disconnect the laptop from the Ethernet switch.**

Default TCP/IP Ports and Services

This section provides a list of services with listening ports and a description of the different port states.

For comprehensive information about securing the Oracle Supercluster M6-32 network, refer to the network documentation for Oracle Solaris:

- Oracle Solaris 11 library:

  http://www.oracle.com/goto/Solaris11/docs

- Oracle Solaris 10 library

  http://www.oracle.com/goto/Solaris10/docs

This table lists the typical listening ports for a logical domain on Oracle SuperCluster M6-32. The state listed represents the state of the port after the system is initially configured and before any users have logged in.

TABLE: Listening Ports

Service	Address Family AF_INET6 is IPv6 AF_INET is IPv4	Port No.	State
/usr/lib/nfs/mountd	AF_INET6	39124*	IDLE
	AF_INET	40167*	IDLE
	AF_INET6	41858*	IDLE
	AF_INET	64956*	IDLE
/usr/lib/ep/eptelemon	AF_INET	61666	IDLE
/usr/sbin/cupsd	AF_INET6	631	LISTEN
	AF_INET	631	LISTEN
/usr/lib/nfs/lockd	AF_INET6	4045	LISTEN
	AF_INET	4045	LISTEN
/usr/lib/nfs/statd	AF_INET6	46535*	IDLE
	AF_INET6	33612*	IDLE
	AF_INET	63711*	IDLE
	AF_INET	41346*	IDLE
/usr/sbin/rpcbind	AF_INET6	111	LISTEN
	AF_INET6	44464*	IDLE
	AF_INET	111	LISTEN
	AF_INET	64773*	IDLE
/usr/lib/ldoms/vntsd	AF_INET	5001	LISTEN
	AF_INET	5002	LISTEN
/opt/SUNWldm/bin/ldmd	AF_INET	64535	IDLE
	AF_INET	56967	IDLE
	AF_INET	6482	ESTABLISHED
	AF_INET	8101	LISTEN
/usr/lib/nfs/nfs4cbd	AF_INET6	51946*	IDLE
	AF_INET	35389*	IDLE
/usr/lib/nfs/nfsd	AF_INET6	2049	LISTEN
	AF_INET	2049	LISTEN
/usr/lib/inet/inetd	AF_INET	50197*	IDLE
	AF_INET6	54077*	IDLE
	AF_INET6	69	IDLE

TABLE: Listening Ports *(Continued)*

Service	Address Family AF_INET6 is IPv6 AF_INET is IPv4	Port No.	State
/usr/lib/ssh/sshd	AF_INET6	22	LISTEN
/usr/bin/sendmail	AF_INET	25	LISTEN
	AF_INET6	25	LISTEN
	AF_INET	587	LISTEN
/usr/lib/inet/ntpd	AF_INET	123	IDLE
	AF_INET6	123	IDLE

* The service uses a range of different ports so the port number might be different each time the service runs, but the number is similar to the number shown in the table.

This table provides descriptions of the different states.

TABLE: Port States

State	Description
BOUND	Bound, ready to connect or listen.
CLOSED	Socket is not being used.
CLOSING	Closed, remote shutdown and awaiting acknowledgment.
CLOSE_WAIT	Remote shutdown is waiting for the socket to close.
ESTABLISHED	Connection established.
FIN_WAIT_1	Socket closed and connection is shutting down.
FIN_WAIT_2	Socket closed and waiting for remote shutdown.
IDLE	Idle, opened but not bound.
LAST_ACK	Remote shutdown and closed, awaiting acknowledgement.
LISTEN	Listening for incoming connections.
SYN_RECEIVED	Initial synchronization of the connection is underway.
SYN_SENT	Actively trying to establish connection.
TIME_WAIT	Wait after close for remote shutdown retransmission.

Keeping Oracle SuperCluster M6-32 Secure

These topics describe the Oracle SuperCluster M6-32 features that you can use to maintain security over the life of the system:

- "Managing SuperCluster Security" on page 23
- "Monitoring and Auditing" on page 26
- "Software and Firmware Updating" on page 28

Managing SuperCluster Security

Oracle SuperCluster M6-32 leverages the security management capabilities of a variety of products including Oracle ILOM, Oracle Enterprise Manager Ops Center, Oracle Enterprise Manager, and Oracle's Identity Management Suite. These sections describe the details:

- "Oracle ILOM for Secure Management" on page 23
- "Oracle Identity Management Suite" on page 24
- "Oracle Key Manager" on page 24
- "Oracle Enterprise Manager" on page 25
- "Oracle Enterprise Manager Ops Center (Optional)" on page 25

Oracle ILOM for Secure Management

Oracle ILOM is a service processor embedded in many Oracle SuperCluster M6-32 components. Use Oracle ILOM to perform these out-of-band management activities:

- Provide secure access to perform secure lights-out management of the SuperCluster components. 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 an RBAC model. Assign individual users to specific roles that limit the functions that they can perform.
- Provide an audit record of all logins and configuration changes. Each audit log entry lists the user performing the action and a timestamp. This capability enables you to detect unauthorized activity or changes and attribute those actions back to specific users.

For more information, refer to the Oracle Integrated Lights Out Manager 3.1 documentation at: http://docs.oracle.com/cd/E24707_01

Oracle Identity Management Suite

Oracle Identity Management suite manages the end-to-end lifecycle of user identities and accounts across an organization. The Oracle Identity Management suite includes support for single sign-on, web-based access control, web services security, identity administration, strong authentication, and identity and access governance.

Oracle Identity Management can provide a single point for managing identity and access to not only applications and services running on Oracle SuperCluster M6-32, but also for the underlying infrastructure and services that manage it.

For more information, refer to the Oracle Identity Management documentation at: http://www.oracle.com/technetwork/middleware/id-mgmt/documentation/index.html

Oracle Key Manager

Oracle Key Manager is a comprehensive key management system (KMS) that simplifies the management and monitoring of encryption keys that protect information at rest.

Oracle Key Manager supports enterprise-class environments with a highly scalable and available architecture that can manage thousands of devices and millions of keys. This feature operates on a hardened operating environment, enforces strong access control and role separation for key management and monitoring operations, and optionally supports the secure storage of keys in Oracle's Sun Crypto Accelerator 6000 PCIe Card, a FIPS 140-2 rated hardware secure module.

In the context of Oracle SuperCluster M6-32, the Oracle Key Manager can authorize, secure, and manage access to encryption keys used by Oracle StorageTek encrypting tape drives, Oracle Databases encrypted using Transparent Data Encryption, and encrypted ZFS file systems available on the Oracle Solaris 11 OS.

For more information, refer to the Oracle Key Manager documentation at:
http://docs.oracle.com/cd/E26076_02

Oracle Enterprise Manager

Oracle Enterprise Manager suite is a comprehensive and integrated cloud management solution that focuses on lifecycle management of applications, middleware, databases, and physical and virtual infrastructure (using Oracle Enterprise Manager Ops Center). Oracle Enterprise Manager provides these management technologies:

- Supports detailed monitoring, event notification, patching, change management, continuous configuration, and compliance management, and reporting for the application, middleware, and database.
- Enables you to centrally maintain security configuration settings as well as access control and auditing policies for groups of databases. Access to these functions can be limited to authorized individuals, ensuring that management access supports compliance mandates for separation of duty, least privilege, and accountability.
- Supports strong authentication using a variety of methods, fine-grained access controls, and comprehensive auditing, ensuring that management of the Oracle SuperCluster M6-32 environment can be accomplished in a secure manner.

For more information, refer to Oracle Enterprise Manager documentation at:
http://www.oracle.com/technetwork/oem/grid-control/documentation/oem-091904.html

Oracle Enterprise Manager Ops Center (Optional)

Oracle Enterprise Manager Ops Center is an optional technology that you can use to manage some security aspects of Oracle SuperCluster M6-32.

Part of the Oracle Enterprise Manager suite, Oracle Enterprise Manager Ops Center is a converged hardware management solution that provides a single administrative interface for servers, OSs, firmware, virtual machines, zones, storage, and network fabrics. Oracle Enterprise Manager Ops Center is installed by default on Oracle SuperClusterM6-32.

You can use Oracle Enterprise Manager Ops Center to assign administrative access to collections of physical and virtual systems, monitor administrator activity, detect faults, and configure and manage alerts. Oracle Enterprise Manager Ops Center supports a variety of reports that enable you to compare systems against known configuration baselines, patch levels, and security vulnerabilities.

For more information, refer to the Oracle Enterprise Manager Ops Center documentation at: http://docs.oracle.com/cd/E27363_01/index.htm

---

Note – For previous versions of Oracle Enterprise Manager Ops Center, the Ops Center software was installed and run from the SuperCluster system. Beginning with the Oracle Enterprise Manager Ops Center 12c Release 2 (12.2.0.0.0) release, the Ops Center software must be installed and run on a system outside of the SuperCluster system.

Monitoring and Auditing

Whether for compliance reporting or incident response, monitoring and auditing are critical functions that you must use to gain increased visibility into the IT environment. The degree to which monitoring and auditing is employed is often based upon the risk or critical nature of the environment.

Oracle SuperCluster M6-32 provides comprehensive monitoring and auditing functionality at the server, network, database, and storage layers, ensuring that information can be made available in support of audit and compliance requirements.

These sections describe workload and database monitoring and auditing:

- "Workload Monitoring and Auditing" on page 26
- "Database Activity Monitoring and Auditing" on page 27
- "Monitoring the Network" on page 27

Workload Monitoring and Auditing

The Oracle Solaris OS has a comprehensive auditing facility that can monitor administrative actions, command-line invocations, and even individual kernel-level system calls. This facility is highly configurable, offering a global, per-zone, and even per-user auditing policies.

When the system is configured to use Oracle Solaris Zones, audit records for each zone can be stored in the global zone to protect them from tampering.

Oracle Solaris auditing provides the ability to send audit records to remote collection points using the system log (`syslog`) facility. Many commercial intrusion detection and prevention services can use Oracle Solaris audit records as an additional input for analysis and reporting.

Oracle VM Server for SPARC leverages the native Oracle Solaris auditing facility to record actions and events associated with virtualization events and domain administration.

For more information, refer to the Monitoring and Maintaining Oracle Solaris Security section in the Oracle Solaris Security Guidelines at: http://docs.oracle.com/cd/E26502_01

Database Activity Monitoring and Auditing

Oracle Database support of fine-grained auditing enables you to establish policies that selectively determine when audit records are generated. This capability helps you focus on other database activities and reduces the overhead that is often associated with audit activities.

Oracle Audit Vault and Database Firewall centralizes the management of database audit settings and automates the consolidation of audit data into a secure repository. This software includes built-in reporting to monitor a wide range of activities, including privileged user activity and changes to database structures. The reports generated by Oracle Audit Vault and Database Firewall provide visibility into various application and administrative database activities, and provide detailed information to support accountability of actions.

Oracle Audit Vault and Database Firewall enables the proactive detection and alerting of activities that might indicate unauthorized access attempts or abuse of system privileges. These alerts can include both system and user-defined events and conditions, such as the creation of privileged user accounts or the modification of tables containing sensitive information.

Oracle Audit Vault and Database Firewall Remote Monitor can provide real-time database security monitoring. This feature queries database connections to detect malicious traffic, such as application bypass, unauthorized activity, SQL injection, and other threats. Using an accurate SQL grammar-based approach, this software helps you quickly identify suspicious database activity.

For more information, refer to the Oracle Audit Vault and Database Firewall documentation at: http://docs.oracle.com/cd/E37100_01/index.htm

Monitoring the Network

After the networks are configured based on the security guidelines, regular review and maintenance is needed.

Follow these guidelines to ensure the security of local and remote access to the system:

- Review logs for possible incidents and archive them in accordance with your organization's security policies.
- Perform periodic reviews of the client access network to ensure that host and Oracle ILOM settings remain intact.

For more information, refer to the security guides for the Oracle Solaris OS:

- Oracle Solaris 11 OS – http://www.oracle.com/goto/Solaris11/docs
- Oracle Solaris 10 OS – http://www.oracle.com/goto/Solaris10/docs

Software and Firmware Updating

Oracle SuperCluster M6-32 updates are provided in QFSDP. Installing the QFSDP updates all components at the same time. This practice ensures that all components continue to run on a combination of software versions that have been fully tested together by Oracle.

Obtain the latest QFSDP from My Oracle Support at:
http://support.oracle.com

For details about the supported software and firmware, refer to the *Oracle SuperCluster M6-32 Product Notes*. This document is available on the first compute node in this directory: `/opt/oracle/node/doc/E41531_01/index.html`

Note – Only Upgrade, update, or patch individual components in isolation for reactive maintenance under the advice of Oracle support.

Index

A

access restrictions, 7
accessing
  security information, 3
  security resources, 1
activations keys, 8
auditing and monitoring, 26

C

changing
  default user passwords, 16
  Ethernet switch passwords, 18
  Exadata storage server passwords, 18

D

database activity monitoring, 27
default
  security settings, 15
  TCP/IP ports and services, 19
  user accounts and passwords, 17
  user passwords, 16
drives, 8

E

Ethernet switch
  changing passwords, 18
  default password, 17
Exadata storage servers
  changing passwords, 18
  default passwords, 17

F

firmware updating, 28
firmware, SPARC, 9

H

hardware security
  SPARC M6-32, 9
  understanding, 7

I

IB switch, default passwords, 17

K

keeping the system secure, 23

L

Listening ports, 19

M

managing SuperCluster security, 23
Monitoring and auditing, 26

N

network
  monitoring, 27
  security considerations, 11

O

OBP, 9
Oracle Enterprise Manager, 25
Oracle Enterprise Manager Ops Center, 25
Oracle Identity Management Suite, 24
Oracle ILOM
  default passwords, 17
  secure management, 23
Oracle Key Manager, 24
overview of security tasks, 1

P

PDU firmware updating, 28
physical restrictions, 7
port states, 19

R

RBAC facility, 16
resources, security, 3

S

sanitation of drives, 8
secure management
  Oracle Identity Management Suite, 24
  Oracle ILOM, 23
secure WAN boot, 9
security
  considerations for the network, 11
  default settings, 15
  guidelines for software, 11
  guides, 3
  information, 3
  managing, 23
  resources, 1
  settings and services, 15
  task overview, 1
  white papers, 3
serial numbers, 8
software security guidelines, 11
software updating, 28
SPARC M6-32
  default passwords, 17
  hardware security, 9

T

tasks, security, 1
TCP/IP ports and services, default, 19

U

understanding
  hardware security, 7
  security settings and services, 15
user accounts and passwords, 17

W

WAN boot, secure, 9
white papers, security, 3
workload monitoring, 26