An Oracle Technical White Paper
February 2014

# Oracle SuperCluster T5-8 Security Technical Implementation Guide (STIG) Validation and Best Practices on the Database Servers

## 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 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.

# Methodology

A half-rack 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 UNIX and Oracle STIG scripts were loaded on the Oracle Database 11*g* Release 2 database domain and the general-purpose 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 12*c* 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 ZFS Storage Appliance without performance degradation
- Functional and performance testing using the iGen benchmark test suite, which exercised both the 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 10 STIG dated June 4, 2012 was utilized as the baseline for the identification of Potential Discrepancy Items (PDI) and documentation of remedy or exception handling. Although the Oracle SuperCluster uses Oracle Solaris 11, most of the recommendations from the Oracle Solaris 10 STIG can be followed. The review was performed manually and documented in a comprehensive spreadsheet identifying open and closed issues. The DISA Oracle Solaris 10 STIG document can be found at:

http://iase.disa.mil/stigs/os/unix/solaris.html

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 in Common Criteria evaluation 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 T4 chip design. Oracle VM Server for SPARC was used during our testing to enable the creation of separate database and general-purpose domains, all of which were secured.

### Oracle Database 11*g* 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 11*g* system. The Oracle Database 11*g* 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 11*g* scripts and documented in this report. Version 8 release 1.8 of the Database SRRs was used. Version 11.2.0.3 of Oracle Database was used in the testing.

## STIG Findings and Resolution Actions

Oracle reviewed 571 Oracle Solaris–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 spreadsheets 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 11*g* Security Checklist findings
- 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 |
|---|---|
| 571 | Total Oracle Solaris items reviewed |
| 89 | Open findings on standard Oracle SuperCluster installation before remediation |
| 3 | Open findings after remediation |
| 43 | Manual, site-specific policy or procedural requirements |
| 525 | Not a finding after remediation |

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

- The Reliable Datagram Sockets (RDS) protocol must be disabled or not installed unless it is required.
- The IPv6 protocol handler must not be bound to the network stack unless it is needed.
- The IPv6 protocol handler must be prevented from dynamic loading unless it is needed.

These are the result of the required InfiniBand network connections. They are configured to use RDS and IPv6 by default and should not be changed. They will need to be documented by the customer staff as required services.

### Oracle Database 11*g* Security Checklist Findings

The Oracle Database 11*g* 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 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 11*g* 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 diagnostic utilities and instant messaging utilities.

Oracle Database 11*g* 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 11*g* 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 guidelines, which are documented in the standard documentation set: http://docs.oracle.com/cd/E23824_01/html/819-3195/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 11*g* 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) or Tripwire 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.

### SPARC T5-8 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.

### ZFS Storage Appliance

The 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 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 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.

### 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.

### InfiniBand Switches

The InfiniBand switches provide 40 Gb/sec bandwidth interconnection between the compute, storage, and 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.

### Ethernet Switch

The Ethernet switch is an unmanaged 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

## 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 recommendation 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.

# References

Detailed STIG Compliance spreadsheets for Oracle Solaris and Oracle Database are available from your Oracle Sales team. In addition, see the following resources.

- Product security guides:
  - "Oracle SuperCluster T5-8 Platform Security Principles and Capabilities": http://www.oracle.com/technetwork/server-storage/sun-sparc-enterprise/documentation/o13-052-osc-t5-8-security-1989641.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) 3.1 Security Guide*: http://docs.oracle.com/cd/E24707_01/pdf/E24526.pdf
  - *Sun Datacenter InfiniBand Switch 36 Hardware Security Guide*: http://docs.oracle.com/cd/E19197-01/E26701/E26701.pdf
  - *Oracle SPARC T5 Series Servers Security Guide* http://docs.oracle.com/cd/E35199_01/pdf/E29503.pdf
  - "Secure Deployment of Oracle VM Server for SPARC": http://www.oracle.com/technetwork/articles/systems-hardware-architecture/secure-ovm-sparc-deployment-294062.pdf
  - *Oracle Solaris 10 Security Guidelines*: http://docs.oracle.com/cd/E23823_01/pdf/E23335.pdf
  - *Oracle Solaris 11 Security Guidelines*: http://docs.oracle.com/cd/E23824_01/pdf/819-3195.pdf
  - *Oracle Database 11g Release 2 Security Guide*: http://www.oracle.com/pls/db112/to_pdf?pathname=server.112/e10575.pdf
- Oracle Common Criteria status page: http://www.oracle.com/technetwork/topics/security/oracle-common-criteria-095703.html

## General White Papers and Documentation

- "Oracle SuperCluster T5-8: Servers, Storage, Networking and Software – Optimized and Ready to Run":

  http://www.oracle.com/us/products/servers-storage/servers/sparc/supercluster/supercluster-t5-8/ssc-t5-8-wp-1964621.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

- Oracle Solaris 11 Network Virtualization and Network Resource Management
  http://www.oracle.com/technetwork/server-storage/solaris11/documentation/o11-137-s11-net-virt-mgmt-525114.pdf
- Effective Resource Management Using Oracle Solaris Resource Manager
  http://www.oracle.com/technetwork/articles/servers-storage-admin/o11-055-solaris-rm-419384.pdf

### Oracle Database 11g

- 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 11gR2
  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 11gR2
  http://www.oracle.com/technetwork/database/security/owp-security-database-vault-11gr2-1-131473.pdf
- DBA Administrative Best Practices with Oracle Database Vault
  http://www.oracle.com/technetwork/database/security/twp-databasevault-dba-bestpractices-199882.pdf
- Oracle Label Security with Oracle Database 11gR2
  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 T5 and SPARC M5 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 T5 and SPARC M5 servers":

  http://www.oracle.com/technetwork/server-storage/sun-sparc-enterprise/documentation/o13-044-t5-ebssecurity-1964593.pdf

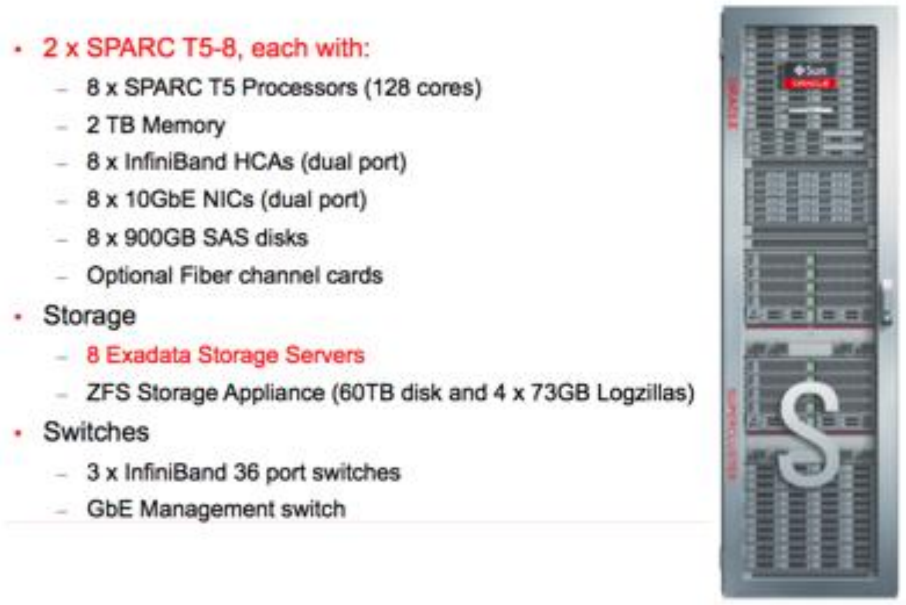
- High Performance Security for Oracle WebLogic Applications Using Oracle SPARC T-Series Servers
  http://www.oracle.com/technetwork/articles/systems-hardware-architecture/security-weblogic-t-series-168447.pdf

- High Performance Security for SOA and XML Web Services Using Oracle SPARC T-Series Servers
  http://www.oracle.com/technetwork/articles/systems-hardware-architecture/hi-perf-soa-xml-svcs-172821.pdf

# Appendix

## About the Oracle SuperCluster Platform

The Oracle SuperCluster T5-8 delivers extreme performance and scalability for all database applications including Online Transaction Processing (OLTP), Data Warehousing (DW), and consolidation of mixed workloads. Built using industry-standard hardware and intelligent database and storage software from Oracle, the Oracle SuperCluster is fully integrated with a complete optimized package of software, servers, and storage. The Oracle SuperCluster maintains complete binary compatibility with existing Oracle Solaris SPARC-based customer applications and supports both Oracle Solaris 11 and Oracle Solaris 10 operating systems.



- 2 x SPARC T5-8, each with:
  - 8 x SPARC T5 Processors (128 cores)
  - 2 TB Memory
  - 8 x InfiniBand HCAs (dual port)
  - 8 x 10GbE NICs (dual port)
  - 8 x 900GB SAS disks
  - Optional Fiber channel cards
- Storage
  - 8 Exadata Storage Servers
  - ZFS Storage Appliance (60TB disk and 4 x 73GB Logzillas)
- Switches
  - 3 x InfiniBand 36 port switches
  - GbE Management switch

Figure 1. Oracle SuperCluster T5-8 full rack configuration.

### Building Blocks

The principal building blocks that comprise the Oracle SuperCluster are the following:

- SPARC T5-8 Compute Nodes: These are the servers where Oracle Solaris, customer applications, and the Oracle Database and database options are installed and configured. These are Oracle's powerful SPARC T5-8 servers with 2 TB of RAM each running virtualized Oracle Solaris 11 or Oracle Solaris 10 operating system images. Separate virtual machines are used for database and general-purpose applications under the control of Oracle VM Server for SPARC. Two servers are supported in a rack.
- Exadata Storage Servers: Exadata Storage Servers store Oracle Database data. The storage servers are pre-imaged and preconfigured network storage devices isolated to the database servers on a private InfiniBand network. Four or eight storage servers are supported offering up to 288 TB of

database storage. Customers can choose between high-performance or high-capacity disk storage. Each Exadata Storage Server also includes Flash Cache acceleration.

- ZFS Storage Appliance: Sixty TB of shared NAS storage is provided via a ZFS Storage Appliance mounted in the rack. This is connected to the high-speed InfiniBand network and can be used by applications to store file, log, program, or graphic data. The appliance is accessible only to the compute nodes on the system.
- Network Connectivity: Database and storage servers are connected via a private InfiniBand network. Administrative access is provided via a management Ethernet network. A 10 Gb/sec client-access network provides customer data center connectivity. Network hardware is included and integrated into the Oracle SuperCluster.

Prior to shipment to customer sites, the Oracle SuperCluster is integrated in fully racked configurations; only network address configuration and installation/configuration of Oracle Solaris 11 and Oracle Database on the database servers is performed on site. The systems utilized in this testing were installed and configured in the same manner as systems that would be shipped to customer sites.

The Oracle SuperCluster is available in two configurations (half rack and full rack) comprised of various combinations of Oracle Database servers, Exadata Storage Servers, and the various network components for interconnection.

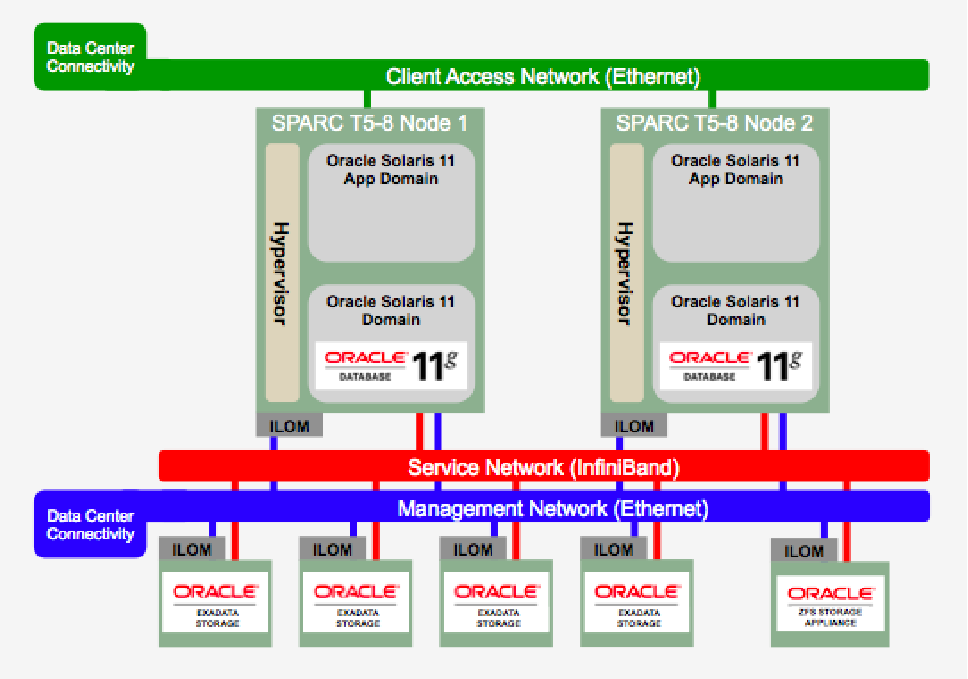


Figure 2. Domain configuration as tested.

### Network Connectivity

The Oracle SuperCluster includes internal network connectivity as well as connections from the database servers to the client network.

Each database server includes these network components and interfaces:

- Four embedded dual-port 10 Gb Ethernet
- Four dual-port InfiniBand Quad Data Rate (QDR)
- One Ethernet port for Oracle Integrated Lights Out Manager (Oracle ILOM) remote management

Each Exadata Storage Server includes these network components and interfaces:

- One embedded Gigabit Ethernet port (NET0)
- One dual-port QDR InfiniBand Host Channel Adapter (BOND0)
- One Ethernet port for Oracle ILOM remote management

The ZFS Storage Appliance includes one dual-port InfiniBand Host Channel Adapter.

There are up to five networks for the Oracle SuperCluster, as shown in Figure 2. Each network is configured on a distinct and separate subnet from the others. The network descriptions are as follows:

- Client-access network: This network is used for client access to the database servers. Applications access the database through this network using Single Client Access Name (SCAN) and Oracle RAC Virtual IP (VIP) addresses. Optionally, Virtual LANs (VLANs) can be used to isolate traffic.
- InfiniBand private network: This private network connects the database domains, general-purpose domains, ZFS Storage Appliance, and Exadata Storage Servers to the InfiniBand switches in the rack. Oracle Database uses this network for storage and Oracle RAC cluster interconnect traffic. This network is fully contained in the Oracle SuperCluster and does not connect to the customer's existing networks.
- Management network: This network is used for administrative work for all components of the Oracle SuperCluster and may be connected to existing customer management networks for remote administrative access. It connects the servers, Oracle ILOM, and switches connected to the Ethernet switch in the rack. There is one uplink from the Ethernet switch in the rack to an existing management network and one uplink from the KVM in the rack to an existing management network.
    - Each database server and Exadata Storage Server has two network interfaces for management. One provides management access to the operating system through the NET0 Ethernet interface, and the other provides access to Oracle ILOM through the ILOM Ethernet interface. The Oracle SuperCluster is delivered with the NET0 and ILOM interfaces connected to the Ethernet switch on the rack. The NET0 interface on the database servers should not be used for client or application network traffic. Cabling or configuration changes to these interfaces on Exadata Storage Servers are not permitted.
    - The management network is used for administrative work for all components of the Oracle SuperCluster. It connects the NET0 network interface on all servers, Oracle ILOM, and InfiniBand switches to the Ethernet switch in the rack.

- Additional optional networks: Database servers may be configured to connect to one or two additional existing networks through the NET2 and NET3 ports. If channel bonding is used for the client-access network, then only one additional port (NET3) is available.

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

Oracle SuperCluster T5-8 Security Technical Implementation Guide (STIG) Validation and Best Practices on the Database Servers
February 2014 Version 1.0

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200

oracle.com

Hardware and Software, Engineered to Work Together