



Oracle SuperCluster—Secure Private Cloud Architecture Overview

ORACLE TECHNICAL WHITE PAPER | NOVEMBER 2015



ORACLE®



Table of Contents

Introduction	1
Oracle SuperCluster: A Secure Private Cloud Architecture	2
Oracle SuperCluster: Typical Deployment Scenario	2
Secure Isolation	3
Data Protection	6
Access Control	9
Monitoring and Logging	12
Compliance Guidance and Verification	13
Secure Multitenancy on Oracle SuperCluster: A Cloud Provider Perspective	14
Summary	15
References	15



Introduction

IT infrastructure operators and service providers are under increasing pressure to be more agile and to dynamically align their business goals with cloud-centric operating models. This typically requires that they provide on-demand self-service, elastic growth and contraction of provisioned application or database environments and fine-grained infrastructure (compute, storage, and network) resource sharing. Security becomes a paramount concern when hosting multiple such business user *tenants*, each with many individual applications and databases, all using the shared resources of a cloud. The Oracle SuperCluster system features a defense-in-depth security architecture for hosting multiple tenants in a single platform using a layered set of security controls such as secure isolation, comprehensive data protection, end-to-end access control, and comprehensive logging and compliance auditing automation.

This technical white paper presents a high-level architectural overview of the available technical security controls for supporting a secure cloud architecture on the Oracle SuperCluster system, including the Oracle SuperCluster T5, M6, and M7 models. However, the specific architecture presented in this white paper is intended to be a high-level representation. Readers are encouraged to discuss their specific situation with their Oracle sales representatives in order to determine how the Oracle SuperCluster system can be architected to best meet their requirements and to request detailed deployment guidance.



Oracle SuperCluster: A Secure Private Cloud Architecture

The Oracle SuperCluster system is a secure cloud infrastructure for database applications, whereby multiple separate legal entities (subsidiaries, operating units, outside companies, or internal departments who have distinct liability and regulatory compliance needs) are able to deploy, operate, and manage their databases and applications on a single, physical shared Oracle SuperCluster system.

Organizations deploying private cloud infrastructures for databases and applications on Oracle SuperCluster will benefit from a well-rounded security foundation enabled by the underlying server, network, and storage hardware, the virtualization and operating system technologies, and the databases themselves, as well as a suite of complementary services. Together, these layers combine to provide a layered, defense-in-depth security architecture at every level of the technology stack by offering well-integrated security capabilities such as secure isolation, comprehensive data protection, end-to-end access control, and efficient monitoring and auditing to meet regulatory compliance requirements. Oracle SuperCluster is readily able to meet even the most demanding security requirements of mission-critical cloud infrastructures. Further, Oracle SuperCluster's flexibility allows organizations to customize their architecture to meet their specific workload objectives and security and compliance mandates, without sacrificing reliability, availability, or performance. As a result, Oracle SuperCluster is ideally suited to help cloud providers securely deploy and consolidate individual databases and applications.

Oracle SuperCluster combines the compute power of Oracle's SPARC M7 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 Server technology, and the innovative network-attached storage (NAS) capabilities of Oracle ZFS Storage Appliance.

Each of these core components is connected over a high-performance, redundant InfiniBand (IB) fabric that enables low-latency and high-performance network communication between all of the components. In addition, a 10 GbE network is employed allowing clients to access services running on Oracle SuperCluster. Finally, a GbE network provides the conduit through which all Oracle SuperCluster components can be managed.

Oracle SuperCluster: Typical Deployment Scenario

The Oracle SuperCluster system supports a variety of configuration and deployment options. The diagram in Figure 1 illustrates a typical deployment of Oracle SuperCluster M7 that consolidates Oracle Database instances and Oracle Fusion Middleware applications. It also shows the client access, management, and service networks, as well as Oracle Integrated Lights Out Manager (Oracle ILOM), Oracle Exadata Storage Servers, Oracle ZFS Storage Appliance, and Oracle Key Manager (which is optional).

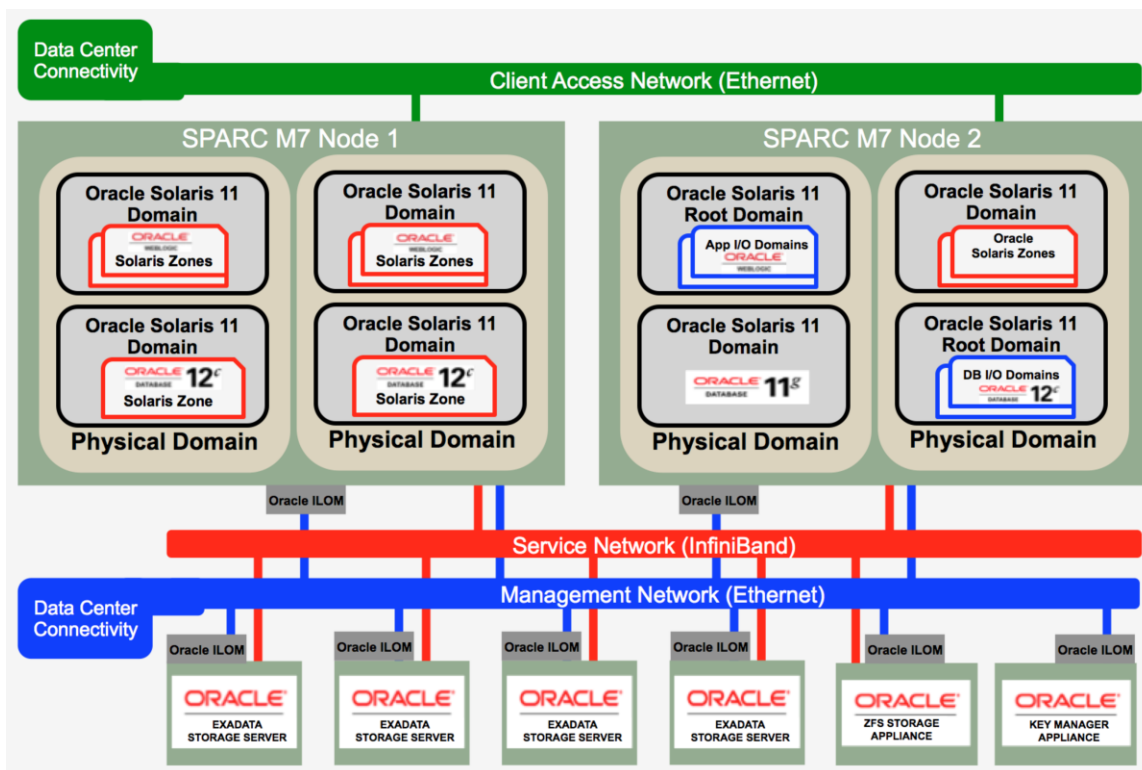


Figure 1. Typical secure, multitenant deployment of software workloads on an Oracle SuperCluster M7.

The Oracle SuperCluster system features Oracle VM Server for SPARC, a firmware-based virtualization technology that provides ready-to-run, secure virtual machines. Oracle's SPARC M7 processors used in the Oracle SuperCluster system provide always-on hardware-assisted cryptographic acceleration that helps cloud-hosted entities protect their data—on media, in memory, and in transit over networks—by leveraging the SPARC M7 processor's Silicon Secured Memory feature. Silicon Secured Memory detects and prevents data corruptions, memory scraping, and attacks that affect application data integrity.

With those robust features and a comprehensive set of security controls, Oracle SuperCluster can be deployed as a full-featured, secure, multitenant architecture for delivering enterprise-class private cloud services. In a typical deployment, a cloud hosting provider organization owns and operates the Oracle SuperCluster system and allows client tenants (either the same or separate legal entities) to remotely access the cloud infrastructure to deploy and manage their own applications and database.

In the following sections, the secure, cloud-based multitenant deployment scenarios on Oracle SuperCluster are discussed from the perspective of addressing critical cloud security requirements in terms of secure isolation, data protection, and access control, as well as compliance monitoring and auditing. The security controls presented can be augmented or adapted based upon an organization's unique policies and requirements.

Secure Isolation

Oracle SuperCluster supports a variety of isolation strategies that cloud providers can 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.

Oracle SuperCluster supports 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, and availability needs, as well as other needs. To simplify this discussion, several example isolation strategies are discussed below.

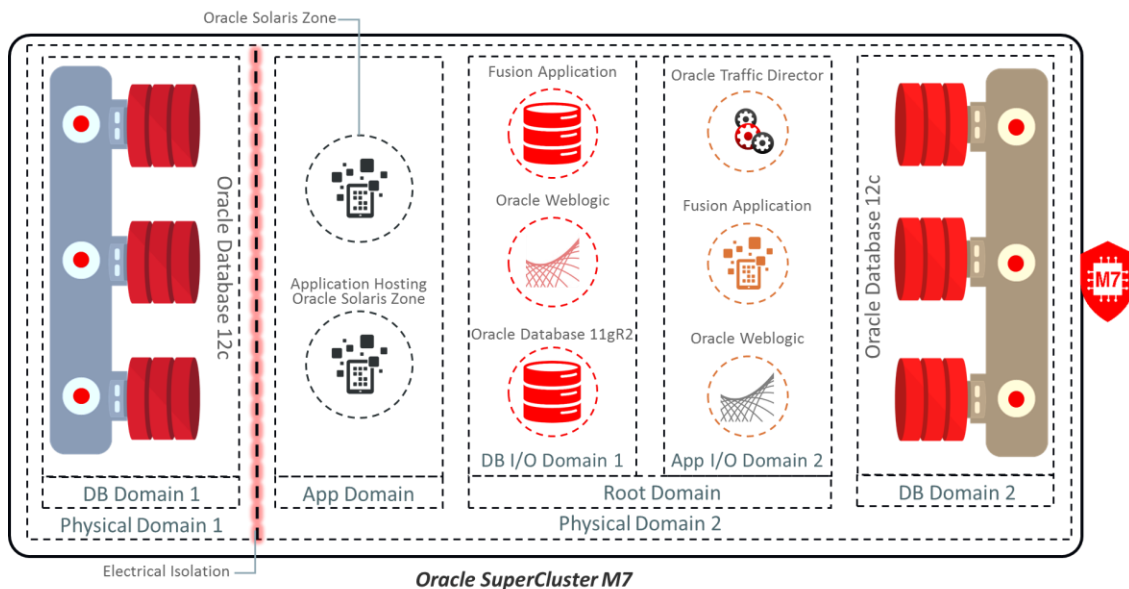


Figure 2. Secure isolation with dynamic tenant configuration flexibility.

Cloud providers can use *physical domains* (also called PDoms) for situations in which their tenants 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 virtual machines (referred to as *domains*) are used to create environments that isolate application and/or database instances. Domains each run their own unique instance of the Oracle Solaris operating system, and access to physical resources is mediated by the firmware-based hypervisor integrated into the SPARC server platform. So-called *dedicated domains* are static, and are defined only at the time the Oracle SuperCluster system is installed.

Oracle SuperCluster also supports a type of dynamic virtual machine called an *I/O domain*. I/O domains may be created and destroyed at will and Oracle SuperCluster M7 includes a browser-based tool to create and manage them. During installation, Oracle SuperCluster allows customers to create a special type of static domain referred to as a *root domain*, which leverages single-root I/O virtualization (SR-IOV) technology. Root domains own one or two InfiniBand HCAs and 10 GbE NICs or other I/O devices and provide virtualized I/O devices to *I/O domains*. This technology allows Oracle SuperCluster to host many more I/O domains than the physical I/O devices the system has while still providing near bare-metal I/O performance.

Within each of these domains, however, tenants can leverage Oracle Solaris Zones technology to create additional isolated environments, each with dedicated virtual processors, storage, administrative access control, runtime security, and auditability. Using Oracle Solaris 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 operating system kernel. This lightweight approach to virtualization is used to create a stronger security boundary around deployed services.

Tenants hosting multiple applications and databases on Oracle 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, Oracle 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 operating system is a good first step. However, it is equally important to consider—from the perspective of the three primary networks used in the Oracle SuperCluster: the client access network, the InfiniBand service network, and the management network—the network isolation capabilities and how communications flowing over the network are protected.

The network traffic flowing over Oracle SuperCluster's 10 GbE client access network can be isolated using a variety of techniques. In Figure 3, 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 Oracle SuperCluster to use VLANs, network traffic can be isolated between Oracle VM Server for SPARC dedicated domains as well as between Oracle Solaris Zones.

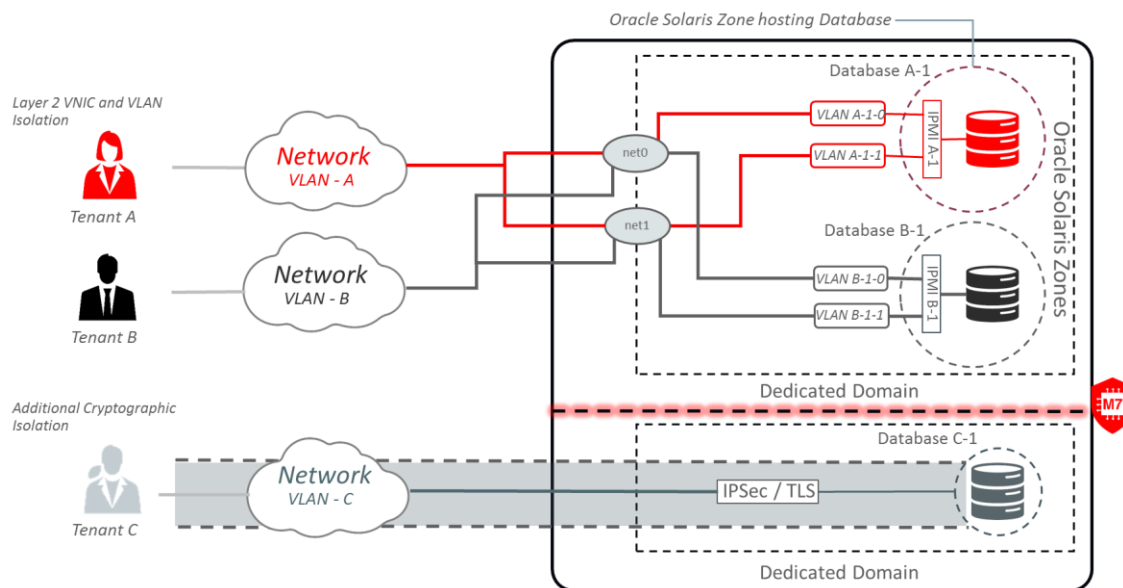


Figure 3. Secure network isolation—client access 10 GbE network.

In addition to the client access network, Oracle SuperCluster includes a private InfiniBand network that is used by database instances to access the information stored on the Oracle Exadata Storage Servers and the Oracle ZFS Storage Appliance, as well as to perform the internal communications needed for clustering and high availability.

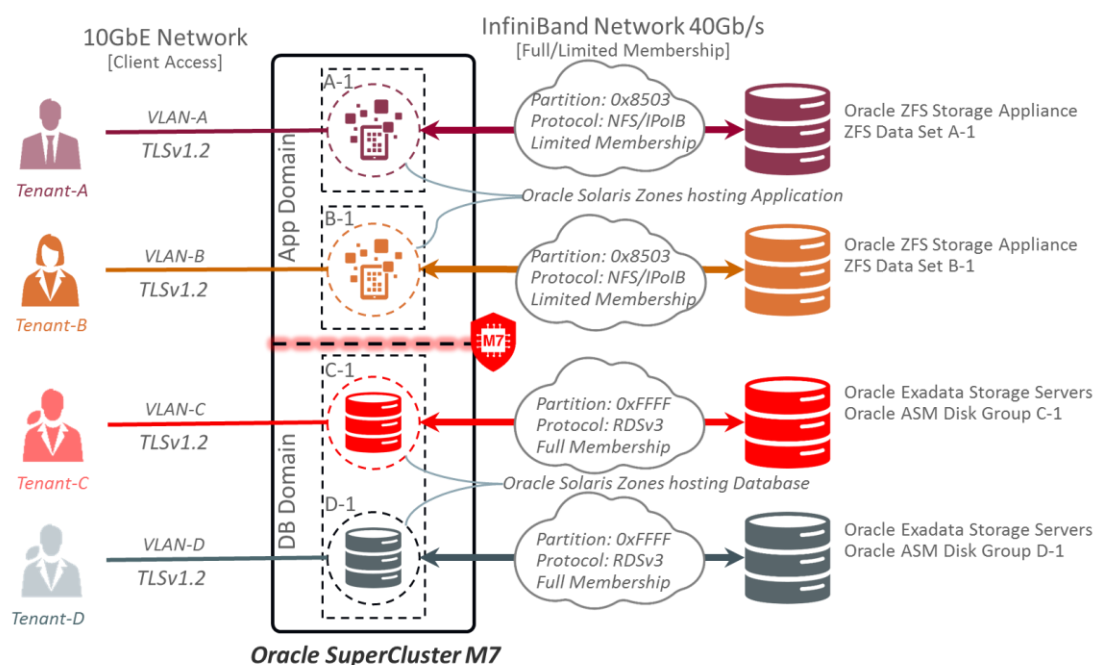


Figure 4. Secure network isolation—InfiniBand 40 Gb/sec service network.

By default, Oracle SuperCluster's InfiniBand network is partitioned into six distinct partitions during installation and configuration. While these default partitions are not to be changed, Oracle does support the creation and use of additional dedicated partitions in situations in which further segmentation of the InfiniBand network is required. In addition, the InfiniBand 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 any nodes on the partition. The Oracle applications' I/O domains and Oracle Solaris 11 Zones can be configured as limited members of their respective InfiniBand partitions ensuring that they will be able to communicate only with the Oracle ZFS Storage Appliance and not with other limited membership nodes that might exist on that same partition.

Oracle 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, Oracle SuperCluster can further reduce the network attack surface that is exposed over the client access and InfiniBand 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 M7 processor in Oracle SuperCluster facilitates hardware-assisted, high-performance encryption for the data protection needs of security-sensitive IT environments. The SPARC M7 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.

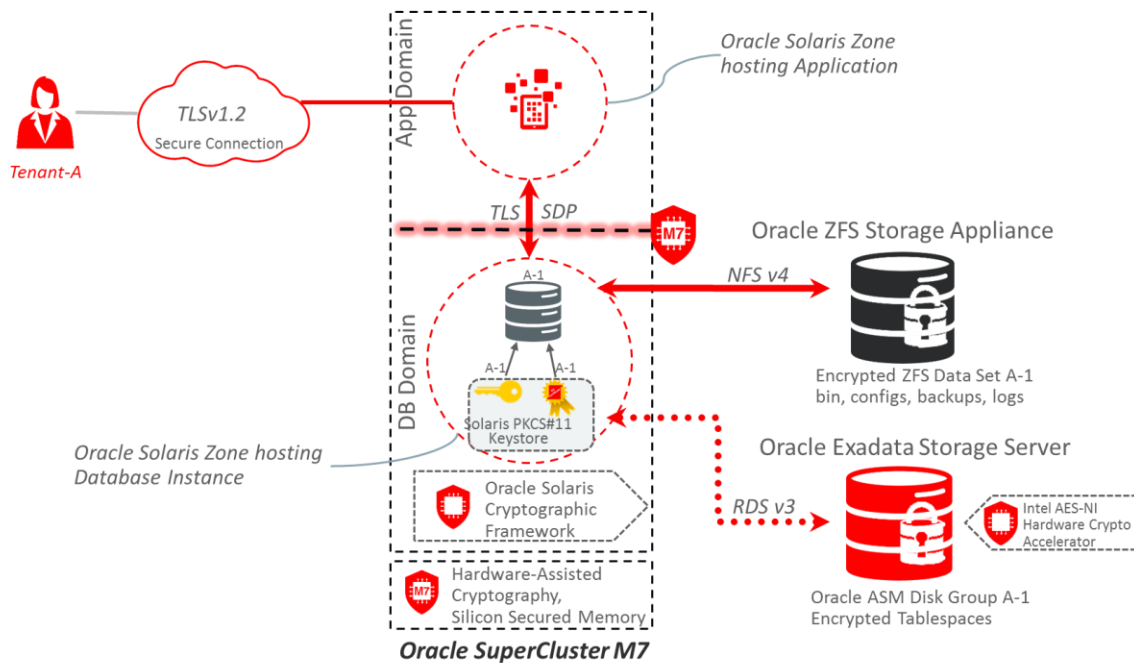


Figure 5. Data protection—hardware-assisted cryptographic acceleration and memory intrusion protection.

For secure multitenant architectures, where data protection figures into nearly every aspect of the architecture, Oracle SuperCluster and its supporting software enables organizations to meet their security and compliance objectives without having to sacrifice performance. Oracle SuperCluster leverages on-core based cryptographic instructions and Silicon Secured Memory capabilities, which are designed into its SPARC 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 operating system 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 operating system and the SPARC processor used by Oracle 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. The use of IPSec (IP Security) and IKE (Internet Key Exchange) is recommended to protect the confidentiality and integrity of tenant-specific, inter-zone, IP-based communications flowing over the InfiniBand network.

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 Oracle 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 Oracle 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 Oracle 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.

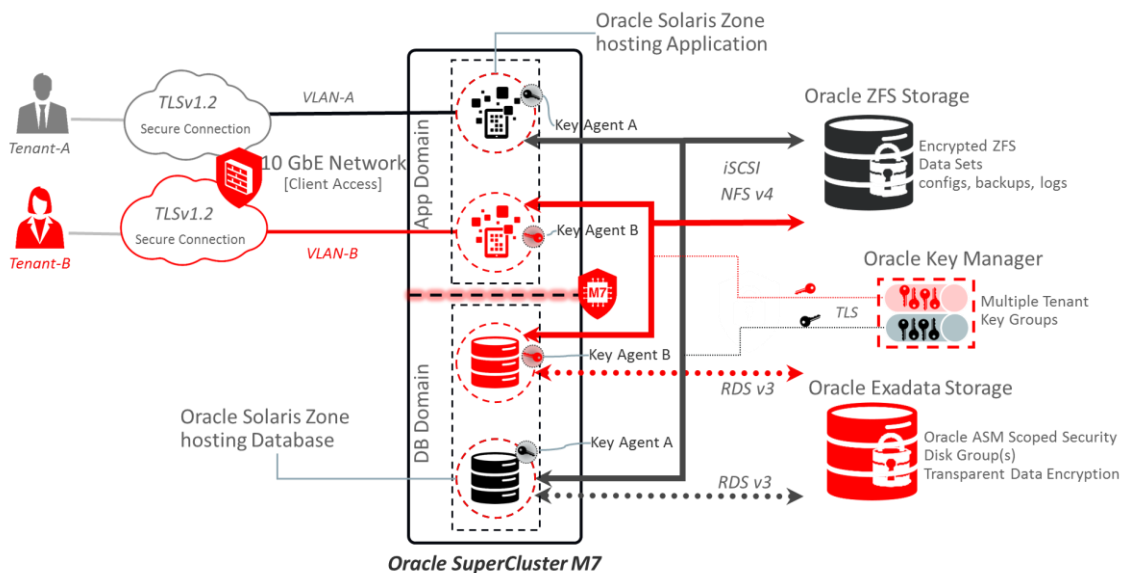



Figure 6. Data protection—multitenant key-management scenario using Oracle Key Manager.



To address key management complexities and issues associated with multiple hosts and applications in a cloud-based multitenant environment, Oracle SuperCluster recommends the use of Oracle Key Manager as an optional 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 Oracle ZFS Storage Appliance, and it supports Oracle's StorageTek encrypted tape drives. Having the encryption policy and key management at the ZFS dataset (file system) level delivers assured deletion of tenant file systems via key destruction.

Oracle Key Manager is a complete key management appliance that supports lifecycle key management operations and trusted key storage. When configured with an additional Sun Crypto Accelerator 6000 PCIe Card from Oracle, on 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 Oracle 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.

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.

Oracle 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 operating system 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 operating system, 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 Oracle 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 should 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.

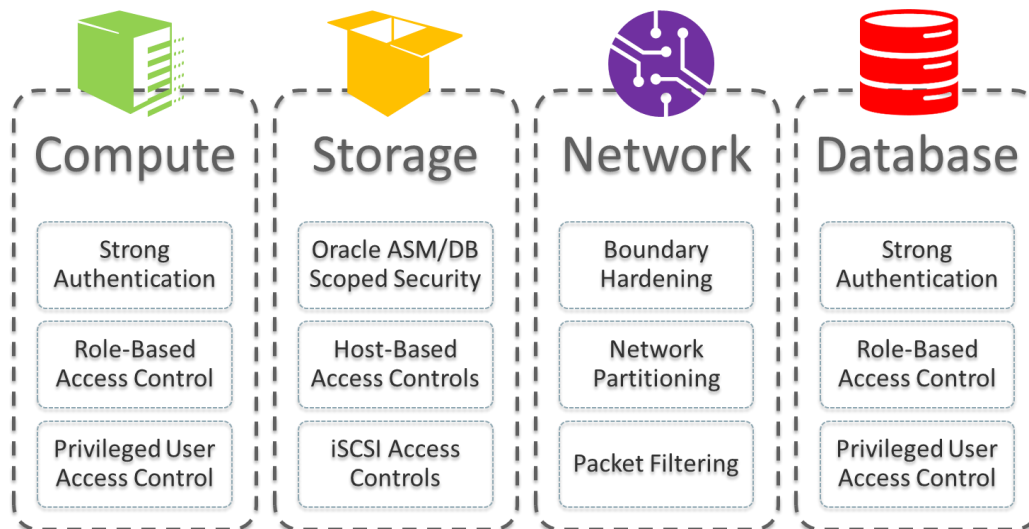


Figure 7. End-to-end access control—summary of features.

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 Oracle SuperCluster that operate many network interfaces and support a variety of inbound and outbound network communications.

On Oracle 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 operating system 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 multifactor 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. Oracle 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 Oracle 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. Figure 8 shows Oracle ASM-scoped security along with ZFS security. That said, in situations where there are large numbers of Oracle Database instances being deployed on the Oracle SuperCluster system, 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 Oracle Exadata Storage Server.

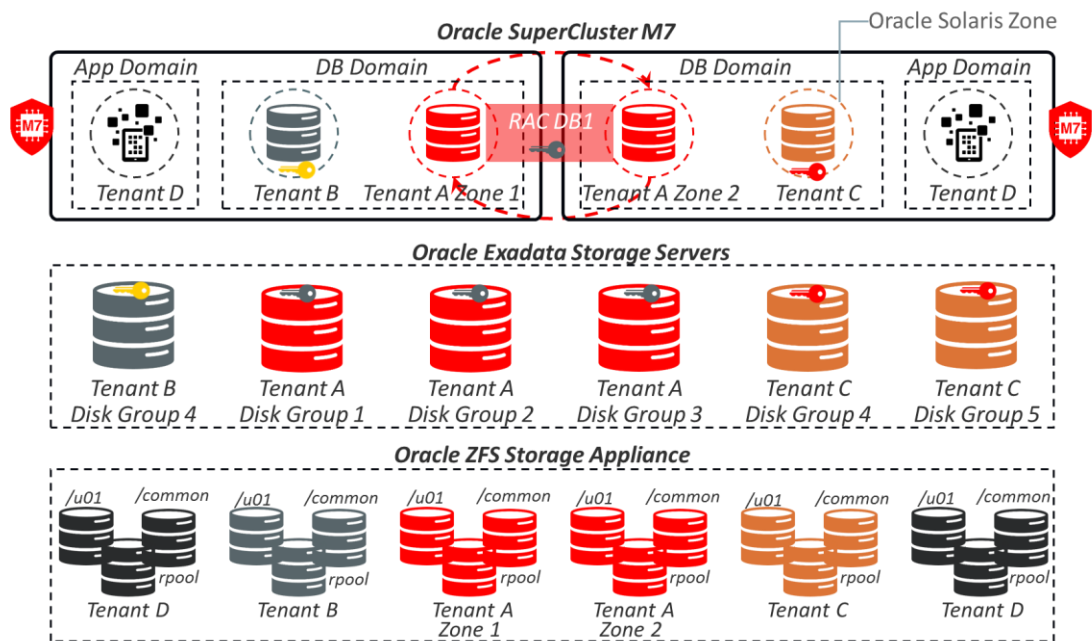



Figure 8. Per-tenant Oracle ASM-scoped security.

Oracle 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 Oracle Exadata Storage Servers, it is strongly recommended that such access be restricted. The Oracle 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 Oracle SuperCluster database domains (which are operated by the cloud provider). This ensures that the Oracle 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) operating system 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 Logging

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 Oracle 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 Oracle 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.

Oracle Exadata Storage Servers and Oracle 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 Oracle ZFS Storage Appliance.

Similarly, the Oracle Exadata Storage Server audit is a rich collection of system events that can be used along with hardware and configuration alert information provided by Oracle's 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, Oracle 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.

Compliance Guidance and Verification

Compliance to industry security standards ensures more-secure computing environments and supports adopting many external and internal security requirements, which are critical to many security-sensitive organizations. In addition, a compliance validation process and a supporting auditing policy help a cloud provider map its enforced security controls to system compliance and enable it to test, maintain, and protect the environment from known attack vectors.

Oracle SuperCluster provides tools that assess and report the compliance of the Oracle Solaris runtime environment residing in dedicated domains and zones. Compliance utilities are part of Oracle Solaris and based on the Security Content Automation Protocol (SCAP) implementation.

The Oracle Solaris compliance utility is used 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: the Oracle Solaris Compliance Recommended profile (based on the Center of Internet Security benchmark) and the Payment Card Industry Data Security Standard (PCI DSS). These profiling tools map security controls to the compliance requirements mandated by the industry standards, and the associated compliance reports can reduce significant auditing time and costs.

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 tenant administrator may add or change a benchmark and create a new guide. Additional scripts can be used to meet other regulatory environment standards, such as the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), Sarbanes Oxley (SOX), and the Federal Information Security Management Act (FISMA).

The cryptographic applications hosted on Oracle 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 may 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.

Secure Multitenancy on Oracle SuperCluster: A Cloud Provider Perspective

A wide array of security controls and capabilities are used in supporting secure multitenancy on the Oracle SuperCluster system. The use of multiple, independent, and mutually reinforcing security controls is a defense-in-depth strategy implemented on Oracle SuperCluster that helps to support most organizations' security requirements for delivering a secure multitenant cloud architecture solution.

Collectively, the extensive set of security controls and capabilities available on the Oracle SuperCluster system provide a well-rounded security foundation upon which organizations can deploy services on their secure multitenant cloud infrastructure. Figure 9 illustrates an example representation of a secure multitenant cloud architecture deployment using Oracle SuperCluster, including all security controls.

Cloud-based multitenant architectures are ultimately based upon a pool of IT resources that are shared across a community of tenant consumers. Whenever shared service architectures are considered, it is important to understand how individual consumer workloads and data are isolated from other tenants operating on the same platform. Throughout this paper, there has been extensive discussion of secure isolation capabilities at the compute, network, storage, and database level. Organizations are encouraged to consider the various capabilities presented so that an appropriate balance can be achieved between managing risk, enabling agility, and increasing operational efficiency.

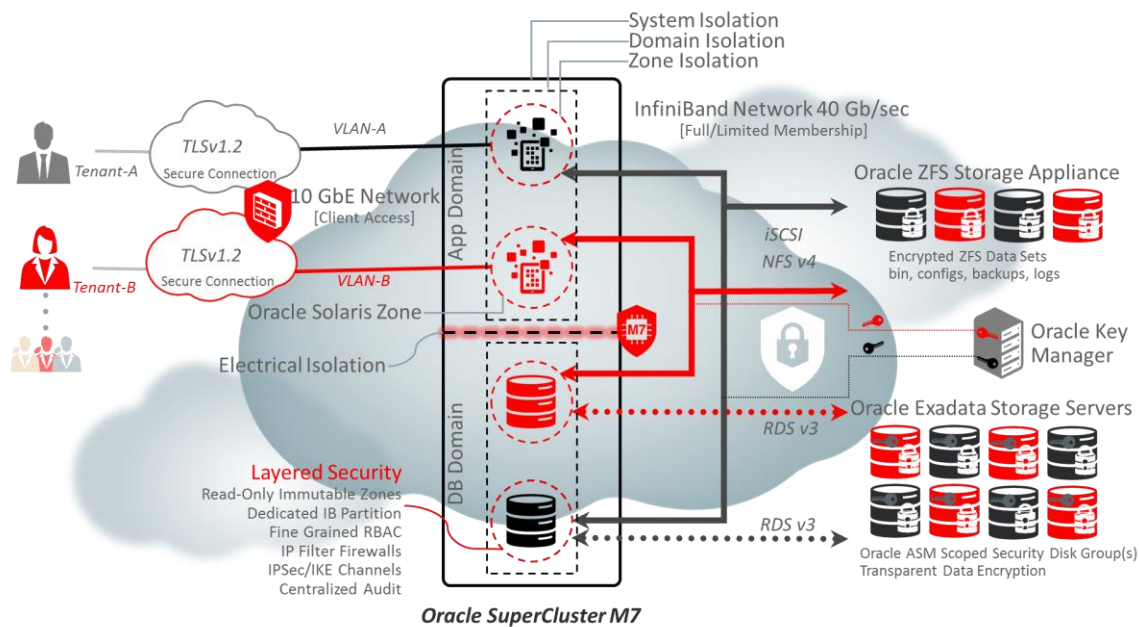



Figure 9. Secure private cloud architecture—a cloud provider perspective.

It is important that cloud service providers understand how these technologies work when employed together, as well as their relative strengths and differences, in order to select those that are most appropriate for themselves and their tenant consumers. Cloud providers should realize that most if not all of this functionality can be effectively “hidden” so that consumers can benefit from these techniques without having to worry about their implementation, configuration, and maintenance. As mentioned earlier, cloud service providers should incorporate security service capabilities and metrics into their service definitions so that the tenant consumers can select those that are best aligned to their security needs.



To learn more about deploying a secure private cloud environment on Oracle SuperCluster, please refer to the latest version of “Secure Multi-tenancy on Oracle SuperCluster: A Technical Deployment Cookbook,” which is available from the Oracle SuperCluster support teams.

Summary

As a complete secure cloud infrastructure for database and application, the Oracle SuperCluster system enjoys a level of security synergy not often found in other comparable systems. Because of both its high degree of engineering innovation and end-to-end integration, the security posture and potential of this platform is greater than the sum of its individual components. More importantly, however, is the balance that has been achieved between the tight integration of its components and the level of configuration and operational flexibility, which allows organizations to customize the security posture of the Oracle SuperCluster system based upon their policies and requirements. This reinforced yet flexible security architecture makes this engineered system an ideal platform for cloud providers consolidating applications and databases, operating multitier enterprise applications, or delivering multitenant private cloud services.

References

- » [“Oracle SuperCluster M7 Platform Security Principles and Capabilities”](#)
- » [Oracle Solaris 11 Security Guidelines](#)
- » [Oracle SuperCluster M7 Series Security Guide](#)
- » [Oracle Database Security Guide 12c Release 1 \(12.1\)](#)
- » [“Oracle SuperCluster T5-8 Security Technical Implementation Guide \(STIG\) Validation and Best Practices on the Database Servers”](#)
- » [“Oracle SuperCluster and PCI Compliance”](#)

**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



facebook.com/oracle



twitter.com/oracle



oracle.com

Integrated Cloud Applications & Platform Services

Copyright © 2015, 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—Secure Private Cloud Architecture Overview
November 2015

Author: Ramesh Nagappan, Saran Selvaraj
Contributing Author: Sujeet Vasudevan



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