

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

ORACLE TECHNICAL WHITE PAPER | MARCH 2018 | E94758-01





## Table of Contents

Disclaimer	1
Introduction	2
Target Audience and Assumed Knowledge	2
Methodology	3
Oracle Solaris Security Checklist	3
Oracle Database 12c Security Checklist	4
STIG Findings and Resolution Actions	4
Summary Findings	4
Oracle Solaris Security Checklist Findings	4
Oracle Database 12c Security Checklist Findings	5
Sun ZFS Storage Appliance Findings	5
Summary of Resolution Actions	5
Configuration Settings	6
Patches and Updates	6
Software Uninstallation	7
Security Software	8
Additional Security Practices	8
Management Network Security Recommendations	8
SPARC M8 Compute Nodes	8
Sun ZFS Storage Appliance	8
Exadata Storage Servers	9
InfiniBand Switches	9



Management Switch	9
Software and Firmware Patching	9
Oracle Storage Server Software Security Configuration	9
Open Security Mode	10
Oracle Automatic Storage Management–Scoped Security Mode	10
Database-Scoped Security Mode	10
Oracle Database Security on the Oracle SuperCluster	10
Conclusion	11
Appendix	12
About the Oracle SuperCluster M8 Platform	12
References	14
Product security guides	14
General White Papers and Documentation	15
Security White Papers and Documentation	15



## Disclaimer

The document is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle. This information has not been reviewed or approved by a US Department of Defense accreditation official.



## Introduction

The United States Defense Information Systems Agency (DISA) creates and maintains a series of security guidelines for Department of Defense (DOD) information systems. These guides, called Security Technical Implementation Guides (STIGs), identify configuration settings and procedural actions that should be taken to improve the security posture of deployed systems. Many government agencies require that systems comply with these guidelines before connecting to a network. This white paper has been created as a recommended practices guide and to provide validation that the security guidelines can be successfully implemented on the Oracle SuperCluster.

The recommendations contained within this paper were developed as a result of the successful STIG application and testing of a live Oracle SuperCluster M8 at the Oracle Enterprise Technology Center in a project conducted by Oracle. While all efforts were made to ensure best security practices, there are no guarantees that Oracle's recommendations will be accepted by accrediting authorities.

## Target Audience and Assumed Knowledge

This document is intended for security practitioners, who should be familiar with Oracle SuperCluster M8, Oracle Solaris 11, Oracle Database 12c and its security features.

## Methodology

A full configuration of the Oracle SuperCluster was utilized as the target for STIG application and testing. Refer to the appendix for a description of the Oracle SuperCluster platform architecture. The system was configured in the same manner, as it would be for delivery to customer sites. The Solaris 11 and Oracle STIG scripts were loaded on the Oracle Database 12c database domain and the general-purpose zone within the domain. After remediation of the open issues, a number of tests were performed to validate correct operation of the system, database, and application services:

- Verification of system reboot without error
- Successful connectivity testing to the servers and storage units via SSH
- Successful connectivity testing to the database via SQL\*Net
- Check of the system logs for errors
- Verification of database and overall cluster health with the database console utility
- Installation and testing of the Oracle Enterprise Manager Ops Center 12c management suite
- Functional and performance testing of the database instances via connections and load from the Swingbench load generator running the "Order Entry" benchmark before and after configuration changes
- Verification of functional operations to Oracle's Sun ZFS Storage Appliance without performance degradation
- Functional and performance testing using the iGen benchmark test suite, which exercised both the Sun ZFS Storage Appliance and the Oracle database

The target system remained stable and functional throughout testing with all of the tests above yielding positive results.

## Oracle Solaris Security Checklist

The DISA published document for the Oracle Solaris 11 STIG Version 1 Release 13 dated October, 27<sup>th</sup> 2017 was utilized as the baseline for the identification of Potential Discrepancy Items (PDI) and documentation of remedy or exception handling. The review was performed with a combination of security automation tools and manually and documented in a comprehensive logs identifying open and closed issues. The DISA Oracle Solaris 11 STIG document can be found at:

<http://iase.disa.mil/stigs/os/unix-linux/Pages/solaris.aspx>

Oracle Solaris 11 is the required base operating system for the Oracle SuperCluster although Oracle Solaris 10 virtual machines and Oracle Solaris 10 zones within Oracle Solaris 11 can also be used. Oracle Solaris 11 is currently certified by Common Criteria at the EAL 4+ level and based on proven Oracle Solaris technologies developed over the last 30 years.

Oracle VM Server for SPARC is the virtualization technology supporting execution of multiple virtual machines in each physical node. Oracle VM Server for SPARC is a proven, mission-critical hypervisor built into the firmware of



Oracle's SPARC M8 chip design. Oracle VM Server for SPARC was used during our testing to enable the creation of separate database and general-purpose zones, all of which were secured.

## Oracle Database 12c Security Checklist

The Oracle Database Security Readiness Review (SRR) scripts are also provided by DISA and intended to identify potential issues that might jeopardize the overall security and integrity of an Oracle Database 12c system. The Oracle Database 12c Security Checklist identifies a series of known security-related items identified in the Database STIG. A security review of the installed Oracle database on the Oracle SuperCluster platform was performed using the checks incorporated into the SRR Oracle Database 12c scripts and documented in this report. Version 8 release 1.8 of the Database SRRs was used. Version 12.1.0.2 of Oracle Database was used in the testing.

## STIG Findings and Resolution Actions

The following sections provide information on configuring security for applications running on Oracle Solaris 11 and SPARC servers.

Oracle reviewed 238 Oracle Solaris 11 based STIG items and 180 Oracle Database items. Our testing documented the status of findings using the following categories:

- Open: We were unable to provide a technical resolution.
- Not a finding: Proper mitigation was applied either by default characteristics or manual intervention.
- Manual: Items that are procedural or site-specific and must be applied by customers.

Separate documents itemizing the exact status of every item are available from your Oracle sales team.

### Summary Findings

The findings from the STIG testing are presented in the following categories:

- Oracle Solaris Security Checklist findings
- Oracle Database 12c Security Checklist findings
- Sun ZFS Storage Appliance findings

### Oracle Solaris Security Checklist Findings

The Oracle Solaris Security Checklist findings are classified into several categories, as shown in Table 1.

**TABLE 1. CATEGORIES FOR ORACLE SOLARIS SECURITY CHECKLIST FINDINGS**

CATEGORY	DESCRIPTION
238	Total Oracle Solaris items reviewed
98	Open findings on standard Oracle SuperCluster installation before remediation
4	Open findings after remediation
38	Manual, site-specific policy or procedural requirements
231	Not a finding after remediation

The four open items for Oracle Solaris 11 were as follows:

- SOL-11.1-040280: CAT 2 – The 'RO' in /etc/user\_attr.d/dcsvcs - prevents 'usermod -f 35 dcsvcs' from being set in /etc/shadow for this system user account.
- SOL-11.1-70130: CAT 2 - UIDs 0-99 are reserved in /etc/passwd - Found UID 22 that is used for user sshd. Note this user was only found in a non-global zone.
- SOL-11.1-090030: CAT 3 - Direct logins must not be permitted to shared, default, application, or utility accounts. The user account 'oracle' is a shared account.
- SOL-11.1-090115: CAT 2 - The operating system must employ PKI solutions – Note a solution is in process.

### Oracle Database 12c Security Checklist Findings

The Oracle Database 12c Checklist evaluated a total of 180 items classified into the categories shown in Table 2.

TABLE 2. CATEGORIES FOR ORACLE DATABASE CHECKLIST FINDING

CATEGORY	DESCRIPTION
180	Total Oracle Database items reviewed
24	Open findings before remediation
0	Open findings after remediation
119	Manual, site-specific policy or procedural requirements
46	Not a finding in default configuration

### Sun ZFS Storage Appliance Findings

The Sun ZFS Storage Appliance provides a Web-based interface and network file services (NFS, iSCSI, SFTP, and so on) to the members of the cluster. The network services are available only via the InfiniBand interconnect and they are not accessible to any other systems on the client access network.

The Web console management interface is available only via the management network, which should be secured and accessed only by storage administration staff. The management network and client access network should not be connected.

### Summary of Resolution Actions

This section contains a summary of the remedial actions that should be taken to resolve the open findings. For clarity, the resolutions are sorted into the following categories for application to the database servers in the Oracle SuperCluster targeted for STIG application:

- **Configuration Settings:** Configuration setting changes to the operating system, utilities, or database
- **Patches and Upgrades:** The application of patches or software/firmware upgrades

- **Software Uninstallation:** Removing installed software from the target system
- **Process or Procedure:** The creation of documentation as well as process or procedure implementation
- **Security Software:** The installation and configuration of software or utilities on the target system, for example anti-virus or host intrusion tools.

## Configuration Settings

Oracle Solaris 11 settings and modifications include the following:

- Login and password system, login, and tty settings
- Removal of, changes to, or disabling of individual accounts and groups
- File or directory ownership and permissions changes or removal
- Initialization files such as bashrc
- The audit subsystem to incorporate new rules and audit log rotation
- cron and scheduling systems
- Firewall, TCP wrappers, and network configuration settings
- Core dump configuration
- Disabled or removed packaged utilities
- Addition of approved DoD login banners, messages, and warnings
- Password contents, according to published policy
- /etc/hosts allow and deny settings
- Configuration of terminal lockout
- NTP server configuration

Oracle Database 12c settings and modifications include the following:

- Enabling and configuring database auditing
- Setting resource limits on user profiles
- Changing system parameters to harden database access
- Implementing a custom password-verify function to comply with STIG password complexity requirements
- Modifying SQL\*Net settings to enforce expiration, connect times, and allowed clients as well as cnt versions
- Setting file or directory ownership and permissions
- Changing passwords on accounts to comply with STIG complexity rules
- Modifying password system configuration and authentication settings
- Establishing SYSMAN permission grants and schema settings
- Implementing encryption for sensitive data
- Configuring TNS Listener according to the STIG checklist

## Patches and Updates

The primary delivery vehicle for SSC Proactive Maintenance is the Quarterly Maintenance Update, which will be released as the Quarterly Full Stack Download Patch (QFSDP) for Oracle SuperCluster.



For Reactive Maintenance situations (break/fix or critical security fix in between quarterly updates), the affected components can be updated as needed in consultation with Oracle Engineered Systems support.

### Software Uninstallation

Oracle Solaris 11 software uninstallation includes network protocols (FTP, NIC, TFTP/installadm, telnet, UUCP, finger), VNC, and instant messaging (pidgin).

Oracle Database 12c software uninstallation includes STIG checklist recommendations, including the uninstallation and removal of database components that are not required or not licensed, as well as the removal of any database SCHEMA, objects, or applications that exclusively support them. This modification is typically performed on a case-by-case basis to support the intended operation and functionality of the database system. Examples of Oracle Database 12c components in this category include Oracle Partitions, Oracle Real Application Clusters (Oracle RAC), and Data Guard. Required components are documented in the application design specification and listed in the System Security Plan.

#### Process or Procedure

The creation and implementation of processes and procedures will be highly site-dependent and dependent on the local security policy. Most of the items in this category are the findings identified as “Open with customer action required.” The following suggested remedial actions summarize a broad spectrum of individual actions to remedy each potential finding identified by the STIG checklist script.

- Applying Oracle Solaris 11 security and hardening guidelines, which are documented in the standard documentation set: [http://docs.oracle.com/cd/E53394\\_01/html/E54807/index.html](http://docs.oracle.com/cd/E53394_01/html/E54807/index.html)
- Ensuring system physical security, including attachment of any external devices
- Periodic application of vendor-recommended patches and security patches
- Maintaining baseline backups and checking file systems against baselines; the Solaris Basic Accounting and Reporting Tool (BART) can help to meet this requirement
- Documenting the system and any variances from STIG policy with the Information Assurance Officer according to STIG recommendations and local policy
- Performing user password and account policy actions
- Maintaining strong separation between the client access network and the management network
- Oracle Database 12c database-scoped processes or procedures include the following:
  - Development and documentation of management and operations policies and processes
  - Verification of the configuration to compliance standards
  - Implementation and testing of database backup and recovery
  - Database change and configuration management
  - Data labeling, encryption, key management, and validation according to compliance requirements, where required
  - Implementation and management of audit information
  - Documentation and implementation of account, access control, and authorization procedures and policies
  - Auditing and compliancy to STIG recommendations and DBMS classification levels

- Configuration and security of network configuration, remote administration encryption, and network perimeter protection.

### Security Software

Oracle Solaris 11 installation of security software or utilities includes the following:

- Installing and configuring a utility such as Oracle Solaris 11 Basic Accounting and Reporting Tool (BART) to create and maintain a system baseline
- Installing and configuring a system vulnerability tool
- Installing and configuring approved virus scan software

## Additional Security Practices

This section contains additional practices that can be utilized to improve the overall security of the Oracle SuperCluster. The practices range from system patching to access control of elements on the management network.

### Management Network Security Recommendations

The Oracle SuperCluster management network provides critical access to the components of the system and it needs to be secured properly. Penetration of the management network allows attempts at access to the Oracle Integrated Lights Out Manager (Oracle ILOM) ports of the various components of the system. Having access to the Oracle ILOM port is similar to having physical access to the system. A user with Oracle ILOM access can power off the system, install new software, or change the root password. Oracle ILOM security controls allow the creation of roles with limited capabilities. Access to the management network should be restricted to a limited population of properly skilled and cleared administration staff using SSH. Oracle ILOM can be accessed via SSH for command-line management or via an SSL-encrypted Web session. Additional ILOM hardening guidance can be found in MOS Doc ID: 2235125.1 *Oracle Whitepaper: Oracle Integrated Lights Out Manager - Security Configuration Supplement for the United States Department of Defense*.

### SPARC M8 Compute Nodes

When configured properly per the Oracle Solaris STIG, these nodes will have complex PROM and root passwords preventing access to the system itself. In addition, the Oracle ILOM admin password should be configured to DISA standards to prevent unauthorized power cycling of the system via the Oracle ILOM console or Web interface. Roles can be used in Oracle Solaris 10 and 11 as well as the Oracle ILOM to allow administration of the system without providing complete root powers.

### Sun ZFS Storage Appliance

The Sun ZFS Storage Appliance is accessed and administered via a Web interface at <https://<ip-address>:215>. It is recommended to change the root password to comply with the DISA standard. In addition, you should create additional users with management roles to allow administrators to configure the system without requiring the root password. The Oracle ILOM admin password should be set to prevent unauthorized power cycling of the system via the Oracle ILOM console or Web interface. The default session timeout for the Web interface is 15 minutes.

The Sun ZFS Storage Appliance is connected via a private InfiniBand domain so that the data services are accessible only to general-purpose domains as assigned during the initial installation and configuration of the



system. The Sun ZFS Storage Appliance can advertise a number of network services to the compute nodes including NFS, FTP, iSCSI, SMB, NDMP, and so on. It should be configured only with the services that are required by the applications. Additional ZFS Storage Appliance hardening guidance can be found in MOS Doc ID: 2273784.1 *Oracle Whitepaper: Oracle ZFS Storage Appliance - Security Configuration Supplement for the United States Department of Defense.*

### **Exadata Storage Servers**

Oracle's Exadata Storage Servers are Intel-based servers running Oracle Linux with Oracle ILOM access via SSH. Ensure that the Oracle ILOM password and root password for each system conforms to the DISA standard. These are considered storage appliances and additional changes to security or configuration settings are not supported. Additional Exadata Storage Servers hardening guidance can be found in MOS Doc ID: 2274231.1 *Oracle Whitepaper: Oracle Exadata Storage Server - Security Configuration Supplement for the United States Department of Defense*

### **InfiniBand Switches**

The InfiniBand switches provide 40 Gb/sec bandwidth interconnection between the compute, storage, and Sun ZFS Storage Appliance nodes. Oracle ILOM for the switches can be accessed via SSH. Refer to the InfiniBand switch hardware security guide for a description of the login names available. Change the passwords for these names so that they conform to the DISA standard. Additional InfiniBand Switch 36 hardening guidance can be found in MOS Doc ID: 2274215.1 *Oracle Whitepaper: Oracle Sun Data Center InfiniBand Switch 36 - Security Configuration Supplement for the United States Department of Defense*

### **Management Switch**

The Management switch is an unmanaged Ethernet switch. Although it has a management port, by default, it is accessible only via telnet, which is not secure. Oracle recommends that the management port not be connected to the management network. The Cisco Catalyst switch can be configured to use SSH if network access is required. This process is documented at:

[http://www.cisco.com/en/US/tech/tk583/tk617/technologies\\_tech\\_note09186a00800949e2.shtml](http://www.cisco.com/en/US/tech/tk583/tk617/technologies_tech_note09186a00800949e2.shtml)

### **Software and Firmware Patching**

Effective proactive patch management is a critical component of any system's security. The application of Oracle-suggested patches and security patches is a minimum recommendation for the establishment of baseline security.

### **Oracle Storage Server Software Security Configuration**

Exadata Cell security is implemented by controlling which Oracle Automatic Storage Management clusters and database servers can access specific grid disks on storage cells.

- To set up security so that all database clients of an Oracle Automatic Storage Management cluster have access to specific grid disks, configure Oracle Automatic Storage Management–scoped security.
- To set up security so that specific database servers of an Oracle Automatic Storage Management cluster have access to specific grid disks, configure database-scoped security.



## Open Security Mode

Exadata Cell security allows open security, Oracle Automatic Storage Management–scoped security, or database security. Open security mode enables access by any database server to a grid disk. Open security mode is useful for test or development databases where there are no security requirements. This is the default security mode after creating a new storage cell. To use this security mode, you do not set up any security functionality for an Oracle Automatic Storage Management cluster or a database server that accesses the grid disk. You do not set up any security key files.

## Oracle Automatic Storage Management–Scoped Security Mode

Oracle ASM-scoped security mode enables access by all the database servers which access Oracle ASM cluster to grid disks on cells. Oracle ASM-scoped security is appropriate when you want all databases on a host cluster to have access to grid disks on cells that compose the Oracle ASM disk groups managed by the Oracle ASM cluster. This includes the case when there is only one database in an Oracle ASM cluster. When Oracle ASM-scoped security is set up for an Oracle ASM cluster and grid disks, the grid disks are available only to the databases on the Oracle ASM cluster.

## Database-Scoped Security Mode

Database-scoped security mode configures access to specific grid disks on cells for specific database servers that are members of an Oracle Automatic Storage Management cluster. This security mode is appropriate when multiple databases are accessing cells, and you want to control which databases can access specific grid disks that comprise Oracle Automatic Storage Management disk groups. Set up Oracle Automatic Storage Management–scoped security for your initial security mode, and then set up database-scoped security for specific database servers and grid disks. After setting up database-scoped security among the database servers and grid disks, only those specific grid disks are available to the specified database servers. When using database-scoped security, there is one key file per database per host and one access control list (ACL) entry per database on each cell.

## Oracle Database Security on the Oracle SuperCluster

From the outset, Oracle has delivered the industry's most advanced technology to safeguard data where it lives—in the database. Oracle provides a comprehensive portfolio of security solutions to ensure data privacy, protect against insider threats, and enable regulatory compliance. Key Oracle Database security products include the following:

- Oracle Database Vault
- Oracle Audit Vault and Database Firewall
- Oracle Configuration Manager
- Oracle Total Recall
- Oracle Advanced Security
- Oracle Data Masking Pack
- Oracle Label Security
- Oracle Secure Backup



With Oracle's powerful privileged user and multifactor access control, data classification, transparent data encryption, auditing, monitoring, and data masking, you can deploy reliable data security solutions that do not require any changes to existing applications, saving time and money.

## Conclusion

The goal of successfully applying STIG-recommended configuration settings to the Oracle SuperCluster platform without negatively affecting the system was achieved and has been documented in this paper. While there is no single formula for application of STIG recommendations in all situations and configurations, the implementation and testing performed during the course of this project has proven that it is reasonable and possible to apply STIG recommendations to the Oracle SuperCluster platform to meet the needs of government and commercial organizations who are required or elect to comply with the recommendations created by DISA for the Department of Defense.

## Appendix

### About the Oracle SuperCluster M8 Platform

The Oracle SuperCluster M8 system is a multipurpose engineered system that combines the computing power of Oracle's SPARC M8 processor, the efficient virtualization capabilities of Oracle VM Server for SPARC, the performance and scalability of the Oracle Solaris operating system, the optimized database performance of Oracle Database integrated with Oracle Exadata Storage Servers, and the innovative network-attached storage capabilities of Oracle ZFS Storage Appliance. Each of these core components is connected over a redundant InfiniBand fabric that enables low latency and high-performance network communications between all of the components. In addition, a 10 GbE network is employed allowing clients to access services running on the Oracle SuperCluster system. Finally, GbE network provides the conduit through which all of the system's components can be managed.

### Oracle SuperCluster M8 Elastic Base: Base Infrastructure for SuperCluster M8 Elastic Configurations

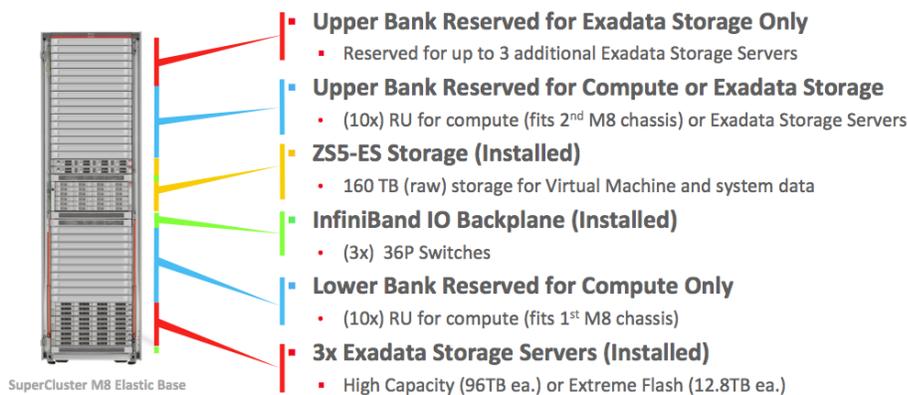


Figure 1. Oracle SuperCluster M8 hardware architecture

The SPARC M8 processor in the system features hardware-assisted virtualization that facilitates ready-to-run secure virtual machines for cloud infrastructure, always-on hardware-assisted cryptographic functionality that helps Oracle SuperCluster–hosted entities to protect their information with high-performance data protection—at rest, in use, and in transit. The processor also features the Silicon Secured Memory capability, which detects and prevents attacks related to memory data corruptions and memory scraping, thereby ensuring the integrity of application data. By default, Oracle SuperCluster M8 is preconfigured with out-of-box security controls that reduce the attack surface of the system by disabling services, ports, and protocols that are not absolutely necessary and by configuring the exposed services to accept only trusted connections.

The system supports a variety of configuration and deployment options. Figure 2 illustrates a typical deployment that consolidates Oracle Database and Oracle WebLogic applications workloads.

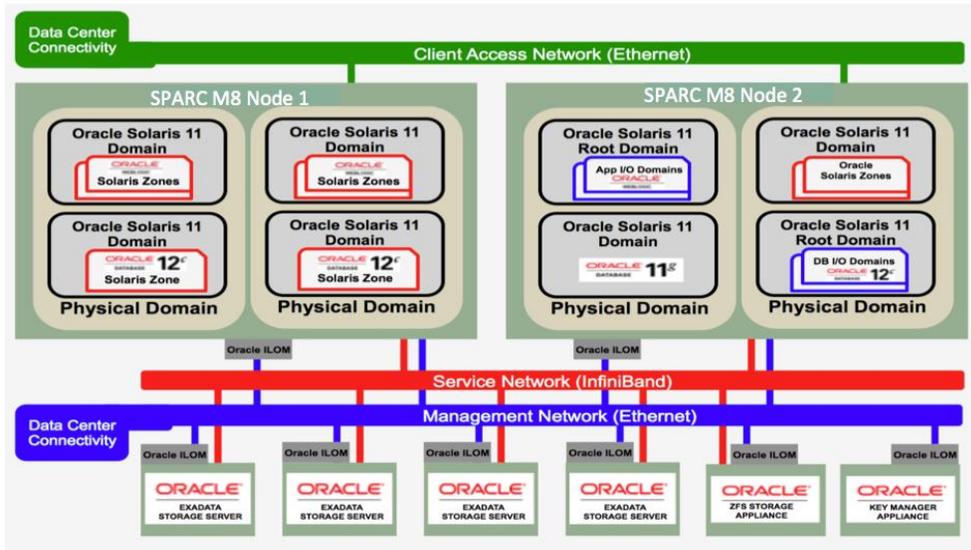


Figure 2. Typical deployment of software workloads on an Oracle SuperCluster M8 system

It is important to have an appreciation for the security capabilities that are exposed by each of the core components engineered into the Oracle SuperCluster M8 architecture. To simplify the presentation of these capabilities in the following sections, they have been grouped into seven distinct categories: namely, secure isolation, access control, data protection services, monitoring and auditing, quality of service, compliance reporting (for example, PCI-DSS, FIPS-140), and security management.

## References

Detailed and current versions of STIG Compliance documents for Oracle Solaris and Oracle Database are available from the DISA website. In addition, see the following resources.

### Product security guides

- “Oracle SuperCluster M7 Platform Security Principles and Capabilities”  
<http://www.oracle.com/us/products/servers-storage/servers/sparc-enterprise/supercluster/supercluster-t4-4/ssc-security-pac-1716580.pdf>
- “Oracle SuperCluster M8 and SuperCluster M7 Security Guide”  
[http://docs.oracle.com/cd/E58626\\_01/pdf/E58630.pdf](http://docs.oracle.com/cd/E58626_01/pdf/E58630.pdf)
- “Oracle SuperCluster – Secure Private Cloud Architecture”  
<http://www.oracle.com/technetwork/server-storage/engineered-systems/oracle-supercluster/documentation/supercluster-secure-multi-tenancy-2734706.pdf>
- “Secure Database Consolidation Using the Oracle SuperCluster T5-8 Platform”:  
<http://www.oracle.com/technetwork/server-storage/sun-sparc-enterprise/documentation/o13-053-securedb-osc-t5-8-1990064.pdf>
- Oracle Integrated Lights Out Manager (ILOM) Security Guide For Firmware Releases 3.x and 4.x:  
[http://docs.oracle.com/cd/E37444\\_01/pdf/E37451.pdf](http://docs.oracle.com/cd/E37444_01/pdf/E37451.pdf)
- Sun Datacenter InfiniBand Switch 36 Hardware Security Guide:  
<http://docs.oracle.com/cd/E19197-01/E26701/E26701.pdf>
- SPARC M8 and SPARC M7 Servers Security Guide  
[http://docs.oracle.com/cd/E55211\\_01/pdf/E55218.pdf](http://docs.oracle.com/cd/E55211_01/pdf/E55218.pdf)
- “Oracle VM Server for SPARC 3.5 Security Guide”  
[https://docs.oracle.com/cd/E80106\\_01/pdf/E80111.pdf](https://docs.oracle.com/cd/E80106_01/pdf/E80111.pdf)
- “Oracle Solaris 10 Security Guidelines”  
[http://docs.oracle.com/cd/E26505\\_01/pdf/E37990.pdf](http://docs.oracle.com/cd/E26505_01/pdf/E37990.pdf)
- “Oracle Solaris 11 Security and Hardening Guidelines”  
[http://docs.oracle.com/cd/E53394\\_01/pdf/E54807.pdf](http://docs.oracle.com/cd/E53394_01/pdf/E54807.pdf)
- “Oracle Database Security Guide 11g Release 2:”  
[https://docs.oracle.com/cd/E11882\\_01/network.112/e36292/toc.htm](https://docs.oracle.com/cd/E11882_01/network.112/e36292/toc.htm)
- “Oracle Database 12c Release 2 Security Guide:”  
<https://docs.oracle.com/database/122/DBSEG/title.htm>
- Oracle Common Criteria status page:  
<http://www.oracle.com/technetwork/topics/security/oracle-common-criteria-095703.html>

## General White Papers and Documentation

- “A Technical Overview of Oracle SuperCluster M8”:

<http://www.oracle.com/us/products/servers-storage/servers/sparc/supercluster/oracle-supercluster-m8-ds-3884269.pdf>

## Security White Papers and Documentation

### Oracle VM Server for SPARC

- Increasing Application Availability by Using the Oracle VM Server for SPARC Live Migration Feature: An Oracle Database Example

<http://www.oracle.com/technetwork/server-storage/vm/ovm-sparc-livemigration-1522412.pdf>

### Oracle Solaris 11 Operating System

- Managing Network Virtualization and Network Resources in Oracle Solaris 11.3

[http://docs.oracle.com/cd/E53394\\_01/html/E54790/index.html](http://docs.oracle.com/cd/E53394_01/html/E54790/index.html)

- Administering Resource Management in Oracle Solaris 11.3

[http://docs.oracle.com/cd/E53394\\_01/pdf/E54740.pdf](http://docs.oracle.com/cd/E53394_01/pdf/E54740.pdf)

### Oracle Database

- Oracle Defense in Depth Guide

<http://www.oracle.com/technetwork/database/security/sol-home-086269.html>

- Cost Effective Security and Compliance with Oracle Database 11g Release 2

<http://www.oracle.com/technetwork/database/security/owp-security-database-11gr2-134651.pdf>

- Oracle Advanced Security with Oracle Database 11g Release 2

<http://www.oracle.com/technetwork/database/owp-security-advanced-security-11gr-133411.pdf>

- Oracle Advanced Security Transparent Data Encryption Best Practices

<http://www.oracle.com/technetwork/database/security/twp-transparent-data-encryption-bes-130696.pdf>

- Oracle Database Vault with Oracle Database 11g Release 2

<http://www.oracle.com/technetwork/database/security/owp-security-database-vault-11gr2-1-131473.pdf>

- DBA Administrative Best Practices with Oracle Database Vault 12c

<http://www.oracle.com/technetwork/database/security/twp-databasevault-dba-bestpractices-199882.pdf>

- Oracle Label Security with Oracle Database 11g Release 2

<http://www.oracle.com/technetwork/database/security/owp-security-label-security-11gr2-133601.pdf>

- Effective Resource Management Using Oracle Database Resource Manager

<http://www.oracle.com/technetwork/articles/servers-storage-admin/o11-056-oracledb-rm-419380.pdf>



Oracle Middleware

- “High Performance Security for Oracle WebLogic Applications using SPARC servers”:  
<http://www.oracle.com/technetwork/articles/systems-hardware-architecture/security-weblogic-t-series-168447.pdf>
- “Securing E-Business Suite Applications using Oracle Solaris 11 on SPARC servers”:  
<http://www.oracle.com/technetwork/server-storage/sun-sparc-enterprise/documentation/o13-044-t5-cbssecurity-1964593.pdf>
- High Performance Security for Oracle WebLogic Applications Using Oracle SPARC Servers  
<http://www.oracle.com/technetwork/articles/systems-hardware-architecture/security-weblogic-t-series-168447.pdf>
- High Performance Security for SOA and XML Web Services Using Oracle SPARC Servers  
<http://www.oracle.com/technetwork/articles/systems-hardware-architecture/hi-perf-soa-xml-svcs-172821.pdf>



**Oracle Corporation, World Headquarters**

500 Oracle Parkway  
Redwood Shores, CA 94065, USA

**Worldwide Inquiries**

Phone: +1.650.506.7000  
Fax: +1.650.506.7200

CONNECT WITH US

-  [blogs.oracle.com/oracle](https://blogs.oracle.com/oracle)
-  [facebook.com/oracle](https://facebook.com/oracle)
-  [twitter.com/oracle](https://twitter.com/oracle)
-  [oracle.com](https://oracle.com)

**Integrated Cloud Applications & Platform Services**

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0615

Oracle SuperCluster M8 Security Technical Implementation Guide (STIG) Validation and Best Practices  
March 2018

Authors: Kevin Rohan, Ramesh Nagappan  
Contributors: Sujeet Vasudevan, Ramin Moazeni



Oracle is committed to developing practices and products that help protect the environment