Oracle® SuperCluster M8 and SuperCluster M7 Security Guide

Part No: E58630-11
June 2020

ORACLE

Oracle SuperCluster M8 and SuperCluster M7 Security Guide

Part No: E58630-11

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: E58630-11

Restrictions de licence/Avis d'exclusion de responsabilité en cas de dommage indirect et/ou consécutif

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.

Exonération de garantie

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.

Avis sur la limitation des droits

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 embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

Avis sur les applications dangereuses

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 un risque de 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 des applications dangereuses.

Marques

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 Inside 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, Epyc, et le logo AMD sont des marques ou des marques déposées d'Advanced Micro Devices. UNIX est une marque déposée de The Open Group.

Avis d'exclusion de responsabilité concernant les services, produits et contenu tiers

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.

Date de publication et mention de la version préliminaire de Disponibilité Générale ("Pre-GA")

Version préliminaire de Disponibilité Générale ("Pre-GA") : 15.01.2020

Avis sur la version préliminaire de Disponibilité Générale ("Pre-GA") de la documentation

Si ce document est fourni dans la Version préliminaire de Disponibilité Générale ("Pre-GA") à caractère public ou privé :

Cette documentation est fournie dans la Version préliminaire de Disponibilité Générale ("Pre-GA") et uniquement à des fins de démonstration et d'usage à titre préliminaire de la version finale. Celle-ci n'est pas toujours spécifique du matériel informatique sur lequel vous utilisez ce logiciel. Oracle Corporation et ses affiliés déclinent expressément toute responsabilité ou garantie expresse quant au contenu de cette documentation. Oracle Corporation et ses affiliés ne sauraient en aucun cas être tenus pour responsables des pertes subies, des coûts occasionnés ou des dommages causés par l'utilisation de cette documentation.

Mention sur les informations confidentielles Oracle

INFORMATIONS CONFIDENTIELLES ORACLE. Destinées uniquement à un usage autorisé. Ne pas distribuer à des tiers.

Avis sur la reconnaissance du revenu

Si ce document est fourni dans la Version préliminaire de Disponibilité Générale ("Pre-GA") à caractère privé :

Les informations contenues dans ce document sont fournies à titre informatif uniquement et doivent être prises en compte en votre qualité de membre du customer advisory board ou conformément à votre contrat d'essai de Version préliminaire de Disponibilité Générale ("Pre-GA") uniquement. Ce document ne constitue en aucun cas un engagement à fournir des composants, du code ou des fonctionnalités et ne doit pas être retenu comme base d'une quelconque décision d'achat. Le développement, la commercialisation et la mise à disposition des fonctions ou fonctionnalités décrites restent à la seule discrétion d'Oracle.

Accessibilité de la documentation

Pour plus d'informations sur l'engagement d'Oracle pour l'accessibilité de 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

Using This Documentation

- **Overview** – Provides information about planning, configuring, and maintaining a secure environment for Oracle SuperCluster M8 and SuperCluster M7 systems.
- **Audience** – Technicians, system administrators, and authorized service providers
- **Required knowledge** – Advanced experience with UNIX and database administration.

Product Documentation Library

Documentation and resources for this product and related products are available at http://docs.oracle.com/cd/E58626_01/index.html.

Feedback

Provide feedback about this documentation at http://www.oracle.com/goto/docfeedback.

Understanding Security Principles

This guide provides information about planning, configuring, and maintaining a secure environment for Oracle SuperCluster M8 and SuperCluster M7 systems.

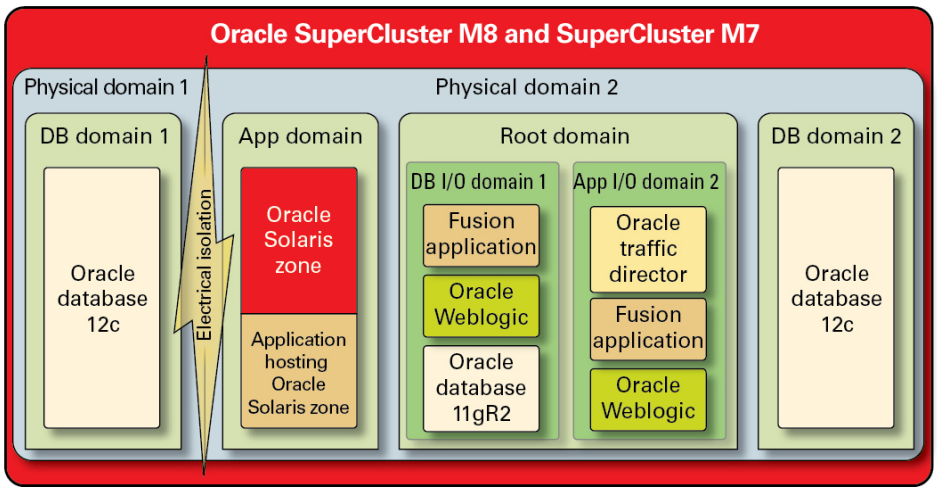
These topics are covered in this section:

Secure Isolation

SuperCluster M8 and SuperCluster M7 support a variety of isolation strategies that cloud providers select based upon their security and assurance requirements. This flexibility allows cloud providers to create a customized, secure multitenant architecture that is tailored for their business.

SuperCluster M8 and SuperCluster M7 support a number of workload isolation strategies, each with its own unique set of capabilities. While each implementation strategy can be used independently, they can also be used together in a hybrid approach allowing cloud providers to deploy architectures that can more effectively balance their security, performance, availability needs, and other needs.

FIGURE 1 Secure Isolation with a Dynamic Tenant Configuration



Cloud providers can use physical domains (also called PDomains) for situations in which their tenant hosts are running applications and databases that must be physically isolated from other workloads. Dedicated physical resources might be required for a deployment due to its criticality to the organization, the sensitivity of the information it contains, compliance mandates, or even simply because the database or application workload will fully utilize the resources of an entire physical system.

For organizations that require hypervisor-mediated isolation, Oracle VM Server for SPARC domains, referred to as dedicated domains, are used to create virtual environments that isolate application and/or database instances. Created as part of the SuperCluster installation, dedicated domains each run their own unique instance of the Oracle Solaris OS. Access to physical resources is mediated by the hardware-assisted hypervisors built into the SPARC processors.

In addition, SuperCluster enables you to create additional domains referred to as root domains, which leverage single root I/O virtualization (SR-IOV) technology. Root domains own one or two IB HCAs and 10 GbE NICs. You can choose to dynamically create additional domains, referred to as I/O domains, on top of root domains. SuperCluster M7 and SuperCluster M7 includes a browser-based tool to create and manage them.

Within each of these domains, however, cloud consumer tenants can leverage Oracle Solaris Zones technology to create additional isolated environments. Using zones, it is possible to deploy individual application or database instances or groups of application or database

instances into one or more virtualized containers that collectively run on top of a single OS kernel. This lightweight approach to virtualization is used to create a stronger security boundary around deployed services.

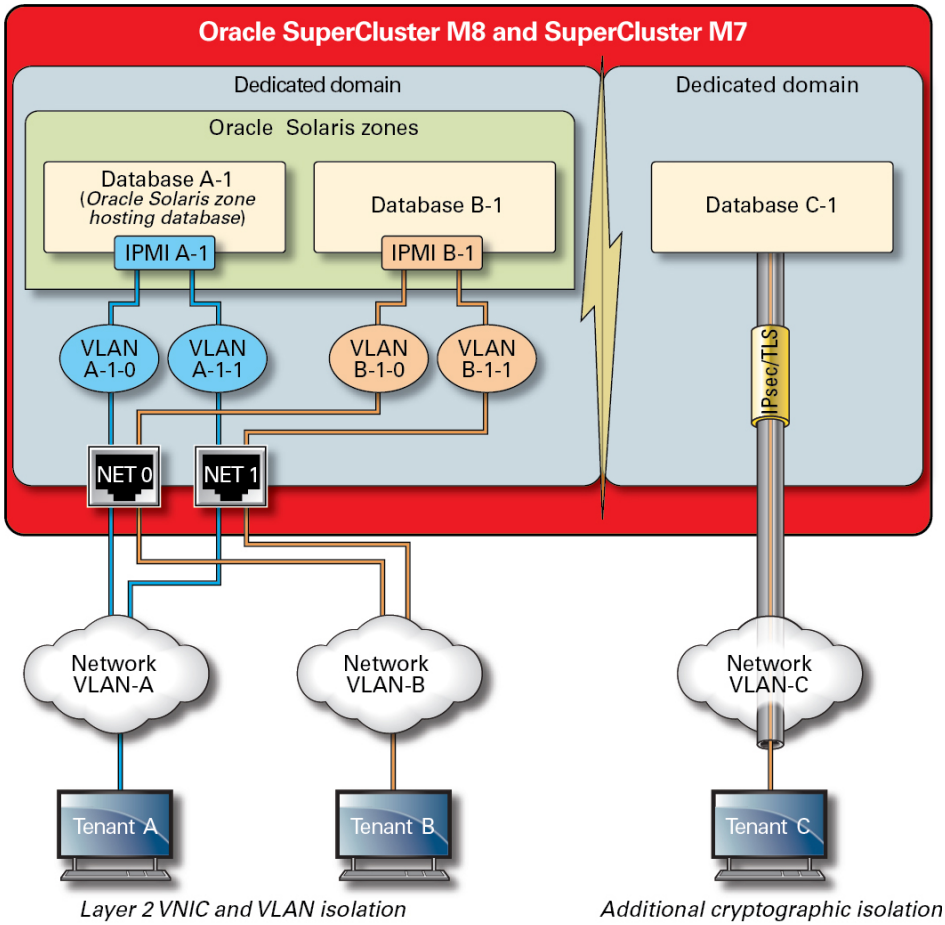
Tenants hosting multiple applications and databases on SuperCluster can also choose to employ a hybrid approach, using a combination of isolation strategies based on Oracle Solaris Zones, I/O domains, and dedicated domains to create flexible yet resilient architectures that align to their cloud infrastructure needs. With a host of virtualization options, SuperCluster enables cloud-hosted tenants to be securely isolated at the hardware layer, and it provides Oracle Solaris Zones for enhanced security and further isolation in the runtime environment.

Ensuring that individual applications, databases, users, and processes are properly isolated on their host OS is a good first step. However, it is equally important to consider the three primary networks used in the SuperCluster and how the network isolation capabilities and communications flowing over the network are protected:

- 10 GbE Client access network
- Private IB service network
- Management network

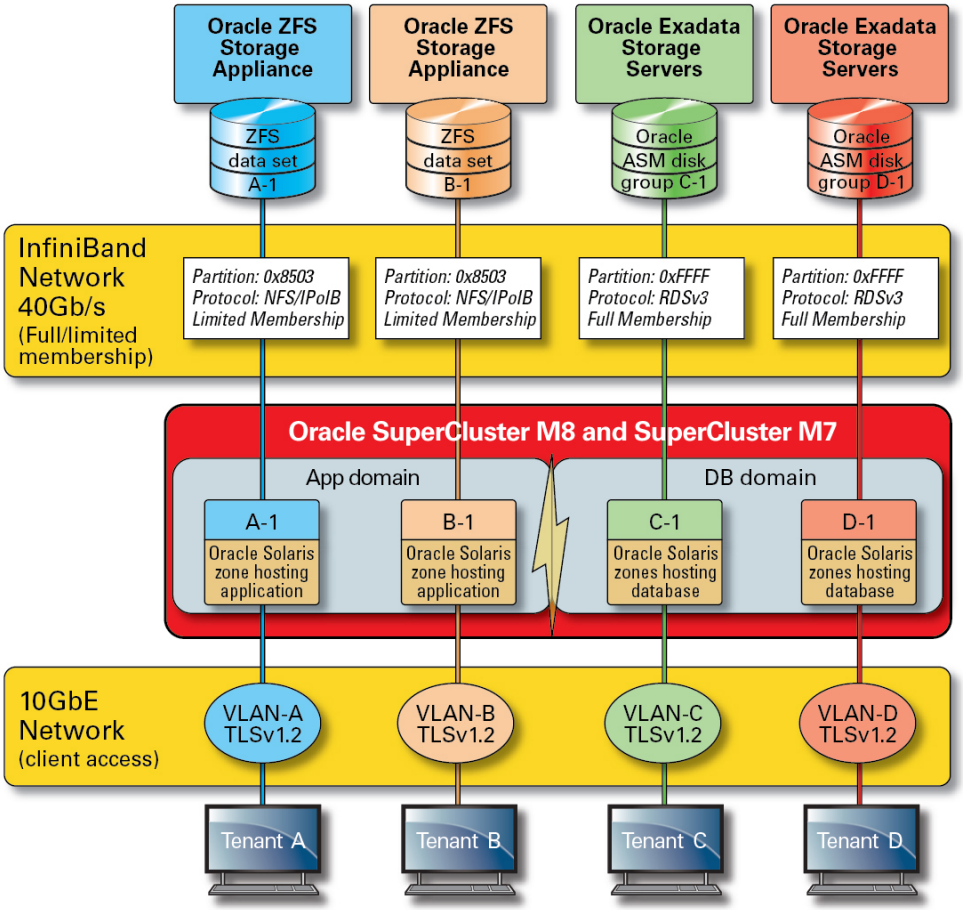
The network traffic flowing over the SuperCluster client access network can be isolated using a variety of techniques. In this figure, one possible configuration is shown in which four database instances are configured to operate on three distinct virtual LANs (VLANs). By configuring the network interfaces of SuperCluster to use VLANs, network traffic can be isolated between Oracle VM Server for SPARC dedicated domains as well as between Oracle Solaris Zones.

FIGURE 2 Secure Network Isolation Over the Client Access Network



SuperCluster includes a private IB network that is used by database instances to access the information stored on the Exadata storage servers and the ZFS storage appliance,and to perform the internal communications needed for clustering and high availability. This illustration shows secure network isolation on SuperCluster M8 and SuperCluster M7.

FIGURE 3 Secure Network Isolation on the 40 Gbs IB Network



By default, the SuperCluster IB network is partitioned into six distinct partitions during installation and configuration. While you cannot change the default partitions, Oracle does support the creation and use of additional dedicated partitions in situations where further segmentation of the IB network is required. In addition, the IB network supports the notion of both limited and full partition membership. Limited members can communicate only with full members, whereas full members can communicate with all nodes on the partition. The application I/O domains and Oracle Solaris 11 Zones can be configured as limited members of their respective IB partitions ensuring that they are able to communicate only with the ZFS

storage appliance, which is configured as a full member, and not with other limited membership nodes that might exist on that same partition.

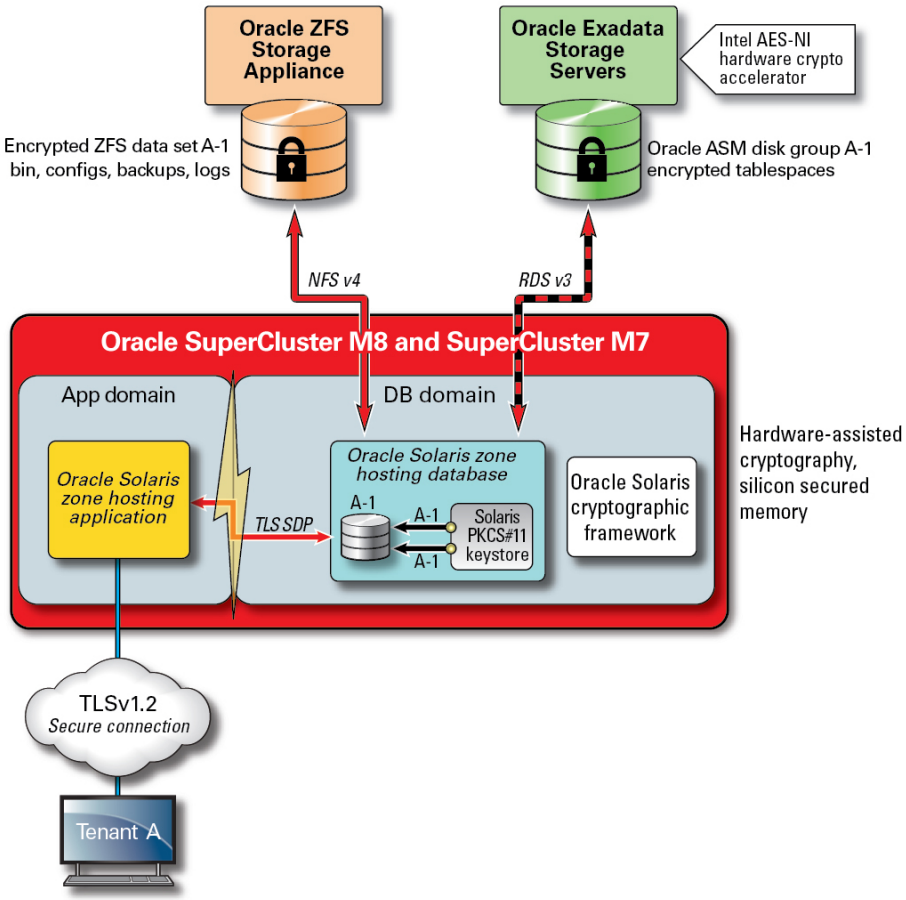
SuperCluster also includes a dedicated management network through which all of its core components can be managed and monitored. This strategy keeps sensitive management and monitoring functions isolated from the network paths that are used to process client requests. By keeping the management functions isolated to this management network, SuperCluster can further reduce the network attack surface that is exposed over the client access and IB networks. Cloud providers are strongly encouraged to follow this recommended practice and isolate management, monitoring, and related functions so they are accessible only from the management network.

Data Protection

For cloud providers, data protection is at the heart of their security strategy. Given the importance of privacy and compliance mandates, organizations considering multitenant architectures should strongly consider the use of cryptography to protect information flowing to and from their databases. The use of cryptographic services for data protection is systemically applied to ensure the confidentiality and integrity of information as it flows across the network and when it resides on disk.

The SPARC M8 and M7 processors in SuperCluster facilitate hardware-assisted, high-performance encryption for the data protection needs of security-sensitive IT environments. The processor also features Silicon Secured Memory technology that ensures the prevention of malicious application-level attacks such as memory scraping, silent memory corruption, buffer overruns, and related attacks.

FIGURE 4 Data Protection Provided by the Hardware-Assisted Cryptographic Acceleration and Memory Intrusion Protection



For secure multitenant architectures, where data protection figures into nearly every aspect of the architecture, SuperCluster and its supporting software enables organizations to meet their security and compliance objectives without having to sacrifice performance. SuperCluster leverages on-core based cryptographic instructions and Silicon Secured Memory capabilities, which are designed into its SPARC M8 or M7 processor for accelerating cryptographic operations and ensuring memory intrusion protection without a performance impact. These capabilities yield improved cryptographic performance and provide memory intrusion checking,

and they also improve overall performance, because more compute resources can be dedicated to servicing tenant workloads.

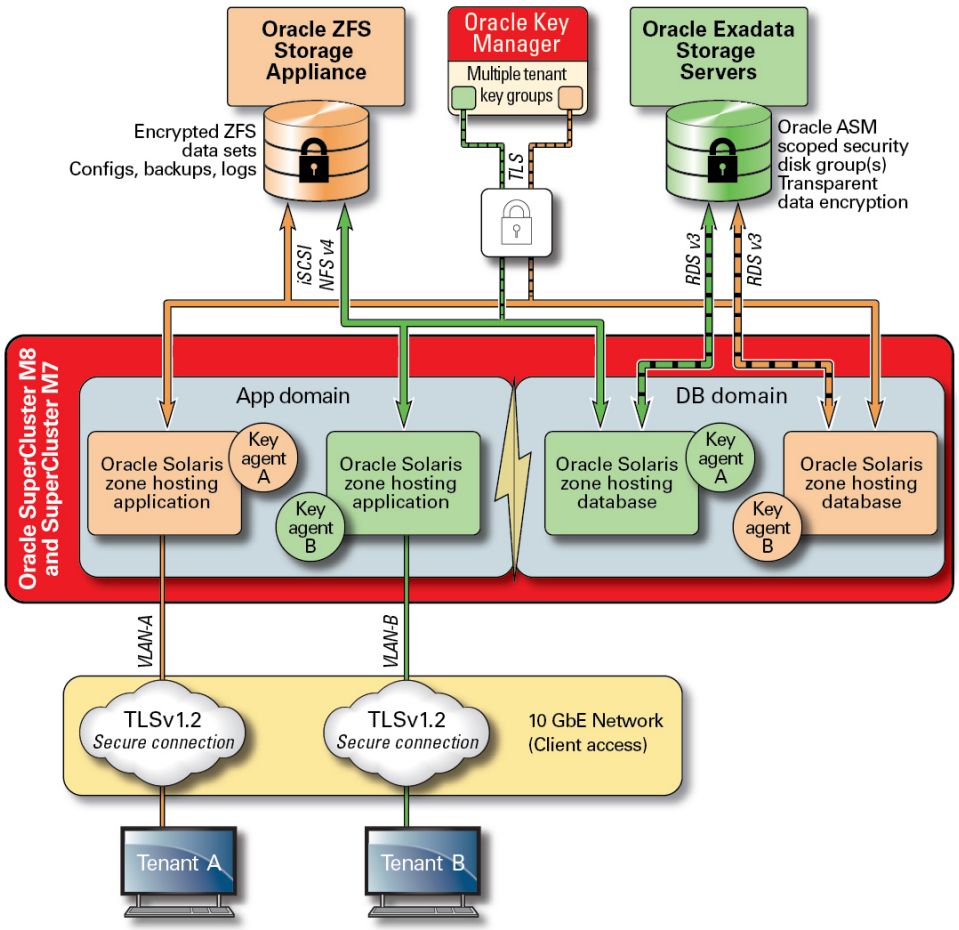
The SPARC processor enables hardware-assisted cryptographic acceleration support for over 16 industry-standard cryptographic algorithms. Together, these algorithms support most modern cryptographic needs including public-key encryption, symmetric-key encryption, random number generation, and the calculation and verification of digital signatures and message digests. In addition, at the OS level, cryptographic hardware acceleration is enabled by default for most core services including Secure Shell, IPSec/IKE, and encrypted ZFS data sets.

Oracle Database and Oracle Fusion Middleware automatically identify the Oracle Solaris OS and the SPARC processor used by SuperCluster. This enables the database and middleware to automatically use the hardware cryptographic acceleration capabilities of the platform for TLS, WS-Security, tablespace encryption operations. It also allows them to use the Silicon Secured Memory feature for ensuring memory protection, and it ensures application data integrity without the need for end-user configuration. To protect the confidentiality and integrity of tenant-specific, interzone, IP-based communications flowing over the IB network use IPSec (IP Security) and IKE (Internet Key Exchange).

Any discussion of cryptography would be incomplete without discussing how encryption keys are managed. Generating and managing encryption keys, especially for large collections of services, has traditionally been a major challenge for organizations, and the challenges grow even more significant in the case of a cloud-based multitenant environment. On SuperCluster, ZFS data set encryption and Oracle Database Transparent Data Encryption can leverage an Oracle Solaris PKCS#11 keystore to securely protect the master key. Using the Oracle Solaris PKCS#11 keystore automatically engages the SPARC hardware-assisted cryptographic acceleration for any master key operations. This allows SuperCluster to significantly improve the performance of the encryption and decryption operations associated with encryption of ZFS data sets, Oracle Database tablespace encryption, encrypted database backups (using Oracle Recovery Manager [Oracle RMAN]), encrypted database exports (using the Data Pump feature of Oracle Database), and redo logs (using Oracle Active Data Guard).

Tenants using a shared-wallet approach can leverage ZFS storage appliance to create a directory that can be shared across all the nodes in a cluster. Using a shared, centralized keystore can help tenants better manage, maintain, and rotate the keys in clustered database architectures such as Oracle Real Application Clusters (Oracle RAC), because the keys will be synchronized across each of the nodes in the cluster.

FIGURE 5 Data Protection Through a Multitenant Key-Management Scenario Using Oracle Key Manager



To address key management complexities and issues associated with multiple hosts and applications in a cloud-based multitenant environment, use the optional Oracle Key Manager as an appliance integrated into the management network. Oracle Key Manager centrally authorizes, secures, and manages access to encryption keys used by Oracle Database, Oracle Fusion applications, Oracle Solaris, and the ZFS storage appliance. Oracle Key Manager also supports Oracle's StorageTek encrypting tape drives. Having the encryption policy and key

management at the ZFS data set (file system) level delivers assured deletion of tenant file systems through key destruction.

Oracle Key Manager is a complete key management appliance that supports life-cycle key management operations and trusted key storage. When configured with an additional Sun Crypto Accelerator 6000 PCIe Card from Oracle, Oracle Key Manager offers FIPS 140-2 Level 3 certified key storage of AES 256-bit encryption keys as well as FIPS 186-2–compliant random number generation. Within SuperCluster, all database and application domains, including their global zones and non-global zones, can be configured to use Oracle Key Manager for managing keys associated with applications, databases, and encrypted ZFS data sets. In fact, Oracle Key Manager is able to support key management operations associated with individual or multiple database instances, Oracle RAC, Oracle Active Data Guard, Oracle RMAN, and the Data Pump feature of Oracle Database.

Finally, separation of duties, enforced by Oracle Key Manager, enables each tenant to maintain complete control over its encryption keys with consistent visibility into any key management operations. Given how important keys are for the protection of information, it is critical that tenants implement the necessary levels of role-based access control and auditing to ensure that keys are properly safeguarded throughout their lifetime.

Related Information

- “Oracle Key Manager” on page 124

Access Control

For organizations adopting a cloud-hosted environment strategy, access control is one of the most critical challenges to be solved. Tenants must have confidence that information stored on the shared infrastructure is protected and available only to authorized hosts, services, individuals, groups, and roles. Authorized hosts, individuals, and services must further be constrained, in accordance with the principle of least privilege, such that they have only the rights and privileges needed for a particular operation.

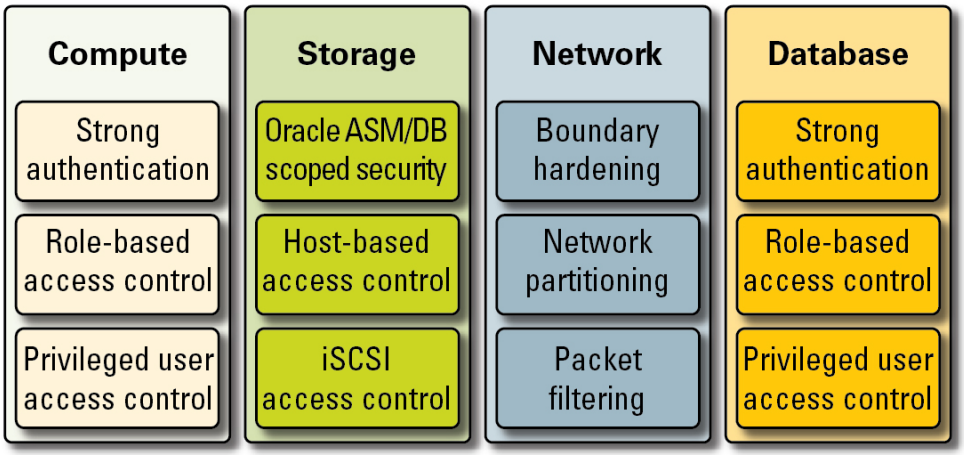
SuperCluster facilitates a flexible, layered access control architecture covering every layer of the stack and supporting a variety of roles including end users, database administrators, and system administrators. This enables organizations to define policies that protect hosts, applications, and databases individually and to protect the underlying compute, storage, and network infrastructure on which those services run.

At the virtualization and OS layers, access control begins with reducing the number of services exposed on the network. This helps to control access to Oracle VM Server for SPARC consoles,

domains, and zones. By reducing the number of entry points through which systems can be accessed, the number of access control policies can also be reduced and more easily maintained over the life of the system.

Within the Oracle Solaris OS, access controls are implemented using a combination of POSIX permissions along with the Oracle Solaris role-based access control (RBAC) facility. Equally important is the ability to protect the hosts, applications, databases, and related services running on SuperCluster from network-based attacks. To do this, tenants should first verify that only approved network services are running and listening for incoming network connections. Once the network attack surface has been minimized, tenants then configure the remaining services such that they are listening for incoming connections only on approved networks and interfaces. This simple practice will help ensure that management protocols, such as Secure Shell, are not accessible from anywhere other than the management network.

FIGURE 6 Summary of End-to-End Access Control



In addition, tenants can also choose to implement a host-based firewall such as the IP Filter service of Oracle Solaris. Host-based firewalls are useful because they provide hosts with a more feature-rich way of controlling access to network services. For example, IP Filter supports stateful packet filtering, and it can filter packets by IP address, port, protocol, network interface, and traffic direction. These capabilities are important for platforms such as SuperCluster that operate many network interfaces and support a variety of inbound and outbound network communications.

On SuperCluster, IP Filter can be configured inside an Oracle VM Server for SPARC domain or operated from within an Oracle Solaris Zone. This allows network access control policy to

be enforced in the same OS container in which database services are offered. In a multitenant scenario, the amount of outbound network activity will likely be minimal and can easily be categorized so that a policy can be created that limits communications to specific network interfaces and destinations. All other traffic would be denied and logged as part of a “default deny” policy to block unauthorized communications, both inbound and outbound.

Oracle end user security allows tenants to integrate their applications and databases with their existing identity management services in order to support single sign-on (SSO) and centralized user and role management. Specifically, Oracle End User Security helps by centralizing (1) provisioning and deprovisioning of database users and administrators, (2) password management and self-service password reset, and (3) management of authorizations using global database roles. Organizations requiring multi-factor authentication methods, such as Kerberos or PKI, can leverage Oracle Advanced Security.

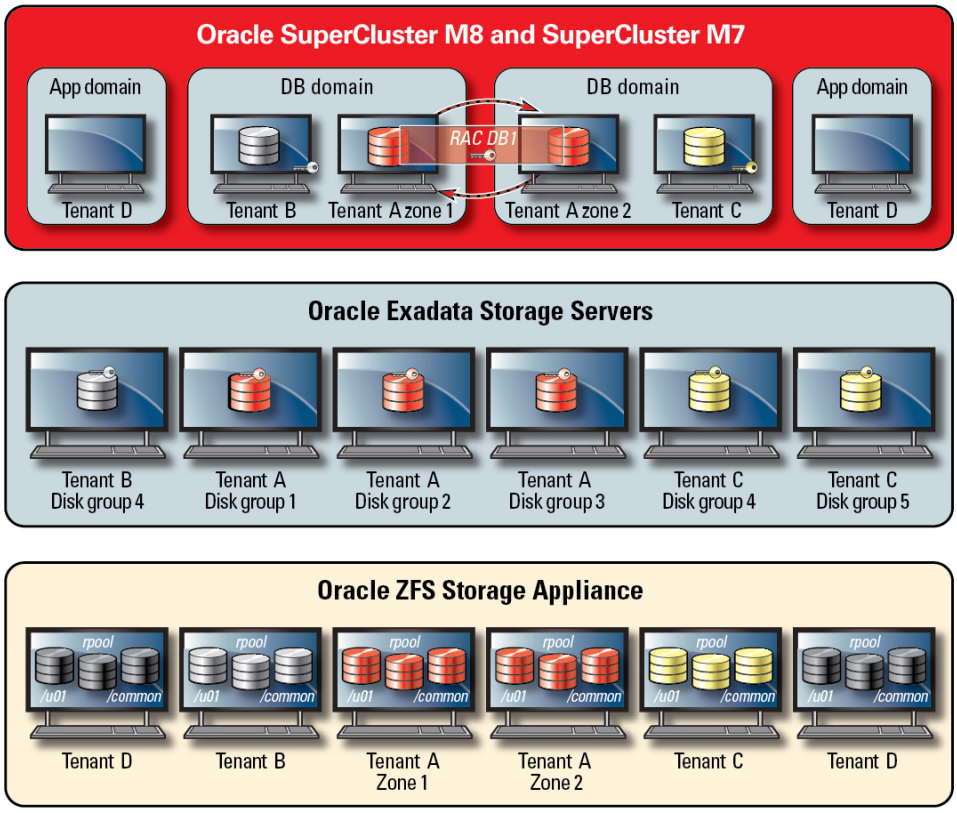
Oracle Exadata Storage Server technology supports a predefined set of user accounts, each with distinct privileges. Administrators performing Oracle Exadata Storage Server administration must use one of these predefined roles to access the system. ZFS storage appliance, on the other hand, supports the creation of local and remote administrative accounts, both of which are capable of supporting the individual assignment of roles and privileges.

By default, the Oracle Exadata Storage Servers used in SuperCluster are accessed by the database domains using the Oracle Automatic Storage Management facility. This facility allows cloud providers to create distinct disk groups for each tenant that are capable of satisfying their capacity, performance, and availability requirements. In terms of access control, Oracle Automatic Storage Management supports three access control modes: open security, Oracle Automatic Storage Management–scoped security, and database-scoped security.

In a multitenant scenario, database-scoped security is recommended, because it offers the most fine-grained level of access control. In this mode, it is possible to configure disk groups such that they can be accessed by only a single database. Specifically, this means that both database administrators and users can be limited to accessing only those grid disks that contain information for which they have access privileges. In database consolidation scenarios in which individual databases might be supporting different organizations or tenants, it is important that each tenant be able to access and manipulate only their own storage. In particular, when combined with the workload and database isolation strategies discussed earlier, it is possible for tenants to effectively compartmentalize access to individual databases.

Database-scoped security is an effective tool for limiting access to Oracle ASM grid disks. This figure shows Oracle ASM–scoped security along with ZFS security. In situations where there are large numbers of Oracle Database instances being deployed on the SuperCluster platform, a per-tenant Oracle ASM–scoped security strategy might make more sense, because it significantly reduces the number of keys that have to be created, assigned, and managed. Further, because database-scoped security requires separate disk groups to be created for each database, this approach will also significantly reduce the number of separate grid disks that have to be created on an Exadata Storage Server.

FIGURE 7 Per-Tenant Oracle ASM-Scoped Security



SuperCluster leverages Oracle Solaris data link protection, which seeks to prevent the potential damage that can be caused by malicious tenant virtual machines to the network. This integrated Oracle Solaris feature offers protection against the following basic threats: IP and MAC address spoofing as well as L2 frame spoofing (for example, Bridge Protocol Data Unit attacks). Oracle Solaris data link protection must be applied individually to all Oracle Solaris non-global zones deployed within the multitenant environment.

Because individual tenants should never require administrative or host-level access to the Exadata Storage Servers, it is strongly recommended that such access be restricted. The Exadata Storage Servers should be configured to prevent direct access for tenant non-global zones and database I/O domains while still permitting access from SuperCluster database domains

(which are operated by the cloud provider). This ensures that the Exadata Storage Servers can be managed only from trusted locations on the management network.

Once the security configuration of the tenants has been defined and implemented, service providers can consider the additional step of configuring tenant-specific global and non-global zones to be immutable as read-only environments. Immutable zones create a resilient, high-integrity operating environment within which tenants may operate their own services. Building upon the inherent security capabilities of Oracle Solaris, immutable zones ensure that some (or all) OS directories and files are unable to be changed without intervention by the cloud service provider. The enforcement of this read-only posture helps to prevent unauthorized changes, promote stronger change management procedures, and deter the injection of both kernel and user-based malware.

Monitoring and Compliance Auditing

Proactive monitoring and logging in a cloud environment is very important and in many cases helps mitigate attacks originating from security loopholes and vulnerabilities. Whether for compliance reporting or incident response, monitoring and auditing is a critical function for the cloud provider, and tenant organizations must enforce a well-defined logging and auditing policy to gain increased visibility into their hosting environment. The degree to which monitoring and auditing is employed is often based upon the risk or criticality of the environment being protected.

The SuperCluster cloud architecture relies on the use of the Oracle Solaris audit subsystem to collect, store, and process audit event information. Each tenant-specific non-global zone will generate audit records that are stored locally to each of the SuperCluster dedicated domains (global zone). This approach will ensure that individual tenants are not able to alter their auditing policies, configurations, or recorded data, because that responsibility belongs to the cloud service provider. The Oracle Solaris auditing functionality monitors all administrative actions, command invocations, and even individual kernel-level system calls in both tenant zones and domains. This facility is highly configurable, offering global, per-zone, and even per-user auditing policies. When configured to use tenant zones, audit records for each zone can be stored in the global zone to protect them from tampering. Dedicated domains and I/O domains also leverage the native Oracle Solaris auditing facility to record actions and events associated with virtualization events and domain administration.

The Python programming language is used to create SuperCluster-specific utilities such as the SuperCluster Virtual Assistant. The SuperCluster 2020 Q2 Quarterly Patch Update provides utilities that are based on Python 3. Prior to the 2020 Q2 update, the utilities were developed using Python 2. To determine your SuperCluster software version, see “Determine the SuperCluster Software Version” on page 56.

Exadata Storage Servers and ZFS storage appliance support login, hardware, and configuration auditing. This enables organizations to determine who accessed a device and what actions were taken. While not directly exposed to the end user, Oracle Solaris auditing provides the underlying content for information presented by ZFS storage appliance.

Similarly, the Exadata Storage Server audit is a rich collection of system events that can be used along with hardware and configuration alert information provided by Exadata Storage Server Software. With the IP Filter capability of Oracle Solaris, the cloud provider can selectively record both inbound and outbound network communications, and the capability can be applied at the level of both the domain and non-global zone. This helps organizations segment their network policies and verify activity records. Optionally, the Oracle Audit Vault and Database Firewall appliance can be deployed to securely aggregate and analyze audit information from a variety of Oracle and non-Oracle databases as well as audit information from Oracle Solaris.

Through integration with Oracle Enterprise Manager, SuperCluster is able to support a variety of cloud self-service operations. Cloud providers can define pools of resources, assign pools and quota to individual tenants, identify and publish service catalogs, and ultimately support the monitoring and logging of application and database resources.

Related Information

- “Auditing for Compliance” on page 117
- “Monitoring Security” on page 127

Additional Resources for SuperCluster Security Best Practices

For additional information about SuperCluster security, architecture, and best practices, refer to these resources:

- Oracle SuperCluster M8 Security Technical Implementation Guide (STIG) Validation and Best Practices

  https://docs.oracle.com/cd/E58626_01/pdf/E94758.pdf
- Oracle SuperCluster M7 Security Technical Implementation Guide (STIG) Validation and Best Practices

  https://community.oracle.com/docs/DOC-997077
- Oracle SuperCluster M7 - Secure Private Cloud Architecture

  http://www.oracle.com/technetwork/server-storage/engineered-systems/oracle-supercluster/documentation/supercluster-secure-multi-tenancy-2734706.pdf

- Comprehensive Data Protection on Oracle SuperCluster

  https://community.oracle.com/docs/DOC-918251
- Secure Database Consolidation on Oracle SuperCluster

  http://www.oracle.com/technetwork/server-storage/sun-sparc-enterprise/documentation/o13-053-securedb-osc-t5-8-1990064.pdf
- Oracle SuperCluster and PCI Compliance

  http://www.oracle.com/technetwork/server-storage/engineered-systems/sparc-supercluster/supercluster-pci-dss-compliance-2372543.pdf
- Oracle Solaris 11 Security Compliance Guides
  - Oracle Solaris 11.4 Compliance Guide
  - Oracle Solaris 11.3 Security Compliance Guide

  https://docs.oracle.com/cd/E36784_01/html/E36855/index.html
- Oracle Solaris 11 Audit Quick Start

  https://www.oracle.com/technical-resources/articles/solaris11/sol-audit-quick-start.html
- Oracle Solaris 11 Security Guidelines

  http://docs.oracle.com/cd/E53394_01/html/E54807/index.html
- Oracle Database Security Guide 12c Release 1 (12.1)

  http://docs.oracle.com/database/121/DBSEG/toc.htm

Reviewing the Default Security Configuration

These topics describe the default security configuration for SuperCluster M8 and SuperCluster M7:

Default Security Settings

SuperCluster M8 and SuperCluster M7 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.

Default User Accounts and Passwords

This table lists the default user accounts and passwords for SuperCluster M8 and SuperCluster M7. Additional instructions for changing the passwords is provided in subsequent chapters for each component.

Component	User Name	Password	User Account and Password Information
Oracle ILOM on: ■ SPARC M8 and M7 servers ■ Exadata Storage Servers ■ ZFS storage appliance	■ `root`	`welcome1`	Refer to the Oracle ILOM documentation at `http://docs.oracle.com/cd/E24707_01/html/E24528`.
SPARC M8 and SPARC M7 servers	■ `root` ■ `oracle` ■ `grid`	`welcome1` `welcome1` `welcome1`	See "Log into a Compute Server" on page 55. Also refer to these resources: ■ **Oracle Solaris 11.4** – Refer to the security documentation at `https://docs.oracle.com/cd/E37838_01/index.html`. ■ **Oracle Solaris 11.3** – Refer to the security documentation at `http://docs.oracle.com/cd/E53394_01/index.html`. ■ **Oracle Solaris 10** – Refer to security documentation at `https://docs.oracle.com/cd/F24622_01/index.html`.

Exadata storage servers	■ `root`
	■ `celladmin`
	■ `cellmonitor`
		`welcome1`
		`welcome`
		`welcome`
			See "Change Storage Server Passwords" on page 92.

Oracle ZFS Storage ZS3-ES and Oracle ZFS Storage ZS5-ES	■ `root`	`welcome1`	See "Change the ZFS Storage Appliance `root` Password" on page 82.
InfiniBand switches	■ `root` ■ `nm2user`	`welcome1` changeme	See "Change `root` and `nm2user` Passwords" on page 106. Also refer to the *Sun Datacenter InfiniBand Switch 36 HTML Document Collection for Firmware Version 2.1* at `http://docs.oracle.com/cd/E36265_01`.
InfiniBand Oracle ILOM	■ `ilom-admin` ■ `ilom-operator`	ilom-admin ilom-operator	See "Change IB Switch Passwords (Oracle ILOM)" on page 107. Also refer to the InfiniBand documentation at `http://docs.oracle.com/cd/E36265_01`

Component	User Name	Password	User Account and Password Information
Ethernet management switch	■ `admin`	`welcome1`	See “Change the Ethernet Switch Password” on page 114
Oracle I/O Domain Creation tool	■ `admin`	welcome1	Refer to the *Oracle I/O Domain Administration Guide*.
Oracle Engineered Systems Hardware Manager	■ `admin` ■ service	welcome1 welcome1	See “Oracle Engineered Systems Hardware Manager” on page 125. Also refer to the *Oracle I/O Domain Administration Guide*.

Note - When the `root` or `admin` password for this component is changed, it must also be changed in the Oracle Engineered Systems Hardware Manager. Refer to the *Oracle SuperCluster M8 and SuperCluster M7 Administration Guide* for instructions. See also “Passwords Known by Oracle Engineered Systems Hardware Manager” on page 33.

Passwords Known by Oracle Engineered Systems Hardware Manager

Oracle Engineered Systems Hardware Manager must be configured with the accounts and passwords for the components in this table.

Note - Oracle Engineered Systems Hardware Manager does not need to know the passwords for any logical domains or zones.

Component	Account
All Oracle ILOMs	`root`
Exadata storage servers OS	`root`
ZFS storage controllers OS	`root`
IB switches	`root`
Ethernet management switch	`admin`
PDUs	`admin`

For more information about Oracle Engineered Systems Hardware Manager, see "Oracle Engineered Systems Hardware Manager" on page 125 and refer to the *Oracle SuperCluster M8 and SuperCluster M7 Administration Guide*.

Securing the Hardware

These sections describe security guidelines for securing the hardware:

Access Restrictions

- Install Oracle SuperCluster M8 and SuperCluster M7 systems 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 FRUs (field-replaceable units) or CRUs (customer-replaceable units) 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 (power distribution units), and network switches can have USB connections. Restricting physical access is a more secure method of accessing a component, because it is not susceptible to network-based attacks.

Serial Numbers

- Record the serial numbers of the components in SuperCluster M8 and SuperCluster M7 systems.
- Security-mark all significant items of computer hardware, such as replacement parts. Use special ultraviolet pens or embossed labels.
- Keep records of 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 `format` command, to completely erase all data from the drive. For more information, refer to the Oracle Solaris `format(1M)` man page.
- 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. For more information, 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.

OpenBoot

By default, the SPARC M8 and M7 OpenBoot are not password-protected. You can enhance the security of the system by restricting access to the OpenBoot by performing these actions:

- Implement password protection.
- Check for failed OpenBoot logins.

- Provide an OpenBoot power-on banner.

Additional Hardware Resources

All of the security principles that are outlined in the *SPARC M8 and SPARC M7 Servers Security Guide* (available at https://docs.oracle.com/cd/E55211_01) apply to the SPARC M7 and SPARC M8 servers in SuperCluster.

Securing Oracle ILOM

Oracle ILOM provides advanced service processor hardware and software that is used to manage and monitor Oracle SuperCluster components including the compute servers, storage servers, ZFS storage appliance, and IB switches.

Oracle ILOM enables you to actively manage and monitor the underlying servers and devices independently of the OS state, providing a reliable lights out management capability.

To fully secure Oracle ILOM on SuperCluster M8 and SuperCluster M7, you must apply configuration settings to all the Oracle ILOM enabled components individually. These components have Oracle ILOM:

- Compute servers
- Storage servers
- ZFS storage appliance
- IB switches

Perform these tasks to secure Oracle ILOM:

▼ Log in to the Oracle ILOM CLI

1. **On the management network, log into Oracle ILOM.**

   In this example, replace *ILOM_SP_ipaddress* with the IP address of Oracle ILOM for the component you want to access:

- Compute servers
- Storage servers
- ZFS storage appliance
- IB switches

IP addresses for your configuration are listed in the Deployment Summary provided by Oracle personnel.

```
% ssh root@ILOM_SP__ipaddress
Enter the Oracle ILOM root password.
```

2. **See “Default User Accounts and Passwords” on page 32.**

▼ Determine the Oracle ILOM Version

To leverage the most recent features, capabilities and security enhancements, update the Oracle ILOM software to the latest supported version.

1. **On the management network, log into Oracle ILOM.**

   See “Log in to the Oracle ILOM CLI” on page 39.

2. **Display the Oracle ILOM version.**

   In this example, the Oracle ILOM software is version 3.2.4.1.b.

```
-> version
SP firmware 3.2.4.1.b
SP firmware build number: 94529
SP firmware date: Thu Nov 13 16:41:19 PST 2014
SP filesystem version: 0.2.10
```

Note - To update the version of Oracle ILOM on any of the SuperCluster components, install the most recent SuperCluster Quarterly Full Stack Download Patch available from My Oracle Support.

Note - Oracle Engineered Systems such as SuperCluster are restricted in what versions of the Oracle ILOM that can be used and how those versions are updated. For further details, contact your Oracle representative.

(If Required) Enable FIPS-140 Compliant Operation (Oracle ILOM)

The use of FIPS 140 validated cryptography is required for U.S. Federal Government customers.

By default, Oracle ILOM does not operate using FIPS 140 validated cryptography. However, the use of FIPS 140 validated cryptography can be enabled, if required.

Some Oracle ILOM features and capabilities are not available when configured for FIPS 140 compliant operation. A list of those features is covered in the *Oracle ILOM Security Guide* in the section titled "Unsupported Features When FIPS Mode Is Enabled" (see "Additional Oracle ILOM Resources" on page 53).

Also see "FIPS-140-2 Level 1 Compliance" on page 120.

Caution - This task requires you to reset Oracle ILOM. A reset results in the loss of all user-configured settings. For this reason, you must enable FIPS 140 compliant operation before any additional site-specific changes are made to the Oracle ILOM. For systems where site-specific configuration changes have been made, back up the Oracle ILOM configuration so that it can be restored after Oracle ILOM is reset, otherwise those configuration changes will be lost.

1. **On the management network, log into Oracle ILOM.**

   See "Log in to the Oracle ILOM CLI" on page 39.

2. **Determine if the Oracle ILOM is configured for FIPS 140 compliant operation.**

```
-> show /SP/services/fips state status
/SP/services/fips
Properties:
state = enabled
status = enabled
```

   FIPS 140 compliant mode in Oracle ILOM is represented by the `state` and `status` properties. The `state` property represents the configured mode in Oracle ILOM, and the `status` property represents the operational mode in Oracle ILOM. When the FIPS `state` property is changed, the change does not affect the operational mode FIPS `status` property until the next Oracle ILOM reboot.

3. **Enable FIPS 140 compliant operation.**

```
-> set /SP/services/fips state=enabled
```

4. **Restart the Oracle ILOM service processor.**

   The Oracle ILOM SP must be restarted for this change to take effect.

   ```
   -> reset /SP
   ```

Default Exposed Network Services (Oracle ILOM)

This table lists the default network services that re exposed by Oracle ILOM.

For additional information about these services, refer to the *Oracle ILOM Security Guide* (see "Additional Oracle ILOM Resources" on page 53).

Service Name	Protocol	Port	Description
SSH	TCP	22	Used by the integrated Secure Shell service to enable administrative access to Oracle ILOM using a CLI.
HTTP (BUI)	TCP	80	Used by the integrated HTTP service to enable administrative access to Oracle ILOM using a browser interface. While TCP/80 is typically used for clear-text access, by default Oracle ILOM automatically redirects incoming requests to the secure version of this service running on TCP/443.
NTP	UDP	123	Used by the integrated Network Time Protocol (NTP) (client only) service used to synchronize the local system clock to one or more external time sources.
SNMP	UDP	161	Used by the integrated SNMP service to provide a management interface to monitor the health of Oracle ILOM and to monitor received trap notifications.
HTTPS (BUI)	TCP	443	Used by the integrated HTTPS service to enable administrative access to Oracle ILOM over an encrypted (SSL/TLS) channel using a browser interface.
IPMI	TCP	623	Used by the integrated Intelligent Platform Management Interface (IPMI) service to provide a computer interface for various monitoring and management functions. This service should not be disabled, because it is used by Oracle Enterprise Manager Ops Center to collect hardware inventory data, FRU descriptions, hardware sensor information, and hardware component status information.
Remote KVMS	TCP	5120 5121 5123 5555 5556 7578 7579	Collectively, the remote KVMS ports provide a set of protocols that provide remote keyboard, video, mouse, and storage capabilities that can be used with the Oracle Integrated Lights Out Manager.
ServiceTag	TCP	6481	Used by the Oracle ServiceTag service. This is an Oracle discovery protocol used to identify servers and facilitate service requests. This service is used by products such as Oracle Enterprise Manager Ops Center to discover Oracle ILOM software and to integrate with other Oracle automatic service solutions.

Service Name	Protocol	Port	Description
WS-Man over HTTPS	TCP	8888	Used by the integrated WS-Man service to provide a standards-based, web-services interface that is used to manage the Oracle ILOM over the HTTPS protocol. Disabling this service prevents Oracle ILOM from being managed using this protocol. This service is no longer included as of Oracle ILOM version 3.2.
WS-Man over HTTP	TCP	8889	This port is used by the integrated WS-Man service to provide a standards-based, web-services interface that is used to manage the Oracle ILOM over the HTTP protocol. Disabling this service will prevent the Oracle ILOM from being managed using this protocol. This service is no longer included as of Oracle ILOM version 3.2.
Single Sign-On	TCP	11626	This port is used by the integrated Single Sign-On feature that reduces the number of times a user has to enter a user name and password. Disabling this service prevents launching KVMS without having to reenter a password.

Hardening the Oracle ILOM Security Configuration

These topics describe how to secure Oracle ILOM through various configuration settings.

▼ Disable Unnecessary Services (Oracle ILOM)

Disable any services that are not required to support the operational and management requirements of the platform.

By default, Oracle ILOM employs a network secure-by-default configuration whereby nonessential services are already disabled. However, based on your security policies and requirements, it might be necessary to disable additional services.

1. **On the management network, log in to Oracle ILOM.**
   See "Log in to the Oracle ILOM CLI" on page 39.

2. **Determine the list of service supported by Oracle ILOM.**

   ```
   -> show /SP/services
   ```

3. **Determine if a given service is enabled.**
   Replace *servicename* with the name of the service identified in Step 2.

   ```
   -> show /SP/services/servicename servicestate
   ```

   While the majority of services recognize and use the `servicestate` parameter to record whether the service is enabled or disabled, there are a few services, such as `servicetag`, `ssh`, `sso`, and `wsman`, that use a parameter called `state`. Regardless of the actual parameter used, a service is enabled if the `servicestate` or `state` parameter returns a value of `enabled`, as shown in these examples:

   ```
   -> show /SP/services/https servicestate
   /SP/services/https
   Properties:
   servicestate = enabled

   -> show /SP/services/ssh state
   /SP/services/ssh
   Properties:
   state = enabled
   ```

4. **To disable a service that is not required, set the service state to `disabled`.**

   ```
   -> set /SP/services/http servicestate=disabled
   ```

5. **Determine if any of these services should be disabled.**
   Depending on the tools and methods used, these additional services can be disabled if they are not required or used:

   - **For a browser administrative Interface (HTTP, HTTPS), type:**

     ```
     -> set /SP/services/http servicestate=disabled
     -> set /SP/services/http secureredirect=disabled
     -> set /SP/services/https servicestate=disabled
     ```

   - **For the keyboard, video, mouse service (KVMS), type:**

     ```
     -> set /SP/services/kvms servicestate=disabled
     ```

   - **For Web services management (WS-Man over HTTP/HTTPS) - (Oracle ILOM version 3.1 and older), type:**:

```
-> set /SP/services/wsman state=disabled
```

- **For Single-Sign On services (SSO), type:**

```
-> set /SP/services/sso state=disabled
```

▼ Configure HTTP Redirection to HTTPS (Oracle ILOM)

By default, the Oracle ILOM is configured to redirect incoming HTTP requests to the HTTPS service to ensure that all of the browser-based communications are encrypted between Oracle ILOM and the administrator.

1. **On the management network, log in to Oracle ILOM.**
   See "Log in to the Oracle ILOM CLI" on page 39.

2. **Verify that secure redirection is enabled.**

```
-> show /SP/services/http secureredirect
/SP/services/https
Properties:
secureredirect = enabled
```

3. **If the default has been changed, you can enable secure redirection.**

```
-> set /SP/services/http secureredirect=enabled
```

4. **Verify the setting by repeating Step 2.**

Disable Unapproved Protocols

Use these topics to disable unapproved protocols:

▼ Disable the SSLv2 Protocol for HTTPS

By default, the SSLv2 protocol is disabled for the HTTPS service.

For security purposes it is very important that SSLv2 is disabled.

1. **On the management network, log in to Oracle ILOM.**
   See "Log in to the Oracle ILOM CLI" on page 39.

2. **Determine if the SSLv2 protocol is disabled for the HTTP service.**

```
-> show /SP/services/https sslv2
/SP/services/https
Properties:
sslv2 = disabled
```

3. **If the service is enabled, disable the SSLv2 protocol.**

```
-> set /SP/services/https sslv2=disabled
```

4. **Verify the setting by repeating Step 2.**

▼ Disable the SSLv3 Protocol for HTTPS

By default, the SSLv3 protocol is enabled for the HTTPS service.

For security purposes, disable the SSLv3 protocol.

1. **On the management network, log into Oracle ILOM.**
   See "Log in to the Oracle ILOM CLI" on page 39.

2. **Determine if the SSLv3 protocol is disabled for the HTTP service.**

```
-> show /SP/services/https sslv3
/SP/services/https
Properties:
sslv3 = enabled
```

3. **Disable the SSLv3 protocol.**

```
-> set /SP/services/https sslv3=disabled
```

4. **Verify the setting by repeating Step 2.**

▼ Disable Unapproved TLS Protocols for HTTPS

By default, the TLSv1.0, TLSv1.1, and TLSv1.2 protocols are enabled for the HTTPS service.

You can disable one or more TLS protocol versions that do not comply with your security policies.

For security purposes, use TLSv1.2 unless support for older versions of the TLS protocol is required.

1. **On the management network, log in to Oracle ILOM.**
   See "Log in to the Oracle ILOM CLI" on page 39.

2. **Determine the list of TLS protocol versions that are enabled for the HTTPS service.**

```
-> show /SP/services/https tlsv1 tlsv1_1 tlsv1_2
/SP/services/https
Properties:
tlsv1 = enabled
tlsv1_1 = enabled
tlsv1_2 = enabled
```

3. **Disable TLSv1.0.**

```
-> set /SP/services/https tlsv1_0=disabled
```

4. **Disable TLSv1.1.**

```
-> set /SP/services/https tlsv1_1=disabled
```

5. **Verify the setting by repeating Step 2.**

▼ Disable SSL Weak and Medium-Strength Ciphers for HTTPS

By default, Oracle ILOM disables the use of weak and medium-strength ciphers for the HTTPS service.

1. **On the management network, log in to Oracle ILOM.**
   See "Log in to the Oracle ILOM CLI" on page 39.

2. **Determine if weak and medium-strength ciphers are disabled.**

```
-> show /SP/services/https weak_ciphers
/SP/services/https
Properties:
weak_ciphers = disabled
```

3. **If the default has been changed, you can disable the use of weak and medium-strength ciphers.**

```
-> set /SP/services/https weak_ciphers=disabled
```

4. **Verify the setting by repeating Step 2.**

▼ Disable Unapproved SNMP Protocols (Oracle ILOM)

By default, only the SNMPv3 protocol is enabled for the SNMP service that is used to monitor and manage the Oracle ILOM. Ensure that older versions of the SNMP protocol remain disabled unless required.

Some Oracle and third-party products are limited in their support for newer SNMP protocol versions. Refer to the product documentation associated with those components to confirm their support for specific SNMP protocol versions. Ensure that Oracle ILOM is configured to support any protocol versions required by those components.

Note - Version 3 of the SNMP protocol introduced support for the User-based Security Model (USM). This functionality replaces the traditional SNMP community strings with actual user accounts that can be configured with specific permissions, authentication, and privacy protocols, and passwords. By default, Oracle ILOM does not include any USM accounts. Configure SNMPv3 USM accounts based upon your own deployment, management, and monitoring requirements.

---

1. **On the management network, log into Oracle ILOM.**
See “Log in to the Oracle ILOM CLI” on page 39.

2. **Determine the status of each of the SNMP protocols.**

```
-> show /SP/services/snmp v1 v2c v3
/SP/services/snmp
Properties:
v1 = disabled
```

```
v2c = disabled
v3 = enabled
```

3. **If needed, disable SNMPv1 and SNMPv2c.**

```
-> set /SP/services/snmp v1=disabled
-> set /SP/services/snmp v2c=disabled
```

4. **Verify the setting by repeating Step 2.**

▼ Configure SNMP v1 and v2c Community Strings (Oracle ILOM)

This task is only applicable if SNMP v1 or SNMPv2c is enabled and configured for use.

For SNMP to operate correctly, a client and server must agree on the community string that is used to authenticate access. Therefore, when changing SNMP community strings, ensure that the new string is configured on both Oracle ILOM and for all components that will attempt to connect with Oracle ILOM using the SNMP protocol.

Because SNMP is often used to monitor the health of the device, it is important that the default SNMP community strings used by the device be replaced with customer-defined values.

1. **On the management network, log in to Oracle ILOM.**

See "Log in to the Oracle ILOM CLI" on page 39.

2. **Create a new SNMP community string.**

In this example, replace these items in the command line:

- *string* – Replace with a customer-defined value that is compliant with U.S. Department of Defense requirements regarding the composition of SNMP community strings.
- *access* – Replace with either `ro` or `rw`, depending on whether this is a read-only or read-write access string.

```
-> create /SP/services/snmp/communities/string permission=access
```

Once new community strings are created, the default community strings must be removed.

3. **Remove the default SNMP community strings.**

```
-> delete /SP/services/snmp/communities/public
-> delete /SP/services/snmp/communities/private
```

4. **Verify the SNMP community strings.**

```
-> show /SP/services/snmp/communities
```

▼ Replace Default Self-Signed Certificates (Oracle ILOM)

Oracle ILOM uses self-signed certificates to enable the out-of-the-box use of the SSL and TLS protocols. Whenever possible, replace self-signed certificates with certificates that are approved for use in your environment and signed by a recognized certificate authority.

Oracle ILOM supports a variety of methods that can be used to access the digital certificate and private key, including HTTPS, HTTP, SCP, FTP, TFTP, and pasting the information directly into a web browser interface. For more information, refer to the *Oracle ILOM Configuration and Maintenance Guide* (see "Additional Oracle ILOM Resources" on page 53).

1. **Determine if Oracle ILOM is using a default self-signed certificate.**

```
-> show /SP/services/https/ssl cert_status
/SP/services/https/ssl
Properties:
cert_status = Using Default (No custom certificate or private key loaded)
```

2. **Install your organization's certificate.**

```
-> set /SP/services/https/ssl/custom_cert load_uri=URI_method
-> set /SP/services/https/ssl/custom_key load_uri=URI_method
```

▼ Configure Administrative Browser Interface Inactivity Timeout

Oracle ILOM supports the ability to disconnect and log out administrative sessions that have been inactive for more than a pre-defined number of minutes. By default, the browser interface session times out after 15 minutes.

The session timeout parameters associated with the HTTPS and HTTP services are set and managed independently. Be sure to set the `sessiontimeout` parameter associated with each service.

1. **On the management network, log in to Oracle ILOM.**

   See "Log in to the Oracle ILOM CLI" on page 39.

2. **Check the inactivity timeout parameter associated with the HTTPS service.**

```
-> show /SP/services/https sessiontimeout
/SP/services/https
Properties:
sessiontimeout = 15
```

3. **Set the inactivity timeout parameter.**

   Replace *n* with a value specified in minutes.

```
-> set /SP/services/https sessiontimeout=n
```

4. **Check the inactivity timeout parameter associated with the HTTP service.**

```
-> show /SP/services/http sessiontimeout
/SP/services/http
Properties:
sessiontimeout = 15
```

5. **Set the inactivity timeout parameter.**

   Replace *n* with a value specified in minutes.

```
-> set /SP/services/http sessiontimeout=n
```

6. **Verify the setting by repeating Step 2 and Step 4.**

▼ Configure the Administrative Interface Timeout (Oracle ILOM CLI)

Oracle ILOM supports the ability to disconnect and log out administrative CLI sessions that have been inactive for more than a predefined number of minutes.

By default, the SSH CLI has no specified timeout value, and consequently, administrative users accessing this service remain logged in indefinitely.

For security purposes, set this parameter to match the value associated with the browser user interface. This could be 15 minutes or some other value.

1. **On the management network, log in to Oracle ILOM.**

See “Log in to the Oracle ILOM CLI” on page 39.

2. **Check the inactivity timeout parameter associated with the CLI.**

```
-> show /SP/cli timeout
/SP/cli
Properties:
timeout = 15
```

3. **Set the inactivity timeout parameter.**

Replace *n* with a value specified in minutes.

```
-> set /SP/cli timeout=n
```

4. **Verify the setting by repeating Step 2.**

▼ Configure Login Warning Banners (Oracle ILOM)

Oracle ILOM supports the ability to display customer-specific messages both before and after an administrator has connected to the device.

The Oracle ILOM connect message is displayed prior to authentication, whereas the login message is displayed after authentication.

Optionally, you can configure Oracle ILOM to require acceptance of the login message prior to being granted access to Oracle ILOM functions. Both the connection and login messages and the optional acceptance requirement are implemented by both the browser and command-line access interfaces.

Oracle ILOM supports connection and login messages up to a maximum of 1,000 characters.

1. **On the management network, log in to Oracle ILOM.**

See “Log in to the Oracle ILOM CLI” on page 39.

2. **Determine if connect and login messages are configured.**

```
-> show /SP/preferences/banner connect_message login_message
/SP/preferences/banner
Properties:
connect_message = (none)
login_message = (none)
```

3. **Set a connection or login message.**

```
-> set /SP/preferences/banner connect_message="Authorized Use Only"
-> set /SP/preferences/banner login_message="Authorized Use Only"
```

4. **Determine if login message acceptance is enabled.**

```
-> show /SP/preferences/banner login_message_acceptance
/SP/preferences/banner
Properties:
login_message_acceptance = disabled
```

5. **(Optional) Enforce acceptance of the login message.**

Caution - Requiring login message acceptance might inhibit the correct operation of automated management processes that use SSH, because they might not be able or configured to respond to the acceptance request. As a result, such connections can hang or time out because Oracle ILOM will not permit use of the CLI until the message acceptance requirement has been satisfied.

```
-> set /SP/preferences/banner login_message_acceptance=enabled
```

6. **Verify the setting by repeating Step 2 and Step 4.**

Additional Oracle ILOM Resources

For more information on Oracle ILOM administration and security procedures, refer to the Oracle ILOM documentation library that corresponds to the version running on SuperCluster M8 and SuperCluster M7:

- Access to documentation for all Oracle ILOM releases

  https://docs.oracle.com/en/servers/management.html
- *Oracle ILOM Security Guide Firmware Releases 3.0, 3.1, and 3.2*:

  http://docs.oracle.com/cd/E37444_01/html/E37451

Securing the Compute Servers

One or two SPARC M7 servers (compute servers) are installed in SuperCluster M7, or one or two SPARC M8 servers (compute servers) are installed in SuperCluster M8. Each compute server is divided into two hardware partitions (two PDomains). Each PDomain includes half of the possible processors, memory, and PCIe expansion slots in the chassis. Both PDomains operate as a separate server within the same chassis. A redundant pair of service processor modules (SPMs) manages each partition.

You must secure each PDomain.

This section provides a set of security controls for the compute servers.

▼ Log into a Compute Server

To access a single PDomain through Oracle ILOM, you must log in to the active SPM controlling that PDomain. You can power on, reboot, or manage one partition while the other partition continues to operate normally.

There are a variety of methods you can use to log into a SuperCluster compute server. The method described in this task involves logging into Oracle ILOM CLI on the compute server's SPM. This method enables you to access the server in any of these states:

- Standby power mode
- System powered on, but host not running
- OS is booting

- Fully powered on, and the OS is running

1. **On the management network, log in using the `ssh` command.**

   ```
   $ ssh root@compute_server_SPM_ILOM_IP-address
   ```

2. **When prompted, enter the password.**
   If you are prompted to change the password, do so.
   At this point, you can perform any security tasks that are performed on the Oracle ILOM on the compute server.

3. **If you want to access the compute server's host console, start the host console.**

   ```
       -> start /Servers/PDomains/PDomain_0/HOST/console
   Are you sure you want to start /Servers/PDomains/PDomain_0/HOST/console (y/n)? y

   Serial console started.  To stop, type #.

   root@system-identifier-pd0:~#
   ```

   Note - You will not see the PDomain prompt if the host is not running.

   Note - To switch back to the Oracle ILOM prompt, type the escape characters (`#.` are the default characters).

4. **If needed, assume a superuser role.**
   Use the `su` (switch user) command to switch to a user that is configured with the `root` role.

▼ Determine the SuperCluster Software Version

1. **Log in to one of the compute servers and access the host console.**
   See "Log into a Compute Server" on page 55.

2. **Type this command.**

   ```
   # beadm list
   ```

   The output shows the active boot environment in the form `SCMU_`*YYYY.QQ*. For example, SCMU_2018.Q3 refers to the 3rd quarter 2018 SuperCluster Quarterly Full Stack Download Patch.

To update the version of the SuperCluster software, install the most recent SuperCluster Quarterly Full Stack Download Patch available from My Oracle Support.

Note - For SuperCluster, additional restrictions might limit what versions of software can be used and how those versions are updated. In these situations, contact your Oracle representative.

▼ Configure the Secure Shell Service

Performing this task helps improve the Secure Shell security configuration deployed in the Oracle SuperCluster.

The `/etc/ssh/sshd_config` file is a system-wide configuration file where you configure parameters for the Secure Shell service.

1. **Log in to one of the compute servers and access the host console as superuser.**

   See "Log into a Compute Server" on page 55.

2. **Edit the `/etc/ssh/sshd_config` file.**

3. **Review other `sshd_config` parameters and set them according to site requirements.**

   These settings secure the Secure Shell service:

   ```
   Protocol 2
   Banner /etc/issue
   PermitEmptyPasswords no
   PermitRootLogin no
   StrictModes yes
   IgnoreRhosts yes
   PrintLastLog yes
   X11Forwarding no
   ClientAliveInterval 600
   ClientAliveCountMax 0
   ```

4. **Save the `sshd_config` file.**

5. **Restart the service.**

   You must restart the service for the changes to take effect.

   ```
   # svcadm restart ssh
   ```

Verify That `root` Is a Role

By default, Oracle Solaris is configured so that `root` is a role and not a user account. Additionally, the SuperCluster configuration does not permit anonymous `root` user logins. Instead, all users must log in as a regular user prior to assuming the root role. All SuperCluster administration operations must be carried out using `root` as a role.

1. **Log in to one of the compute servers and access the host console.**
   See "Log into a Compute Server" on page 55.

2. **Verify that `root` attributes are set to `type=role`.**

   ```
   # grep root /etc/user_attr
   root::::type=role
   ```

3. **(Optional) Assign any regular user the `root` role.**

   ```
   # usermod -R root user_name
   ```

Default Exposed Network Services (Compute Servers)

This table lists the default network services that re exposed on the compute servers..

Service Name	Protocol	Port	Description
SSH	TCP	22	Used by the integrated Secure Shell service to enable administrative access to the compute servers using a CLI.
HTTP (BUI)	TCP	80	Used by the integrated HTTP service to enable administrative access to the compute servers using a browser interface.
HTTPS (BUI)	TCP	443	Used by the integrated HTTPS service to enable administrative access to the compute servers over an encrypted (SSL/TLS) channel using a browser interface.
SNMP	UDP	161	Used by the integrated SNMP service to provide a management interface to monitor the health of the compute servers and to monitor received trap notifications.

Hardening the Compute Server Security Configuration

These topics describe how to securely configure the compute servers.

▼ Disable Unnecessary Services (Compute Servers)

1. **Log in to one of the compute servers and access the host console as superuser.**

   See “Log into a Compute Server” on page 55.

2. **Disable the NFS server service on a system that is not an NFS file server.**

Caution - Do NOT disable the NFS server service on the master control domain (the primary domain of the first PDomain), because this service is required for I/O domain creation.

The NFS server service handles client file system requests over NFS versions 2, 3, and 4. If this system is not an NFS server, disable the service.

```
# svcadm disable svc:/network/nfs/server
```

3. **If you are either not using FedFS for DNS SRV records or LDAP-based referrals, disable the service.**

   The Federated file system (FedFS) client service manages defaults and connection information for LDAP servers that store FedFS information.

   ```
   # svcadm disable svc:/network/nfs/fedfs-client
   ```

4. **Disable the `rquota` service.**

   The `remote` quota server returns quotas for a user of a local file system which is mounted over NFS. The results are used by `quota` command to display user quotas for remote file systems. The `rquotad` daemon is normally invoked by `inetd` command. The daemon provides information about the network to potentially malicious users. For more information, refer to the Oracle Solaris `quota`(1M) man page, the `rquotad`(1M) man page, or the `inetd`(1M) man page.

   ```
   # svcadm disable svc:/network/nfs/rquota
   ```

5. **Disable the `cbd` service.**

   The `cbd` service manages communication endpoints for the NFS Version 4 protocol. The `nfs4cbd` daemon runs on the NFS Version 4 client and creates a listener port for callbacks. For more information, refer to the Oracle Solaris `nfs4cbd`(1M) man page.

   ```
   # svcadm disable svc:/network/nfs/cbd
   ```

6. **Disable the `mapid` service if you are not using NFSv4.**

   The NFS user and group ID mapping daemon service maps to and from NFS version 4 `owner` and `owner_group` identification attributes and local UID and GID numbers used by both the NFS version 4 client and server.

   ```
   # svcadm disable svc:/network/nfs/mapid
   ```

7. **Disable the `ftp` service.**

   The FTP service provides unencrypted file transfer service and uses plain text authentication. Use the secure copy `scp` program instead of `ftp`, because it provides encrypted authentication and file transfer. For more information, refer to the Oracle Solaris `scp`(1) man page.

   ```
   # svcadm disable svc:/network/ftp:default
   ```

8. **Disable the remote volume manager service.**

   The removable volume manager is a HAL-aware volume manager that can automatically mount and unmount removable media and hot-pluggable storage. Users might import malicious

programs, or transfer sensitive data off the system. For more information, refer to the Oracle Solaris `rmvolmgr(1M)` man page.

This service only runs in the Oracle Solaris global zone.

```
# svcadm disable svc:/system/filesystem/rmvolmgr
```

9. **Disable the `smserver` service.**

   The `smserver` service is used to access removable media devices.

   ```
   # svcadm disable rpc/smserver:default
   ```

10. **Specify `pam_deny.so.1` as the module for the authentication stack for the `r-protocol` services in the `/etc/pam.d` directory.**

    By default, legacy services such as the `r-protocols`, `rlogin` and `rsh`, are not installed. These services, however, are defined in `/etc/pam.d` file. If you remove the service definitions from the `/etc/pam.d` file, the services use the other services (SSH, for example) in the event that the legacy services are enabled. For more information, refer to the Oracle Solaris `rlogin(1)` man page or the `rsh(1)` man page.

    ```
    # cd /etc/pam.d
    # cp rlogin rlogin.orig
    # pfedit rlogin
    auth definitive pam_deny.so.1
    auth sufficient pam_deny.so.1
    auth required pam_deny.so.1
    # cp rsh rsh.orig
    # pfedit rsh
    auth definitive pam_deny.so.1
    auth sufficient pam_deny.so.1
    auth required pam_deny.so.1
    ```

11. **Edit the `/etc/default/keyserv` file to change the value of `ENABLE_NOBODY_KEYS` to `NO`.**

    The `keyserv` service cannot use the `nobody` user key. The value of `ENABLE_NOBODY_KEYS` is `YES` by default.

    ```
    # pfedit /etc/default/keyserv
    . . .
    ENABLE_NOBODY_KEYS=NO
    ```

12. **Add users to the `ftpusers` file to restrict `ftp` access.**

    FTP file transfers must not be available to all users, and must require qualified users to supply their names and password. In general, system users should not be allowed to use FTP. This check verifies that system accounts are included in the `/etc/ftpd/ftpusers` file, so that they are not allowed to use FTP.

The file `/etc/ftpd/ftpusers` is used to prohibit users from using the FTP service. As a minimum, include all system users, such as `root`, `bin`, `adm`, and so on.

```
# pfedit /etc/ftpd/ftpusers
....
root
daemon
bin
...
```

13. Set a strong default file creation mask for files created by the FTP server.

The FTP server does not necessarily use the user's system file creation mask. Setting the FTP umask ensures that the files transmitted over FTP use a strong file creation umask.

```
# pfedit /etc/proftpd.conf
Umask          027
```

14. Disable responses to network topology queries.

It is important to disable responses to echo requests. ICMP requests are managed using the `ipadm` command.

These settings prevent the dissemination of information about the network topology.

```
# ipadm set-prop -p _respond_to_echo_multicast=0 ipv4
# ipadm set-prop -p _respond_to_echo_broadcast=0 ip
```

15. Disable redirect ICMP messages.

Routers use ICMP redirect messages to inform hosts of more direct routes to a destination. An illicit ICMP redirect message can result in a man-in-the-middle attack.

```
# ipadm set-prop -p _ignore_redirect=1 ipv4
```

16. Disable the messaging to prevent access to remote terminals.

```
# mesg -n
```

For more information, refer to the Oracle Solaris `mesg(1)` man page, the `talk(1)` man page, and the `write(1)` man page.

17. (Optional) Review and disable unnecessary services listening on the network.

By default, `ssh` is the only network service that can send and receive network packets. For more information, refer to the Oracle Solaris `ssh(1)` man page.

```
# svcadm disable FMRI_of_unneeded_service
```

Enable Strict Multi-homing

For systems that are gateways to other domains, such as a firewall or a VPN node, strict multi-homing must be enabled. The `hostmodel` property controls the send and receive behavior for IP packets on a multi-homed system. Set strict mult-homing to `1` so that packets don't get accepted on a different interface. The default is `0`.

1. **Log in to one of the compute servers and access the host console as superuser.**

   See "Log into a Compute Server" on page 55.

2. **Set strict multi-homing to `1`.**

```
# ipadm set-prop -p _strict_dst_multihoming=1 ipv4
```

Enable ASLR

Note - Do not enable ASLR in Database Domains or in Database Zones.

Oracle Solaris tags many user binaries to enable address space layout randomization (ASLR). ASLR randomizes the starting address of key parts of an address space. This security defense mechanism can cause Return Oriented Programming (ROP) attacks to fail when they try to exploit software vulnerabilities. Zones inherit this randomized layout for their processes. Because the use of ASLR might not be optimal for all binaries, ASLR is configurable at the zone and binary level.

1. **Log in to one of the compute servers and access the host console as superuser.**

   See "Log into a Compute Server" on page 55.

2. **Enable ASLR.**

```
# sxadm delcust aslr
# sxadm info
EXTENSION    STATUS                CONFIGURATION
aslr         enabled (tagged-files) System default (default)
```

Configure TCP Connections

Setting the maximum half-open TCP connections to 4096 per IP address per port helps to defend against SYN flood denial of service attacks. Setting the maximum number of queued incoming connections TCP to at least 1024 helps prevent certain distributed denial of service (DDoS) attacks.

1. **Log in to one of the compute servers and access the host console as superuser.**
   See "Log into a Compute Server" on page 55.

2. **Set the maximum half-open and queued incoming TCP connections.**

```
# ipadm set-prop -p _conn_req_max_q0=9096 tcp
# ipadm set-prop -p _conn_req_max_q=1024 tcp
```

Set Password History Logs and Password Policies for PCI Compliance

The `HISTORY` parameter in the `/etc/default/passwd` file prevents users from using similar passwords with the `HISTORY` value.

If `MINWEEKS` is set to `3` and `HISTORY` is set to `10`, passwords cannot be reused for 10 months.

1. **Log in to one of the compute servers and access the host console as superuser.**
   See "Log into a Compute Server" on page 55.

2. **Edit the `/etc/default/passwd` file and set the password parameters.**

```
# pfedit /etc/default/passwd
. . .
#Compliance to the PCI-DSS benchmark is 10
#HISTORY=0
HISTORY=10
MINDIFF=4
MINDIGIT=1
MINUPPER=1
MINWEEKS=3
MAXWEEKS=13
```

3. **Edit the `/etc/default/login` file to include these parameters.**

```
# pfedit /etc/default/login
```

```
. . .
# Compliance edit
#PASSLENGTH=6
PASSLENGTH=14
. . .
```

Ensure That User Home Directories Have Appropriate Permissions

Home directories must be writable and searchable by their owners. Typically, other users do not have rights to modify those files or add files to the user's home directory. To ensure that this is the case, set permissions on the user's directory.

1. **Log in to one of the compute servers and access the host console as superuser.**
See "Log into a Compute Server" on page 55.

2. **Set permissions on a user's directory.**

```
# chmod 750 /export/home/user_home_directory
```

Enable the IP Filter Firewall

IP Filter is a host-based firewall that provides stateful packet filtering and network address translation (NAT). Packet filtering provides basic protection against network-based attacks. IP Filter also includes stateless packet filtering, and can create and manage address pools.

1. **Log in to one of the compute servers and access the host console as superuser.**
See "Log into a Compute Server" on page 55.

2. **Enable the IP filter firewall.**

```
# svcadm svc:/network/ipfilter:default
```

Ensure That Name Services Only Use Local Files

The OS uses a number of databases of information about hosts, `ipnodes`, users, and `groups`. Data for these items come from a variety of sources. Host names and host addresses, for

example, can be found in the `/etc/hosts`, NIS, LDAP, DNS, or Multicast DNS. Oracle strongly recommends use of DNS with SuperCluster, particularly for database SCAN addresses. Oracle cannot guarantee the successful operation of all SuperCluster features in the absence of DNS. However, systems in restricted environments are more secure if only local file entries are used for these items. For more information, refer to the Oracle Solaris `passwd(4)` man page, the `shadow(4)` man page, and the `user_attr(4)` man page.

1. **Log in to one of the compute servers and access the host console as superuser.**
   See "Log into a Compute Server" on page 55.

2. **Configure name services to use only local files.**

```
# svccfg -s name-service/switch setprop config/default = astring: "files"
# svccfg -s name-service/switch setprop config/host = astring: "files"
# svccfg -s name-service/switch setprop config/password = astring: "files"
# svccfg -s name-service/switch setprop config/group = astring: "files"
# svccfg -s name-service/switch:default refresh
```

Enable Sendmail and NTP Services

The sendmail service must be running, otherwise important system mail to `root` is not delivered.

1. **Log in to one of the compute servers and access the host console as superuser.**
   See "Log into a Compute Server" on page 55.

2. **Enable sendmail.**

```
# svcadm enable smtp:sendmail
```

3. **If needed, install the NTP service.**
   The `ntp` service must be installed on all systems where security and compliance is desired.

```
# pkg install service/network/ntp
```

4. **Configure the NTP service as a client and enable the service.**
   The Network Time Protocol daemon must be enabled and properly configured as a client. The `/etc/inet/ntp.conf` file must include at least one server definition. The file must also contain the line `restrict default ignore` to prevent the client from also acting as a server.

```
# vi /etc/inet/ntp.conf
. . .
```

```
server server_IP_address iburst
restrict default ignore ...
# svcadm enable ntp
```

Disable GSS (Unless Using Kerberos)

The GSS (generic security service) manages the generation and validation of GSS-API (Generic Security Service Application Program Interface) security tokens. The `gssd` daemon operates between the kernel `rpc` and the GSS-API. For more information, refer to the Oracle Solaris `gssd`(1M) man page.

Note - Kerberos uses this service. Disable the `rpc/gss` service if Kerberos is not configured and not in use.

---

1. **Log in to one of the compute servers and access the host console as superuser.**
   See "Log into a Compute Server" on page 55.

2. **Enable `rpc/gss`.**

   ```
   # svcadm enable rpc/gss
   ```

3. **Set a size limit for `/tmpfs`.**
   The size of the `tmpfs` file system is not limited by default. To avoid a performance impact, you can limit the size of each `tmpfs` mount. For more information, refer to the Oracle Solaris `mount_tmpfs`(1M) man page and the `vfstab`(4) man page.

   ```
   # pfedit /etc/vfstab
   ...
   swap - /tmp tmpfs - yes size=sz
   ```

4. **Reboot the compute server.**

   ```
   # reboot
   ```

Set the Sticky Bit for World-Writable Files

The sticky bit on a directory prevents files in a world-writable directory from being deleted or moved by anyone except the owner of the file, or the `root` role. This is useful in directories that are common to many users, such as the `/tmp` directory.

1. **Log in to one of the compute servers and access the host console as superuser.**
   See "Log into a Compute Server" on page 55.

2. **Set the sticky bit on `/tmp` and on any other world-writable files.**

```
# chmod 1777 /tmp
```

Protect Core Dumps

Core dumps can contain sensitive data. Protections can include file permissions and logging core dump events. For more information, refer to the Oracle Solaris `coreadm(1M)` man page and the `chmod(1)` man page.

Use the `coreadm` command to view and set the current configuration.

1. **Log in to one of the compute servers and access the host console as superuser.**
   See "Log into a Compute Server" on page 55.

2. **View the current configuration.**

```
# coreadm
global core file pattern: /var/share/cores/core.%f.%p
global core file content: default
init core file pattern: core
init core file content: default
global core dumps: enabled
per-process core dumps: enabled
global setid core dumps: disabled
per-process setid core dumps: disabled
global core dump logging: enabled
```

3. **Configure the core files and protect the core dump directory.**

```
# coreadm -g /var/cores/core_%n_%f_%u_%g_%t_%p \
          -e log -e global -e global-setid \
          -d process -d proc-setid
```

4. **Check the permissions.**

```
# ls -ld /var/share/cores
drwx------ 2 root root 2 Aug 2 2015 cores/
```

5. **Set the permissions correctly on the directory.**

```
# chmod 700 /var/share/cores
```

Enforce Nonexecutable Stacks

Enabling nonexecutable stacks is a very useful technique for thwarting certain kinds of buffer overflow attacks. When Oracle Solaris `nxstack` is enabled, the process stack memory segment is marked nonexecutable. This extension defends against attacks that rely on injecting malicious code and executing it on the stack.

1. **Log in to one of the compute servers and access the host console as superuser.**
   See "Log into a Compute Server" on page 55.

2. **Enable `nxstack`.**

   ```
   # sxadm set model=all nxstack
   ```

3. **Verify the configuration.**

   ```
   # sxadm get all nxstack
   EXTENSION     PROPERTY     VALUE
   nxstack         model        all
   ```

Enable Encrypted Swap Space

Encrypt swap space, whether it is a ZFS volume or raw device. Encryption ensures that any sensitive data, such as user passwords, are protected if the system needs to swap those pages out to disk.

1. **Log in to one of the compute servers and access the host console as superuser.**
   See "Log into a Compute Server" on page 55.

2. **Edit the `/etc/vfstab` file and set `swap` to `encrypted`.**

   ```
   # pfedit /etc/vfstab
   ...
   /dev/zvol/dsk/rpool/swap - - swap - no encrypted
   ```

3. **Create and initialize a PKCS #11 keystore.**

   ```
   # pktool setpin keystore=pkcs11
   ```

```
Enter token passphrase: ********
Create new passphrase: ************
Re-enter new passphrase: ************
```

4. **Generate a symmetric key and store it in a PKCS #11 keystore.**

```
# pktool genkey keystore=pkcs11 keytype=aes keylen=256 label=globalzone-key
```

Enable Auditing

Make sure audit logs capture all administrative actions, including commands with arguments.

1. **Log in to one of the compute servers and access the host console as superuser.**
See "Log into a Compute Server" on page 55.

2. **Configure the audit facility.**

```
# auditconfig -setpolicy +argv
# auditconfig -setflags lo,ad,ex >& /dev/null
# auditconfig -setpolicy +zonename
```

Enable Data Link (Spoofing) Protection on Global Zones

Oracle Solaris data link protection prevents the potential damage that can be caused by malicious guest VMs to the network.

Enabling the snoop proofing configuration improves network performance, by enabling the virtual environment's network traffic to be isolated from the wider traffic that is received or sent by the host system. The link protection prevents the damage that can be caused by potentially malicious guest VMs to the network. The feature offers protection from these basic threats:

- IP and MAC spoofing
- L2 frame spoofing such as Bridge Protocol Data Unit (BPDU) attacks

---

Note - For more information about Oracle Solaris zones, refer to the Oracle Solaris zones documentation in the Oracle Solaris 11.4 Information Library at https://docs.oracle.com/cd/E37838_01/index.html and the Oracle Solaris 11.3 Information Library at http://docs.oracle.com/cd/E53394_01.

---

1. **Log in to one of the compute servers and access the host console as superuser.**

   See "Log into a Compute Server" on page 55.

2. **Set link protection.**

   ```
   # dladm set-linkprop -p protection=mac-nospoof,restricted,ip-nospoof,dhcp-nospoof netx
   ```

   Where `net`*x* corresponds to each physical link connected to the 10Gb client network.

3. **Confirm the configuration.**

   ```
   # dladm show-linkprop -p protection netx
   LINK         PROPERTY     PERM     VALUE         EFFECTIVE         DEFAULT     POSSIBLE
   net0         protection     rw     mac-nospoof   mac-nospoof        --         mac-
   nospoof,
                                     restricted    restricted         --
    restricted,
                                     ip-nospoof    ip-nospoof         --         ip-
   nospoof,
                                     dhcp-nospoof  dhcp-nospoof       --         dhcp-
   nospoof
   ```

   Where `net`*x* corresponds to each physical link connected to the 10Gb client network.

4. **Set allowed IPs on the link.**

   ```
   # dladm set-linkprop -p allowed-ips=10.0.0.1,10.0.0.2 netx
   ```

▼ Enable Data Link (Spoofing) Protection on Non-Global Zones

Oracle Solaris data link protection can also be applied individually to all Oracle Solaris non-global zones deployed within the SuperCluster environment.

Note - For more information about Oracle Solaris zones, refer to the Oracle Solaris zones documentation in the Oracle Solaris 11.4 Information Library at `https://docs.oracle.com/cd/E37838_01/index.html` and the Oracle Solaris 11.3 Information Library at `http://docs.oracle.com/cd/E53394_01`.

---

1. **Log in to one of the compute servers and access the host console as superuser.**

   See "Log into a Compute Server" on page 55.

2. **Enforce data link protection on a particular network interface using the `zonecfg` command.**
   Ensure that the list of allowed IP address is accurate and complete. The list must include any virtual IP addresses used by Oracle Solaris IPMP, Oracle Real Application Clusters, and so on. Also note that changes made to the SuperCluster non-global zone configuration do not take effect until after the non-global zone is restarted. For more information, refer to the Oracle Solaris `zonecfg(1M)` man page.

```
# zonecfg –z zonename
zonecfg:zonename> select anet linkname=network-link-name
zonecfg:zonename:anet> set allowed-address="list_of_allowed_IP_addresses"
zonecfg:zonename:anet>  set link-protection=mac-nospoof,ip-nospoof,restricted
zonecfg:zonename:anet>  set configure-allowed-address=false
zonecfg:zonename:anet>  end
zonecfg:zonename>  commit
zonecfg:zonename>  exit
```

▼ Create Encrypted ZFS Data Sets

Organizations requiring *data-at-rest* protection, can opt to further protect zone deployed applications and information using encrypted ZFS data sets. To ensure that each non-global zone is able to start without administrator intervention, the encrypted ZFS data sets are configured to access ZFS encryption keys that are stored locally within the individual database or application domain. Encrypted data sets are only supported with application zones on Oracle SuperCluster. Encrypted data sets with database zones require tool changes and is not supported.

1. **Log in to one of the compute servers and access the host console as superuser.**
   See "Log into a Compute Server" on page 55.

2. **Create ZFS encryption keys.**
   A simple way to create the required key is to use commands similar to these:

```
# zfs createzfs_pool_name/zfskeystore
$ chown root:root /zfs_pool_name/zfskeystore
$ chmod 700 /zfs_pool_name/zfskeystore
$ pktool genkey keystore=file keytype=aes keylen=256 \
outkey=/zfs_pool_name/zfskeystore/zone_name.key
```

3. **Create the encrypted zone root ZFS data set.**

```
# zfs create -o encryption=aes-256-ccm -o \
keysource=raw,file:///zfs_pool_name/zone_name.key \
```

zfs_pool_name/*zone_name*

4. **Encrypt the application data sets.**

   This same approach can be used to encrypt the application data sets, using either the same (SuperCluster-specific) key or a unique key per data set depending upon site-specific requirements and policies. In this example, the application data set is created using the same key created in Step 3. Note that additional ZFS configuration parameters, such as compression, can also be defined during the creation of these additional data sets.

   ```
   # zfs create -o compression=on -o encryption=aes-256-ccm -o \
   keysource=raw,file:///zfs_pool_name/zfskeystore/zone_name.key zfs_pool_name/app
   ```

▼ (Optional) Set a Passphrase for Key Store Access

The previous task,"Create Encrypted ZFS Data Sets" on page 72, uses a locally defined (raw) key file that must be stored directly on a file system. Another key storage technique leverages a passphrase protected PKCS#11 keystore, called the *Sun Software PKCS#11 Softtoken*. To use this method, perform this task.

The PKCS#11 key store must be manually unlocked prior to the key being made available to ZFS. Ultimately, this means that manual administrative intervention is required to mount the encrypted ZFS data set (and start the non-global zone if the zone is also using an encrypted ZFS data set). For more information on other key storage strategies, refer to the Oracle Solaris `zfs_encrypt(1M)` man page.

1. **Log in to one of the compute servers and access the host console as superuser.**

   See "Log into a Compute Server" on page 55.

2. **Set a PIN (passphrase) that will be required to access the key store.**

   The default PIN associated with a new PKCS#11 keystore is `changeme`. Use this passphrase at the first prompt in this example.

   ```
   # pktool setpin keystore=pkcs11
   Enter token passphrase:
   Create new passphrase:
   Re-enter new passphrase:
   ```

3. **Define a `${SOFTTOKEN}` environment variable to store the key in a different location.**

   The key material used by the PKCS#11 Softtoken is stored by default in the `/var/user/${USERNAME}/pkcs11_softtoken` directory. The `${SOFTTOKEN}` environment variable can be

defined to store the key material in a different location. You can use this capability to enable SuperCluster-specific storage for this passphase protected key material.

```
# export SOFTTOKEN=/<zfs_pool_name>/zfskeystore
# pktool setpin keystore=pkcs11
Enter token passphrase:
Create new passphrase:
Re-enter new passphrase:
```

4. **Create a key.**

```
# pktool genkey keystore=pkcs11 keytype=aes keylen=256 label=zone_name_rpool
Enter PIN for Sun Software PKCS#11 softtoken:
```

5. **Create the encrypted ZFS data set, referencing the key created in the previous step.**

```
# zfs create -o encryption=aes-256-ccm -o keysource=raw,pkcs11:
object=<zone_name>_rpool zfs_pool_name/zone_name
Enter PKCS#11 token PIN for 'zfs_pool_name/zone_name':
```

▼ Create Immutable Global Zones

Tamper-proofing with immutability enables global zones and non-global zones to create a resilient, high-integrity operating environment within which SuperCluster compute servers operate their own services. Building upon the inherent security capabilities of Oracle Solaris global and non-global zones, immutable zones ensure that (some or all) OS directories and files are unable to be changed (without administrator intervention). The enforcement of this read-only posture helps to prevent unauthorized changes, promotes stronger change management procedures, and deters the injection of both kernel and user-based malware.

Note - Once an immutable zone is configured, it cannot be updated other then through the Trusted Path login or when the system is rebooted using writeable mode by using the `reboot -- -w` command.

While you should always confirm that application software operates as expected in an immutable environment, be aware that Oracle Database instances and Oracle RAC clusters are verified to run correctly within Oracle Solaris immutable non-global zones.

Note - For more information about Oracle Solaris zones, refer to the Oracle Solaris zones documentation in the Oracle Solaris 11.4 Information Library at `https://docs.oracle.com/cd/E37838_01/index.html` and the Oracle Solaris 11.3 Information Library at `http://docs.oracle.com/cd/E53394_01`.

1. **Log in to the Oracle Solaris global zone (Dedicated Domain, Root Domain, or I/O Domain) as superuser.**

   See "Log into a Compute Server" on page 55.

2. **Modify the Oracle Solaris global zone configuration by setting the `file-mac-profile` property.**

   ```
   # zonecfg -z global set file-mac-profile=fixed-configuration
   zonecfg:global> commit
   ```

3. **Reboot the Oracle Solaris global zone for the changes to take effect. Log into the domain through the ILOM console.**

4. **Start the immutable global zone trusted path console.**

   As the immutable global zone is configured, it is important to enter the console login using one of these break sequences:

   - **Graphical console** – F1-A
   - **Serial console** – <Break> or the alternate break sequence (CR~ Ctrl-b)

   ```
   trusted path console login:
   ```

5. **Log into the global zone of the I/O Domain and assume the `root` role to perform any specific updates to the system, then reboot the system to bring it back to read-only mode.**

   ```
   # reboot
   ```

▼ Configure Immutable Non-Global Zones

To configure an Oracle Solaris non-global zone to be immutable, perform this task.

Note - The Oracle Solaris 11 OS supports additional immutable zone configurations beyond the one identified in this task (fixed-configuration). For more information on these options, refer to the Oracle Solaris `zonecfg(1M)` man page. However, only the fixed-configuration option was tested as part of the SuperCluster architecture.

Caution - Adding, modifying, or deleting zone user accounts and passwords cannot be done once Oracle Solaris non-global zone immutability is enabled, as described in this task. This issue can be resolved, however, by deploying an LDAP directory to contain zone-specific information such as users, roles, groups, rights profiles, and so on.

Caution - The Oracle Solaris immutable zone functionality is limited to those ZFS data sets that are implemented by default in an Oracle Solaris non-global zone. Additional file systems, pools, or data sets are not subject to the immutable zone policy, although access to those file elements can be controlled using other means such as the use of read-only loopback mounts.

Note - For more information about Oracle Solaris zones, refer to the Oracle Solaris zones documentation in the Oracle Solaris 11.4 Information Library at `https://docs.oracle.com/cd/E37838_01/index.html` and the Oracle Solaris 11.3 Information Library at `http://docs.oracle.com/cd/E53394_01`.

1. **Log in to one of the compute servers and access the host console as superuser.**

   See "Log into a Compute Server" on page 55.

2. **Ensure that the Oracle Solaris non-global zone is shut down.**

   If this command returns a value, then the Oracle Solaris non-global zone is running an you must shut it down.

   Note - While the zone can be halted using the `zoneadm` command, follow the proper shut down procedures your organization has established to avoid the potential for service interruption and data loss. For more information, refer to the Oracle Solaris `zoneadm(1M)` man page.

   ```
   # zoneadm list | grep -w "zone_name"
   ```

3. **Adjust the Oracle Solaris non-global zone configuration by setting the `file-mac-profile` zone configuration property.**

   ```
   # zonecfg -z zone_name set file-mac-profile=fixed-configuration
   ```

4. **If required, disable the non-global zone immutable configuration.**

```
# zonecfg -z zone_name set file-mac-profile=none
```

5. **Restart the Oracle Solaris non-global zone for the changes to take effect.**

```
# zoneadm -z zone_name boot
```

▼ Enable Secure Verified Boot (Oracle ILOM CLI)

Use this task to enable secure verified boot through the Oracle ILOM CLI. Alternatively, you can use the Oracle ILOM web interface. See "Secure Verified Boot (Oracle ILOM Web Interface)" on page 79.

Verified boot refers to verification of object modules before execution using digital signatures. Oracle Solaris protects against the loading of rogue kernel modules. Verified boot increases the security and robustness of Oracle Solaris by verifying kernel modules before execution.

If enabled, Oracle Solaris verified boot checks the factory-signed signature in a kernel module before loading and executing the module. This check detects accidental or malicious modification of a module. The action taken is configurable and, when enabled, will either print a warning message and continue loading and executing the module, or will fail and not load and execute the module.

1. **Access Oracle ILOM on the compute server.**

   See "Log into a Compute Server" on page 55.

2. **Enable verified boot.**

```
-> set /HOST/verified_boot/ module_policy=enforce
Set 'module_policy' to 'enforce'
```

3. **Access and display the Oracle provided certificate.**

   A preinstalled verified boot certificate file, `/etc/certs/ORCLS11SE`, is provided as part of Oracle ILOM.

```
# more /etc/certs/ORCLS11SE
-----BEGIN CERTIFICATE-----
MIIFEzCCA/ugAwIBAgIQDfuxWi0q5YGAhus0XqR+7TANBgkqhkiG9w0BAQUFADCB
….
CXZousDBt9DdhjX6d0ZPLkdzBxqm8Bxg9H3iKtZBPuhZBl9iXvLEOzY8sS0AW7UF
UHGOvZ9U6m4Tq5+KDiJ8QXZG2ipTeat5XdzLmzA9w2jrrfx0N+NcgvIVjdPXD8C4
wgaJllToqg==
```

```
-----END CERTIFICATE-----
```

4. **Initiate the loading of the certificate.**

```
-> set /HOST/verified_boot/user_certs/1 load_uri=console
```

5. **Copy the contents of the `/etc/certs/ORCLS11SE` file and paste into the Oracle ILOM console.**

   Enter Ctrl-z to save and process information.

   Enter Ctrl-c to exit and discard changes.

```
-----BEGIN CERTIFICATE-----
MIIFEzCCA/ugAwIBAgIQDfuxWi0q5YGAhus0XqR+7TANBgkqhkiG9w0BAQUFADCB
….
CXZousDBt9DdhjX6d0ZPLkdzBxqm8Bxg9H3iKtZBPuhZBl9iXvLEOzY8sS0AW7UF
UHGOvZ9U6m4Tq5+KDiJ8QXZG2ipTeat5XdzLmzA9w2jrrfx0N+NcgvIVjdPXD8C4
wgaJllToqg==
-----END CERTIFICATE-----^Z
Load successful.
```

6. **Verify the certificate.**

```
-> show /HOST/verified_boot/user_certs/1/
/HOST/verified_boot/user_certs/1
Targets:
Properties:
clear_action = (Cannot show property)
issuer = /C=US/O=Oracle Corporation/OU=VeriSign Trust Network/OU=Class 2 Managed PKI
 Individual
Subscriber CA/CN=Object Signing CA
load_uri = (Cannot show property)
subject = /O=Oracle Corporation/OU=Corporate Object Signing/OU=Solaris Signed Execution/
CN=Solaris 11
valid_from = Mar 1 00:00:00 2012 GMT
valid_until = Mar 1 23:59:59 2015 GMT
Commands:
cd
load
reset
show
->
```

7. **Verify that the OpenBoot `use-nvram` parameter is set to `false`.**

   When you use verified boot, the OpenBoot `use-nvram` parameter must be set to `false`. This prevents OpenBoot from being modified to disable verified boot functionality. The default value is false. Log into Oracle Solaris and type:

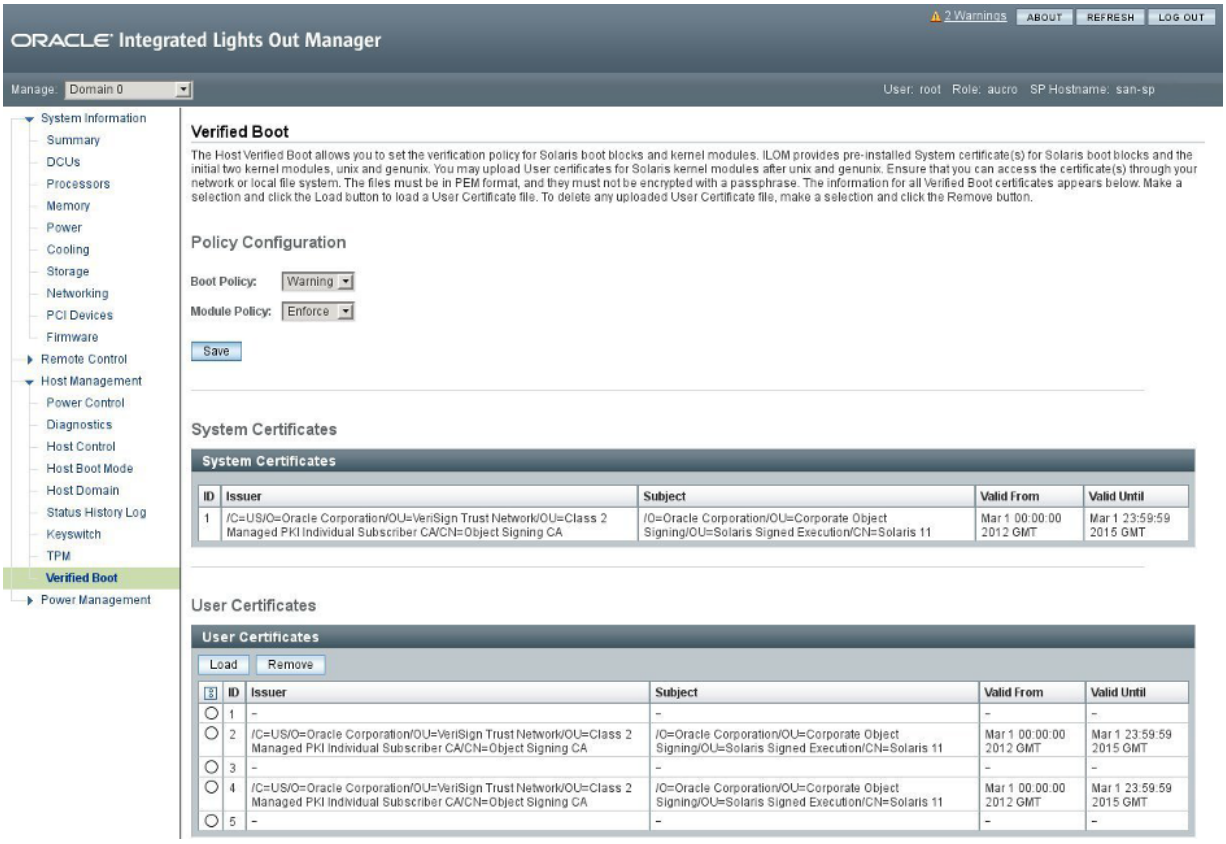
```
$ /usr/sbin/eeprom/eeprom use-nvramrc?

use-nvramrc?=false
```

Secure Verified Boot (Oracle ILOM Web Interface)

The Oracle ILOM web interface also supports setting of the verified boot policy variables and management of Certificate files, providing the same functionality as the CLI. Navigate to the Verified Boot link under the Host Management navigation menu.

For example:



Additional Compute Server Resources

For Oracle Solaris OS and Oracle Solaris Cluster security guides, refer to the documentation library that corresponds to your version of the OS. The libraries are available at http://docs.oracle.com/en/operating-systems.

For security information on Oracle VM Server for SPARC refer to the *Oracle VM Server for SPARC 3.4 Security Guide*http://docs.oracle.com/cd/E62357_01.

For security information about the compute server hardware, refer to the *SPARC M8 and SPARC M7 Servers Security Guide* available at https://docs.oracle.com/cd/E55211_01.

Securing the ZFS Storage Appliance

The ZFS storage appliance is one of the SuperCluster components for supporting storage consolidation in a variety of demanding workloads, including business intelligence, data warehousing, virtualization, development and test, and data protection.

The ZFS storage appliance includes two redundant ZFS storage controllers. You must secure both controllers.

These sections describe the ZFS storage appliance security guidelines and features:

▼ Log into the ZFS Storage Appliance

To perform the security tasks in this section, you log into the ZFS storage appliance through the management network.

This task describes how to log in using the CLI. For equivalent instructions for logging into the Oracle ILOM web interface, see "Additional ZFS Storage Appliance Resources" on page 89. You can also refer to the *Oracle ZFS Storage Appliance Administration Guide* for the release that corresponds to your storage appliance. The documentation for the various releases is available at: `https://docs.oracle.com/en/storage/`.

1. **On your management network, use `SSH` to connect to the ZFS storage appliance.**

   If you have not configured other users to administer the appliance, you must log in as `root`.

```
% ssh root@ZFS_Storage_App_IPaddress_or_hostname
Password:
Last login: Mon Oct 13 15:43:05 2015
hostname:>
```

2. **If needed, access the CLI help.**

   The `help` command provides context-specific help. Help on a particular topic is available by specifying the topic as an argument to `help`. Available topics are displayed by tab-completing the help command, or by typing `help topics`.

Determine the ZFS Storage Appliance Software Version

Use this procedure to determine the version of software on the ZFS storage appliance.

1. **Log in to the ZFS storage appliance.**

   See "Log into the ZFS Storage Appliance" on page 81.

2. **Display the software version.**

```
hostname:> configuration version show
[...]
Appliance Product: Sun ZFS Storage 7320
Appliance Type: Sun ZFS Storage 7320
Appliance Version: 2013.06.05.2.10,1-2.1.1.1
[...]
```

In this example, the ZFS storage appliance software is version `2013.06.05.2.10`.

To update the version of the ZFS storage appliance software, install the most recent SuperCluster Quarterly Full Stack Download Patch available from My Oracle Support.

Note - For SuperCluster, additional restrictions might limit what versions of the ZFS storage appliance software can be used and limit how those versions are updated. In these situations, contact your Oracle representative.

Change the ZFS Storage Appliance `root` Password

The ZFS storage appliance itself is not preconfigured with a default `root` password. Initial configuration of the ZFS storage appliance is performed through a console session from

its embedded Oracle ILOM. The `root` password for the appliance is set during this initial configuration session.

When you initially access the console of the appliance, a shell interface configuration screen appears. Verify the information on the screen and enter the required values. The `root` password to the ZFS storage appliance is set during this process.

Note - Oracle ILOM for the appliance does have a default `root` account and password. See "Default User Accounts and Passwords" on page 32.

Once you have a `root` account, you can change the password any time as described in this task.

Note - When a password is changed for any SuperCluster component that Oracle Engineered Systems Hardware Manager manages(such as the AFS storage controller OS), you must also update the password in Oracle Engineered Systems Hardware Manager. For details, refer to the *Oracle SuperCluster M8 and SuperCluster M7 Administration Guide*.

---

1. **Log into the ZFS storage appliance.**
   See "Log into the ZFS Storage Appliance" on page 81.

2. **Change the `root` password.**
   In this example, replace *password* with a password that complies with U.S. Department of Defense password complexity policies.

```
hostname:> configuration users select root set initial_password=password initial_password = **********
hostname:configuration users> done
```

For more information on the initial installation and configuration of the ZFS storage appliance, see "Additional ZFS Storage Appliance Resources" on page 89. You can also refer to the *Oracle ZFS Storage Appliance Installation Guide For ZS5-x, ZS4-4, ZS3-x, 7x20 Controllers, and DEx-24, Sun Disk Shelves, Release OS8.7.x* at `https://docs.oracle.com/cd/E79446_01`.

Default Exposed Network Services (ZFS Storage Appliance)

This table lists the default network services that are exposed by the ZFS storage appliance.

Service	Protocol	Port	Description
SSH	TCP	22	Used by the Secure Shell service to enable administrative access to the ZFS storage appliance using a CLI.

Service	Protocol	Port	Description
PORTMAP	TCP/UDP	111	Used by the RPC (Remote Procedure Call port mapping daemon (known as `rpcbind` or `portmap`). This service is required to support NFS version 3.
NTP	UDP	123	Used by the integrated NTP (Network Time Protocol) service (client only) to synchronize the local system clock to one or more external time sources.
HTTPS (BUI)	TCP	215	Used by the integrated HTTPS service to enable administrative access to the ZFS storage appliance over an encrypted (SSL/TLS) channel using a browser interface.
Remote Replication	TCP	216	Used by the integrated remote data replication service. Remote data replication duplicates and synchronizes projects and shares between ZFS storage appliances over an encrypted (SSL/TLS) channel.
NFS	TCP/UDP	2049 4045 various	Used by the NFS (network file system) service. NFS provides the network file sharing service. The actual number of ports depends on which version of the NFS protocol is used. NFS version3 relies upon the RPC port mapping daemon (listed above) and dynamically allocated ports to provide mounting, status, quota and related services. NFS version 4, however, relies only on TCP/2049.The NFS locking service uses TCP/4045.
iSCSI / iSNS	TCP	3260	Used by the iSCSI service that provides an IP-based storage networking protocol for linking data storage facilities. The ZFS storage appliance can be configured to share iSCSI devices (called LUNs) with networked clients.
Service Tags	TCP	6481	Used by the Oracle ServiceTag service. This is an Oracle discovery protocol used to identify servers and facilitate service requests. This service is used by products such as Oracle Enterprise Manager Ops Center to discover ZFS storage appliance software and to integrate with other Oracle automatic service solutions.
NDMP	TCP	10000	Used by the NDMP (Network Data Management Protocol) service that enables the ZFS storage appliance to participate in remotely coordinated backups.

The ZFS storage appliance also supports a variety of other services that are disabled by default including `HTTP`, `FTP`, `SFTP`, `TFTP`, `WebDAV`, and so on. Additional network ports might be exposed if those services are enabled after installation.

Hardening the ZFS Storage Appliance Security Configuration

These topics describe how to harden the security configuration of the ZFS storage appliance:

- “Configure SNMP Authorized Networks” on page 88

Implement Oracle ILOM Security Configuration Hardening

The ZFS storage appliance includes an embedded Oracle ILOM as part of the product. As with other Oracle ILOM implementations, there are security relevant configuration changes that you can implemented to improve the default security configuration of the device.

- **Secure the ZFS storage appliance Oracle ILOM interface by performing the procedures in “Securing Oracle ILOM” on page 39.**

Disable Unnecessary Services (ZFS Storage Appliance)

Disable any services that are not required to support the operational and management requirements of the platform.

By default, the ZFS storage appliance employs a network *secure-by-default* configuration whereby nonessential services are disabled. However, based on your security policies and requirements, it might be necessary to enable or disable additional services. Do not disable any of the NFS, iSCSI, DNS, IPMP, NTP, or SSH services.

1. **Log into the ZFS storage appliance.**

   See “Log into the ZFS Storage Appliance” on page 81.

2. **Display the list of services supported by the ZFS storage appliance.**

   hostname:> **configuration services**

3. **Determine if a given service is enabled.**

   Replace *servicename* with the name of a service identified in Step 2.

   hostname:> **configuration services** *servicename* **get <status>**

   A service is enabled if the service state parameter returns a value of `enabled`. For example:

   hostname:> **configuration services ndmp get <status>**

```
<status> = online
```

4. **Disable a service that is no longer required.**

   Set the service state to disable. For example:

   hostname:> **configuration services ndmp disable**

Disable Dynamic Routing

The ZFS storage appliance is configured to run the dynamic routing protocol by default.

Before disabling the dynamic routing service, ensure that the ZFS storage appliance is either directly connected to any network with which it must communicate, or ensure that it has been configured to use static routing or a default route. This step is needed to ensure that there is no loss of connectivity once dynamic routing is disabled.

1. **Log in to the ZFS storage appliance.**

   See "Log into the ZFS Storage Appliance" on page 81.

2. **Disable dynamic routing.**

   hostname:> **configuration services dynrouting disable**

3. **To determine if dynamic routing is enabled, type:**

   hostname:> **configuration services dynrouting get <status>**

Configure the Administrative Interface Inactivity Timeout (HTTPS)

The ZFS storage appliance supports the ability to disconnect and log out administrative sessions that have been inactive for a predefined number of minutes. By default, the browser user interface (HTTPS) times out a session after 15 minutes.

Note - No equivalent parameter enforces an inactivity timeout on the SSH command line interface of the ZFS storage appliance.

Use this procedure to set the inactivity timeout parameter to a custom value.

1. **Log in to the ZFS storage appliance.**

   See “Log into the ZFS Storage Appliance” on page 81.

2. **View the current inactivity timeout parameter that is associated with the browser interface.**

```
hostname:> configuration preferences get session_timeout
session_timeout = 15
```

3. **Configure the timeout parameter.**

   The `session_timeout` value is specified in minutes (10 minutes in this example).

```
hostname:> configuration preferences set session_timeout=10
session_timeout = 10
```

4. **Verify the timeout parameter by repeating Step 2.**

▼ Disable Unapproved SNMP Protocols

By default, SNMPv1 and SNMPv2c are enabled on the ZFS storage appliance. The ZFS storage appliance supports SNMPv1/v2c across all supported versions of the product. Starting with version 2013.1.2, the ZFS storage appliance also supports SNMPv3.

Note - Version 3 of the SNMP protocol introduced support for the USM (User-based Security Model). This functionality replaces the traditional SNMP community strings with actual user accounts that can be configured with specific permissions, authentication, and privacy protocols, and passwords. By default, the ZFS storage appliance does not include a user name or password for the integrated (read-only) USM account. For security purposes, configure the USM credentials and protocols based upon deployment, management, and monitoring requirements.

Ensure that unused or older versions of the SNMP protocol are disabled unless they are required.

1. **Log in to the ZFS storage appliance.**

   See “Log into the ZFS Storage Appliance” on page 81.

2. **Determine which version of the SNMP protocol is used by the device.**

```
hostname:> configuration services snmp get version
version = v2
```

3. **Enable the use of SNMPv3 (if available).**

   The use of SNMPv1/v2c and SNMPv3 is mutually exclusive, so when you enable SNMPv3, SNMPv1/v2c are disabled.

   ```
   hostname:> configuration services snmp set version=v3
   version = v3
   ```

4. **Verify the version of SNMP.**

   ```
   hostname:> configuration services snmp get version
   version = v3
   ```

Configure SNMP Community Strings

Only perform this task if the ZFS storage appliance is configured to use SNMPv1 or v2.

Because SNMP is often used to monitor the health of the device, it is important that the default SNMP community string used by the device be changed to a customer-defined value.

1. **Log in to the ZFS storage appliance.**

   See "Log into the ZFS Storage Appliance" on page 81.

2. **Change the SNMP community string.**

   In this example, replace *string* with a value that is compliant with U.S. Department of Defense requirements regarding the composition of SNMP community strings.

   ```
   hostname:> configuration services snmp set community=string
   community = value
   ```

3. **Verify the SNMP community string.**

   ```
   hostname:> configuration services snmp get community
   ```

Configure SNMP Authorized Networks

Only perform this task if the ZFS storage appliance is configured to use SNMPv1 or v2.

To minimize the disclosure of system configuration information, SNMP queries should only be accepted from approved network or host sources.

1. **Log in to the ZFS storage appliance.**

   See "Log into the ZFS Storage Appliance" on page 81.

2. **Configure the SNMP authorized network parameter.**

```
hostname:> configuration services snmp set network=127.0.0.1/8
network = 127.0.0.1/8
```

3. **Check the value of the SNMP authorized network parameter.**

   In this example, setting the network parameter to `127.0.0.1/8` effectively blocks all network-based SNMP queries. This value should be adjusted as needed to permit approved hosts and networks.

   A value of `0.0.0.0/0` permits queries from any network location.

```
hostname:> configuration services snmp get network
network = 127.0.0.1/8
```

Additional ZFS Storage Appliance Resources

For additional security guidelines for the ZFS storage appliance, refer to the security guide that corresponds to the release running on the ZFS storage appliance. See "Determine the ZFS Storage Appliance Software Version" on page 82.

These guides provide additional information on the product's security features, capabilities, and configuration options:

- *Oracle ZFS Storage Appliance Release Security Guide* (Release 2013.1.4.0)

  http://docs.oracle.com//cd/E56047_01
- *Oracle ZFS Storage Appliance Release Security Guide* (Release 2013.1.3.0)

  http://docs.oracle.com/cd/E56021_01
- *Oracle ZFS Storage Appliance Release Security Guide* (Release 2013.1.2.0)

  http://docs.oracle.com/cd/E51475_01

Securing the Exadata Storage Servers

The Exadata storage servers (storage servers) are the storage building block of SuperCluster. Each storage server is delivered preinstalled and integrated as part of SuperCluster M8 and SuperCluster M7 with all of the necessary compute, storage, and software components.

Note - You are only permitted to make changes to the configuration through the application of approved methods, patches, or updates. The storage server software may not be altered in any other manner.

SuperCluster M8 and SuperCluster M7 have a minimum of three storage servers. Additional storage servers might be installed in the main SuperCluster rack and in optional expansion racks. You must secure each individual storage server.

These topics describe how to secure the storage servers:

▼ Log into the Storage Server OS

- **On the management network, log into one of the storage servers as `celladmin`.**

  See "Default User Accounts and Passwords" on page 32.

```
# ssh celladmin@Storage_Server_IP_address
```

Change Storage Server Passwords

For a list of default accounts and passwords, see "Default User Accounts and Passwords" on page 32.

Note - When a password is changed for any SuperCluster component that Oracle Engineered Systems Hardware Manager manages (such as the Exadata storage server OS), you must also update the password in Oracle Engineered Systems Hardware Manager. For details, refer to the *Oracle SuperCluster M8 and SuperCluster M7 Administration Guide*.

1. **Log into the storage server as `celladmin`.**

   See "Log into the Storage Server OS" on page 91.

2. **Change a password using one of these methods.**

   - **Change the password for an account on the server you are logged into.**

     ```
     # passwd account_name
     ```

   - **Change an account password across all the storage servers.**

     The `cell_group` is a simple text file listing the host names of all of the storage servers (one per line).

     In this example, replace these command line items:

     - *new_password* – Replace with the new password that is compliant with site policies.
     - *account_name* – Replace with the name of the Oracle Linux account.

     ```
     # dcli -g cell_group -l root "echo new_password | passwd --stdin account_name"
     ```

Determine the Exadata Storage Server Software Version

1. **Log in to one of the storage servers.**

   See "Log into the Storage Server OS" on page 91.

2. **Type this command.**

   In this example, the storage server software version is 12.1.2.1.1.150316.2.

   ```
   # imageinfo -ver
   12.1.2.1.1.150316.2
   ```

To update the version of the software, install the most recent SuperCluster Quarterly Full Stack Download Patch available from My Oracle Support.

Note - For SuperCluster, additional restrictions might limit what versions of software can be used and how those versions are updated. In these situations, contact your Oracle representative.

Default Exposed Network Services (Storage Servers)

Service Name	Protocol	Port	Description
SSH	TCP	22	Used by the Secure Shell service which is integrated into the storage server software to provide administrative access to the system using a CLI. By default, the Secure Shell server is configured to respond to connection requests only on the management (NET 0) and IB (BONDIB0) networks.

The storage server also communicates with Oracle Database Domains on SuperCluster using the Reliable Datagram Sockets (RDSv3) protocol over remote direct memory access (RDMA) interfaces. This point-to-point communication does not use TCP/IP and is limited to the internal IB network partition onto which both the Oracle Database Domains on SuperCluster and storage servers reside.

Hardening the Storage Server Security Configuration

Note - The storage server includes an embedded Oracle ILOM as part of the product. As with other Oracle ILOM implementations, there are security relevant configuration changes that can be implemented to improve upon the default security configuration of the device. For more information, see "Securing Oracle ILOM" on page 39.

These topics describe how to harden the security of the storage servers:

Security Configuration Restrictions

The host_access_control utility is the only permitted and supported method to implement security configuration changes on the storage servers. You are not permitted to make manual changes to the configuration of these devices per Oracle Support notice 1068804.1. Further, before using this tool, you must first obtain explicit approval from Oracle SuperCluster Support to change the security configuration of their storage servers. To request this approval, open a service request with Oracle Support.

The host_access_control command, available as of Exadata software version 11.2.3.3.0, is used to implement a limited set of access and security configuration settings:

- Restricting remote root access.
- Restricting network access to certain accounts.
- Implementing password aging and complexity policies.
- Implementing login warning banner
- Defining account lockout and session timeout policies.

▼ Display Available Security Configurations With host_access_control

To see what is available in the host_access_control utility, perform these steps.

1. **Log into the storage server OS.**

See “Log into the Storage Server OS” on page 91.

2. **(Optional) Display `host_access_control` help for details.**

```
# /opt/oracle.cellos/host_access_control --help
```

Configure a System Boot Loader Password

You can configure the storage servers to require a system boot loader password whenever an administrator attempts to access the boot loader (GRUB) editor or command interface.

1. **Log into the storage server as `celladmin`.**

   See “Log into the Storage Server OS” on page 91.

2. **Configure a system boot loader password.**

```
# /opt/oracle.cellos/host_access_control grub-password
New GRUB password: password
Retype new GRUB password: password
[...]
```

3. **Verify the setting.**

   If the command returns a value similar to this example, then a boot loader password is installed.

```
# grep "^password" /etc/grub.conf
password --md5 $1$Hdner/$Q2VoiZeTJwmNQsFnH9oFy.
```

Disable Oracle ILOM System Console Access

Each of the storage servers includes an embedded Oracle ILOM to enable remote monitoring and management. Oracle ILOM can also be used to provide remote access to the storage server system console.

Perform this procedure if you want to disable access to the storage server through Oracle ILOM.

1. **Log into the storage server as `celladmin`.**

   See “Log into the Storage Server OS” on page 91.

2. **Disable Oracle ILOM system console access.**

```
# /opt/oracle.cellos/host_access_control access-ilomweb --lock
```

3. **Verify the setting.**

```
# /opt/oracle.cellos/host_access_control access-ilomweb --status
```

Restrict Remote root Access Using SSH

By default, the root user is permitted to remotely access each of the storage servers.

1. **Log into the storage server as celladmin.**

See "Log into the Storage Server OS" on page 91.

2. **Disable remote root access through SSH.**

```
# /opt/oracle.cellos/host_access_control rootssh --lock
```

3. **Verify the setting.**

```
# /opt/oracle.cellos/host_access_control rootssh --status
```

Configure System Account Lockout

By default, the storage servers are configured to lock system accounts after five consecutive failed authentication attempts.

To change this threshold, perform this procedure.

1. **Log into the storage server as celladmin.**

See "Log into the Storage Server OS" on page 91.

2. **Change the threshold.**

To comply with U.S. Department of Defense security requirements, specify a value of 3. If necessary, replace that value with one that is compliant with your local site policy.

```
# /opt/oracle.cellos/host_access_control pam-auth --deny 3
```

3. **Verify the setting.**

```
# /opt/oracle.cellos/host_access_control pam-auth --status | grep deny=
```

Configure Password Complexity Rules

By default, the storage servers do not implement any significant restrictions governing the complexity of system account passwords.

1. **Log into the storage server as `celladmin`.**

   See "Log into the Storage Server OS" on page 91.

2. **Define a password complexity policy.**

   For example:

```
# /opt/oracle.cellos/host_access_control pam-auth --passwdqc N0,N1,N2,N3,N4
```

   Replace *N0,N1,N2,N3,N4* with a comma-separated set of five values. These five values collectively set the actual system password complexity policy.

   - *N0* –Used for passwords consisting of only one character class (digits, lowercase characters, uppercase characters, and special characters). In general, this parameter is set to `disabled` because simple passwords are not secure.
   - *N1* – Used for passwords consisting of two character classes that do not meet the requirements for a passphrase. For this rule to apply, the password must be at least N1 characters in length.
   - *N2* – Used for passwords consisting of a passphrase. For this rule to apply, the password must be at least N2 characters in length and must meet the passphrase requirement.
   - *N3* – Used for passwords consisting of at least three character classes. For this rule to apply, the password must be at least N3 characters in length.
   - *N4* – Used for passwords consisting of at least four character classes. For this rule to apply, the password must be at least *N4* characters in length.

   To comply with U.S. Department of Defense security requirements, set the *N0,N1,N2,N3, N4* parameters to `disabled,disabled,disabled,disabled,15`. This ensures that the only passwords that are accepted consist of at least four character classes (uppercase, lowercase, numeric, and special) and are at least 15 characters in length.

   Note - Uppercase letters at the beginning of the password, and digits at the end of the password are not counted when calculating the number of character classes.

For example, to set password complexity that meets U.S. Department of Defense requirements, type:

```
# /opt/oracle.cellos/host_access_control pam-auth --passwdqc disabled,disabled,disabled,disabled,15
```

3. **Verify the current status of this setting.**

```
# /opt/oracle.cellos/host_access_control pam-auth --status | grep min=
```

Configure a Password History Policy

By default, the storage servers define a password history policy that prevents users from reusing their last 10 passwords.

1. **Log into the storage server as `celladmin`.**

   See "Log into the Storage Server OS" on page 91.

2. **View the current setting.**

```
# /opt/oracle.cellos/host_access_control pam-auth --status | grep remember=
```

3. **Change the password history.**

   To comply with U.S. U.S. Department of Defense security and PCI-DSS requirements, set the password history policy to `5`. This ensures that an account cannot reuse any of the five previous passwords assigned to the account. If necessary, replace that value with one that is compliant with your local site policies.

   ```
   # /opt/oracle.cellos/host_access_control pam-auth --remember 5
   ```

4. **To verify the setting, repeat Step 2.**

Configure a Failed Authentication Lock Delay

By default, the storage servers implement a policy where a system account is locked for 10 minutes after any single failed authentication attempt.

To change this threshold, perform this procedure.

1. **Log into the storage server as `celladmin`.**
   See "Log into the Storage Server OS" on page 91.

2. **View the current setting.**

```
# /opt/oracle.cellos/host_access_control pam-auth --status | grep lock_time=
```

3. **Change the threshold.**
   To comply with U.S. Department of Defense security requirements, set the value to 4 seconds. If necessary, replace that value with one that is compliant with your local site policies.

```
# /opt/oracle.cellos/host_access_control pam-auth --lock 4
```

4. **To verify the setting, repeat Step 2.**

Configure Password Aging Control Policies

The storage servers support a variety of password aging controls, including parameters to control the maximum number of days a password is used, the minimum number of days between passwords changes, and the number of days in advance of password expiration that a user is warned.

To comply with U.S. Department of Defense security and PCI-DSS requirements, use the U.S. Department of Defense values in this table.

Policy	Oracle Default Value	DOD Value
Maximum password lifetime	90 days	60 days
Minimum password lifetime	1 day	1 day
Minimum password length	8 characters	15 characters
Password expiration warning	7 days	7 days

To change any of these parameters, perform this procedure.

1. **Log into the storage server as `celladmin`.**
   See "Log into the Storage Server OS" on page 91.

2. **View the current settings.**

```
# /opt/oracle.cellos/host_access_control password-policy --status
```

3. **Configure these policies according to your site password policies.**

   - **Change the maximum password lifetime parameter.**

     ```
     # /opt/oracle.cellos/host_access_control password-policy --PASS_MAX_DAYS 60
     ```

   - **Change the minimum password lifetime parameter.**

     ```
     # /opt/oracle.cellos/host_access_control password-policy --PASS_MIN_DAYS 1
     ```

   - **Change the minimum password length parameter.**

     ```
     # /opt/oracle.cellos/host_access_control password-policy --PASS_MIN_LEN 15
     ```

   - **Change the password expiration warning parameter.**

     ```
     # /opt/oracle.cellos/host_access_control password-policy --PASS_WARN_AGE 7
     ```

4. **To verify the settings, repeat Step 2.**

Configure the Administrative Interface Inactivity Timeout (Login Shell)

The storage server supports the ability to terminate administrative sessions that are inactive for more than a predefined number of seconds.

To define the administrative interface inactivity timeout for a system account login shell, perform this procedure.

1. **Log into the storage server as `celladmin`.**
   See "Log into the Storage Server OS" on page 91.

2. **View the current setting.**

   ```
   # /opt/oracle.cellos/host_access_control idle-timeout --status | grep Shell
   ```

3. **Define the administrative interface inactivity timeout.**
   To comply with U.S. Department of Defense security and PCI-DSS requirements, specify a value of `900` (seconds). If necessary, replace that value with one that is compliant with your local site policy.

   ```
   # /opt/oracle.cellos/host_access_control idle-timeout --shell 900
   ```

4. **To verify the setting, repeat Step 2.**

Configure the Administrative Interface Inactivity Timeout (Secure Shell)

The storage server supports the ability to terminate administrative SSH sessions that have been inactive for more than a predefined number of seconds.

To define the administrative interface inactivity timeout for an SSH session, perform this procedure.

1. **Log into the storage server as `celladmin`.**

   See "Log into the Storage Server OS" on page 91.

2. **View the current setting.**

   ```
   # /opt/oracle.cellos/host_access_control idle-timeout --status | grep SSH
   ```

3. **Define the administrative interface inactivity timeout for an SSH session.**

   To comply with U.S. Department of Defense security requirements, specify a value of `900` (seconds). If necessary, replace that value with one that is compliant with local site policy.

   ```
   # /opt/oracle.cellos/host_access_control idle-timeout --client 900
   ```

4. **To verify the setting, repeat Step 2.**

Configure a Login Warning Banner (Storage Server)

The storage server supports the ability to display customer-specific messages before a user successfully authenticates to the system.

To define a pre-authentication login warning banner, perform this procedure.

1. **Log into the storage server as `celladmin`.**

   See "Log into the Storage Server OS" on page 91.

2. **Determine the current setting.**

   ```
   # /opt/oracle.cellos/host_access_control banner --status
   ```

3. **Create a text file that contains the approved login warning banner message.**

4. **Define a pre-authentication login warning banner.**

   To comply with U.S. Department of Defense security requirements replace *filename* with the path and name of an file that contains the approved login warning banner message.

   ```
   # /opt/oracle.cellos/host_access_control banner --file filename
   ```

5. **To verify the setting, repeat Step 2.**

Limiting Remote Network Access

You can limit inbound remote network access to the storage servers by implementing a filtering rule set. You can also fine tune network access by defining a custom rule set.

Use these procedures to limit remote access.

- “Storage Server Management Network Isolation” on page 102
- “Limit Remote Network Access” on page 102

Storage Server Management Network Isolation

The storage server is deployed on a dedicated, isolated management network. This helps to shield the storage server from unauthorized or unintended network traffic. Access to the management network must be strictly controlled with access granted only to those administrators requiring this level of access.

▼ Limit Remote Network Access

There are several ways that you can limit remote network access on the storage servers. You can restrict Inbound network access to the storage server by implementing a top-down filtering rule

set that defines access by user account and origin. You can also define a custom rule set to allow or deny access according to U.S. Department of Defense and PCI-DSS requirements.

Caution - Use caution when implementing nondefault policies to ensure that access to the system is not interrupted. When you add new individual rules, the changes take effect immediately.

To implement a rule set, perform this procedure.

1. **Log into the storage server as `celladmin`.**

   See "Log into the Storage Server OS" on page 91.

2. **Examine the active rule set.**

   ```
   # /opt/oracle.cellos/host_access_control access --status
   ```

3. **Export the current rule set to a file and save it as a backup copy.**

   This command exports the rule set to an ASCII text file:

   ```
   # /opt/oracle.cellos/host_access_control access-export --file filename
   ```

4. **Configure the rule set by performing one or more of these commands, based on the method you want to use to create the rule set:**

   - **Implement an open rule set that removes inbound network restrictions.**

     ```
     # /opt/oracle.cellos/host_access_control access --open
     ```

   - **Implement a closed rule set that only permits inbound access using SSH.**

     ```
     # /opt/oracle.cellos/host_access_control access --close
     ```

   - **Modify the existing rule set.**

     Export the current rule set to an ASCII text file:

     ```
     # /opt/oracle.cellos/host_access_control access-export --file filename
     ```

     Use an editor to edit the text file to configure the rule set.

     Import the rule set from the text file, overriding the existing rule set:

     ```
     # /opt/oracle.cellos/host_access_control access-import --file filename
     ```

   - **Add specific rules individually.**

This method includes allowing and denying access based on these parameters:

- **Username** – Valid values include either the keyword `all` or one or more valid, local account user names.
- **Origin** – Valid values include either the keyword `all` or individual entries that describe the source of system access including from the console, virtual console, Oracle ILOM, IP address, network address, host name, or DNS domain.

In this example, access to the storage server is granted to the `celladmin` user when the connection is initiated from the `trustedhost.example.org`host, or any host within the `.trusted.example.com` domain.

```
# /opt/oracle.cellos/host_access_control access --add --user celladmin \
--origins trustedhost.example.org,.trusted.example.com
```

Additional Storage Server Resources

Refer to the Exadata Database Machine Security Guide at http://docs.oracle.com/cd/E50790_01/welcome.html.

Securing the IB and Ethernet Switches

The Oracle Sun Data Center InfiniBand Switch 36 that is used by SuperCluster provides the network foundation for a high performance, highly scalable, and fully redundant backplane across all of the internal components.

The IB switches connect the compute servers, storage cells, and the ZFS storage appliance. The IB switches incorporate an embedded Oracle ILOM to provide advanced management and monitoring capabilities. In particular, the Oracle ILOM enables the monitoring and control of users, hardware, services, protocols, and other configuration parameters.

SuperCluster M8 and SuperCluster M7 have a minimum of two IB switches, with additional IB switches installed as needed for larger configurations. You must secure each individual IB switch.

These topics describe how to secure the IB switches in SuperCluster M8 and SuperCluster M7:

▼ Log Into an IB Switch

This task describes how to log into the Oracle ILOM interface on the switch, where the majority of administrative tasks are preformed.

- **On the management network, log into Oracle ILOM on the IB switch as `ilom-admin`.**
  See "Default User Accounts and Passwords" on page 32.

```
% ssh ilom-admin@IB_Switch_ILOM_IPaddress
->
```

Determine the IB Switch Firmware Version

To leverage the most recent features, capabilities, and security enhancements, ensure that the IB switch is updated with the latest, supported firmware version.

1. **Log into an IB switch as `ilom-admin`.**

   See "Log Into an IB Switch" on page 105.

2. **Display the firmware version.**

   In this example, the IB switch firmware is version `2.1.5-1`.

```
-> version
SP firmware 2.1.5-1
SP firmware build number: 47111
SP firmware date: Sat Aug 24 16:59:14 IST 2013
SP filesystem version: 0.1.22
```

   To update the version of IB switch firmware, install the most recent SuperCluster Quarterly Full Stack Download Patch available from My Oracle Support at `https://support.oracle.com`.

Note - For SuperCluster M8 and SuperCluster M7, additional restrictions might limit the versions of the IB switch software that can be used. The restrictions also dictate how the firmware is updated. In these situations, contact your Oracle representative.

Change `root` and `nm2user` Passwords

The IB switch maintains system accounts in two locations. The `root` and `nm2user` accounts are configured and exposed by the switch's underlying OS. Adding, removing, or changing accounts is not supported at this layer, but you can changevpasswords.

For other accounts and passwords, see "Change IB Switch Passwords (Oracle ILOM)" on page 107.

The IB switch does not have the ability to define or enforce password complexity, aging, history, or other rules. You must ensure that passwords assigned comply with U.S. Department

of Defense password complexity requirements and processes are implemented to ensure passwords are updated in accordance with U.S. Department of Defense policy.

For more information on IB switch account management, including how to create new accounts, assign permissions to existing accounts, or remove accounts, refer to the *Oracle Sun Data Center InfiniBand Switch 36 Hardware Security Guide* and the *Oracle Integrated Lights Out Manager Supplement for the Oracle Sun Data Center InfiniBand Switch 36*. See "Additional IB Switch Resources" on page 114.

Note - When a password is changed for any SuperCluster component that Oracle Engineered Systems Hardware Manager manages (such as the IB switches), you must also update the password in Oracle Engineered Systems Hardware Manager. For details, refer to the *Oracle SuperCluster M8 and SuperCluster M7 Administration Guide*.

---

1. **Log into the IB switch as `root`.**

   ```
   # ssh root@IB_Switch_IP_address
   ```

   See "Default User Accounts and Passwords" on page 32.

2. **Change the `root` password.**

   ```
   $ passwd root
   ```

3. **Change the `nm2user` password.**

   ```
   $ passwd nm2user
   ```

▼ Change IB Switch Passwords (Oracle ILOM)

The IB switch maintains system accounts in two locations. This section describes how to change passwords on the IB switch's Oracle ILOM interface. For other accounts and passwords, see "Change `root` and `nm2user` Passwords" on page 106.

Default IB switch accounts and any customer-defined accounts are managed through the embedded Oracle ILOM on the IB switches.

To view accounts and change passwords, perform this procedure.

1. **Log into an IB switch as `ilom-admin`.**

   See "Log Into an IB Switch" on page 105.

   See "Default User Accounts and Passwords" on page 32.

2. **View configured Oracle ILOM accounts on the IB switch.**

   ```
   -> show /SP/users
   ```

3. **Change the password for the `ilom-admin` account.**

   ```
   -> set /SP/users/ilom-admin password=password
   ```

IB Switch Network Isolation

The management interface of the IB switch is deployed on a dedicated, isolated management network. This shields the IB switch from unauthorized or unintended network traffic.

Access to this management network must be strictly controlled with access granted only to those administrators requiring this level of access.

Default Exposed Network Services (IB Switch)

Service Name	Protocol	Port	Description
SSH	TCP	22	Used by the integrated Secure Shell service to enable administrative access to the IB switch using a CLI.
HTTP (BUI)	TCP	80	Used by the integrated HTTP service to enable administrative access to the IB switch using a browser interface. While TCP/80 is typically used for clear-text access, by default the IB switch automatically redirects incoming requests to the secure version of this service running on TCP/443.
NTP	UDP	123	Used by the integrated NTP (Network Time Protocol) (client only) service used to synchronize the local system clock to one or more external time sources.
SNMP	UDP	161	Used by the integrated SNMP service to provide a management interface to monitor the health of the IB switch and to monitor received trap notifications.
HTTPS (BUI)	TCP	443	Used by the integrated HTTPS service to enable administrative access to the IB switch over an encrypted (SSL/TLS) channel using a browser interface.
IPMI	TCP	623	Used by the integrated Intelligence Platform Management Interface (IPMI) service to provide a computer interface for various monitoring and management functions. Do not disable this service, because it is used by Oracle Enterprise Manager Ops Center to collect hardware inventory data, field replaceable unit descriptions, hardware sensor information, and hardware component status information.
ServiceTag	TCP	6481	Used by the Oracle ServiceTag service. This is an Oracle discovery protocol used to identify servers and facilitate service requests. This service is used by products such as Oracle Enterprise Manager Ops Center to discover IB switch software and to integrate with other Oracle automatic service solutions.

Hardening the IB Switch Configuration

These topics describe how to secure the IB switch through various configuration settings.

▼ Disable Unnecessary Services (IB Switch)

Disable any services that are not required to support the operational and management requirements of the platform. By default, the IB switch employs a network secure-by-default configuration whereby nonessential services are already disabled. However, based upon customer security policies and requirements, it might be necessary to disable additional services.

1. **Log into an IB switch as `ilom-admin`.**

   See "Log Into an IB Switch" on page 105.

2. **Determine the list of services supported by the IB switch.**

```
-> show /SP/services
```

3. **Determine if a given service is enabled.**

   Replace *servicename* with the name of a service from Step 2.

```
-> show /SP/services/servicename servicestate
```

While the majority of services recognize and use the `servicestate` parameter to record whether the service is enabled or disabled, there are a few services such as `servicetag`, `ssh`, `sso`, and `wsman` that use a parameter called `state`. Regardless of the actual parameter used, a service is enabled if the service state parameter returns a value of `enabled`, as shown in these examples:

```
-> show /SP/services/https servicestate
/SP/services/https
Properties:
servicestate = enabled


-> show /SP/services/ssh state
/SP/services/ssh
Properties:
state = enabled
```

4. **To disable a service that is no longer required, set the service state to `disabled`.**

```
-> set /SP/services/http servicestate=disabled
```

5. **Determine if any of these services should be disabled.**

   Depending on the tools and methods used, the HTTP and HTTPS browser services can be disabled if they are not required or used. Type:

```
-> set /SP/services/http servicestate=disabled
-> set /SP/services/http secureredirect=disabled
-> set /SP/services/https servicestate=disabled
```

   - Browser Administrative Interface (HTTP, HTTPS):

     -> **set /SP/services/http servicestate=disabled**

     -> **set /SP/services/http secureredirect=disabled**

     -> **set /SP/services/https servicestate=disabled**

▼ Configure HTTP Redirection to HTTPS (IB Switch)

By default, the IB switch is configured to redirect incoming HTTP requests to the HTTPS service to ensure that all of the browser-based communications are encrypted between the switch and the administrator.

1. **Log into an IB switch as `ilom-admin`.**

   See "Log Into an IB Switch" on page 105.

2. **Verify that secure redirection is enabled.**

```
-> show /SP/services/http secureredirect
/SP/services/https
Properties:
secureredirect = enabled
```

3. **If the default has been changed, you can enable secure redirection.**

```
-> set /SP/services/http secureredirect=enabled
```

▼ Disable Unapproved SNMP Protocols (IB Switch)

By default, SNMPv1, SNMPv2c, and SNMPv3 are all enabled for the SNMP service that is used to monitor and manage the IB switch. Ensure that older versions of the SNMP protocol remain disabled unless required.

Note - Version 3 of the SNMP protocol introduced support for the User-based Security Model (USM). This functionality replaces the traditional SNMP community strings with actual user accounts that can be configured with specific permissions, authentication, and privacy protocols, and passwords. By default, the IB switch does not include any USM accounts. Configure SNMPv3 USM accounts based upon your own deployment, management, and monitoring requirements.

---

1. **Log into an IB switch as `ilom-admin`.**

   See "Log Into an IB Switch" on page 105.

2. **Determine the status of each of the SNMP protocols.**

```
-> show /SP/services/snmp v1 v2c v3
/SP/services/snmp
Properties:
v1 = enabled
v2c = enabled
v3 = enabled
```

3. **If needed, disable SNMPv1 and SNMPv2c.**

```
-> set /SP/services/snmp v1=disabled
-> set /SP/services/snmp v2c=disabled
```

Configure SNMP Community Strings (IB Switch)

This task is only applicable if SNMP v1 or SNMPv2c is enabled and configured for use.

Because SNMP is often used to monitor the health of the device, it is important that the default SNMP community strings used by the device be replaced with customer-defined values.

1. **Log into an IB switch as `ilom-admin`.**

   See "Log Into an IB Switch" on page 105.

2. **Create a new SNMP community string.**

   In this example, replace these items in the command line:

   - *string* – Replace with a customer-defined value that is compliant with U.S. Department of Defense requirements regarding the composition of SNMP community strings.
   - *access* – Replace with either `ro` or `rw`, depending on whether this is a read-only or read-write access string.

   ```
   -> create /SP/services/snmp/communities/string permission=access
   ```

   Once new community strings are created, the default community strings must be removed.

3. **Remove the default SNMP community strings.**

   ```
   -> delete /SP/services/snmp/communities/public
   -> delete /SP/services/snmp/communities/private
   ```

4. **Verify the SNMP community strings.**

   ```
   -> show /SP/services/snmp/communities
   ```

Replace Default Self-Signed Certificates (IB Switch)

The IB switches use self-signed certificates to enable the out-of-the-box use of the HTTPS protocol. As a best practice, replace self-signed certificates with certificates that are approved for use in your environment and signed by a recognized certificate authority.

The IB switch supports a variety of methods that can be used to access the SSL/TLS certificate and private key, including HTTPS, HTTP, SCP, FTP, TFTP, and pasting the information directly into a web browser interface. For more information, refer to the *Oracle Integrated Lights Out Manager Supplement for the Oracle Sun Data Center InfiniBand Switch 36 document*. See "Additional IB Switch Resources" on page 114.

1. **Log into an IB switch as `ilom-admin`.**

   See "Log Into an IB Switch" on page 105.

2. **Determine if the IB switch is using a default self-signed certificate.**

```
-> show /SP/services/https/ssl cert_status
/SP/services/https/ssl
Properties:
cert_status = Using Default (No custom certificate or private key loaded)
```

3. **Install your organization's certificate.**

```
-> load -source URI /SP/services/https/ssl/custom_cert
-> load -source URI /SP/services/https/ssl/custom_key
```

▼ Configure the Administrative CLI Session Timeout (IB Switch)

The IB switches support the ability to disconnect and log out administrative CLI sessions that have been inactive for more than a predefined number of minutes.

By default, the CLI is timed out after 15 minutes.

1. **Log into an IB switch as `ilom-admin`.**

   See "Log Into an IB Switch" on page 105.

2. **Check the inactivity timeout parameter associated with the CLI.**

```
-> show /SP/cli timeout
/SP/cli
Properties:
timeout = 15
```

3. **Set the inactivity timeout parameter.**

   Replace *n* with a value specified in minutes.

```
-> set /SP/cli timeout=n
```

Additional IB Switch Resources

For more information on IB switch administration and security procedures, refer to the Sun Datacenter InfiniBand Switch 36 documentation library at http://docs.oracle.com/cd/E36265_01.

▼ Change the Ethernet Switch Password

Note - When a password is changed for any SuperCluster component that Oracle Engineered Systems Hardware Manager manages (such as the Ethernet switch), you must also update the password in Oracle Engineered Systems Hardware Manager. For details, refer to the *Oracle SuperCluster M8 and SuperCluster M7 Administration Guide*.

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.**

Auditing for Compliance

Use the Oracle Solaris compliance utility to assess and report the compliance of a system to a known benchmark.

The Oracle Solaris `compliance` command maps the requirements of a benchmark to the code, file, or command output that verifies compliance to a specific requirement. Oracle SuperCluster currently supports two security compliance benchmark profiles:

- **Recommended** – A profile based on the Center of Internet Security benchmark.
- **PCI-DSS** – A profile that verifies Payment Card Industry Data Security Standard (PCI DSS) compliance requirements.

These profiling tools map security controls to the compliance requirements, and the resulting compliance reports can reduce significant auditing time. In addition, the compliance feature provides guides that contain the rationale for each security check, and the steps to fix a failed check. Guides can be useful for training and as guidelines for future testing. By default, guides for each security profile are created at installation. The SuperCluster Solaris administrator can add or change a benchmark and create a new guide.

These topics describe how to run compliance reports and describe FIPS-140 compliance:

- "Generate a Compliance Assessment" on page 117
- "(Optional) Run Compliance Reports with a `cron` Job" on page 120
- "FIPS-140-2 Level 1 Compliance" on page 120

▼ Generate a Compliance Assessment

To perform this task, you must be assigned the Software Installation rights profile to add packages to the system. You must be assigned administrative rights for most compliance commands.

1. **Install the compliance package.**

```
# pkg install compliance
```

This message indicates that the package is installed:

```
No updates necessary for this image.
```

For more information, refer to the `pkg(1)` man page.

Note - Install the package in every zone where you plan to run compliance tests.

2. **List available benchmarks, profiles, and any previous assessments.**

   In this example, there are two benchmarks.

   - **`pci-dss`** – includes one profile called `Solaris_PCI-DSS`
   - **`solaris`** – includes two profiles called `Baseliine` and `Recommended`

```
# compliance list -p
Benchmarks:
pci-dss: Solaris_PCI-DSS
solaris: Baseline, Recommended
Assessments:
No assessments available
```

3. **Generate a compliance assessment.**

   Run the `compliance` command with this syntax:

`compliance assess -b` *benchmark* `-p` *profile*

`-b`	Specifies a particular benchmark. if not specified, the value defaults to `solaris`.
`-p`	Specifies the profile. The profile name is case sensitive. if not specified, the value defaults to the first profile.

   Examples:

   - Using the `Recommended` profile.

```
# compliance assess -b solaris -p Recommended
```

     The command creates a directory in `/var/share/compliance/assessments` that contains the assessment in three files: a log file, an XML file, and an HTML file.

   - Using the PCI-DSS profile:

```
# compliance assess -b pci-dss
```

Note - The `pci-dss` benchmark only has one profile, so the profile option (`-p`) is not required on the command line.

4. **Verify that compliance files were created.**

```
# cd /var/share/compliance/assessments/filename_timestamp
# ls
recommended.html
recommended.txt
recommended.xml
```

Note - If you run the same `compliance` command again, the files are not replaced. You must remove the files before reusing an assessment directory.

5. **(Optional) Create a customized report.**

You can run customized reports repeatedly. However, you can only run the assessment once in the original directory.

In this example, the `-s` option is used to select which result types should appear in the report.

By default, all result types appear in the report except `notselected` or `notapplicable`. The result types are specified as a comma separated list to display in addition to the default. Individual results types can be suppressed by preceding them with a `-`, while starting the list with an = specifies exactly which result types should be included. Result types are: `pass`, `fixed`, `notchecked`, `notapplicable`, `notselected`, `informational`, `unknown`, `error`, or `fail`.

```
# compliance report -s -pass,fail,notselected
/var/share/compliance/assessments/filename_timestamp/report_A.html
```

This command creates a report that contains failed and not selected items in HTML format. The report is run against the most recent assessment.

6. **View the full report.**

You can view the log file in a text editor, view the HTML file in a browser, or view the XML file in an XML viewer. For example, to view the customized HTML report from the preceding step, type the following browser entry:

```
file:///var/share/compliance/assessments/filename_timestamp/report_A.html
```

7. **Fix any failures that your security policy requires to pass.**

If the fix includes rebooting the system, reboot the system before running the assessment again.

8. **Repeat the assessment until there are no failures.**

▼ (Optional) Run Compliance Reports with a `cron` Job

- **As superuser, use the `crontab -e` command to add the appropriate entry to the `crontab` file.**

  This list provides examples of `crontab` entries:

  - Runs daily compliance assessments at 2:30 a.m.

    ```
    30 2 * * * /usr/bin/compliance assess -b solaris -p Baseline
    ```

  - Runs weekly compliance assessments at 1:15 a.m. Sundays

    ```
    15 1 * * 0 /usr/bin/compliance assess -b solaris -p Recommended
    ```

  - Runs monthly assessments on the first of the month at 4:00 a.m.,

    ```
    0 4 1 * * /usr/bin/compliance assess -b pci-dss
    ```

  - Runs assessments on the first Monday of the month at 3:45 a.m.,

    ```
    45 3 1,2,3,4,5,6,7 * 1 /usr/bin/compliance assess
    ```

FIPS-140-2 Level 1 Compliance

The cryptographic applications hosted on SuperCluster rely on the Cryptographic Framework feature of Oracle Solaris, which is validated for FIPS 140-2 Level 1 compliance. The Oracle Solaris Cryptographic Framework is the central cryptographic store for Oracle Solaris, and it provides two FIPS 140–verified modules that support the user-space and kernel-level processes. These library modules provide encryption, decryption, hashing, signature generation and verification, certificate generation and verification, and message authentication functions for applications. User-level applications that call into these modules run in FIPS 140 mode.

In addition to the Oracle Solaris Cryptographic Framework, the OpenSSL object module bundled with Oracle Solaris is validated for FIPS 140-2 Level 1 compliance, which supports the cryptography for applications based on the Secure Shell and TLS protocols. The cloud service provider can choose to enable the tenant hosts with FIPS 140–compliant modes. When running in FIPS 140–compliant modes, Oracle Solaris and OpenSSL, which are FIPS 140-2 providers, enforce the use of FIPS 140– validated cryptographic algorithms.

Also see “(If Required) Enable FIPS-140 Compliant Operation (Oracle ILOM)” on page 41.

This table lists FIPS approved algorithms that are supported by Oracle Solaris on SuperCluster M8 and SuperCluster M7.

Key or CSP	Certificate Number	
	v1.0	**v1.1**
Symmetric Key		
AES: ECB, CBC, CFB-128, CCM, GMAC, GCM, and CTR modes for 128-, 192-, and 256-bit key sizes	#2311	#2574
AES: XTS mode for 256- and 512-bit key sizes	#2311	#2574
TripleDES: CBC and ECB mode for keying option 1	#1458	#1560
Asymmetric Key		
RSA PKCS#1.5 signature generation/verification: 1024-, 2048-,bit (with SHA-1, SHA-256, SHA-384, SHA-512)	#1194	#1321
ECDSA signature generation/verification: P-192, -224, -256, -384, -521; K-163, -233, -283, -409, -571; B-163, -233, -283, -409, -571	#376	#446
Secure Hashing Standard (SHS)		
SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	#1425	#1596
(Keyed-) Hash-based Message Authentication		
HMAC SHA-1, HMAC SHA-224, HMAC SHA-256, HMAC SHA-384, HMAC SHA-512	#1425	#1596
Random Number Generators		
swrand FIPS 186-2 Random Number Generator	#1154	#1222
n2rng FIPS 186-2 Random Number Generator	#1152	#1226

Oracle Solaris offer two providers of cryptographic algorithms that are validated for FIPS 140-2 Level 1.

- The Cryptographic Framework feature of Oracle Solaris is the central cryptographic store on an Oracle Solaris system and provides two FIPS 140 modules. The userland module supplies cryptography for applications that run in user space and the kernel module provides cryptography for kernel-level processes. These library modules provide encryption, decryption, hashing, signature generation and verification, certificate generation and verification, and message authentication functions for applications. User- level applications that call into these modules run in FIPS 140 mode, for example, the `passwd` command and IKEv2. Kernel-level consumers, for example Kerberos and IPsec, use proprietary APIs to call into the kernel Cryptographic Framework.
- The OpenSSL object module provides cryptography for SSH and web applications. OpenSSL is the Open Source toolkit for the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols, and provides a cryptography library. In Oracle Solaris, SSH and the Apache Web Server are consumers of the OpenSSL FIPS 140 module. Oracle Solaris ships a FIPS 140 version of OpenSSL with Oracle Solaris 11.2 that is available to all consumers but the version shipped with Oracle Solaris 11.1 is available to Solaris SSH only. Because FIPS 140-2 provider modules are CPU intensive, they are not enabled by default. As the administrator, you are responsible for enabling the providers in FIPS 140 mode and configuring consumers.

For more information on enabling FIPS-140 providers on Oracle Solaris, refer to the document titled *Using a FIPS 140 Enabled System in Oracle Solaris 11.2*, available under the Securing the Oracle Solaris 11 Operating System heading at: http://docs.oracle.com/cd/E36784_01.

Keeping SuperCluster M8 and SuperCluster M7 Systems Secure

These topics describe the SuperCluster M8 and SuperCluster M7 features that you can use to maintain security over the life of the system:

Managing SuperCluster Security

SuperCluster M8 and SuperCluster M7 leverage 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

Oracle ILOM is a service processor embedded in many SuperCluster M8 and SuperCluster M7 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 time stamp. 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 documentation at: https://docs.oracle.com/cd/F24624_01/index.html#ilom.

Oracle Identity Management Suite

Oracle Identity Management suite manages the end-to-end life-cycle of user identities and accounts across an organization. The 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, but also for the underlying infrastructure and services that manage it.

For more information, refer to the Oracle Identity Management documentation at https://www.oracle.com/middleware/technologies/identity-management/.

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 SuperCluster, 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 Engineered Systems Hardware Manager

Oracle Engineered Systems Hardware Manager is a BUI-based rack-level hardware management tool intended for use by Oracle Service personnel. For details, refer to the *Oracle SuperCluster M8 and SuperCluster M7 Administration Guide*.

Oracle Engineered Systems Hardware Manager includes two sets of authentication information:

- **SuperCluster M8 and SuperCluster M7 Component Passwords**

  Oracle Engineered Systems Hardware Manager keeps a secure store of passwords for all of the factory accounts for all of the SuperCluster M8 and SuperCluster M7 hardware. The software uses these passwords to manage the SuperCluster M8 and SuperCluster M7 components.

  When any of these passwords change, you must update the Oracle Engineered Systems Hardware Manager application with the new passwords.
- **Local Authentication**

  Oracle Engineered Systems Hardware Manager has two local user accounts. One account is used by customers to tailor Oracle Engineered Systems Hardware Manager for their environment and to manage the service account. The other account is used by Oracle Service personnel to configure, support, and service SuperCluster M8 and SuperCluster M7 hardware.

Oracle Engineered Systems Hardware Manager provides the following local management resources.

- **Password Policy** – The ability to configure the application passwords according to your corporate policies ensures that the passwords conform to your corporate standards.

  Note - Consult with your Corporate Security Officer for password policy settings.

- **Certificates** – Oracle Engineered Systems Hardware Manager uses certificates to secure communication between the compute servers and the Oracle Engineered Systems Hardware Manager server and BUI. These certificates are created automatically during installation

and are unique to each SuperCluster instance, however, they can be replaced with customer-provided certificates and keys.

- **Ports** – The networking ports used by Oracle Engineered Systems Hardware Manager are configurable in case there is a conflict with your corporate policy. Ports 8001 through 8004 (inclusive) are used.

For configuration instructions, refer to the *Oracle SuperCluster M8 and SuperCluster M7 Administration Guide*.

Oracle Enterprise Manager

Oracle Enterprise Manager suite is a comprehensive and integrated cloud management solution that focuses on life cycle 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, 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 SuperCluster environment can be accomplished in a secure manner.

For more information, refer to Oracle Enterprise Manager documentation at: `https://www.oracle.com/enterprise-manager/technologies/`

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.

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.

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 Security

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.

SuperCluster M8 and SuperCluster 7 systems provide 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" on page 127
- "Database Activity Monitoring and Auditing" on page 128
- "Network Monitoring" on page 128

Workload Monitoring

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 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 Oracle Solaris security information at http://docs.oracle.com/cd/E53394_01/index.html.

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.

Network Monitoring

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 11.4 OS – https://docs.oracle.com/cd/E37838_01/index.html
- Oracle Solaris 11.3 OS – http://docs.oracle.com/cd/E53394_01/index.html
- Oracle Solaris 10 OS – https://docs.oracle.com/cd/F24622_01

Software and Firmware Updating

SuperCluster M8 and SuperCluster M7 system 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 M8 and SuperCluster M7 Product Notes*. Instructions for accessing the Product Notes are available in MOS note 1605591.1.

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

Index

D

E

L

M

N

O

P

R

S

T

U

V

W

Z