ORACLE
OPTIMIZED SOLUTIONS

How to Improve the Efficiency and Performance of an SAP Environment

With Oracle Optimized Solution for SAP

ORACLE WHITE PAPER | LAST UPDATED JUNE 2015

ORACLE

Table of Contents

Introduction

Business-critical SAP environments consist of many components: applications, databases, operating systems, servers, networking, storage, management tools, and backup software. In a typical multivendor approach, careful and complex process of selection, integration, and testing is critical to ensure the infrastructure can deliver expected performance, security, and reliability. Supported by SAP, Oracle Optimized Solution for SAP takes a different approach, providing pre-integrated, pre-tested, highly available infrastructure in a single system for maximum efficiency and optimum performance.

This technical white paper provides a brief overview of Oracle Optimized Solution for SAP on Oracle SuperCluster and illustrates how to use it to consolidate SAP environments. Recommendations and best practices are outlined for improving security, consolidation, availability, and performance of SAP applications while accelerating time to deployment.

Oracle Optimized Solution for SAP

Oracle Optimized Solution for SAP leverages Oracle SuperCluster, a complete, pre-engineered, pre-tested, high-performance, scalable SAP enterprise infrastructure solution. Available in half-rack, full-rack, or multi-rack configurations, Oracle SuperCluster integrates Oracle servers, Oracle Solaris, Oracle Database 11*g*, and Oracle Exadata Storage Servers with a high-bandwidth, low-latency InfiniBand network fabric. The system is optimized and tuned for consolidating enterprise applications such as SAP (Figure 1).

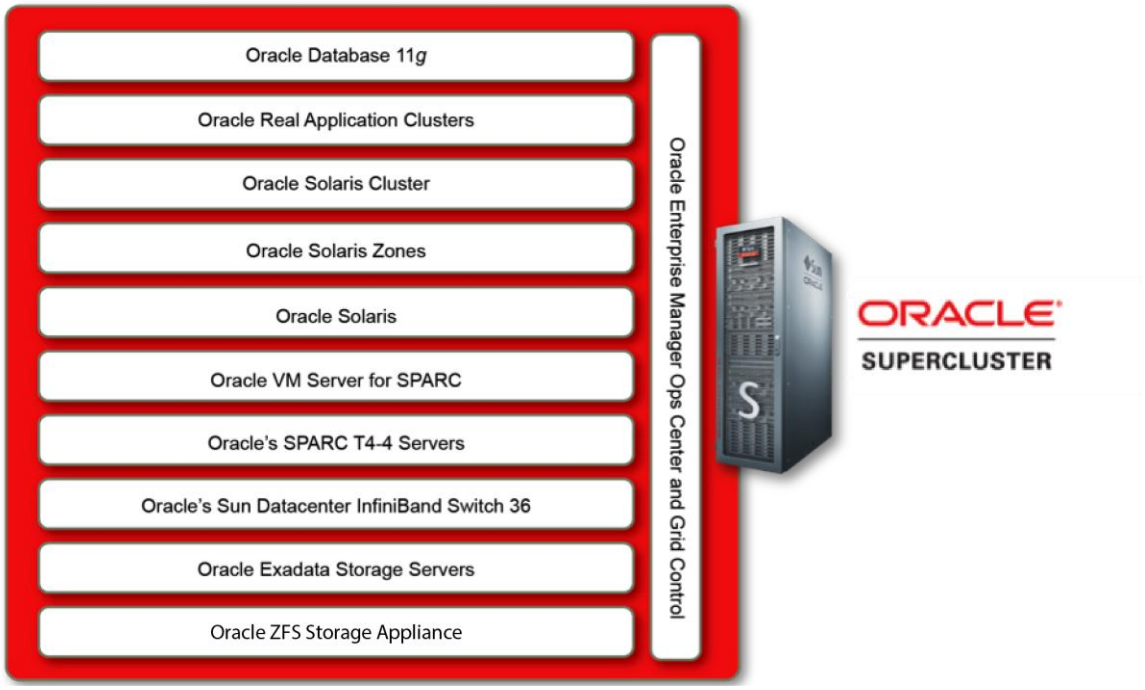

Figure 1. Oracle Optimized Solution for SAP provides the components needed in one system.

SAP Security: Understanding the Threat

ERP systems, including SAP, have transformed core business functions in the modern enterprise, improving and automating processes across the organization, from human resources to product development and from finance to sales. As these systems expand to integrate and unify a multitude of business functions and core processes, they also aggregate an increasing amount of business-critical and confidential data—including intellectual property, financial data, and personal information—into a central repository. This high concentration of critical data and key business processes makes an attractive target for cyber attacks and can increase the risk of security breaches. As a result, security has become a major concern when designing and deploying ERP environments. Several methods exist for increasing data protection and safeguarding ERP systems.

Creating More Secure SAP Environments

Simplify the Infrastructure

Most SAP environments are based on a complex infrastructure, making implementation and management complicated. This complexity increases the risk of security vulnerabilities. An SAP implementation as a whole is only as secure as its most vulnerable component, and it can be challenging to securely configure the myriad of interacting components and products in a heterogeneous system. Oracle Optimized Solutions simplify SAP implementations through the use of consolidation and virtualization technologies. Oracle also offers security guidelines and recommendations and many Oracle components have security built-in by default.

Reduce Implementation Flaws

Secure software is important but not sufficient by itself. Most security vulnerabilities arise from flawed implementation and architecture, including improper configuration and access control, lack of patch management,

unencrypted communications, and inadequate security policies and processes. Based on current security best practices, Oracle Optimized Solutions provide proven and tested architecture recommendations for increased ERP system protection.

Eliminate Performance and Cost Penalties

Many security processes, such as on-the-fly encryption/decryption, can have a significant negative impact on the performance and cost of an SAP system. Oracle Optimized Solutions leverage SPARC-based systems that offer high-performance security using Cryptographic Instruction Accelerators that are directly integrated into the processor cores. By providing wire-speed security capabilities, Oracle systems eliminate the performance and cost penalties typically associated with real-time, secure computing.

Architecture Overview

Within the Oracle SuperCluster engineered system, resource-intensive SAP applications are consolidated onto high-performance Oracle's SPARC servers. All servers run Oracle Solaris, an operating system that is designed to take advantage of the high-performance, massive threading and batch processing, and fast I/O of Oracle's SPARC servers. Databases are stored on Oracle Exadata Storage Servers to accelerate performance. An Oracle ZFS Storage Appliance hosts shared file systems, with flash-enabled Hybrid Storage Pools storing frequently accessed data to speed application response times.

Redundant Configuration

All components within Oracle SuperCluster are interconnected over an InfiniBand fabric to allow the rapid exchange of data among the architecture tiers (Figure 2). The high-speed, low-latency fabric utilizes a pair of redundant (leaf) Sun Datacenter InfiniBand Switch 36 switches from Oracle to interconnect the components. Each database or application domain features dual connections to the InfiniBand networks, using separate interface cards connected to separate PCI buses to support communication with the cluster interconnect, Oracle Exadata Storage Servers, and storage appliances. All tiers within the Oracle SuperCluster architecture communicate using the internal InfiniBand network. A pre-integrated InfiniBand spine switch allows for expansion by connecting additional Oracle ZFS Storage Appliances, Oracle Exadata Storage Servers, or Oracle engineered systems to the InfiniBand fabric. Separate redundant 10 GbE interfaces are used for connection to the data center, and support incoming client connections and external SAP application servers. Optional Fibre Channel (FC) cards in Oracle SuperCluster support access to existing SAN data storage.

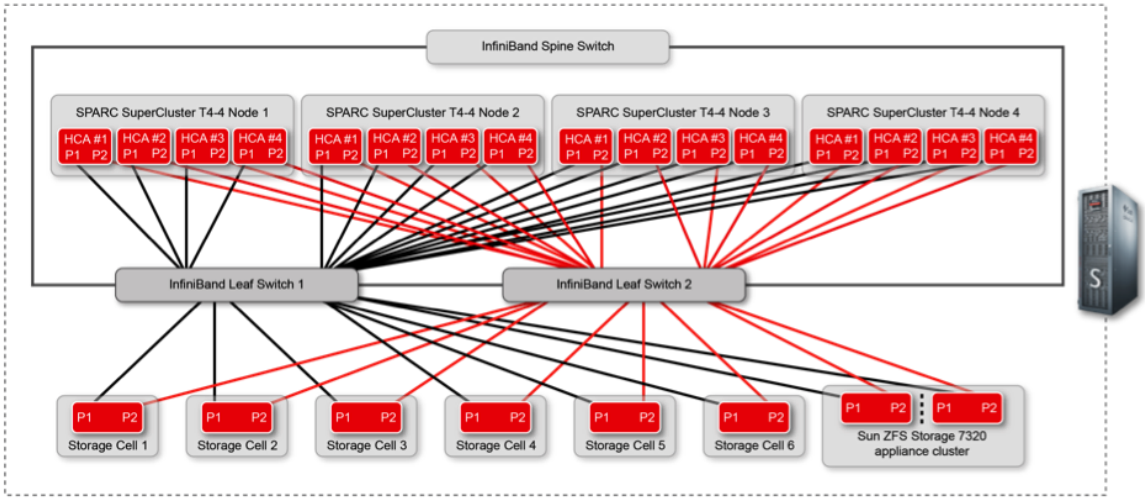

Figure 2. Oracle SuperCluster interconnects all system components over a high-performance, fully redundant InfiniBand fabric.

More information on Oracle SuperCluster can be found in the "A Technical Overview of the Oracle's SPARC SuperCluster T4-4" and "Oracle Solaris: The Foundation for Successful SAP Solutions" white papers.

Secure Isolation

In Oracle Optimized Solution for SAP, the SAP Central Services (SCS and ASCS), SAP Application Servers, and Oracle Database software all are consolidated on the system. Secure isolation and resource control are maintained using two Oracle virtualization technologies. Together, these capabilities enable Oracle Solaris 8, 9, 10, and 11 certified applications to run simultaneously on the system without modification.

- **Oracle VM Server for SPARC**. Oracle VM Server for SPARC (previously called Sun Logical Domains) is a firmware-based hypervisor that is built into SPARC T4-4 servers. It supports multiple virtual machines, called domains, running separate instances of Oracle Solaris on a single system. The hypervisor allocates subsets of system resources (memory, I/O, and CPU) to each domain, isolating each Oracle Solaris instance and SAP workload to a virtual machine with dedicated resources. For I/O-intensive SAP workloads, separate I/O domains are configured to take advantage of the large number of I/O ports to deliver I/O performance at bare-metal speeds within a virtualized environment.
- **Oracle Solaris Zones**. Oracle Solaris Zones (previously known as Oracle Solaris Containers) virtualize servers using flexible, software-defined boundaries. They allow the one-application-per-server deployment model to be maintained while simultaneously sharing hardware resources without overhead. By creating multiple private execution environments within a single Oracle Solaris instance, Oracle Solaris Zones completely isolate SAP applications. Resource management enables applications within a zone to share the resources allocated to the zone, preventing processes in one zone from affecting processes running in another. SAP applications can be deployed on the fly, with no need for additional hardware. In addition, Oracle Solaris Zones support fault isolation, feature extremely fast boot times, and can be configured to instantly restart SAP applications. Supported by SAP Adaptive Computing Controller, Oracle Solaris Zones make it easy to prioritize applications and adjust resource allocations.

Oracle VM Server for SPARC and Oracle Solaris Zones are complementary virtualization technologies that work together to isolate SAP applications and control system resources. In this example architecture, Oracle VM Server for SPARC defines two virtual servers or domains: one for the underlying database and one for the application tier (Figure 3).

To optimize the performance of Oracle Exadata Storage Servers, Oracle Solaris 11 runs in the database domain to support the database and Oracle Real Application Clusters (Oracle RAC). To support SAP applications and Central Services, Oracle Solaris Zones are configured in the application domains (also called general-purpose domains), enabling zone clusters to be created in conjunction with Oracle Solaris Cluster. These application domains run Oracle Solaris 11, or Oracle Solaris 10 to maintain compatibility with applications not yet certified for, or tested with, Oracle Solaris 11.

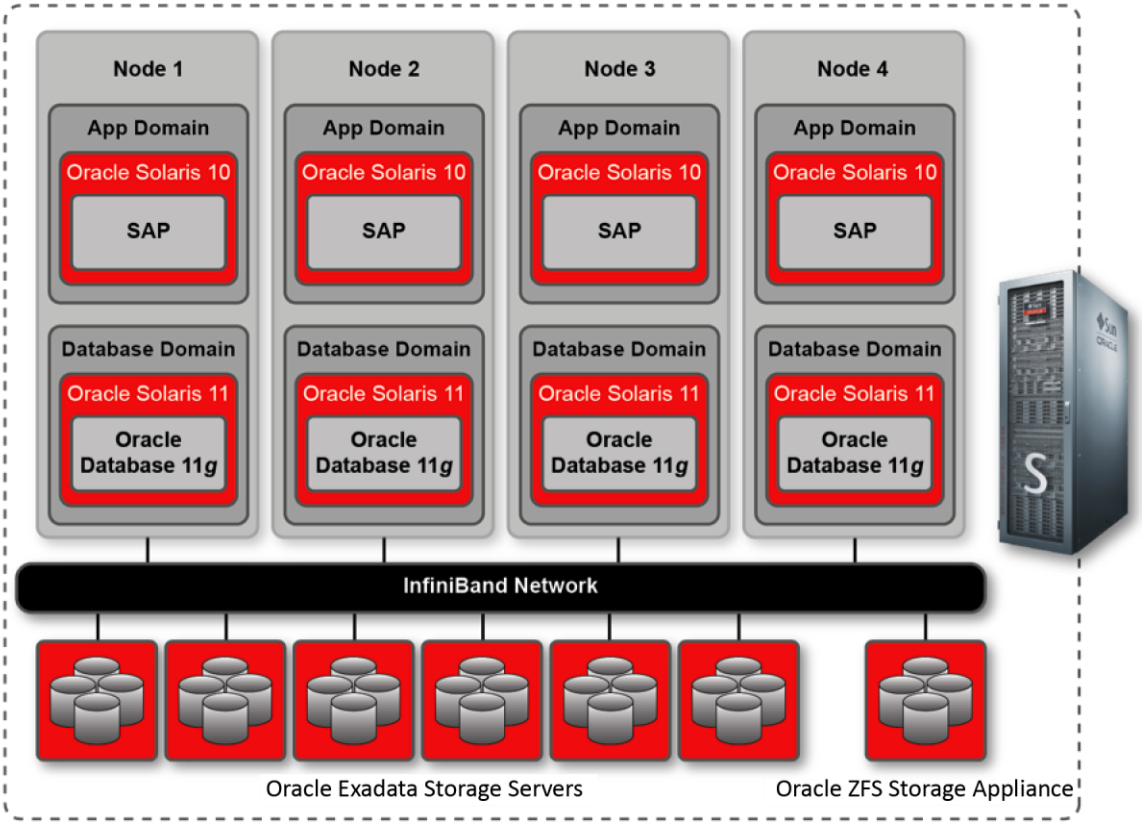

Figure 3. Built-in virtualization technologies provide workload isolation and resource controls.

Clustered Solution

Oracle Optimized Solution for SAP on Oracle SuperCluster provides full built-in redundancy—from compute nodes to storage, network switches to network interface cards (NICs), and power distribution units (PDUs) to power supplies—to support mission-critical SAP applications. Additional software is used to provide application availability.

» **Oracle Solaris Cluster**. Oracle Solaris Cluster ensures the availability of SAP applications by detecting, isolating, and containing failing cluster nodes or specific components, such as NICs, HBAs, networks, and storage. Agents follow failover policies that specify the actions to be taken should a node or service fail or become unavailable. Agents are available for SAP Enqueue (including enqueue and replication servers), central services, the Web application server, SAP J2EE Engine, SAP liveCache, and Oracle Database. The agents implement automated failover for the primary SAP application server, SAP Central Services, and the database tier, as well as failover for

other mission-critical production applications. Administrators can control the impact of resource constraints on critical applications using load-based, application-specific failover policies.

- **Oracle Real Application Clusters**. Oracle RAC supports the transparent deployment of the database across all four servers within the Oracle SuperCluster engineered system, providing database fault tolerance in the event of hardware failures or planned outages.
- **Virtual clustering**. Oracle Solaris Cluster supports virtual clustering, enabling Oracle Solaris Zones to function in the same role as physical cluster nodes. Applications that run within dedicated zone clusters are associated with specific cluster management policies. Agent actions can be layered, such as first trying to restart the service in a different zone before attempting to restart it on a different server. This helps SAP applications achieve the required levels of service.

Shared Storage

Oracle ZFS Storage Appliance offers highly available shared storage that can be used by SAP applications for SAP binaries, configuration files, log files, and more. In addition, it can be used for backup/restore operations, transfers, or storage for non-production databases. Built-in snapshot and cloning capabilities help speed zone duplication for ultra-fast creation of new development or test environments. Accessed over the high-speed InfiniBand network, Oracle ZFS Storage Appliances provide a highly available shared file system. Configured for redundancy, these appliances use the built-in self-healing and data integrity features of Oracle Solaris ZFS with clustered controllers to ensure data availability.

Integrated Database Acceleration

Oracle Exadata Storage Servers play a critical role in the solution architecture. They provide important software technology to accelerate database processing, including: Smart Scan, Smart Flash Cache, Smart Flash Logging, Smart Flash Write Back Cache, I/O Resource Manager, and Storage Indexes. The software is optimized for the hardware and Oracle Database 11*g* Release 2 operations to support transaction-based and decision support SAP workloads. A smart design delivers high I/O performance and bandwidth to the database.

- Oracle Exadata Storage Server CPU cores are dedicated to specific features. For example, Smart Scan SQL processing is executed within the storage tier, offloading the database server.
- Building on the high security capabilities in Oracle Database, Oracle Exadata Storage Servers enable queries to be executed against fully encrypted databases with near zero overhead, delivering hundreds of gigabytes per second. This was made possible by moving decryption processing from software into the Oracle Exadata Storage Server hardware.
- More than 8 terabytes of flash storage is available. Automated caching within flash enables Oracle Exadata Storage Servers to deliver up to 11 GB/second disk data bandwidth, up to 43 GB/second flash data bandwidth, and up to 650,000 flash IOPS.

Remote Management

The solution architecture includes built-in, out-of-band, remote management. All Oracle SuperCluster components are connected to a dedicated 1 GbE management network, ensuring the physical isolation of management and data traffic. The dedicated management switch can be connected to the data center's central management infrastructure. The management software stack includes Oracle Enterprise Manager Ops Center 12c to govern Oracle SuperCluster components and Oracle Enterprise Manager Grid Control to manage Oracle Database (Figure 4).

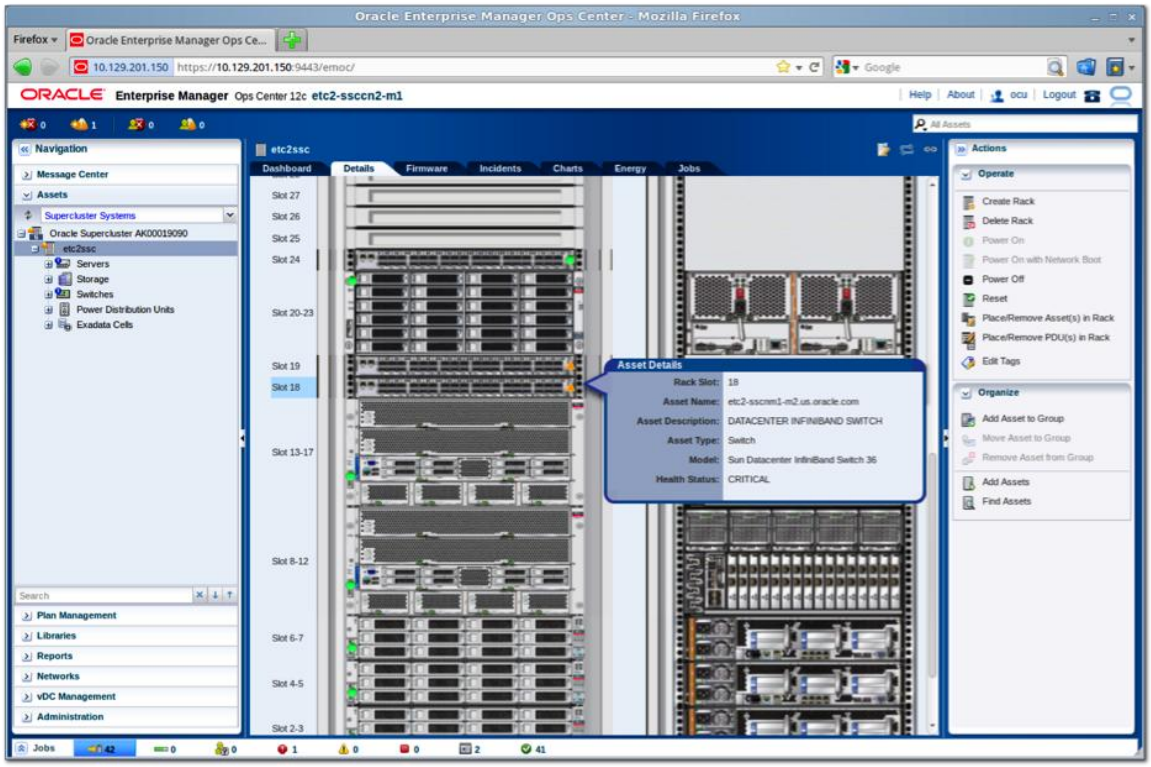

Figure 4. Oracle Enterprise Manager Ops Center 12c simplifies the management of Oracle SuperCluster systems.

How to Map an SAP Environment to Oracle SuperCluster

A typical large-scale SAP landscape is complex, with users at the edge of the network, data center infrastructure hosting the SAP landscapes, and storage systems handling information management. Within the data center, SAP landscapes consist of a minimum of three separate systems, Development (DEV), Test and Quality Assurance (QAS), and Production (PRD), for each SAP Business Suite application and SAP NetWeaver solution. SAP components can be deployed with the SAP application and database server layers residing on a single system (two-tier architecture, common for non-production environments), or with the application and database layers residing on separate systems (three-tier architecture, typical of production environments).

Over time, the independent hosting of each system on multiple separate physical servers results in increasing complexity and infrastructure sprawl that makes adding new SAP services expensive and time consuming. Because individual servers must be sized for peak demand—a condition that might occur only once a week or once a month—they experience very low utilization rates for the rest of the time. With so many servers often running only at 10 to 20 percent of capacity, resource utilization is low, power and cooling demands are high, and data center floor space is over consumed and underutilized. As a result, enterprises running multiple SAP applications on multiple sites quickly find themselves with a complex and fragmented SAP landscape (Figure 5).

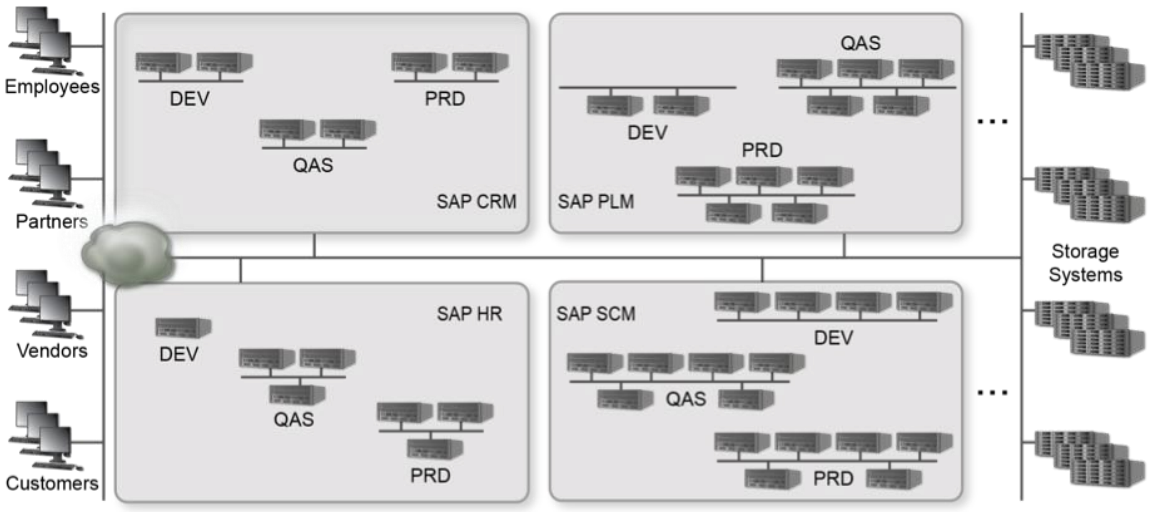

Figure 5. A typical SAP landscape has separate development, test, and production systems for each SAP application.

SAP Landscape Architecture Using Two Oracle SuperCluster Systems

To simplify the SAP landscape, production environments can be consolidated on an Oracle SuperCluster system, with development and testing environments deployed together on a second system (Figure 6). In this scenario, the testing and quality assurance environment can replicate all or a portion of the production system.

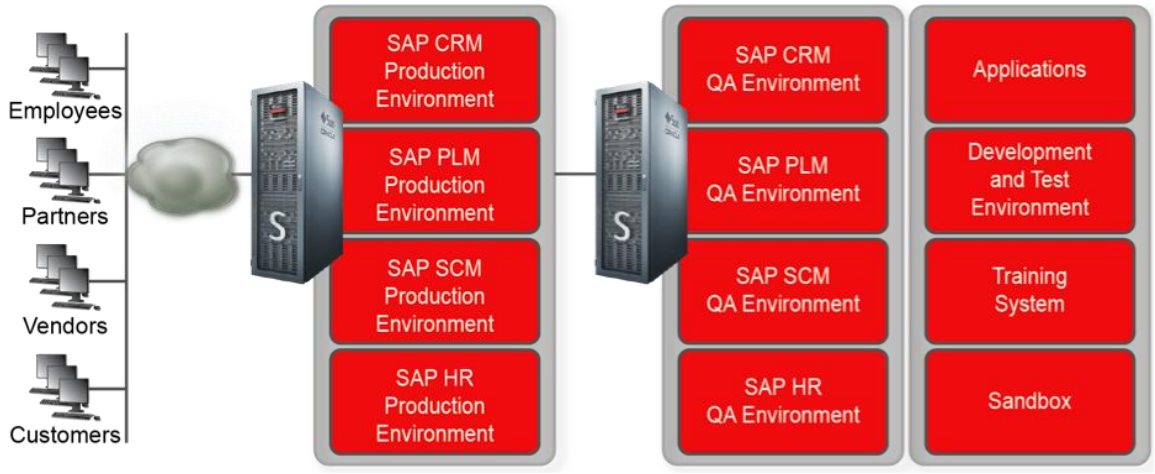

Figure 6. SAP QA, development, and testing environments can be consolidated onto a single Oracle SuperCluster, with production systems deployed on a second Oracle SuperCluster to maintain physical isolation.

Production System

The production system contains live data and is where business processes are executed. To ensure the highest performance and availability, three-tier SAP architectures should be run on Oracle SuperCluster production systems. In this configuration, SAP applications run in Oracle Solaris Zones within an application domain, and can

be configured for failover as needed. Databases run in a separate database domain connected to Oracle Exadata Storage Servers for performance acceleration.

Figure 7 illustrates an Oracle SuperCluster system with consolidated production SAP applications. Oracle Solaris Zones are used to safely run multiple services in a single application domain to get the best efficiency, while zone clusters ensure high availability. Since they generate no system overhead, the number of Oracle Solaris Zones that can run within a domain is limited only by the amount of hardware resources used by each application. Because Oracle Solaris Zones enable isolation, resource control, and separate access rights, multiple departments with separate administrative domains can be consolidated onto a single Oracle SuperCluster.

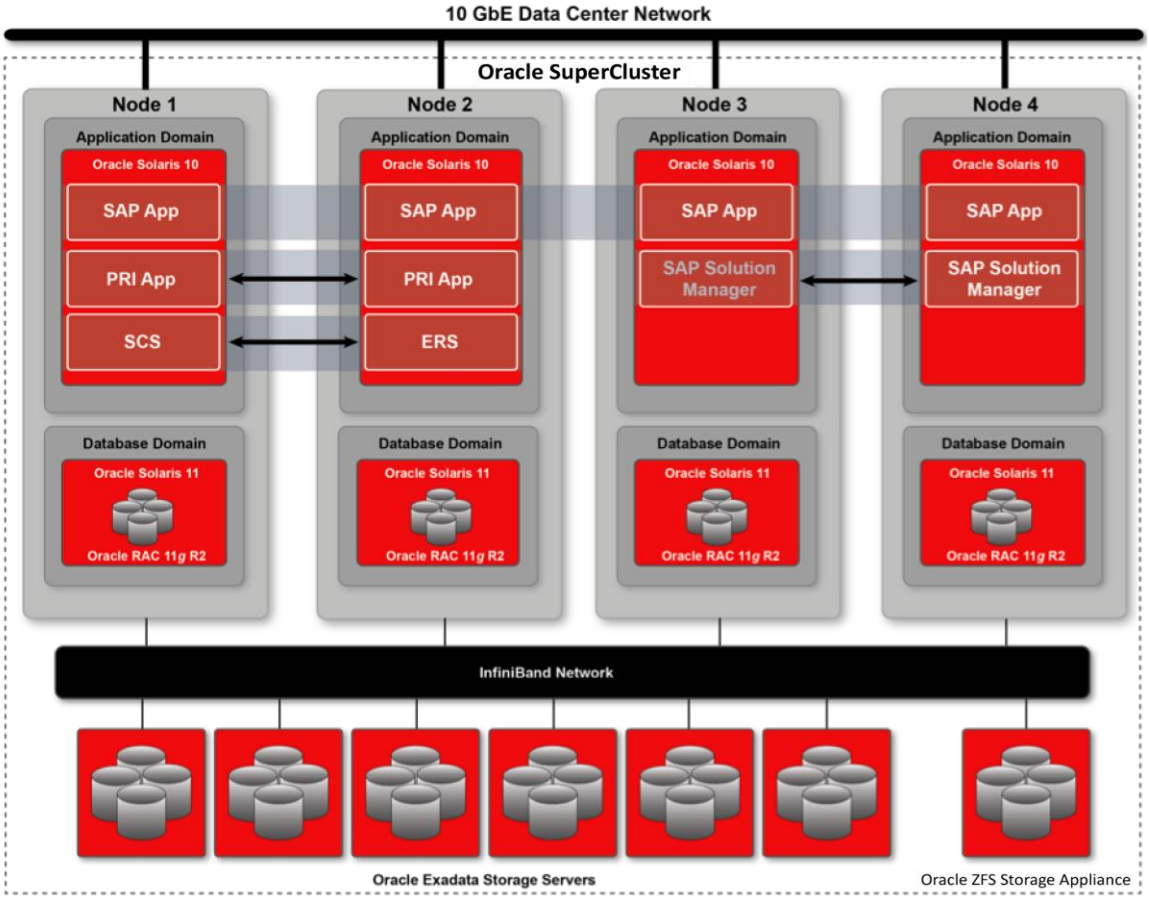

Figure 7. All SAP production systems can be consolidated onto a single Oracle SuperCluster system.

The SAP Central Services and primary application servers run within dedicated zones and are configured with Oracle Solaris zone clusters for high availability. Oracle Solaris Cluster is part of the Oracle SuperCluster engineered systems to eliminate single points of failure and ensure availability of critical SAP components. High availability agents are available for SAP SCS and ASCS, managing the SAP Enqueue Server and Message Server, and are aware of the Replicated Enqueue functionality from SAP. Additional agents support other SAP components,

such as Web Application Servers or SAP liveCache. All agents support a variety of SAP installation types, including ABAP-only instances, Java-only instances, or a double-stack system of ABAP and Java instances.

Providing high availability for SAP System Central Services requires the Standalone Enqueue Server to be replicated. One server node runs the Standalone Enqueue Server and another server runs the Replica Enqueue Server. The SAP Enqueue Server, Replica Server, and Message Server all are configured as Oracle Solaris Cluster failover resources in a zone cluster, in a specific way to perform the recovery of the replicated Enqueue services. In addition, an external Oracle Database proxy resource is configured in the same zone cluster to monitor and represent the availability of the specific database services provided by the Oracle RAC 11*g* Release 2 database domains. The SAP system has a dependency on such database services. This resource enables the coordination of availability between the two types of domains in Oracle SuperCluster systems.

Quality Assurance and Development Systems

The typical "promote to production" scenario requires the creation of a Quality Assurance System and a Development system (DEV) in addition to the production system previously described. A fourth Sandbox (SBX) standalone environment can be used for destructive testing, learning, and training.

- **Quality Assurance System (QAS)**. Ideally, the QAS is identical to the production system to enable issues to be found and fixed during the verification process. If a duplicate environment is not possible, a scaled down system can be used in a ratio that enables technical staff to forecast performance impact.
- **Development system (DEV)**. Customization efforts and the development of new functionality typically take place on a small server and database. All maintenance activities, including break-fixes for production processes, tend to be performed on these systems as well.
- **Sandbox system (SBX)**. Using a small standalone system and database, the sandbox systems makes it easy for developers to gain experience with applications, test scenarios prior to incorporation into the mainstream code base, and conduct feasibility studies for customer-specific requirements or requests.

In all of these environments, developers frequently test new functionality and software products, patch applications, and perform upgrades. Toward this end, many developers and test engineers are given root access to enable them to perform tasks independently.

Consolidating QA and DEV on Oracle SuperCluster

SAP quality assurance systems can be consolidated onto a single Oracle SuperCluster system to simplify the SAP landscape and shorten the time needed to get a new QA system up and running (Figure 8). In this example configuration, the servers are combined into a highly available quality assurance environment that mimics the production system. Each server is divided into two domains (application and database) using Oracle VM Server for SPARC. The application domain is further subdivided into isolated environments using Oracle Solaris Zones, with each SAP application and its QA tools contained within the zone to ensure isolation from other applications. Oracle Solaris Cluster is used to combine zones into clusters to enable failover for SAP Central Services. Oracle Database and Oracle Real Application Clusters run in the database domain connected to Oracle Exadata Storage Servers to support highly available data access.

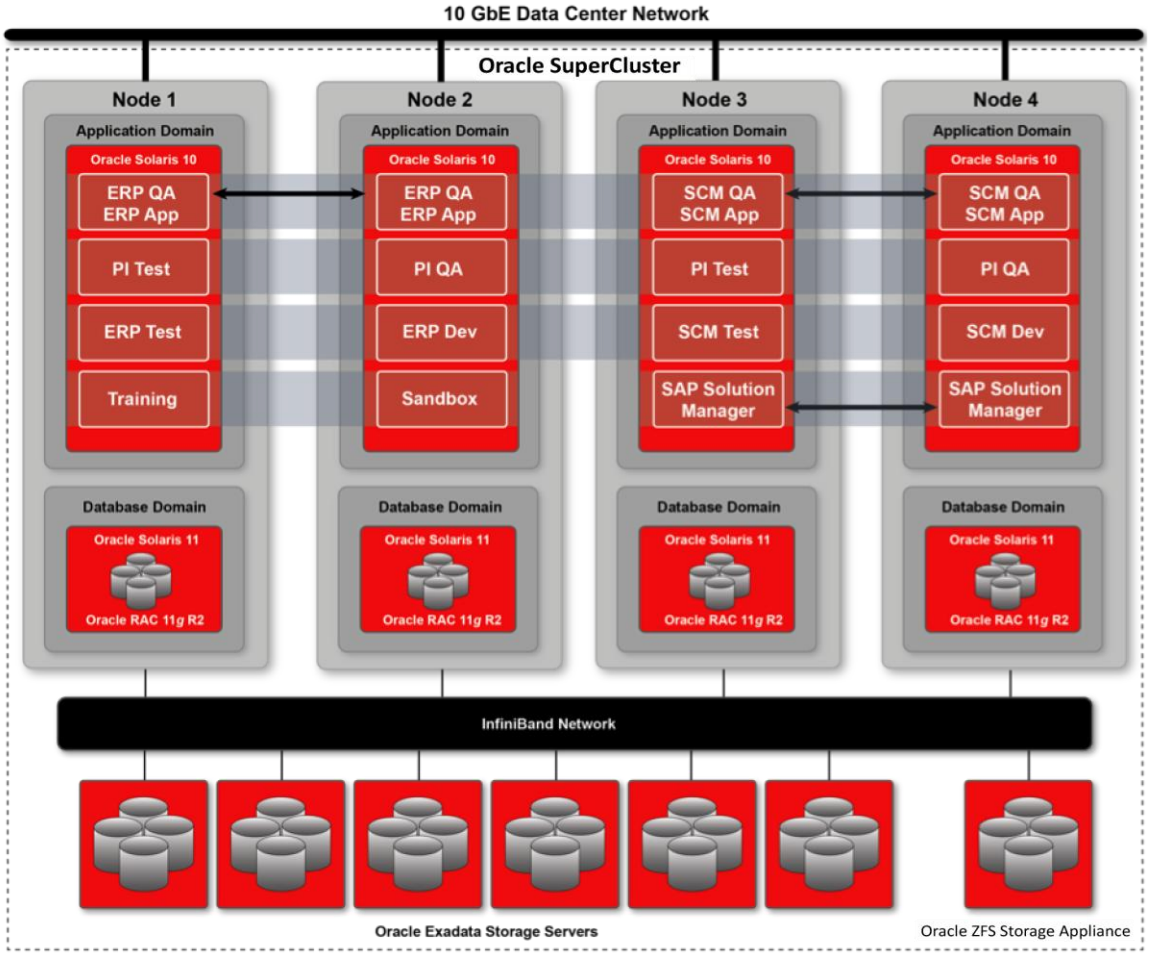

Figure 8. SAP QA systems can be consolidated along with development and test, training, and sandbox systems

The massive scalability and performance of Oracle SuperCluster enable development and test systems to be consolidated onto the system as well. Within the application domain, Oracle Solaris Zones provide a complete runtime environment to SAP applications, and house all programming tools and databases required for development. Each zone provides full resource containment and control, and fault and security isolation, to ensure applications do not hamper one another's access to resources or impact execution. Developers and administrators can manage compute, memory, and I/O resources on a fine-grained basis (statically or during operation) to ensure applications have access to an appropriate amount of resources and that no workload consumes the entire platform. As a result, programmers can maintain a one-application-per-server deployment model while simultaneously sharing hardware resources.

SAP Landscape Architecture Using a Single Oracle SuperCluster

SAP deployments with more moderate performance or scalability requirements can consolidate the entire SAP landscape onto a single, full-rack Oracle SuperCluster system. In such a configuration, all production, quality assurance, development, and other systems run in isolated areas (Figure 9). Development systems run within an Oracle Solaris Zone to maintain the one-application-per-server model preferred by developers, while the production

system runs on two clustered servers to ensure high availability. The quality assurance system replicates all or part of the production environment, enabling applications to be tested in the same environment in which they are to be deployed.

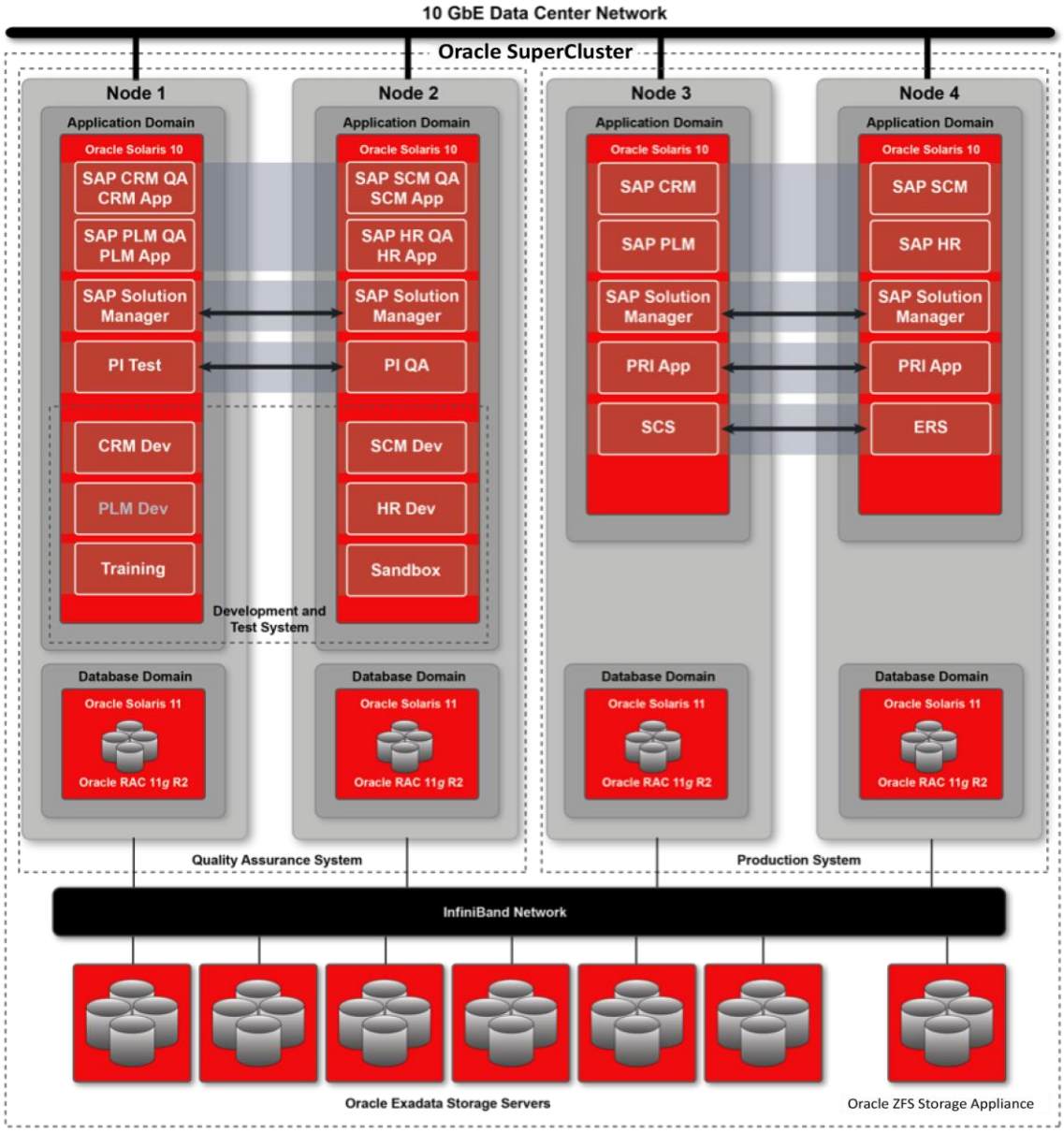

Figure 9. SAP deployments with moderate performance or scalability requirements can be consolidated onto one system.

Backup, Restore, and Disaster Recovery

Backup and Restore

A variety of backup and restore solutions are available that provide short-term data protection and long-term data preservation for Oracle SuperCluster (Figure 10). Options vary according to the type of data (structured or unstructured), data protection needs, recovery time, performance, capacity, and service level requirements.

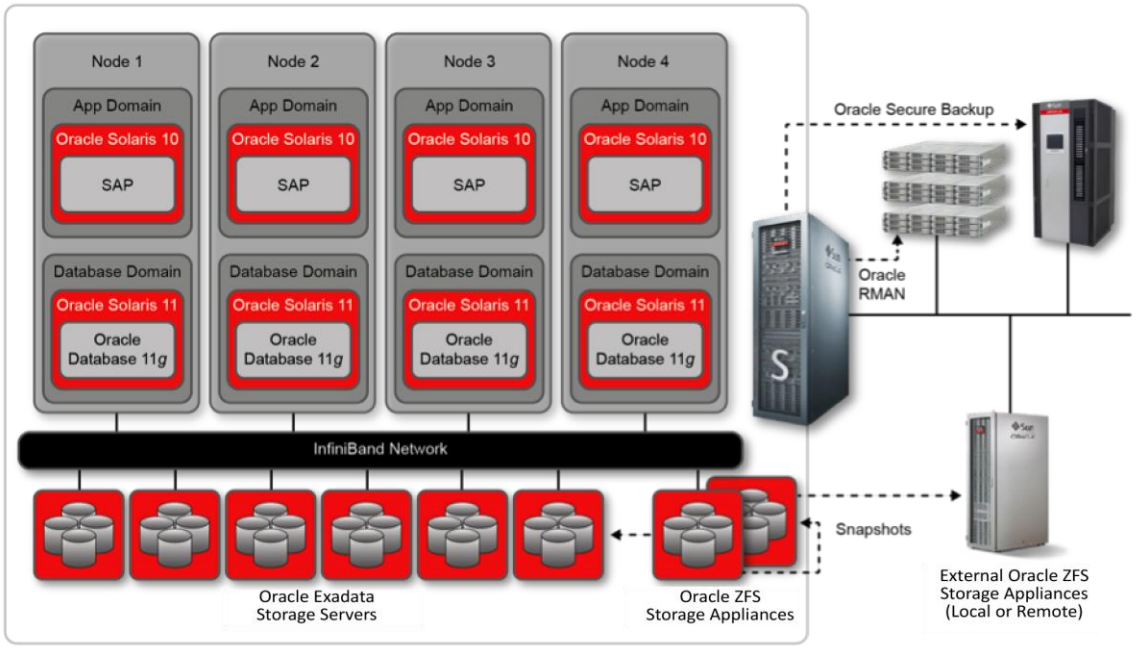

Figure 10. Oracle Optimized Solution for SAP integrates with Oracle backup tools.

- For structured data in Oracle Database, backups can be done with Oracle Recovery Manager (Oracle RMAN) to disk or to tape through Oracle Secure Backup. Oracle offers Oracle Optimized Solution for Oracle Secure Backup, which is designed to perform network backups of heterogeneous clients, including Oracle's engineered systems for Oracle Exadata, Oracle SuperCluster, and Oracle Optimized Solutions. The local Oracle ZFS Storage Appliance can be an efficient first step in a disk-to-disk-to-tape (D2D2T) strategy, with 8 TB/hour backup rates measured. For backup, recovery, and long-term archival, tape remains the most cost-effective and reliable storage media available. For SAP landscapes where longer retention periods and greater capacity are required, Oracle Secure Backup and tape storage can be used for backup, vaulting, and archiving.
- For unstructured data, the Oracle ZFS Storage Appliance in Oracle SuperCluster can be used to generate and store snapshots of the SAP file system. Snapshots are an efficient way of accessing historic data and creating new SAP environments through the use of clones. Snapshots can be stored locally or replicated remotely to another Oracle ZFS Storage Appliance or tape.
- Oracle Optimized Solution for Backup and Recovery delivers accelerated next-generation data protection for Oracle's engineered systems and Oracle Optimized Solutions. The flexible, multi-tier architecture provides virtually unlimited scalability, centralized management, and end-to-end data protection for heterogeneous technologies. Backup costs for these Oracle systems can be reduced, with up to 75 percent lower software license costs compared to offerings from other vendors.

Disaster Recovery

A disaster recovery strategy is necessary to prevent downtime and data loss should a catastrophic event occur, such as a flood, fire, or campus power outage. The goal is to protect mission-critical SAP applications and databases residing on Oracle SuperCluster. This is accomplished by ensuring that services in the application tier are quickly migrated to a secondary site, while databases in the database tier are replicated and data storage is synchronized (Figure 11).

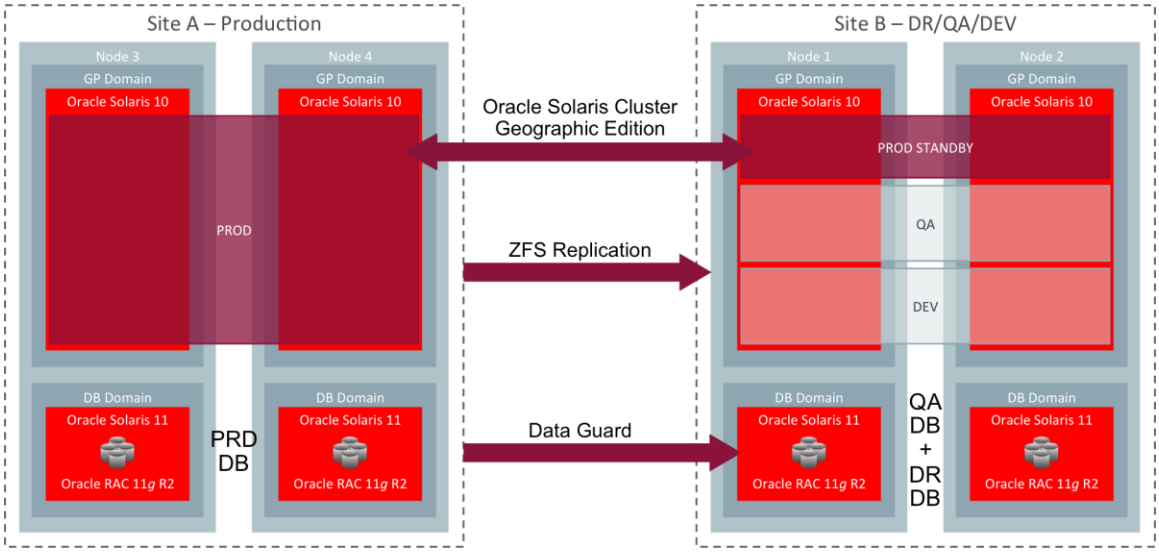

Figure 11. Application tier services are replicated to a secondary site, while databases are replicated and storage is synchronized.

Application Tier

Oracle Solaris Cluster Geographic Edition software protects the SAP application tier from unexpected disruptions. Multiple clusters are separated by long distance, and a redundant infrastructure replicates data between these clusters. A layered extension to Oracle Solaris Cluster, Oracle Solaris Cluster Geographic Edition software provides a consistent interface for the process of switching over data processing between data centers. It enables the controlled migration of production services from a primary cluster to a secondary cluster, either in the event of a disaster or as part of a planned procedure.

Oracle Solaris Cluster Geographic Edition configurations consist of two or more distinct clusters. The software does not perform automatic failovers. Instead, a decision must be made as to whether taking over the production workload at the backup data center is the most appropriate course of action. A manually initiated, automated process orchestrates the orderly shut down of the resource groups that contain the application components on the cluster in the main data center. The software reverses the direction of data replication before bringing the resource group back online at the second (backup) data center. In the event of a real disaster, the software can forcibly take control of a resource group and safely bring it online on at the second data center.

For more information, see “Oracle Solaris and Oracle Solaris Cluster: Extending Oracle Solaris for Business Continuity” located at oracle.com/technetwork/server-storage/solaris-cluster/documentation/solaris-cluster-businesscontinuity-168285.pdf, Oracle Solaris Cluster Geographic Edition Overview located at

docs.oracle.com/cd/E22702_01/pdf/821-2767.pdf, and the Oracle Solaris Cluster product documentation located at oracle.com/technetwork/server-storage/solaris-cluster/documentation/index.html.

Database Tier

Data Guard is Oracle's disaster recovery solution prescribed by the Maximum Availability Architecture (MAA) to protect the mission-critical databases residing on the Oracle Exadata Storage Servers within Oracle SuperCluster. Data Guard can be used to maintain availability should an outage unexpectedly impact the production database, as well as minimize downtime during planned maintenance.

Included with Oracle Database Enterprise Edition, Data Guard provides management, monitoring, and automation software. These tools enable administrators to create and maintain one or more synchronized copies (standby databases) that protect the production database (primary database) from failures, disasters, errors, and corruptions. Data Guard maintains these standby databases as copies of the production database. If the production database is rendered unavailable due to a planned or unplanned outage, Data Guard can switch a standby database to the production role, minimizing the downtime associated with the outage. Data Guard can be used with traditional backup, restoration, and cluster techniques to provide a high level of data protection and data availability.

For more information, see the Data Guard documentation located at oracle.com/technetwork/database/features/availability/data-guard-documentation-152848.html, and "Oracle Data Guard: Disaster Recovery for Oracle Exadata Database Machine" located at oracle.com/technetwork/database/features/availability/maa-wp-dr-dbm-130065.pdf.

Storage Tier

Oracle ZFS Storage Appliances support snapshot-based replication of projects and shares. These items can be used to mirror an appliance for disaster recovery. In the event of a disaster that impacts the service of the primary appliance (or even an entire data center), administrators can activate a service at the disaster recovery site, which takes over using the most recently replicated data.

ZFS Storage Remote Replication can be used to create a copy of the SAP environment stored on the Oracle ZFS Storage Appliance (source) located in the production Oracle SuperCluster system. The environment can be copied to another Oracle ZFS Storage Appliance (target) at a remote location through an interconnecting network that is responsible for propagating the data between them. The target appliance can be located virtually any distance from the source—in the same campus, or on the other side of the world—as long as the interconnecting network has sufficient bandwidth to carry the replication stream data. The replication control protocol is secured with SSL. Data also can be protected with SSL, if desired.

By default, an asynchronous replication method is used. This enables replication over larger distances, as a lower-bandwidth, higher-latency link can be used between the storage systems. This slower link can be used since not all writes must be replicated; the system state only needs to be written at certain points in time; and writes do not need to be confirmed at both sites at the same time.

In addition, Oracle ZFS Storage Appliance can help make the disaster recovery site more productive. Snapshot and cloning features created at the disaster recovery site can be used to quickly create SAP test or development environments.

For more information, see the Sun Storage 7000 Unified Storage System Administration Guide located at docs.oracle.com/cd/E19935-01/pdf/820-4167.pdf, and "Architecture Principles and Implementation Practices for Remote Replication Using Sun ZFS Storage Appliance Systems" located at oracle.com/technetwork/server-storage/sun-unified-storage/documentation/zfssa-replication-2014-1-2120969.pdf .

Migrating an Existing SAP Environment

Organizations that currently utilize previous versions of Oracle Database on Oracle Solaris can take advantage of Oracle SuperCluster. In this scenario, SAP applications and databases are moved to dedicated Oracle Solaris Zones, with the database stored on Oracle ZFS Storage Appliance (Figure 12) or existing storage. Oracle Solaris Cluster can be leveraged to provide failover services for the database (and applications, if desired). This construction enables legacy databases to run on the system and support SAP applications with minimum changes. Over time, IT organizations can progressively test applications against Oracle Real Application Clusters 11*g* Release 2 running in the database domain, and migrate them to a three-tier deployment that benefits from the database performance acceleration of Oracle Exadata Storage Servers.

Oracle Solaris 11 has native support for Oracle Solaris 10 within Oracle Solaris 10 Zones. This enables organizations to run specific applications within an Oracle Solaris 10 environment while seamlessly migrating to Oracle Solaris 11. As a result, organizations can benefit from innovation in Oracle Solaris 11, such as kernel improvements, increased performance, faster kernel patching, and virtualization improvements, while providing access to Oracle Solaris 10 runtime environments for applications that require them. For example, it is possible to migrate pre-existing applications to Oracle Solaris 10 environments and run them alongside new applications that can take advantage of Oracle Solaris 11.

Figure 12 illustrates a production environment with three-tier and two-tier deployments. Nodes 1 and 2 comprise a three-tier production environment that runs SAP applications and SAP Central Services in the application domain, and databases in the database domain on Oracle Exadata Storage Servers. Nodes 3 and 4 comprise a two-tier production environment that runs SAP applications and legacy databases within dedicated zones in the application domain.

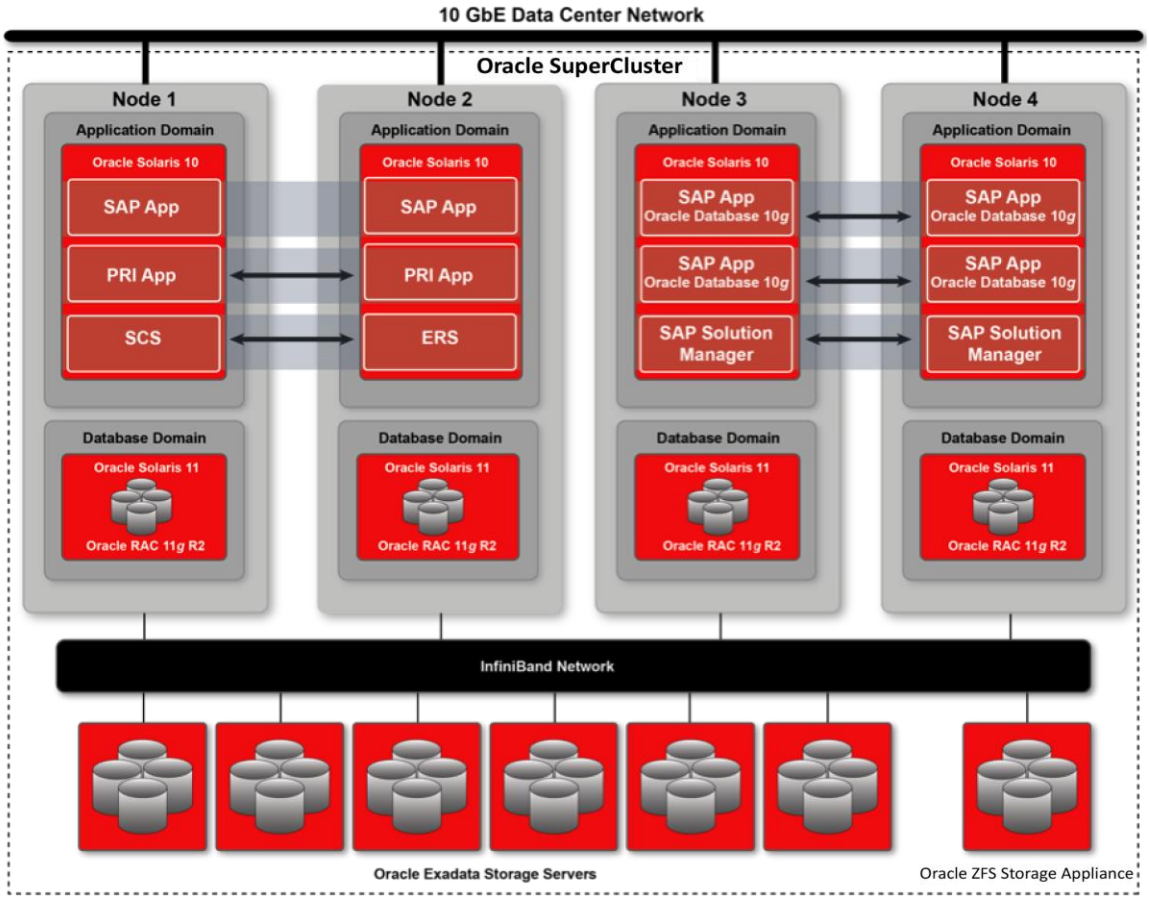

Figure 12. Two-tier SAP landscapes can be run on Oracle SuperCluster.

Oracle to Oracle Online Migration

An Oracle Advanced Customer Support online migration service, named O2O Online or Triple-O (Oracle to Oracle Online), allows database migrations to be performed while the SAP system is up and running on the source system. Certified by SAP, this method uses built-in Oracle functionality for the initial database load and Oracle GoldenGate for data synchronization. It can be used for any R/3 and BW system in any size. There are no limitations for the usage of the SAP system during the migration. Heterogeneous database migrations and direct database upgrades are supported. There is no downtime needed to start or stop the online migration process.

For more details on O2O Online migration services, see SAP Note 1508271 or contact Oracle Advanced Customer Support. More information can be found at oracle.com/acs.

Security Mechanisms

Security should be considered in the initial architecture definition and design phases of SAP systems, rather than during or after implementation. Many security vulnerabilities can be avoided by following recommendations included in Oracle's pre-tested and evaluated implementation documentation. The following are several examples of security mechanisms implemented in this solution.

OS Security

- **Oracle Solaris and Oracle Solaris Cluster Secure by Default**. Upon installation, Oracle Solaris and Oracle Solaris Cluster are configured by default with a large set of network services disabled. This hardened setup is called “Secure By Default” (SBD).
- **Tier isolation using Oracle VM Server and Oracle Solaris Zones**. Oracle VM Server provides isolated execution environments called domains. Each domain is an independent instance in which the Oracle Solaris OS can be hardened using existing security guidelines. Additionally, Oracle Solaris Zones provide an application execution environment that isolates processes from the rest of the system within a single instance of the Oracle Solaris OS. This combination of Oracle VM Server, Oracle Solaris Zones, and network partitioning allows enforcement of strict, role-based administration rights across the SAP environment.

Network Security

- **Network isolation with partitioning (InfiniBand partitions)**. An InfiniBand partition is a subdivision of a local area network at the datalink layer of the protocol stack. Network security can be improved by separating data traffic into multiple, dedicated InfiniBand partitions. Then, groups of users can be assigned to each partition and differing security policies can be enforced for each workgroup on a per-partition basis.
- **Isolation of storage data traffic and application data traffic**. Network security can be further increased by using dedicated InfiniBand partitions to isolate storage data traffic and application data traffic between the application and database tiers.
- **Physically separated systems management network**. In this solution, the systems management network uses a physically separate network infrastructure, including switches, cables, and ports. This isolates management traffic from data traffic and increases network security.
- **Dedicated cluster interconnect networks**. Using separate physical network interfaces, a pair of dedicated, redundant, private interconnects is configured for each cluster, ensuring that IP traffic from one cluster does not interfere with IP traffic from another cluster.

Storage Security

- **Restricted access to NFS file systems using NFS exceptions**. Access to NFS file systems on shared storage is restricted to specific hosts or networks using NFS exceptions.
- **Block storage device security using target groups and initiator groups (iSCSI LUNs)**. Target and initiator groups are defined to grant or restrict access to block storage devices. Target groups define which network interfaces the block storage devices are visible on. Initiator groups define which clients have access to which block devices.
- **Physically isolated data and administrative traffic**. Data traffic and systems management are isolated through the use of physically separate networks and interfaces on Oracle ZFS Storage Appliance.

Analyzing Solution Characteristics

Oracle engineers tested Oracle Optimized Solution for SAP. The goal of the testing effort was to understand and characterize the behavior of the architecture under peak load conditions, determine optimum utilization, and verify solution scalability. The solution was tested at Oracle facilities and customer sites using various SAP workloads. The workloads were chosen to stress the entire architecture, similar to production environments.

SAP SD Benchmark and SAPS Metric

The SAP Sales and Distribution (SD) benchmark and SAP Application Performance Standard (SAPS) metric were not used during the performance testing effort for the solution. Originally introduced as a hardware-independent method to characterize throughput, over time SAPS has become a CPU sizing metric describing only the compute requirements of an SAP system. While SAPS is a critical metric for proper sizing of the compute tier of an SAP

environment, it does not characterize the holistic performance of a complete infrastructure such as Oracle SuperCluster.

Characterizing Holistic Infrastructure Performance

Unique to the Oracle Optimized Solution for SAP on Oracle SuperCluster is its performance as a complete infrastructure for SAP. As a result, Oracle engineers decided to focus testing efforts on workloads that realistically simulate customer production environments—scenarios that stress compute, network, database, and storage components. The results below were produced by running various performance tests in environments as close to production as possible, sometimes using actual customer workloads and datasets, during proof of concept (POC) engagements.

Performance Test #1

Oracle engineers created the test environment by migrating a customer's pre-existing QA environment (Applications, Central Services and Database) to Oracle SuperCluster. Oracle Advanced Customer Support (Oracle ACS) assisted with the build-out of the test environment, migration to Oracle SuperCluster, testing, and data collection. The migration included moving the existing SAP environment, configuring Oracle Solaris Cluster for Applications and Central Services high availability, and configuring Oracle RAC for database high availability.

The process created a fully operational SAP environment on Oracle SuperCluster and was completed within 16 man-days, including testing and validation.

- Application tier migration and HA configuration: 8 man-days
- Database tier migration and Oracle RAC configuration: 8 man-days

To create a fair comparison, the Oracle SuperCluster system was configured to match the customer's previous environment, using the limitations outlined in Table 1.

TABLE 1. CONFIGURATION LIMITS SET ON ORACLE SUPERCLUSTER

Description	Value
CPU capping in Oracle Solaris Zones	Set to 1 CPU
Database SGA	Reduced to 2.8 GB
SAP binaries for SAP applications and Central Services	Copied from previous environment
Tuning and optimization	None

Table 2 describes the existing environment, as well as the application and database tier definitions on the Oracle SuperCluster system.

TABLE 2. CONFIGURATION DETAILS

Components	Existing Environment	Oracle SuperCluster Environment
Servers	SPARC Enterprise M5000 server from Oracle: » *4 SPARC64 VII 2.4 GHz processors* » *4 cores and 2 threads per core per processor* » *16 GB memory (4 DDR2-667 ECC memory DIMMs)*	Application Tier: » *SPARC T4 server from Oracle* » *Domain with 3 CPUs, 768 GB of memory* Database Tier: » *Oracle Exadata Storage Server* » *Domain with 1 CPU, 256 GB of memory*
Operating system	Oracle Solaris 10	Oracle Solaris 10 (Application tier) Oracle Solaris 11 (Database tier)
Storage	Hitachi storage (connected over a SAN)	Internal to Oracle SuperCluster system
Database	Oracle Database 11.2.0.2 single instance	Oracle Database 11*g* R2 (11.2.0.3) with Oracle RAC
Virtualization	SAP Database and Application tier running in Oracle Solaris Zones	Oracle VM Server for SPARC
Clustering	None	Oracle Solaris Cluster 3.3

Several workloads were run, with each test executed twice on the existing environment and the Oracle SuperCluster configuration. The SAP GUI was used to monitor test execution and capture results.

» **Update stats script**. The script generates statistics used by the optimizer on the system hardware and on the database by reading 73,000 database tables. Table 3 shows the script execution time in both environments.

TABLE 3. UPDATE STATS SCRIPT RESULTS

Existing Environment	SPARC SuperCluster T4-4	Differential
3 minutes, 32 seconds	55 seconds	3.8 times faster

» **SGEN**. Typically used after installations or upgrades, the SGEN transaction reads and re-compiles all of the ABAP applications, and saves them in the database. Table 4 shows the SGEN transaction time in both environments.

TABLE 4. SGEN RESULTS

Existing Environment	SPARC SuperCluster T4-4	Differential
6 hours, 8 minutes, 23 seconds	3 hours, 57 minutes, 25 seconds	1.55 times faster

» **Expensive table queries**. Table 5 lists four SQL statements from the existing environment that were identified as creating the most expensive table queries, along with execution results.

TABLE 5. EXPENSIVE TABLE QUERIES RESULTS

SQL Statement	Previous Environment	Oracle SuperCluster	Differential
ZFT_TRANS_TRACK Performs a full table scan of the ZFT_TRANS_TRACK table	457 ms	220 ms	2.1 times faster
CDHDR Generates very heavy disk reads Benefits from fast I/O and storage	2,678 ms	10 ms	268 times faster
EKPO Generates a very large number of physical reads Benefits from high I/O speeds	10 sec	0.8 sec	12.5 times faster
ANLZ, ANLU, ZAA_SF126 Performs a lot of multi-table joins Benefits from the database optimization performed by O2O database migration	7.7 sec	2.7 sec	2.8 times faster

All of the tests showed significant performance improvement when run on the Oracle SuperCluster system. Note: These test results were produced on an Oracle SuperCluster with constrained resources (Table 1) to match the customer's existing production environment. Higher results can be produced without these resource restrictions.

Performance Test #2

Oracle Exadata Storage Servers are known for their acceleration of database-intensive workloads. In this performance test, Oracle engineers sought to demonstrate the performance improvement of workloads with light to moderate database loads using the Oracle Exadata Storage Servers in the Oracle SuperCluster system. Other variables, such as compute and network performance, were eliminated from consideration by running the workload on the Oracle SuperCluster system and pairing it with a database running on an Oracle Exadata Storage Server or an Oracle ZFS Storage Appliance within the system. The SAP Load Generator (SGEN) was used to generate a light database load. Table 6 describes the results and performance improvement observed.

TABLE 6. RESULTS OF SGEN WITH AND WITHOUT ORACLE EXADATA STORAGE SERVERS

Without Oracle Exadata Storage Servers	With Oracle Exadata Storage Servers	Differential
42 minutes	32 minutes	31 percent faster

These results show the Oracle Exadata Storage Servers accelerate workloads on Oracle SuperCluster, even when they are not database-intensive. Note: Running a more I/O intensive workload would show a much higher performance improvement with Oracle Exadata Storage Servers.

Performance Test #3

In this test, a customer's SAP environment, data, and scripts were transferred to the Oracle Solution Center in Santa Clara, California, to benchmark key performance indexes. Testing was performed on a full-rack Oracle SuperCluster system, using only two (out of four) SPARC T4-4 server nodes. Each SPARC T4-4 server was configured with two

domains: a general-purpose domain running Oracle Solaris 10 for SAP applications and SAP Central Instances, and a database domain running Oracle Solaris 11 for Oracle RAC database 11*g* Release 2. Table 7 describes the infrastructure configuration.

TABLE 7. CONFIGURATION DETAILS

Tiers	Other Environments	Other Environments
Application Tier: » *Domain with 2 CPUs, 512 GB of memory* » *Oracle Solaris 10* » *SAP Application Server and SAP Central Instances clustered using Oracle Solaris Cluster 3.3* Database Tier: » *Domain with 2 CPUs, 512 GB of memory* » *Oracle Solaris 11* » *Oracle Database 11g R2 (11.2.03) with Oracle RAC* » *One Oracle RAC instance with 3 database services (on each node)* » *SGA at 80 GB*	Oracle's SPARC T4-2 server: » *2 SPARC T4 processors* » *8 cores, 64 threads, 2.85 GHz per processor* » *512 GB memory (32 DDR3 16 GB DIMMs)* » *2 dual-port 10 GbE cards* » *racle Solaris 10*	HP ProLiant DL380 G7 server » *2 Intel® Xeon® X5670 processors (2.93 GHz, 6 cores)* » *384 GB memory (12 DDR3 32 GB DIMMs)* » *2 HP NC522SFP Dual Port 10 GbE Gigabit Adapters* » *Red Hat Enterprise Linux 5.4*

The SAP IS-Oil & Business Connector workload was tested using the following processes:

» Dialog Processes
» Background Processes
» Remote Function Calls
» Update 1 Processes
» Update 2 Processes

The SAP operating system collector (OS collector) and AWR Reports monitoring tools were used to collect the test results.

The test ran three times on each platform. The results in Table 8 list the average of the three test run results.

TABLE 8. TEST RESULTS

Test Platform	Test Run Time	Differential
SPARC SuperCluster T4-4 system	5 min, 14 sec	1X
SPARC T4-2 server (application and database tiers)	13 min, 18 sec	2.5X
SPARC T4-2 server (application tier) and SPARC T4-2 server (database tier)	13 min, 18 sec	2.5X
HP DL380 server (application tier) and SPARC T4-2 server (database tier)	13 min, 47 sec	2.6X
SPARC SuperCluster T4-4 system	5 min, 14 sec	1X
SPARC T4-2 server (application and database tiers)	13 min, 18 sec	2.5X

These results show the Oracle SuperCluster system consistently outperformed (two to three times faster) standalone SPARC T4 servers and HP DL380 G7 servers. The backup of a ~10 TB database was performed under one hour, with throughput of 12 TB per hour (Table 9).

TABLE 9. BACKUP RESULTS

Backup and Restore Tests	Time	Throughput
Database backup to Oracle ZFS Storage Appliance (9.8 TB)	49 min	12 TB/hr
Database restore from Oracle ZFS Storage Appliance (9.8 TB)	1 hr, 22 min	7.2 TB/hr

Solution Availability Testing

To validate the high availability characteristics of the overall solution, numerous and rigorous failure tests were performed. These tests were executed under load on the application and database architecture tiers, on the entire general-purpose domain (SAP application servers, primary application server, and central services), and on a complete SPARC T4-4 server node. The following tables list the measured results. The numbers provided in this document indicate activity duration and are based on a cluster configuration using default settings.

Test Configuration

Table 10 describes the configuration used during availability testing. When necessary, some of the instances were moved between nodes to accommodate the purpose of the tests. Eight failover SAP application instances were configured (D51 to D58). Two instances ran on each server, with the instances located in a zone cluster configured with four SPARC T4 processor cores (32 operating system cores). The primary application server instance and the SAP Central Services also ran in zone clusters. Oracle RAC 11*g* Release 2 was configured in the database domains. All SAP instances were configured to connect to their respective database service over the InfiniBand connection.

TABLE 10. INITIAL TEST CONFIGURATION

Failover Application Instances	SPARC T4 Server Node	Oracle Solaris Zone Cluster Configuration
D51 and D55	1	Four SPARC T4 cores (32 operating system CPUs)
D52 and D56	2	
D53 and D57	3	
D54 and D58	4	
Other Instances		**Oracle Solaris Zone Cluster Configuration**
Primary application server instance		0.5 SPARC T4 core (4 operating system CPUs) per server
SAP Central Services (Enqueue, message, and enqueue replication servers)		0.5 SPARC T4 core (4 operating system CPUs) per server
Oracle RAC 11*g* R2 Instances		**Oracle Exadata Storage Server Node**
Q011		1
Q012		2
O013		3
Q014		4

Load Generation

The SD benchmark was used as a load generator during the availability testing effort. The benchmark was configured for a total of 3,300 SD users. The test sent 400 users to each of the eight SAP dialogue instances, and 100 users to the primary instance. Under normal conditions, CPU utilization was observed to be 50 percent in the zone clusters running the SAP application instances (dialogue or primary), and less than 5 percent in the database domains. The workload produced approximately 320 dialog steps per second (DS/sec), with dialog step response time under 0.5 second.

Availability Test #1: Loss of SAP Application Server Instances

The first availability test injected an error to cause two SAP Application Server instances to be lost (Figure 13). The zone cluster node running instances D52 and D56 (on node 2) was rebooted abruptly using the `uadmin 1 0` command. Each of the impacted application instances failed over to a different node (a node already running two active instances). If the impacted instances have redundant instances in their SAP GUI logon group, due to the fast (2 sec) failover of their logical hosts, users should be disconnected and allowed to reconnect immediately to another application instance within the logon group.

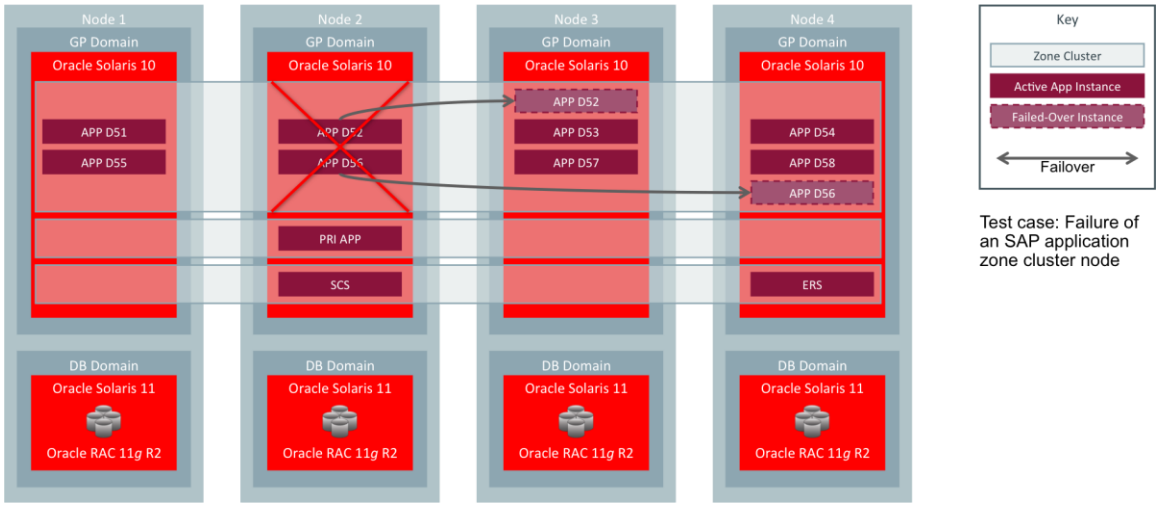

Figure 13. Failure of a SAP Application Server cluster node.

Table 11 lists the failure test observations. While the post-failure workload run showed no errors, it exhibited slightly degraded performance and increased CPU utilization in the zone cluster nodes handling the failed over SAP instances. These results indicate there is no impact to users other than slight performance degradation, with response time remaining under 2 seconds.

TABLE 11. APPLICATION ZONE CLUSTER NODE FAILURE TEST OBSERVATIONS

Failure Detection	**Recovery**
9 sec	2 min, 57 sec
Initial Performance	**Degraded Performance**
320 DS/sec 0.5 sec response time 50 percent CPU utilization (average)	277 DS/sec 1.9 sec response time Up to 80 percent CPU utilization

Availability Test #2: Loss of SAP Primary Application Server

The second availability test explored the solution's response to a loss of the SAP Primary Application Server (Figure 14). To simulate the failure, the zone cluster node running the Primary Application Server instance (on node 2) was rebooted abruptly using the `uadmin 1 0` command. The instance failed over to node 1.

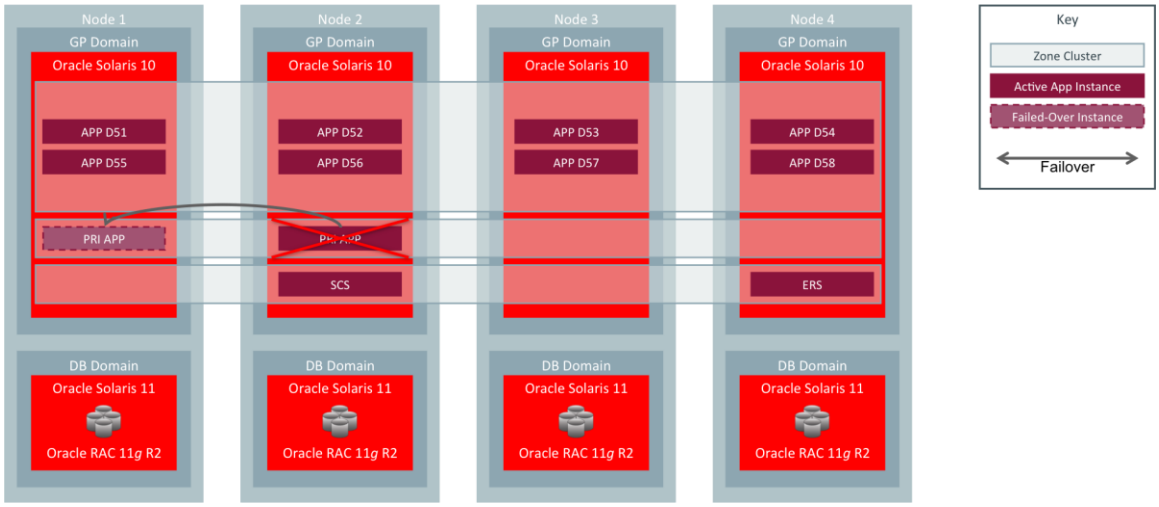

Figure 14. Failure of the Primary Application Server zone cluster node.

Table 12 lists the time needed for failure detection and recovery. The post-failure workload run showed no errors, and no impact to users was observed.

TABLE 12. PRIMARY APP ZONE CLUSTER NODE FAILURE TEST OBSERVATIONS

Failure Detection	Recovery
9 sec	1 min, 16 sec

Availability Test #3: Loss of the Domain Running the SAP Central Services

Another availability test looked at the loss of the general-purpose domain running the SAP Central Services (enqueue and message servers). This domain also was running the primary application server instance and two application server dialogue instances. The domain was panicked using the `uadmin 5 1` command. The impacted instances each failed over to a different node that was running two active instances (Figure 15). If the impacted instances have redundant instances in their SAP GUI logon group, due to the fast (2 sec) failover of their logical hosts, users should be disconnected and allowed to reconnect immediately to the redundant instances before the impacted instances are recovered.

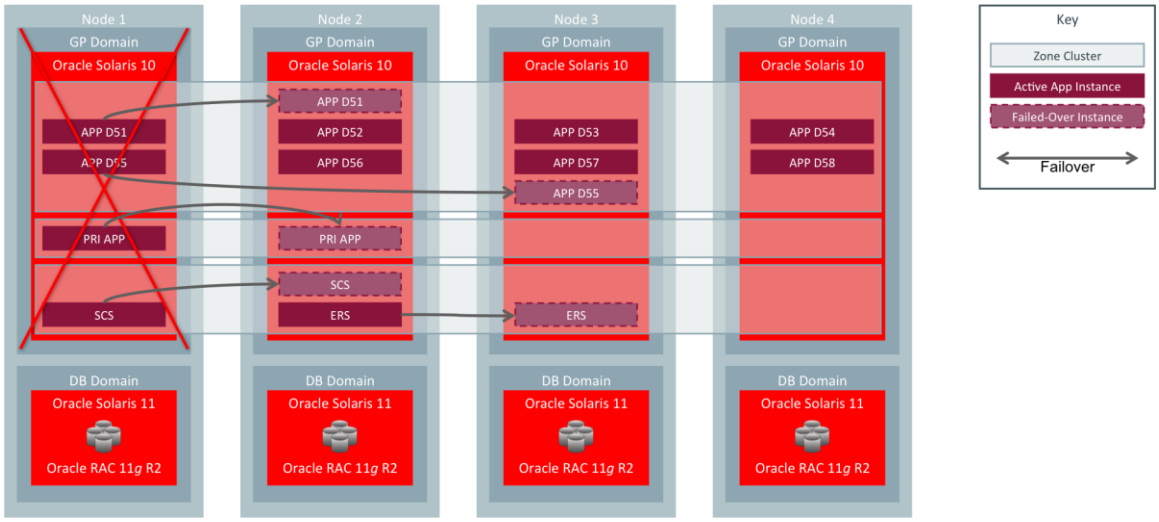

Figure 15. Failure of the general-purpose domain on the node running the SAP Central Services (SCS).

Table 13 lists the failure test observations. While the workload run showed no errors, it exhibited slightly degraded performance and increased CPU utilization in the zone cluster nodes handling the failed over SAP instances. These results indicate there is no impact to users other than slight performance degradation, with response time remaining under 2 seconds.

TABLE 13. PRIMARY APPLICATION ZONE CLUSTER NODE FAILURE TEST OBSERVATIONS

Process Stage	**Time**
Failure detection	1 sec
SCS recovery	43 sec
Enqueue Replication Server Recover	45 sec
Primary Application Server Recovery	1 min, 28 sec
Application Servers Recovery	2 min, 5 sec
Initial Performance	**Degraded Performance**
320 DS/sec 0.5 sec response time 50 percent CPU utilization (average)	277 DS/sec 1.9 sec response time Up to 80 percent CPU utilization

Availability Test #4: Loss of a Database Domain

In this test, the Oracle Database 11*g* Release 2 database domain running the Oracle RAC instance Q012 is panicked using the `uadmin 5 1` command. As shown in Figure 16, the database services on instance Q012 (node 2) failed over to instance Q011 (node 1).

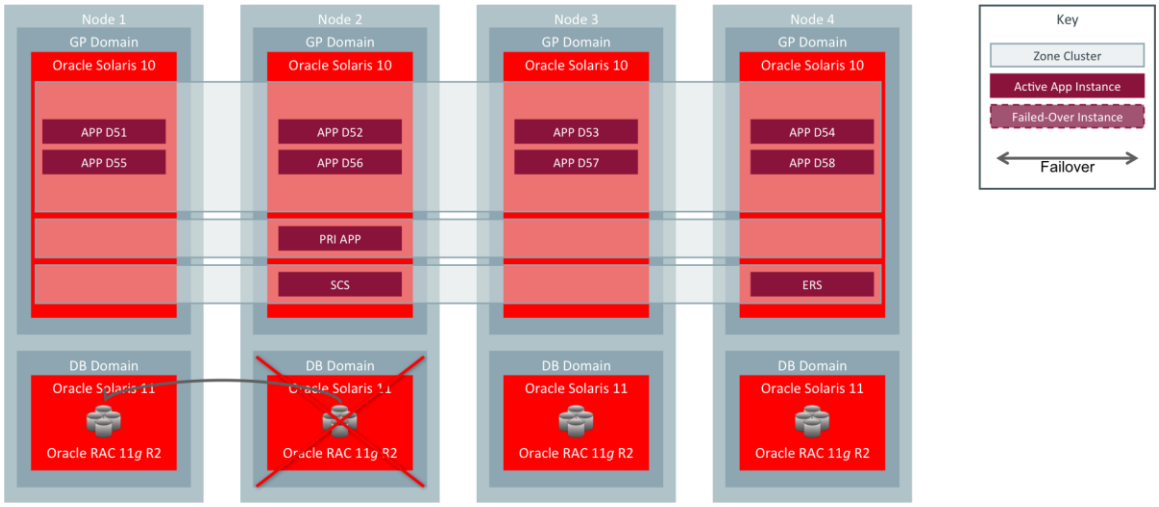

Figure 16. Failure of a database domain.

The post-failure workload showed no errors, but exhibited a slight performance impact, as listed in Table 14. These results indicate there is no impact to users other than slight performance degradation, with response time remaining under 2 seconds.

TABLE 14. DATABASE DOMAIN FAILURE TEST OBSERVATIONS

Failure Detection	Recovery
64 sec	20 sec
Initial Performance	**Degraded Performance**
320 DS/sec 0.5 sec response time	295 DS/sec 1.2 sec response time

Availability Test #5: Loss of the Primary Application Server Instance Host

In this test, a SPARC T4-4 server was powered off in an ungraceful manner. This server (node 2) was running the SAP primary application server instance and the enqueue replication server. The server also was running one Oracle RAC database instance (Q012) and two SAP application server dialogue instances (D52 and D56). The impacted instances each failed over to a different node that was running two active instances (Figure 17). If the impacted instances have redundant instances in their SAP GUI logon group, due to the fast (2 sec) failover of their logical hosts, users should be disconnected and allowed to reconnect immediately. The database services on instance Q012 (node 2) all failed over to instance Q011 (node 1).

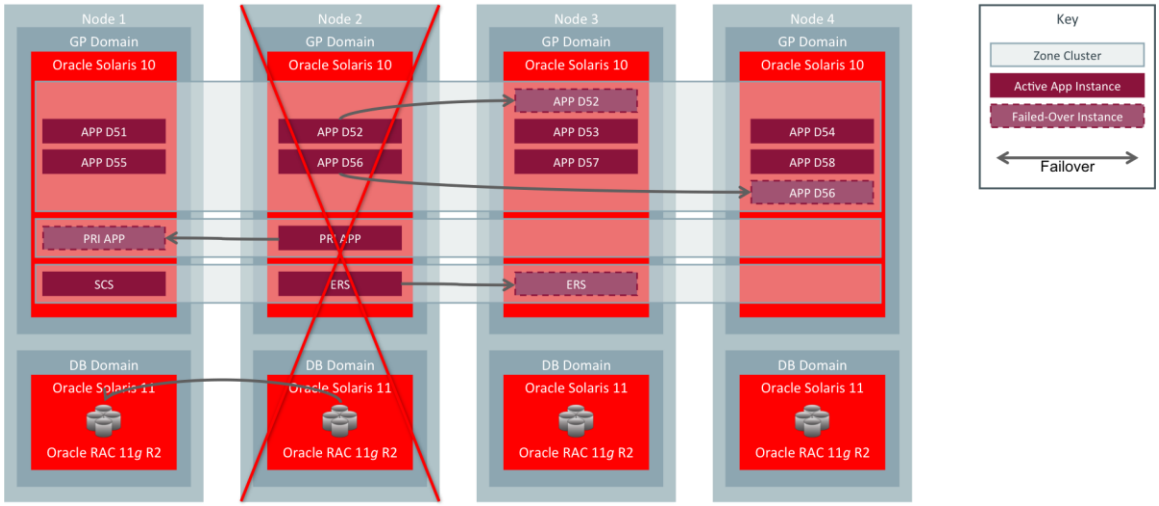

Figure 17. Failure of the Primary Application Server instance host.

Table 15 lists the observed results. While the workload run showed no errors, it exhibited slightly degraded performance (280 DS/sec versus 320 DS/sec) and increased response time (1.8 sec). These results indicate there is no impact to users other than slight performance degradation, with response time remaining under 2 seconds.

TABLE 15. PRIMARY APPLICATION SERVER INSTANCE NODE FAILURE TEST OBSERVATIONS

Process Stage	Time
General-Purpose Domain	
Failure detection	11 sec
Enqueue Replication Server Recover	20 sec
Primary Application Server Recovery	1 min, 26 sec
Application Servers Recovery	1 min, 35 sec
Database Domain	
Failure detection	1 min, 1 sec
Recovery	19 sec

Availability Test #6a: Loss of Two Servers Running Key SAP Software

This scenario examined the solution's behavior after the loss of the two servers running key SAP software (Figure 18). These two SPARC T4-4 servers ran the SAP Primary Application Server instance, the SAP Central Services (enqueue and message servers) instance, and the enqueue replication server instance. In addition, these servers ran two Oracle RAC instances (Q012, Q014) and four SAP Application Server instances (D52, D54, D56, D58). Both servers were powered off in an ungraceful manner. Impacted application server instances failed over to the two

surviving server nodes, with two instanced failed over per node. The database services on impacted instances failed over to Oracle RAC instance Q011.

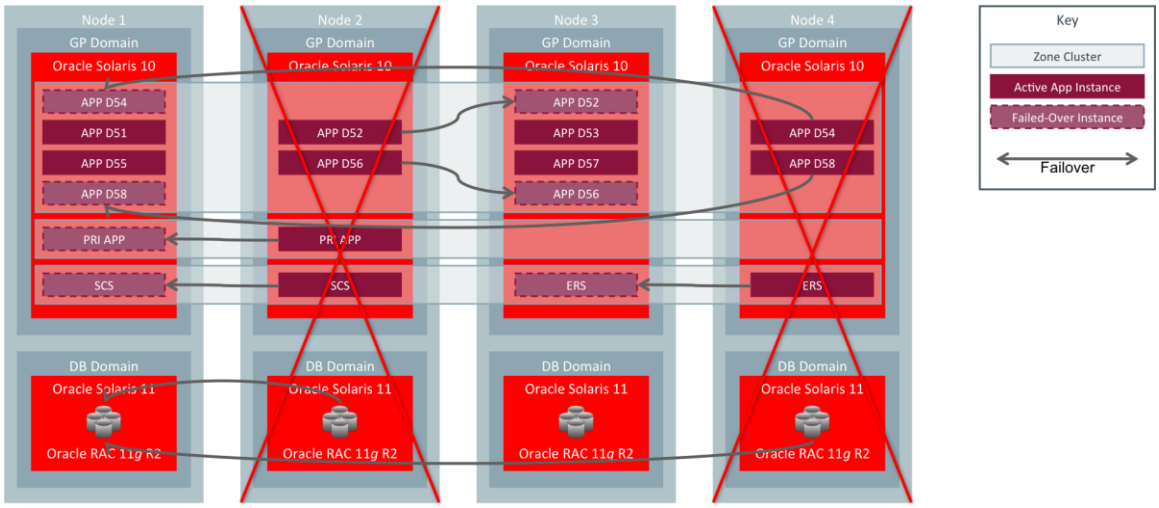

Figure 18. Failure of the server nodes running the SAP Central Service instance and the primary application server instance.

Table 16 lists the results observed. While the post-failure workloads did not indicate an error or warning, severe performance degradation occurred, with response time observed up to 6 seconds. This level of degradation was expected, as four application server instances (twice the initial amount) were running on each surviving node. In addition, each node supported the same user count per instance. CPU utilization in the surviving zone cluster nodes rose to 100 percent.

TABLE 16. PRIMARY APPLICATION SERVER INSTANCE AND CENTRAL SERVICES INSTANCE TWO NODES FAILURE TEST OBSERVATIONS

General-Purpose Domain

Process Stage	**Time**
Failure detection	11 sec
SCS recovery	1 min, 35 sec
Enqueue Replication Server recovery	1 min, 37 sec
Primary Application Server recovery	1 min, 40 sec
Application Servers recovery	1 min, 44 sec
Initial Performance	**Degraded Performance**
320 DS/sec 0.5 sec response time 50 percent CPU utilization (average)	206 DS/sec 6 sec response time 100 percent CPU utilization

Database Domain

Process Stage	Time
Failure detection	60 sec
Recovery	29 sec

Load-based, application-specific failover policies can be implemented to limit the impact of performance degradation on business-critical applications. The next test case uses an identical scenario with the addition of a policy-based failover configuration.

Availability Test #6b: Loss of Two Servers Running Key SAP Software with Policy-based Failover

Flexible load distribution of application services enables administrators to control the impact on critical applications with load-based failover policies. The previous test case (6a) used failover defaults, which distribute the resource group load evenly across all available nodes in the resource group's node list. By treating all applications equally, test 6a created an overload situation that impacted all services equally, regardless of their criticality.

The following test case sought to preserve the performance and user count (workload capacity) for select applications. A policy was configured that assigned a priority and load capacity to application instances. The failover policies were configured as follows:

- Highest priority level (30): application instances D51, D52, and D53
- Medium priority level (20): application instance D54
- Low priority level (10): application instances D55, D56, D57, and D58

Based on the findings from tests 1 and 6a, the policy was configured to limit the number of application server instances per node to a maximum of three. The policies were configured in the application zone cluster (`app-zc`) using the following command sequence.

```
# clnode create-loadlimit -p limitname=cpu_load -p softlimit=24 -p hardlimit=28 +
# clrg set -p load_factors=cpu_load@8 -p priority=30 -p preemption_mode=Never
  D51-rg D52-rg D53-rg
# clrg set -p load_factors=cpu_load@8 -p priority=20 -p preemption_mode=Has_cost D54-rg
# clrg set -p load_factors=cpu_load@8 -p priority=10 -p preemption_mode=Has_cost D55-rg
  D56-rg D57-rg D58-rg
```

After the policies were configured, the fault condition was created. Similar to the previous test (6a), the two SPARC T4-4 servers running the SAP Central Services instances (enqueue and message servers), primary application server instance, and enqueue replication server instance were powered off in an ungraceful manner. These servers (node 2 and node 4) also ran two Oracle RAC instances (Q012, Q014) and four SAP Application Server instances (D52, D54, D56, D58). With this policy-based configuration, only the impacted high and medium priority application server instances (D52 and D54) failed over to the two surviving server nodes (Figure 19). The impacted low priority instances (D56 and D58) were not recovered. In compliance with configured policy, each server node ran no more than three application server instances after the failover.

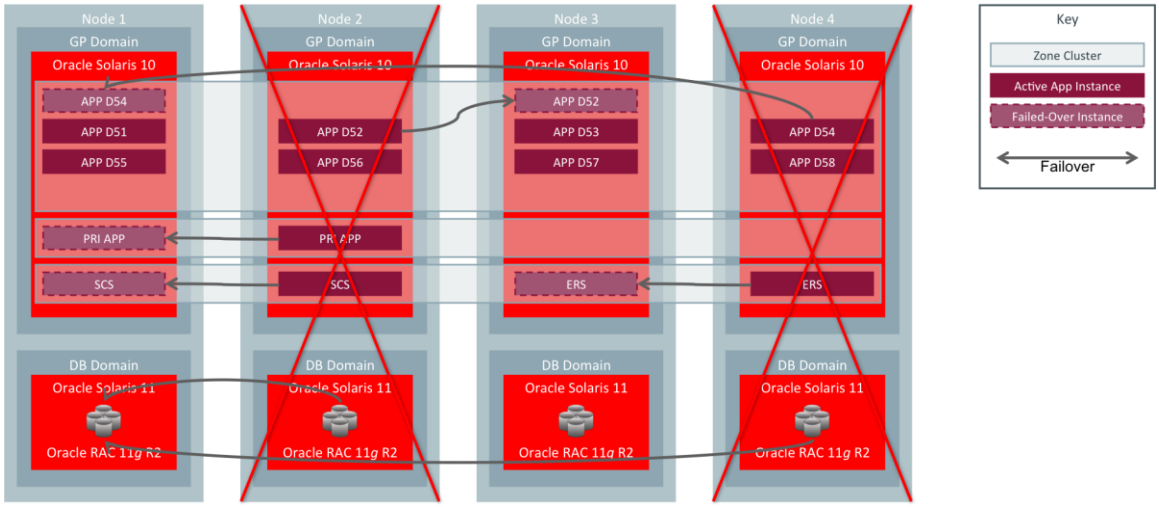

Figure 19. Failure of nodes running the SCS and Primary Application Server instances, using load-based failover policies.

For the post failure workload run, the benchmark parameters were adjusted to maintain the same user counts per available instance on the two surviving server nodes. The D51, D52, D53, D54, D55, D57 instances were set for 400 users, while the Primary Application Server was set for 100 users, for a total of 2,500 users. The run completed without any errors or warnings. The DS response time was 2.6 seconds, as opposed to the 6 seconds observed in test 6a. The database services failover behavior remained the same.

Table 17 lists the test results. The test validated that only the high and medium priority application servers survived, as specified in the load limits set in the failover policies. The impact on surviving services was limited, with a response time of 2.6 seconds.

TABLE 17. TWO NODE FAILURES WITH LOAD-BASED FAILOVER POLICIES TEST OBSERVATIONS

General-Purpose Domain	
Process Stage	**Time**
Failure detection	10 sec
SCS recovery	42 sec
Enqueue Replication Server recovery	40 sec
Primary Application Server recovery	1 min, 38 sec
Application Servers recovery	1 min, 53 sec
Initial Performance	**Degraded Performance**
0.5 sec response time	2.6 sec response time

Database Domain	
Process Stage	**Time**
Failure detection	60 sec
Recovery	28 sec

Availability Test #7: Loss of Three Servers Running Key SAP Software with Policy-based Failover

This test evaluated the behavior of the solution upon the loss of three out of four SPARC T4-4 servers. Oracle engineers observed and validated the failover mechanisms and policies in this extreme, and unlikely, scenario. All three servers (nodes 2, 3, and 4) were shutdown at the same time in an ungraceful manner. Other components were impacted: three Oracle RAC database instances (Q012, Q013, Q014) and six application server instances (D52, D56, D53, D57, D54, D58).

The load-based failover policies used in Test 6b were applied. With the same failover policy in place, only the two impacted high priority dialogue instances (D52, D53) were failed over to node 1. The impacted low and medium priority instances running on nodes 2, 3, and 4 were not recovered. To comply with the three server instances per server policy limit, the low priority application server instance D55 initially running on surviving node 1 was stopped automatically as part of the recovery process. As a result, the surviving server node had three running application server instances (D51, D52, D53).

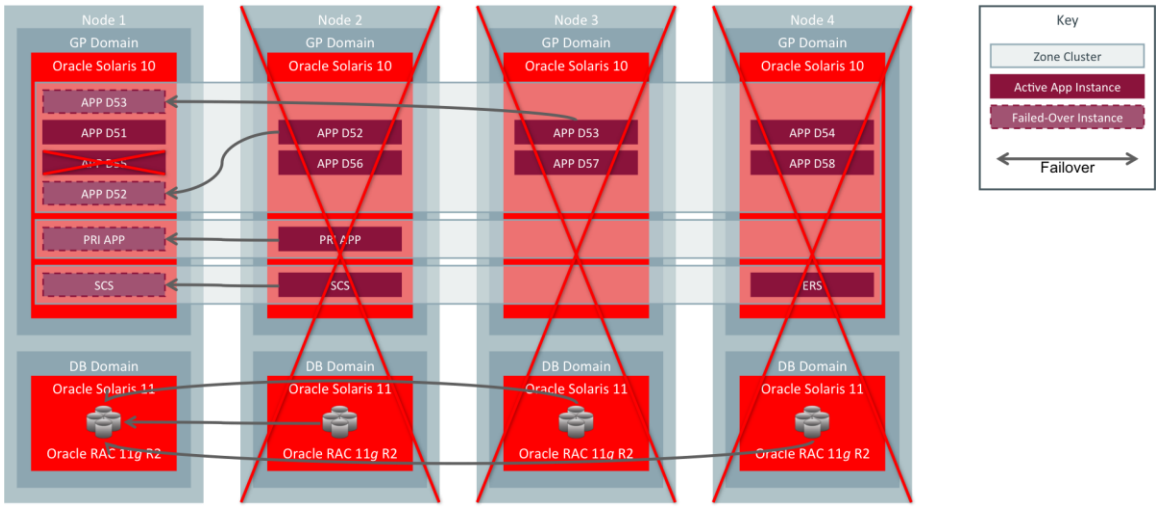

Figure 20. Failure of three nodes running the SCS and Primary Application Server instances using load-based failover policies.

For the post failure workload run, the benchmark parameters were adjusted to maintain the same user counts per available instance on the two surviving server nodes. The D51, D52, D53 instances were set for 400 users, while the Primary Application Server was set for 100 users, for a total of 1,300 users. The run completed without any errors or warnings. The DS response time was 2.6 seconds.

Table 18 lists the test results. The test validated that only the high and medium priority application servers survived, as specified by the failover policies. The impact on surviving services was limited, with a response time of 2.6 seconds.

TABLE 18. LOSS OF THREE NODES WITH LOAD-BASED FAILOVER POLICIES TEST OBSERVATIONS

Process Stage	Time
General-Purpose Domain	
Failure detection	11 sec
SCS recovery	1 min, 53 sec
Enqueue Replication Server recovery	N/A
Primary Application Server recovery	2 min, 23 sec
Application Servers recovery	1 min, 45 sec
Database Domain	
Failure detection	60 sec
Recovery	35 sec

Availability Test 8: Impact of Logical Hosts on Application Server Failover Situations

With this test, Oracle engineers measured the user-level impact of using logical hostnames in failover situations. For the test, two clients (C1 and C2) were connected to an application using the HR1 and HR2 logon groups. Client C1 was connected to logon group HR1, which had redundant server instances using fixed hostnames. Client C2 was connected to logon group HR2, which had redundant server instances using logical hostnames.

During the test, the domain containing the application server instance to which the client was connected was abruptly halted using the `uadmin 1 0` command. The fault caused the operating system instance of the domain to stop immediately, similar to what occurs when the domain operating system encounters a fatal error or the SPARC T4-4 server experiences a power outage.

Table 19 shows the amount of time the clients (C1 and C2) remained unresponsive. Client C1 (an SAP GUI) remained unresponsive for just over nine minutes. Eventually it timed out and closed. At that point, Oracle engineers were able to reconnect to the service using the same logon group—connecting to a different server instance name—and continue transactions. Client C2 (an SAP GUI) was unresponsive for only a few seconds and closed. Oracle engineers were able to reconnect to the service immediately using the same logon group and server name so that transactions could continue. These results show that configuring application servers using logical hostnames rather than fixed hostnames enables clients to reconnect to applications quickly and continue to work in the event of a failure that is covered by failover policies.

TABLE 19. APPLICATION ZONE CLUSTER NODE FAILURE TEST OBSERVATIONS

Process Stage	Time
Client C1 (*fixed hostname instances*)	9 min, 1 sec
Client C2 (*logical hostname instances*)	30 sec

Best Practices for Secure SAP Implementation

SAP systems cannot rely solely on perimeter security. A combination of system-wide security measures and best practices—including rule of least privilege, strong authentication, access control, encryption, auditing, disabling of unnecessary services, anti-malware protections, and configuring system services for enhanced security—should also be implemented for secure operations.

Oracle highly recommends leveraging existing recommendations and guidelines from Product Security Guides, CIS Benchmarks, ISACA publications, or DoD STIGs when designing an SAP environment.

Security Technical Implementation Guides (STIGs)

STIGs are continually updated and currently available for Oracle Integrated Lights Out Manager (Oracle ILOM), Oracle Solaris, Oracle Database, Oracle WebLogic, Oracle ZFS Storage Appliance, InfiniBand and Ethernet switches, and Oracle Exadata Storage Servers. A list of STIGs relevant to this solution is shown in Table 20.

TABLE 20. EXAMPLES OF RELEVANT STIGS

STIG Name	Location
Oracle Solaris	iase.disa.mil/stigs/os/unix-linux/Pages/solaris.aspx
Oracle Database 11*g* Release 2	iasecontent.disa.mil/stigs/zip/Apr2015/U_Oracle_Database_11-2g_V1R3_STIG.zip
Oracle ILOM	iase.disa.mil/stigs/app-security/database/Pages/exadata_lights.aspx
Oracle Exadata Storage Server	iase.disa.mil/stigs/app-security/database/Pages/exadata_storage.aspx
Oracle Sun Data Center InfiniBand Switch 36	iase.disa.mil/stigs/app-security/database/Pages/exadata_infiniband.aspx
Oracle ZFS Storage Appliance	iase.disa.mil/stigs/app-security/database/Pages/exadata_zfs.aspx
Oracle WebLogic Server 12c	iase.disa.mil/stigs/Documents/u_oracle_weblogic_server_12c_v1r1_stig.zip

Component-Level Security Recommendations

Change System Default Passwords

Using known vendor-provided default passwords is a common way cyber criminals gain unauthorized access to infrastructure components. Changing all default passwords to stronger, custom passwords is a mandatory step during infrastructure deployment.

Component Patching

Ensure that all components are using the most recent firmware and software versions to the extent possible. This ensures that each component is protected by the latest security patches and vulnerability fixes.

Leverage Isolated, Purpose-Based Network Interfaces

Network interfaces, virtual or physical, should be used to separate architectural tiers, such as client access and management. In addition, consider using network interfaces to separate tiers within a multi-tier architecture. This enables per-tier security policy monitoring and enforcement mechanisms including network, application, and database firewalls and intrusion detection and prevention systems.

Enable Encrypted Network Communications

Ensure all endpoints use encrypted network-based communications, including secure protocols, algorithms, and key lengths.

For Oracle WebLogic, use the UCrypto provider to ensure that cryptography leverages the hardware assist capabilities of the SPARC platform.

Enable Encrypted Data-at-Rest Protections

Use encrypted `swap`, `/tmp`, and ZFS datasets for any locations that could potentially house sensitive or regulated data. This automatically takes advantage of cryptographic acceleration in Oracle Solaris.

For databases, use Transparent Data Encryption (TDE) to protect tablespaces that may store sensitive or regulated data. This also automatically takes advantage of cryptographic acceleration in Oracle Solaris on SPARC.

Secure the Database

Refer to Oracle Optimized Solution for Oracle Database security best practices and recommendations.

Deploy Application Services in Oracle Solaris Non-Global Zones

Deploying applications within Oracle Solaris non-global zones has several security advantages. These advantages include kernel root kit prevention, prevention of direct memory and device access, and improved control over security configuration (via `zonecfg(1M)`). It also enables higher assurance auditing, because audit data is not stored in the Oracle Solaris non-global zone, but rather in the Oracle Solaris global zone.

Implement a Baseline Auditing Policy

Use audit logs and reports to track user activity—including individual transactions and changes to the system—and to flag events that fall out of normal parameters. These should be implemented at both the Oracle Solaris and database levels. Baseline security audit policy should include login/logout activity, administrative actions, and security actions, as well as specific command executions for Oracle Solaris. This enables auditing of a core set of security critical actions without overburdening the system or database.

Rule of Least Privilege

Increase access control by granting only those privileges that a given individual needs. This should be implemented at both the ERP system level and the infrastructure level.

Strong Authentication

Many intellectual property attacks use stolen credentials. Implementing strong authentication methods, such as Kerberos, RADIUS, and SSL, can help prevent unauthorized access.

Role-Based Access Control

As the number of applications and users increases, user-based identity management can quickly become time consuming and labor intensive for IT staff. Consequentially, many users are granted inappropriate authorities. Though it requires increased efforts during the design and implementation phases, Role-Based Access Control (RBAC) is a popular option for low-maintenance, scalable access control and can help alleviate the burden of identity management.

Table 21 lists Oracle SuperCluster security recommendations. A full list of relevant component security recommendations is shown in Table 22.

TABLE 21. ORACLE SUPERCLUSTER SECURITY RECOMMENDATIONS

Name	Location
Best Practices for Securely Deploying the SPARC SuperCluster T4-4	oracle.com/technetwork/articles/servers-storage-admin/supercluster-security-1723872.html
SPARC SuperCluster T4-4 Platform Security Principles and Capabilities	oracle.com/us/products/servers-storage/servers/sparc-enterprise/supercluster/supercluster-t4-4/ssc-security-pac-1716580.pdf
Oracle SuperCluster T5-8 Security Technical Implementation Guide (STIG) Validation and Best Practices on the Database Servers	oracle.com/technetwork/server-storage/hardware-solutions/stig-sparc-supercluster-1841833.pdf
Secure Database Consolidation Using the Oracle SuperCluster T5-8 Platform	oracle.com/technetwork/server-storage/sun-sparc-enterprise/documentation/o13-053-securedb-osc-t5-8-1990064.pdf

TABLE 22. EXAMPLES OF COMPONENT SECURITY RECOMMENDATIONS

Name	Location
Oracle Solaris 11 Security Guidelines	docs.oracle.com/cd/E36784_01/html/E36837/index.html
Oracle Solaris 11.2 Security Compliance Guide	docs.oracle.com/cd/E36784_01/pdf/E39067.pdf
Secure Deployment of Oracle VM Server for SPARC	oracle.com/technetwork/articles/systems-hardware-architecture/secure-ovm-sparc-deployment-294062.pdf
Oracle Solaris Cluster Security Guide	docs.oracle.com/cd/E39579_01/html/E39649/index.html
User Authentication on the Solaris OS: Part 1	oracle.com/technetwork/server-storage/solaris/user-auth-solaris1-138094.html
Oracle ILOM Security Guide	docs.oracle.com/cd/E37444_01/html/E37451/index.html
Database Advanced Security Administrator's Guide	docs.oracle.com/cd/E11882_01/network.112/e40393/toc.htm
Oracle Database 12c Security and Compliance	oracle.com/technetwork/database/security/security-compliance-wp-12c-1896112.pdf
Best Practices for Deploying Encryption and Managing Its Keys on the Oracle ZFS Storage Appliance	oracle.com/technetwork/server-storage/sun-unified-storage/documentation/encryption-keymgr-1126-2373254.pdf
Securing the Network in Oracle Solaris 11.2	docs.oracle.com/cd/E36784_01/html/E36838/index.html
Securing Users and Processes in Oracle Solaris 11.2	docs.oracle.com/cd/E36784_01/html/E37123/index.html

Securing Systems and Attached Devices in Oracle Solaris 11.2	docs.oracle.com/cd/E36784_01/html/E37121/index.html
Securing Files and Verifying File Integrity in Oracle Solaris 11.2	docs.oracle.com/cd/E36784_01/html/E37122/index.html
Managing Encryption and Certificates in Oracle Solaris 11.2	docs.oracle.com/cd/E36784_01/html/E37124/index.html
Developer's Guide to Oracle Solaris 11 Security	docs.oracle.com/cd/E36784_01/html/E36855/index.html

SAP-Specific Security Recommendations

There are also many security recommendations specific to SAP environments. A list is provided in Table 23.

TABLE 23. EXAMPLES OF SAP SECURITY RECOMMENDATIONS

Name	Location
"Oracle Security Solutions for SAP Environments"	oracle.com/us/solutions/sap/oracle-security-for-sap-2148703.pdf
"Securing Access to Software Owner 'oracle' on Oracle Solaris in SAP Environments"	oracle.com/us/solutions/sap/sudo-security-solaris-sap-wp-2183939.pdf
"Minimal Required Oracle Solaris Packages for SAP Installation with Oracle Database 11*g*"	oracle.com/us/solutions/sap/wp-minimum-required-packages-2311184.pdf
"Oracle Database Security for SAP Applications"	oracle.com/us/products/database/nl20-database-security-396167.pdf
Configuring Secure Network Communications for SAP	docs.oracle.com/cd/E21454_01/pdf/821-2598.pdf
"Oracle Transparent Data Encryption for SAP"	oracle.com/us/solutions/sap/wp-ora4sap-tde11g-303816.pdf
"Oracle Database Vault with SAP"	oracle.com/technetwork/database/security/owp-security-database-vault-sap-133407.pdf
"Setting up Oracle 11*g* Data Guard for SAP Customers"	oracle.com/us/solutions/sap/wp-ora4sap-dataguard11g-303811.pdf

Service Offerings for SAP on Oracle SuperCluster Deployments

Oracle Engineered Systems, such as Oracle SuperCluster, deliver extreme performance through pre-integrated technology that enables rapid time to production. Proper planning, installation, deployment, and support are critical to take full advantage of these Oracle SuperCluster benefits. From strategic architectural design and planning, to on-site installation and configuration and pro-active management services, Oracle pre-sales and service professionals deliver the technical expertise, tools, and best practices to help ensure the smooth and timely deployment of a highly optimized and efficient production SAP implementation.

Oracle SAP Bundle Patches

Oracle works with SAP to release quarterly Patch Set Updates (PSU), as well as SAP-specific Oracle patches that are integration-tested for compatibility, verified, and distributed together as monthly SAP Bundle Patches (SBP). The patches are cumulative. Only the latest SBP must be downloaded and installed. Oracle SBPs can be downloaded

from the SAP Software Distribution Center for Oracle Patches located at service.sap.com/oracle-download. (This site requires a valid SAP Service Marketplace login.)

Joint Customer Support Center

The support center provides a single point of contact for handling customer support calls, escalating issues from or to SAP when needed, and resolving problems. An SAP-aware team of engineers is available through a direct-access hotline and provides assistance for critical service requests (SRs). The Joint Customer Support Center also provides a range of proactive services, including assessments and root cause analysis.

Oracle Solution Centers for SAP

These centers provide presales support, including sizing and IT infrastructure optimization, to help customers discover a proven way to architect SAP deployments on Oracle technology. A simple engagement framework provides access to Oracle's state-of-the-art facilities and Oracle and SAP architects, as well as Oracle Database and hardware support teams. With a global presence and facilities located in Santa Clara (California, US), Walldorf (Germany), and Tokyo (Japan), the Oracle Solution Center team helps IT organizations assess current SAP deployments and achieve optimal results when transitioning to Oracle engineered systems, new Oracle servers, and other Oracle technology.

Staffed with SAP Basis-certified and SAP Migration-certified subject matter experts, the Oracle Solution Center for SAP provides a comprehensive set of services for Oracle engineered systems that range from strategy and capacity planning to SAP architectures, workshops, and proof of concept (POC) deployments.

To learn more about Oracle Solutions Center for SAP, visit oracle.com/osc.

Oracle Support Offerings for Oracle SuperCluster

Oracle offers 24x7 integrated hardware and software support, proactive support tools such as phone home capabilities and automated service requests, and customer incident management to accelerate problem resolution. Additional high availability services are delivered with Oracle Platinum Support for certified Oracle SuperCluster configurations, including remote fault monitoring, patch deployment services, and industry-leading response and restore times, all at no additional cost. Table 24 highlights the services available through Oracle Premier Support and Oracle Platinum Support.

TABLE 24. SUPPORT OFFERINGS FOR ORACLE SUPERCLUSTER

Oracle Premier Support	Oracle Platinum Support

Integrated Support
» *24x7 hardware and software support*
» *Consistent service across the stack from a single vendor*
» *Software and operating system updates*
» *Integrated online support interface (My Oracle Support)*
	Description
	» *Provides the complete support essentials of Oracle Premier Support*
	» *Provides additional high availability services at no additional cost*
	  » *Remote fault monitoring*
	  » *Faster response times*
	  » *Patch deployment services*

Proactive Support Tools » *Automated (phone home) service requests* » *Targeted proactive advice* » *Powerful tools and personalized technical resources* » *Proactive systems management* » *Access to industry experts and peer expertise*	**Remote Fault Monitoring** » *Covered components monitored for faults* » *Monitoring occurs around the clock* » *Single point of accountability for the Oracle stack*

Other Features » *Personalized health checks* » *Advanced knowledge sharing and communities* » *Integrated stack delivery with Oracle Enterprise Manager* » *Converged hardware management with Oracle Enterprise Manager Ops Center* » *Customer Incident Manager (CIM)*	**Industry-Leading Response and Restore Times** » *5-minute fault notification via email* » *15-minute restoration or escalation to development* » *30-minute joint debugging*
Terms » *Assigned for the first 90 days following installation* » *Ensures the best out of Oracle Support for the long term* » *Prioritizes and progresses service requests*	**Risk Mitigation and Business Innovation** » *Remote quarterly updates* » *Patching*

Oracle Advanced Customer Support Services

This extensive range of services is designed to help customers achieve the optimization of SAP on Oracle SuperCluster architectures. Oracle staff members possess deep product knowledge and, together with the Oracle Solution Center for SAP, are used frequently to supply staffing and deliver content for SAP technical events, as well as provide Oracle Database and systems-related SAP Notes. Offering a full range of services—Install and Configuration Diagnostic Review, Installation Service, Configuration Service, SAP-specific Oracle-to-Oracle (O2O) and Oracle-to-Oracle Online (Triple O) Migrations, Production Support Readiness, and a Patch Deployment Service—Oracle Advanced Customer Support can help IT organizations get SAP landscapes up and running on engineered systems quickly.

- **Oracle SuperCluster Start-Up Pack**. This integrated service package ensures optimized planning and deployment of an Oracle SuperCluster system. Oracle systems engineers plan, architect, implement, and project-manage a solution based on each unique environment. Key activities include planning and guidance (assessments and recommendations based on Oracle best practices), installation and configuration, production readiness (technical reviews, project management, and proactive guidance), and a quarterly patch review for one year.
- **Oracle SuperCluster Installation Service**. Highly trained engineers provide comprehensive system installation—using proven, standardized installation methodologies and Oracle best practices and tools—to shorten time to deployment. Key activities include Oracle SuperCluster standard installation; hardware, network, and operating system functionality validation; and development of an installation final summary report.
- **Fixed-scope services**. These services include configuration review and recommendations, performance review and recommendations, and patch review and installation for Oracle SuperCluster systems. Workshops are available to assist IT staff with building their capabilities and confidence in optimizing Oracle Database in SAP environments. The workshops include:
  - Fundamentals of Oracle for SAP ERP (Level I)
  - Oracle Advanced Performance Tuning for SAP ERP (Level II)
  - Oracle Expert for SAP ERP (Level III)
  - Oracle Database 11*g* for SAP Business Suite Technical Skills Workshop
  - Oracle Database Administration for SAP BI (Business/Intelligence)
  - Oracle Real Application Clusters for SAP
  - SAP ERP ABAP Tuning with Oracle Database Platform
- **SAP-aware annual services**. Three standard levels of services are available that focus on overall Oracle SuperCluster system optimization and continued supportability for SAP. An SAP-aware Advanced Service Delivery Manager (ASDM) provides Oracle Advanced Support Assistance. The ASDM ensures the right people and organizations are aligned with meaning action plans for more efficient and effective issue resolution. Oracle Business Critical Assistance provides service request resolution, with proactive advice and assistance tailored to

the customer's operations and projects. The Oracle Solution Support Center provides assistance for critical SRs and a range of proactive services.

» **Customer Oracle and SAP technical engagements**. Additional experience, expertise, and specialized tools are available to help IT organizations support their Oracle and SAP environment. Oracle Advanced Customer Support can establish a statement of work to provide such assistance with varying degrees of involvement. In addition, Oracle Advanced Customer Support engineers have close ties to Oracle Support, Oracle Development, and SAP to ensure the highest level of service.

More detailed information can be found at oracle.com/acs.

Summary

The complexity of SAP landscapes continues to challenge many IT organizations. The complete infrastructure in Oracle Optimized Solution for SAP enables IT staff to simplify the data center by consolidating SAP systems on a pre-tested, ready-to-deploy architecture. By taking advantage of Oracle's integrated solution, IT organizations can put more workloads on a high-performance, highly available system with a very compact data center footprint to achieve significantly better resource utilization. Development, test, and production systems can be isolated from one another, and clustering techniques can be used to ensure SAP applications and databases remain available for users.

Innovative integration and intelligent engineering built into Oracle SuperCluster enable enterprises to take advantage of incremental scalability, accelerate SAP application performance, simplify administration tasks, and reduce day-to-day management demands. Because system integration and testing are handled at the factory, IT managers can rely on the system right out of the box. Plus, the elimination of expensive third-party specialty hardware and security management software reduces the number of software licenses required and lowers overall acquisition costs. These unique characteristics work together to help IT organizations improve overall productivity, lower total cost of ownership, and reduce deployment risk.

For More Information

Additional information and resources can be found in the references listed in Table 25.

TABLE 25. REFERENCES FOR MORE INFORMATION

Relevant SAP Notes
1693680 — Running SAP Software on Oracle SPARC SuperCluster
1669684 — SAP on Oracle Solaris 11
1740958 — Oracle Solaris Cluster 4.0
1738053 — SAPinst with ASM
Key Notes for SAP on Oracle: scn.sap.com/docs/DOC-8664
Key SAP Notes for SAP on Oracle Solaris: scn.sap.com/docs/DOC-23511

Websites

Oracle Database and IT Infrastructure for SAP	oracle.com/sap
Oracle Optimized Solutions	oracle.com/optimizedsolutions
Oracle SuperCluster	oracle.com/supercluster
Oracle's SPARC T-Series Servers	oracle.com/goto/tseries
Oracle Solaris	oracle.com/solaris
Oracle Solaris Cluster	oracle.com/us/products/servers-storage/solaris/cluster/features/index.html
Oracle's Sun ZFS Storage appliance	oracle.com/us/products/servers-storage/storage/unified-storage
SAP on Oracle	scn.sap.com/community/oracle
Oracle and SAP	sap.com/partners/directories/technology/oracle

Newsletters

Oracle for SAP Newsletter	oracle.com/us/solutions/sap/database/sap-tech-update-subscribe-183649.html

Oracle SuperCluster White Papers

A Technical Overview of the Oracle SPARC SuperCluster T4-4	oracle.com/us/products/servers-storage/servers/sparc-enterprise/supercluster-t4-4-arch-wp-1537679.pdf
A Technical Overview of Oracle SuperCluster	oracle.com/technetwork/server-storage/sun-sparc-enterprise/documentation/o13-045-sc-t5-8-arch-1982476.pdf

Oracle Exadata Database Machine White Papers

Moving your SAP Database to Oracle 11*g* R2 ASM: A Best Practices Guide	oracle.com/us/solutions/sap/asm-bestpractices-304655.pdf
Using SAP NetWeaver with the Oracle Exadata Database Machine	oracle.com/us/products/database/sap-exadata-wp-409603.pdf

Oracle Solaris White Papers

Minimizing Planned Downtime of SAP Systems with the Virtualization Technologies in Oracle Solaris 10	oracle.com/us/solutions/sap/database/minimize-planned-downtime-sap-352633.pdf
Oracle Solaris: The Foundation for Successful SAP Solutions	oracle.com/us/solutions/sap/database/oracle-solaris-sap-solutions-1534330.pdf
Oracle Solaris and Oracle SPARC T4 Servers—Engineered Together for Enterprise Cloud Deployments	oracle.com/us/products/servers-storage/solaris/solaris-and-sparc-t4-497273.pdf
Oracle Solaris and Oracle Solaris Cluster: Extending Oracle Solaris for Business Continuity	oracle.com/technetwork/server-storage/solaris-cluster/documentation/solaris-cluster-businesscontinuity-168285.pdf
The Role of Oracle Solaris in Support of SAP Enterprise Applications	oracle.com/us/solutions/sap/database/platform-design-flexibility-352621.pdf

Oracle Database White Papers

Oracle Database: The Database of Choice for Deploying SAP Solutions	oracle.com/us/products/database/039450.pdf
SAP on Oracle Automatic Storage Management 11*g* R2: Configuration Guidelines for UNIX/LINUX	oracle.com/us/solutions/sap/asm-configguidelines-304656.pdf
SAP with Oracle Real Application Clusters 11*g* Release 2 and Oracle Automatic Storage Management 11*g* Release 2	scn.sap.com/docs/DOC-15894

Backup, Recovery, High Availability, and Disaster Recovery White Papers

Oracle Optimized Solution for Oracle Secure Backup	oracle.com/technetwork/articles/systems-hardware-architecture/oo-soln-oracle-sb-350395.pdf
Minimizing Downtime in SAP Environments	oracle.com/us/solutions/sap/database/minimizing-downtime-sap-enviro-352631.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
facebook.com/oracle
twitter.com/oracle
oracle.com

Hardware and Software, Engineered to Work Together