ORACLE

SPARC SUPERCLUSTER

An Oracle Technical White Paper
May 2013

Secure Database Consolidation Using the SPARC SuperCluster T4-4 Platform

ORACLE

Introduction

In this paper, the security capabilities of Oracle SPARC SuperCluster are applied to secure representative, consolidated database architectures. Whether deploying Oracle or third-party database services, SPARC SuperCluster's integrated security capabilities help customers protect their information—at rest, in use, and in transit. In particular, this paper highlights how SPARC SuperCluster enables secure database consolidation using secure isolation, access control, and cryptography, as well as monitoring and auditing controls.

Where appropriate, this paper also offers guidance illustrating how these security goals can be realized using different implementation strategies. This is important so customers can optimize their security architecture against other business requirements such as fault isolation, performance, scalability, and availability. Additional complementary technologies are discussed to reinforce how secure database consolidation architectures can be deployed on SPARC SuperCluster and integrated into a customer's existing IT environment. Finally, a brief discussion of database as a service (DBaaS) security considerations and techniques is provided, shining a light on concerns that are applicable to shared service and cloud computing database architectures.

Product Architecture

SPARC SuperCluster combines the computing power of Oracle's SPARC T4 processor, the efficient virtualization capabilities of Oracle VM Server for SPARC, the performance and scalability of the Oracle Solaris operating system, the optimized database performance of Oracle Database integrated with Oracle Exadata Storage Servers, and the innovative network-attached-storage (NAS) capabilities of Oracle's Sun ZFS Storage Appliance.

Each of these core components is connected over a redundant InfiniBand fabric that enables low-latency and high-performance network communication between all of the components. In addition, a 10-Gb/sec Ethernet network is employed allowing clients to access services running on SPARC SuperCluster. Finally, a 1-Gb/sec Ethernet network provides the conduit through which all of the SPARC SuperCluster components can be managed.

For more information on the SPARC SuperCluster architecture, see the Oracle white paper titled "A Technical Overview of Oracle's SPARC SuperCluster T4-4." Further, for more information on the integrated security capabilities of the platform, see the Oracle white paper titled "SPARC SuperCluster T4-4 Platform Security Principles and Capabilities."

Solution Architecture

Organizations continue to view database consolidation as a way to help reduce infrastructure and operating costs and improve quality of service (QoS) levels, while also improving the speed at which information can be transformed into business value. SPARC SuperCluster is an ideal foundation for consolidating database architectures requiring high performance, reinforced security, and integrated redundancy. The architecture of SPARC SuperCluster enables organizations to simultaneously host a variety of database products, versions, workloads, and environments, each with its own performance, availability, and security requirements.

SPARC SuperCluster supports a variety of full- and half-rack deployment options. Throughout this paper, a half-rack configuration will be used to illustrate representative, consolidated database architectures. While this approach was chosen to help simplify the presentation of this topic, it should be noted that all half-rack and full-rack configurations share the same security capabilities presented here.

The example SPARC SuperCluster configuration, illustrated in the diagram below, includes two SPARC T4-4 nodes from Oracle, each configured with one Database domain running Oracle Database 11*g* Release 2 and one Application domain. This configuration enables organizations to consolidate a variety of Oracle and non-Oracle database products and versions onto SPARC SuperCluster. To simplify the presentation of this content, Oracle Database 11*g* Release 2 will be used on both the Database and Application domains. Similarly, both domains will run the Oracle Solaris 11 operating system. Organizations needing to support other Oracle or third-party database products can leverage Application domains running either the Oracle Solaris 11 or Oracle Solaris 10 operating systems.

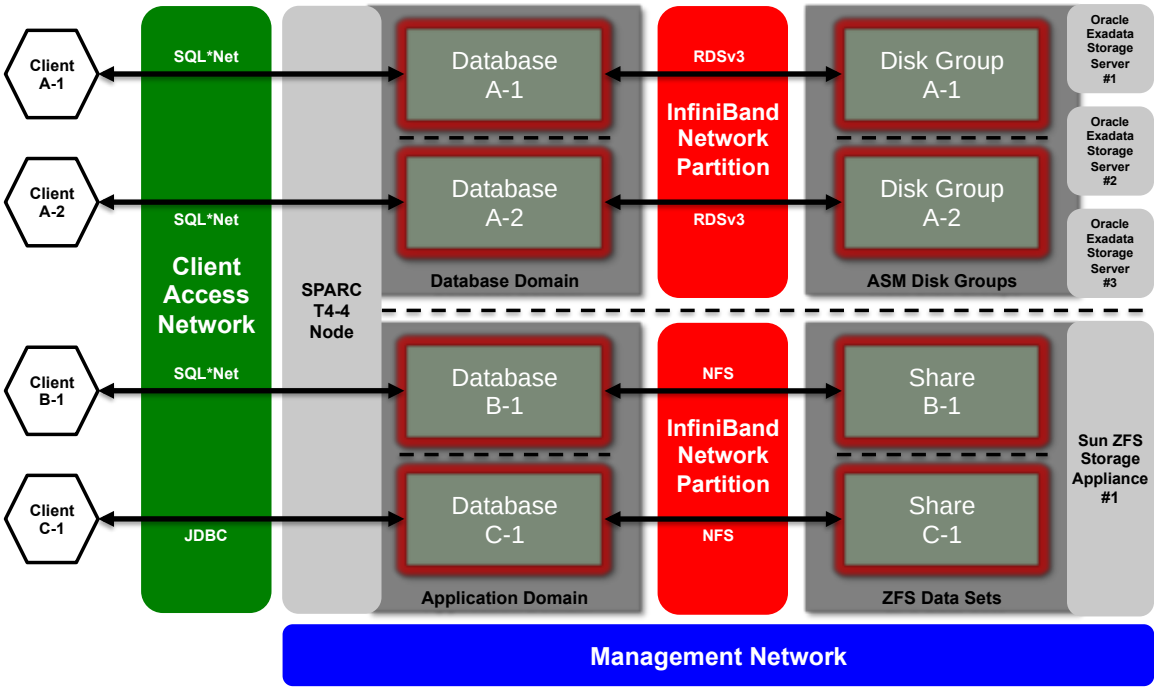

Figure 1. Example SPARC SuperCluster configuration.

In this configuration, Oracle Database 11*g* Release 2 instances running on the Database domains store their information on the integrated Oracle Exadata Storage Servers. Database instances running on the Application domains utilize the Sun ZFS Storage Appliance. While outside of the scope of this document, organizations may also use existing SAN or NAS storage with SPARC SuperCluster.

In the following sections, database consolidation scenarios are discussed from the perspectives of secure isolation, access control, and cryptographic services, as well as monitoring and auditing. The security controls presented can be augmented or adapted based upon an organization's unique policies and requirements.

Secure Isolation

Before consolidating databases, organizations must first understand what requirements exist regarding how individual databases will communicate with and be isolated from their clients as well as other databases or systems. SPARC SuperCluster supports a variety of isolation strategies that organizations can select based upon their security and assurance requirements. This flexibility allows organizations to create a customized, consolidated database architecture that is tailored for their business.

Workload Isolation

SPARC SuperCluster supports a number of workload isolation strategies, each with its own unique set of capabilities. While each implementation strategy can be used independently, they can also be used together in a hybrid approach allowing organizations to deploy architectures that can more effectively balance their security, performance, availability and other needs. To simplify this discussion, several example isolation strategies are discussed below.

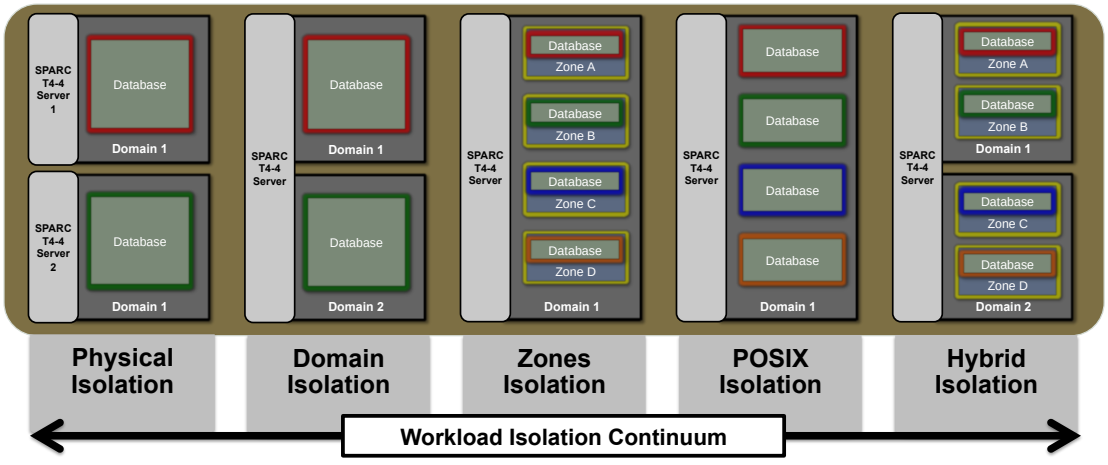

Figure 2. Workload isolation continuum.

Physical Isolation

There are situations in which a database must be physically isolated from other workloads. This can be due to its criticality to the organization, the sensitivity of the information it contains, compliance mandates, or even simply because the database workload will fully utilize the resources of an entire physical system.

SPARC SuperCluster supports physical isolation for both Database and Application domains. Regardless of the domain configuration used, physical isolation is achieved when an organization creates a single domain on a physical system and dedicates all of the resources of that domain to a single database instance. Oracle Solaris Zones, discussed below, can also be leveraged in this scenario to offer even greater security protections. This approach offers organizations the highest level of security isolation by dedicating a physical system to a single workload.

Domain Isolation

For organizations that require hypervisor-mediated isolation, Oracle VM Server for SPARC domains are used to create virtual environments that isolate database instances. Created as part of the SPARC SuperCluster installation, Oracle VM Server for SPARC domains each run their own unique instance of the Oracle Solaris operating system, and access to physical resources is mediated by the hypervisor that is built into the SPARC T4 processors. This ensures that services running in a domain are logically isolated from other domains including their guest operating systems, running services, and data. This approach helps organizations to more efficiency use their resources by allowing multiple workloads to securely share a single physical system.

Zones Isolation

SPARC SuperCluster currently limits the number of Oracle VM Server for SPARC domains to four. Within each of these domains, however, organizations can leverage Oracle Solaris Zones to create additional isolated environments. Using Oracle Solaris Zones, it is possible to deploy individual database instances or groups of database instances into one or more virtualized containers that collectively run on top of a single operating system kernel. This lightweight approach to virtualization is used to create a stronger security boundary around deployed services.

For example, database services running in an Oracle Solaris Zone will not be able to see, manipulate, or adversely impact the processes, memory, or other system resources associated with other databases that might be deployed in other zones on the same system. This security goal is enforced by the Oracle Solaris kernel ensuring that, by default, zones operate with reduced privileges, are not able to access raw memory or devices, are not able to install, load, or unload kernel modules, and much more. For these reasons, the use of Oracle Solaris Zones technology is strongly recommended for service isolation and containment, regardless of other isolation methods used.

Oracle Solaris Zones associated with Application domains can even enforce selective immutability of file system objects, including those associated with the root and `/usr` partitions as well as user-defined spaces, further constraining what changes can be made to a running zone. This enables organizations to maintain stricter control over configuration drift and protect against both accidental and malicious changes to file system objects.

POSIX Isolation

When using a POSIX isolation approach, multiple databases are installed and run on a single operating system. Each database is associated with its own POSIX credentials (that is, a UNIX user and group identifier) that are evaluated by the underlying operating system when making access control decisions. This is necessary to ensure that a database, its processes, and its files are protected from other users and databases that might exist on the same system, domain, or zone.

For example, a process owned by one UNIX user is not able to kill or influence processes of other users. Since most database services do not require extraordinary operating system privileges, the POSIX model of isolation has been widely adopted by organizations seeking to improve server utilization by running multiple databases on a single system.Hybrid Approaches

Organizations consolidating multiple databases onto SPARC SuperCluster can choose to employ a hybrid approach, using a combination of POSIX, Oracle Solaris Zones, and Oracle VM Server for SPARC domain isolation to create flexible yet resilient architectures that align to their needs. By using a combination of these technologies, organizations can limit the number of operating system instances to be managed while at the same time increase database density without sacrificing performance or security.

For example, in the following diagram, a single SPARC T4-4 server has been configured with two domains: a Database domain and an Application domain. The Database domain has been configured with a single Oracle Solaris Zone into which two databases have been provisioned. The Application domain has been configured with two Oracle Solaris Zones, each with a single database instance.

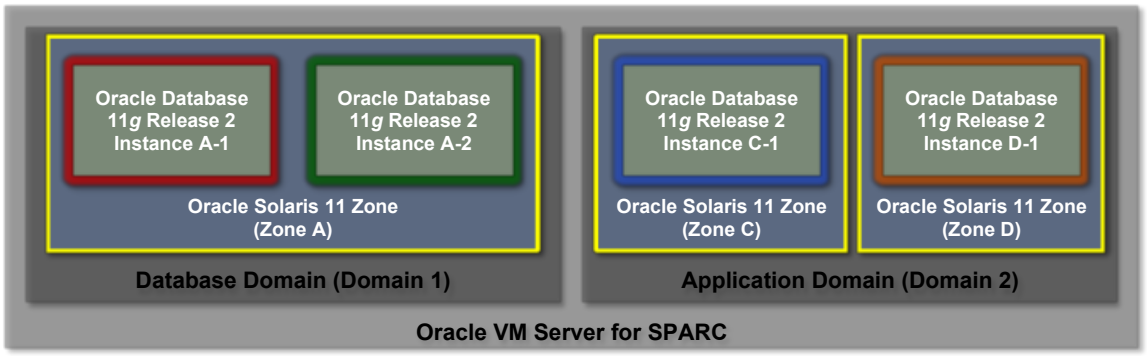

Figure 3. Example hybrid configuration.

As noted above, organizations can deploy a maximum of four Oracle VM Server for SPARC domains (either in Database or Application domains) on SPARC SuperCluster. Additionally, each of these domains supports the use of Oracle Solaris Zones. Multiple database instances can be installed into a domain or zone using POSIX separation allowing SPARC SuperCluster to simultaneously support a variety of database workloads. This allows organizations the flexibility to co-locate or fully isolate databases instances based upon their requirements, security policies, data co-residency and compliance mandates, and other factors.

Network Isolation

While ensuring that individual databases, users, and processes are properly isolated on their host operating systems is a good first step, it is equally important to consider how communications flowing over the network are protected. This section discusses the network isolation capabilities from the perspective of the three primary networks used by SPARC SuperCluster: the client access network, the InfiniBand network, and the management network.

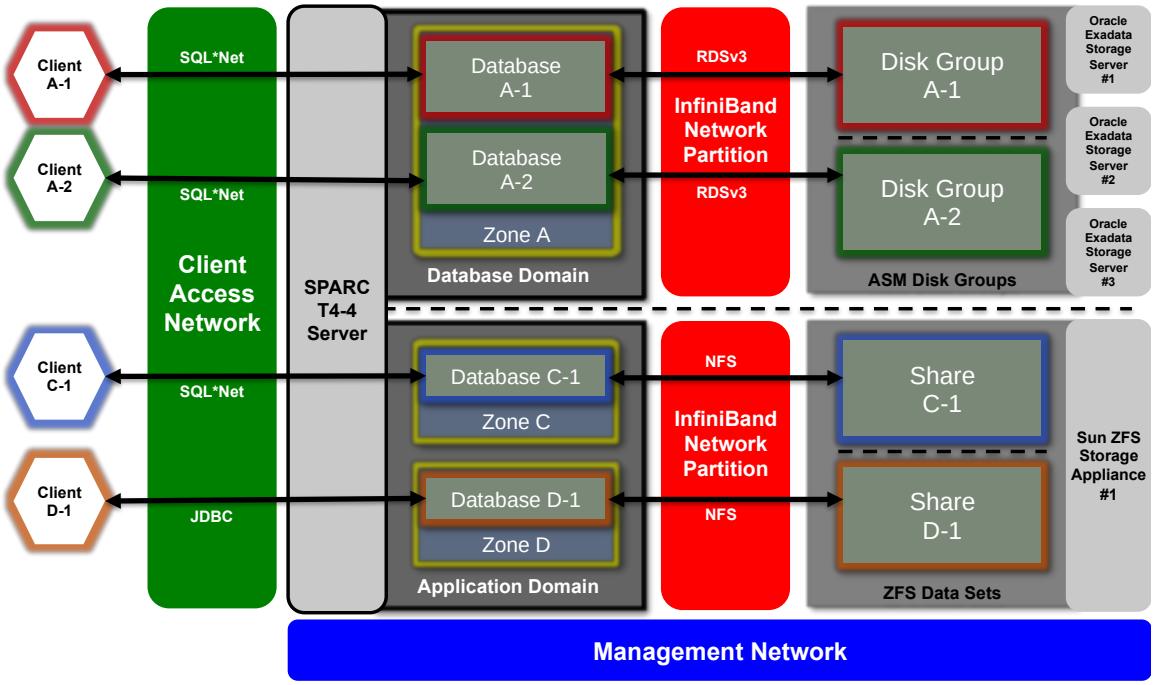

Figure 4. SPARC SuperCluster network isolation configuration.

Client Access Network Isolation

The network traffic flowing over SPARC SuperCluster's client access network can be isolated using a variety of techniques. In the following diagram, one possible configuration is shown in which four database instances are configured to operate on three distinct virtual LANs (VLANs). By configuring the network interfaces of SPARC SuperCluster to use VLANs, network traffic can be isolated between Oracle VM Server for SPARC domains as well as Oracle Solaris Zones. For example, in this configuration, there is no way for the zone attached to VLAN C to see or manipulate traffic flowing over VLANs A or D.

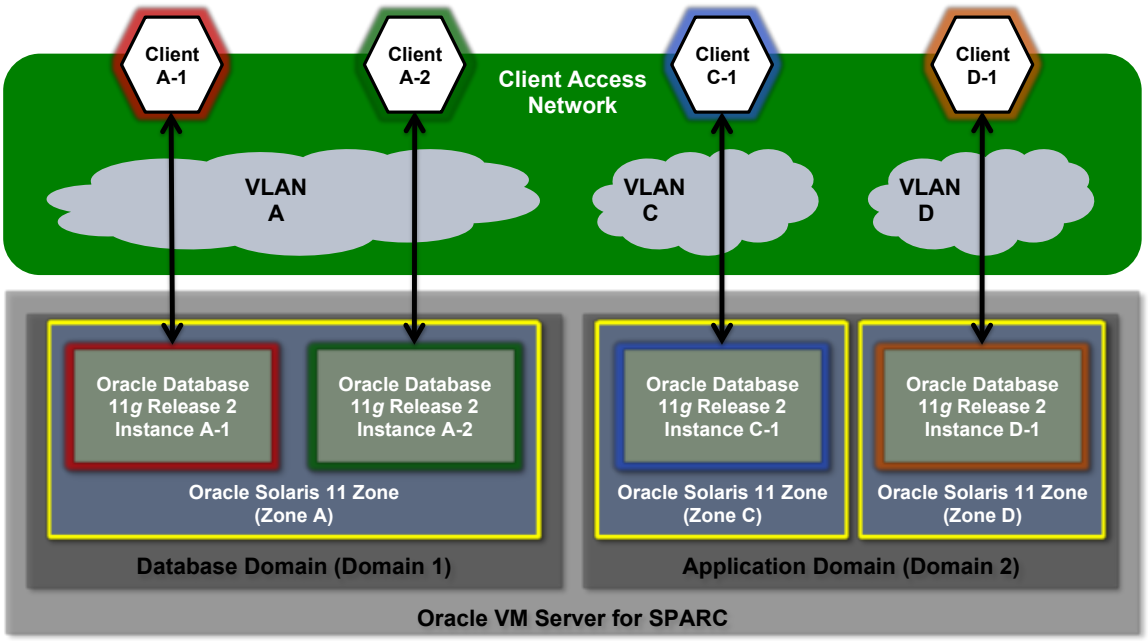

Figure 5. Example configuration: client access network isolation.

While not shown in Figure 5, it is also possible to create and use VLANs within a single Oracle Solaris operating system instance. This would allow database instances A-1 and A-2, for example, to use different VLANs as well. Individual database instances can be assigned to specific IP addresses (and, thereby, to network interfaces and VLANs) to ensure that communication is limited to only those intended.

Additional network access control and cryptographic protections can be employed to provide greater assurance that the network traffic cannot be accessed or decoded by anyone other than its intended recipient. For example, cryptographic isolation using Secure Sockets Layer (SSL)/Transport Layer Security (TLS) is recommended to isolate and protect communications with each of the database instances, regardless of the VLAN that is being used.

InfiniBand Network Isolation

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

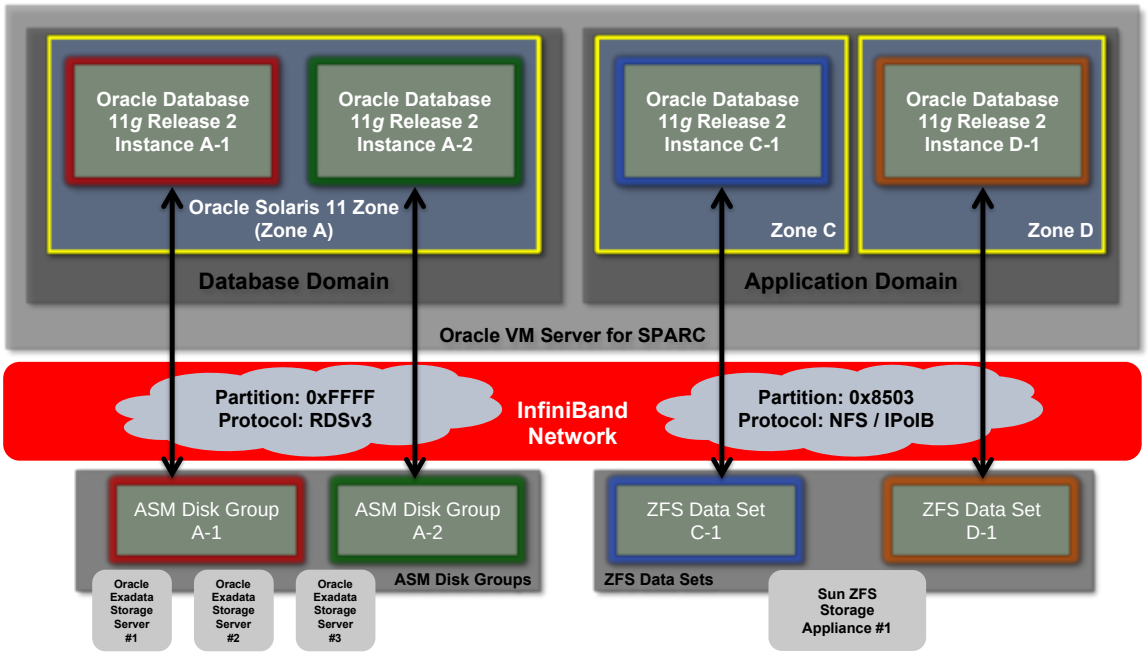

Figure 6. SPARC SuperCluster InfiniBand network isolation.

By default, the SPARC SuperCluster's InfiniBand network is partitioned into six distinct partitions. These partitions are divided to isolate network traffic based upon type, as discussed in Table 1.

TABLE 1. INFINIBAND NETWORK PARTITIONS

IDENTIFIER	DESCRIPTION
0xFFFF	Database domains communicate with the Oracle Exadata Storage Servers using this partition. This partition is also used between Database domains as a private Oracle Real Application Clusters (Oracle RAC) interconnect.
0x8503	Domains communicate with each other as well as with the Sun ZFS Storage Appliance using this partition. By default, all of the domains on SPARC SuperCluster can use this partition.
0x8501 0x8502	Application domains running the Oracle Solaris 10 operating system use these partitions as private cluster interconnects for any Oracle Solaris Cluster nodes that are installed.
0x8511 0x8512	Application domains running the Oracle Solaris 11 operating system use these partitions as a private cluster interconnects for any Oracle Solaris Cluster nodes that are installed.

While these default partitions should not be changed, Oracle does support the creation and use of additional partitions in situations in which further segmentation of the InfiniBand network is required. For example, the following diagram illustrates how to isolate communications between individual domains and the Sun ZFS Storage Appliance. In this diagram, several InfiniBand partitions have been created on the Sun ZFS Storage Appliance and mapped to specific Oracle Solaris 11 zones running database services. This ensures that each Oracle Solaris 11 zone can access only the storage assigned to it. In addition, InfiniBand supports the notion of both limited and full partition membership. Limited members can communicate only with full members, whereas full members can communicate with any nodes on the partition. In Figure 7, the Oracle Solaris 11 zones are limited members of their respective InfiniBand partitions ensuring that they will be able to communicate only with the Sun ZFS Storage Appliance and not with other limited membership nodes that might exist on that same partition.

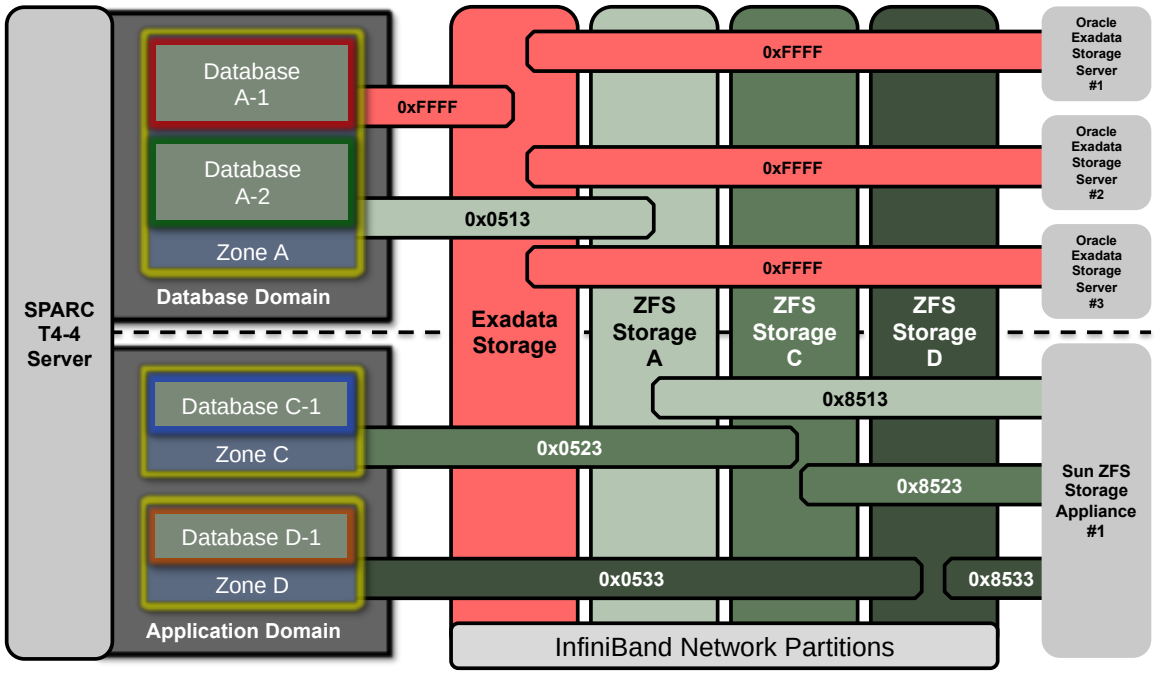

Figure 7. Example showing isolation of communications between domains and the Sun ZFS Storage Appliance.

It should be noted that the use of multiple InfiniBand partitions is not supported for communications with the Oracle Exadata Storage Servers. Communications between domains or zones and the Oracle Exadata Storage Servers must use the default InfiniBand partition, `0xFFFF`.

Management Network Isolation

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

Database Isolation

As discussed above, database instance separation is easily achieved through the use of physical isolation, hypervisor and kernel-based isolation, as well as traditional POSIX permissions. Ultimately, these technologies are used to provide instance-level separation, meaning that each database instance does not share information or interact with other databases running on the platform. For many organizations, this approach is at the heart of their database consolidation plans. SPARC SuperCluster gives organizations the flexibility to implement instance-based isolation in concert with the use of Oracle VM Server for SPARC domains and Oracle Solaris Zones, depending upon their organizational policies and requirements. All of these controls, however, represent just the start of what can be done to promote strong isolation within and between databases running on SPARC SuperCluster.

Database consolidation is not simply about running multiple instances in the same operating system. In fact, database consolidation can be viewed as a continuum that spans a wide array of possibilities—from physical and virtual isolation to shared schema and even row-level isolation within tables. To extend upon the previous workload isolation continuum, the following diagram identifies additional isolation strategies that can be enabled within the database.

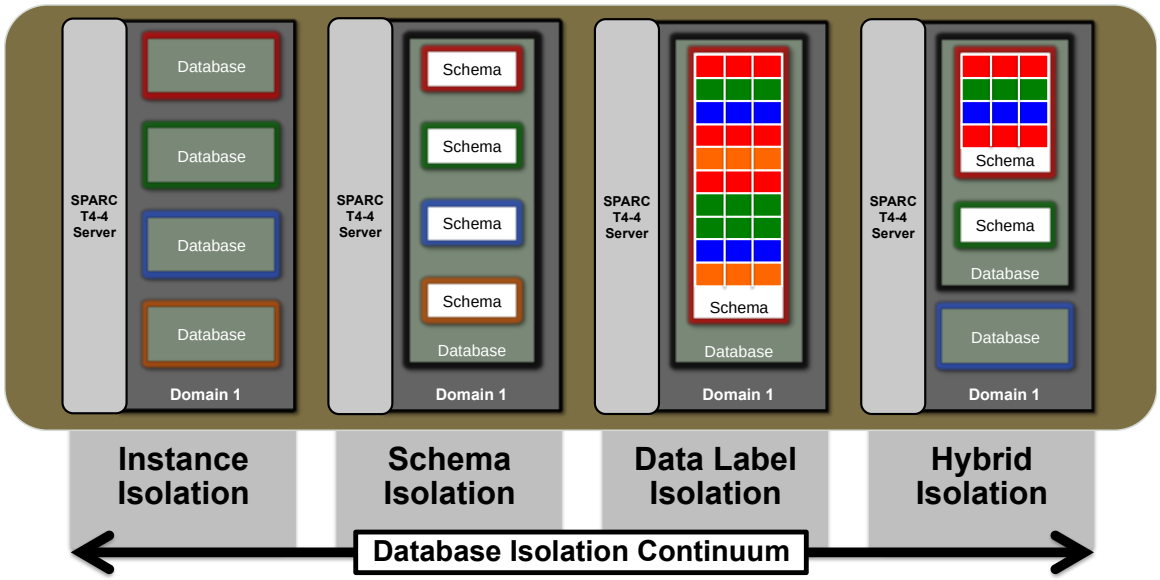

Figure 8. Database isolation strategies.

Instance Isolation

From a technical perspective, multi-instance isolation is essentially the same as the POSIX model of separation already discussed above. POSIX separation requires that database services be operating under unique UNIX user and group identifiers. This ensures that at the operating system level, different users and their processes cannot easily interfere with each other. In the context of database isolation, however, the focus is on who has access to each of the database instances, including both database end users and administrators. Often, databases deployed using this model may serve different purposes or groups, so it is important to limit who has access to each of the databases. That said, it is recommended that organizations consider adopting a POSIX isolation model when employing multi-instance isolation strategies (for example, using Oracle Database instance caging with Oracle RAC).

Schema Isolation

Another approach often used in the context of multitenant database designs is multischema isolation. Rather than storing information in multiple independent databases, this approach relies upon a single, shared database within which users have access to their own distinct tables and tablespaces. By sharing a common database server, organizations can minimize the overhead associated with running and managing multiple, unique database (and possibly operating system) instances. Since most of the security controls that enable this isolation design are based upon controlling access to tables and information, the specifics of these capabilities are covered in the "Database Access Control" section below.

Data Label Isolation

The multischema approach is useful when each user needs access to a different set of tables. There are situations, however, when multiple users or applications need isolated access to a common set of tables. This situation can arise, for example, when supporting multitenant shared application services. In this case, multiple users must be able to access only their own data, despite the fact it resides in a table shared with other users.

Rather than deploy multiple, essentially identical databases, Oracle Label Security can be used to realize isolation on a common, shared services platform. By assigning individual labels, either hierarchical or disjoint, to both users and information, a row-level access control policy can be created and enforced such that users see only their own information. This allows organizations to satisfy their security policies and compliance mandates without having to duplicate their infrastructure or increase their administrative burden. Again, just as with multischema isolation, this approach relies heavily on database access control functionality and is further discussed in the "Database Access Control" section below.

Hybrid Isolation

While each of these database approaches has been presented individually, it is important to underscore that they, too, can be used together and even combined with the workload isolation strategies presented earlier. This allows organizations to balance their security needs against other concerns such as cost, agility, complexity, and operational efficiency.

Ultimately, there is no silver bullet as to which isolation strategy is best. Before selecting any combination of workload and database isolation models, organizations are encouraged to carefully consider their workloads, use cases, and requirements. Regardless of the isolation models chosen, organizations can rely on the architectural flexibility of SPARC SuperCluster to enable cost-effective isolation without sacrificing performance, availability, or scalability.

Storage Isolation

Within SPARC SuperCluster, database content is stored on either the Oracle Exadata Storage Servers or the Sun ZFS Storage Appliance based upon the specific Oracle VM Server for SPARC domain configuration used. This allows for physical isolation of content in situations where that is a requirement. Most organizations, however, will use logical isolation strategies to realize greater performance and utilization of their storage subsystems. In addition to these two storage locations, an organization's existing external NAS or SAN storage can also be used with SPARC SuperCluster. This allows the platform to more easily integrate with an organization's existing storage architecture.

Database Domains

Oracle Automatic Storage Management is used by databases running on SPARC SuperCluster Database domains to access disks residing in the Oracle Exadata Storage Servers. As noted previously, all databases deployed in this manner use the same InfiniBand partition to communicate with each other (when clustered) and to access storage from the Oracle Exadata Storage Servers. Logical isolation can be achieved through the use of multiple Oracle Automatic Storage Management instances (per domain or zone) and by partitioning the Oracle Exadata Storage Servers into multiple disk groups. This allows each database instance to have its own dedicated storage space.

Organizations can employ Oracle Automatic Storage Management security protections to assign disk groups to specific Oracle Automatic Storage Management instances or even to specific databases. In addition, cryptographic isolation can be employed, using the Transparent Data Encryption feature of Oracle Database, to protect database information while it is stored on the Oracle Exadata Storage Servers. Collectively, these controls ensure that databases are able to access and manipulate only the storage that has been assigned to them.

Application Domains

Databases running on one or more of the Application domains will access the Sun ZFS Storage Appliance over the Oracle Direct NFS protocol for their storage needs. Communication with the Sun ZFS Storage Appliance occurs over one or more dedicated InfiniBand partitions. This use of multiple partitions allows database content to be logically isolated while flowing over the network. Database content can be further isolated using individual ZFS data sets that can be assigned to specific IP addresses associated with database instances or clusters. Just as with Database domains, cryptographic isolation can also be employed to protect database information stored on the Sun ZFS Storage Appliance.

It should be noted that the Sun ZFS Storage Appliance is able to share content with both Database and Application domains using industry-standard protocols, such as NFSv4 (for applications and data) and iSCSI (for Oracle Solaris Zones root storage.) This allows the domains to access and use shared NAS storage services across multiple nodes and zones, which can be useful in a variety of cases, such as when a shared Oracle Wallet is needed for a database cluster.

Access Control

For organizations adopting a database consolidation strategy, access control is one of the most critical challenges to be solved. Organizations must have confidence that information stored on the shared infrastructure is protected and available only to authorized individuals, groups, or roles. Authorized individuals and services must further be constrained, in accordance with the principle of least privilege, such that they have only the rights and privileges needed for their role.

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

Workload Access Control

At the virtualization and operating system layers, access control begins with reducing the number of services exposed on the network. This helps to control access to Oracle VM Server for SPARC consoles, domains, and zones. By reducing the number of entry points through which systems can be accessed, the number of access control policies can also be reduced and more easily maintained over the life of the system. Within the Oracle Solaris operating system, access controls are implemented using a combination of POSIX permissions along with the Oracle Solaris role-based access control (RBAC) facility.

POSIX Access Control

As discussed in the "Workload Isolation" section above, POSIX user and group identifiers form the basis for the most primitive access control decisions in the Oracle Solaris operating system. Assigned to each user is a unique user identifier, a primary group identifier and, optionally, additional groups to which the user belongs. Based upon these values, the user is able to perform a variety of process and file management operations. For this reason, it is recommended that databases with different database administrators operate using distinct POSIX credentials. This helps to ensure that databases and their database administrators do not have overlapping permissions to access each other's programs, files, and services.

It should be noted that POSIX permissions are concerned primarily with authorization. That is, they come into focus when a decision needs to be made regarding whether a user is able to access some file or perform some action. Authentication, on the other hand, is focused on validating the identity credentials provided by users when they attempt to access a resource. The Oracle Solaris operating system supports a pluggable architecture that enables organizations to select from a variety of authentication methods including passwords, asymmetric keys, and multifactor tokens. In fact, the Oracle Solaris 11 operating system allows organizations to define per-user authentication policies that can be used to ensure access to administrative accounts is possible only when using two-factor authentication methods.

Role-Based Access Control

In addition to POSIX access control capabilities, the Oracle Solaris operating system also includes a fine-grained, role-based access control facility. Oracle Solaris RBAC is actually a collection of capabilities that enable organizations to group together authorizations, operations, and privileges. Collectively, these rights can be selectively assigned to individuals based upon need to help organizations satisfy their least-privilege requirements. The Oracle Solaris operating system includes a rich collection of default RBAC settings including over 100 rights profiles, 200 authorizations, and 80 privileges that can either be used "as is" or modified as needed to align with organizational policies.

Often, the assignment of these rights is tied to the Oracle Solaris notion of roles. An Oracle Solaris role is similar to a user or administrative account, but it must comply with two very important restrictions. First, it is not possible for a role to directly log in to a system. Users wishing to access a role must first log in to the system as themselves before assuming the role. This helps to ensure proper accountability when multiple users share a role. Next, a role can be successfully assumed only if a user has been authorized to use that role. This added protection ensures that unauthorized users are not able to access a role even if they have the correct password or other authentication credential.

When consolidating databases onto the Oracle Solaris operating system, Oracle Solaris RBAC should be used to segment the rights and privileges of individual database and system administrators. In the following diagram, for example, Oracle Solaris roles are used to group the rights and privileges associated with two different database administrators. Each administrator is able to manage only their own respective databases through a combination of POSIX and role-based access controls. This approach offers organizations a scalable way to manage access because multiple users can be assigned to roles to centralize access management policy while promoting strong accountability and least privilege.

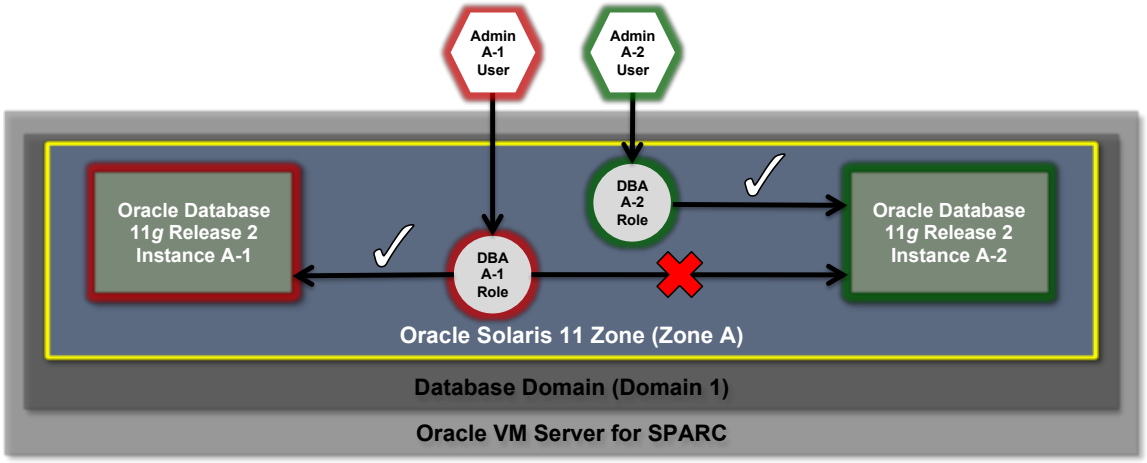

Figure 9. Example of Oracle Solaris RBAC.

In addition, the Oracle Solaris RBAC facility is used to delegate administrative access to the Oracle Solaris operating system, including any deployed zones, and to manage Oracle VM Server for SPARC domains and their underlying configuration. As such, it is strongly recommended that security-critical administrative privileges such as these be strictly limited. Similarly, organizations are encouraged to avoid using the `root` (that is, super-user) account in favor of a more fine-grained approach built upon Oracle Solaris RBAC capability that ensures least privilege and separation of duty and accountability.

Lastly, it is also possible to configure the Oracle Database software owner, usually the `oracle` UNIX account, as an Oracle Solaris role. Often, this is done to prevent direct, remote access to the account, thereby improving overall accountability in the operating system audit trails.

Oracle Integrated Lights Out Manager Access Control

The Oracle Integrated Lights Out Manager (Oracle ILOM) is used to provide out-of-band administrative and management access to various SPARC SuperCluster compute and storage servers. Similar to the Oracle Solaris operating system, Oracle ILOM supports a role-based access control model that allows organizations to determine which users may have administrative, unprivileged, read-only, or other access to this management service. Further, the Oracle ILOM access control model can be used to determine which users may access the device console, control device power, and reset Oracle ILOM itself. Again, it is important that organizations promote accountability by ensuring that all users with Oracle ILOM access have a unique login, password, and role assignment.

Network Access Control

Enforcing access control policies on the operating system is necessary, but it is only a step towards a comprehensive access control strategy. Equally important is being able to protect the databases and related services running on SPARC SuperCluster from network-based attacks. To do this, organizations should first verify that only approved network services are running and listening for incoming network connections. Once the network-attack surface has been minimized, organizations should then configure the remaining services such that they are listening for incoming connections only on approved networks and interfaces. This simple practice will help ensure that management protocols, such as Secure Shell, are not accessible from anywhere other than the management network.

At the database level, database listener services can be configured to support valid-node checking. Using the valid-node checking functionality, the database listener will accept communications only from approved sources. This is a useful feature when there is a known set of clients that is permitted to access database services, as is often the case with consolidated database architectures that are fronted by a collection of application servers. Alternatively, for more-complex requirements, organizations might want to consider using the Oracle Connection Manager and Pooling, a filtering, highly available proxy through which clients can communicate with the actual database listeners.

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

On SPARC SuperCluster, IP Filter can be configured inside an Oracle VM Server for SPARC domain or operated from within an Oracle Solaris Zone. This allows network access control policy to be enforced in the same operating system container in which database services are offered.

For example, each of the Oracle Solaris Zones shown in the diagram below can communicate with the Sun ZFS Storage Appliance using IP over InfiniBand across a shared InfiniBand partition. In a database consolidation scenario, it would be expected that traffic flowing over this partition be limited to domains or zones communicating with the Sun ZFS Storage Appliance, likely over the NFS protocol. Consequently, organizations can easily install a network access control policy that limits the communication accordingly. This simple step will ensure that an individual domain or zone is not able to communicate with others over this shared IP network. Each domain or zone, however, will still be able to initiate communication and use the NFS services of the Sun ZFS Storage Appliance.

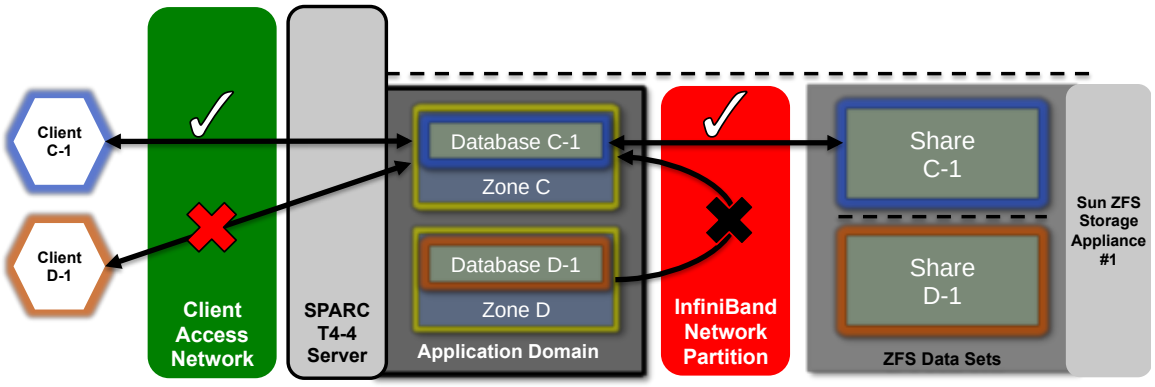

Figure 10. Example network access control policy.

Another important reason why organizations should consider host-based firewall technologies is to limit outbound communication. While this scenario is not often considered, it is important to be able to limit outbound network communications because they can be used as a means of subverting more-traditional inbound filtering practices. In a database consolidation scenario, the amount of outbound network activity will likely be minimal and can easily be categorized so that a policy can be created that limits communications to specific network interfaces and destinations. All other traffic would be denied and logged as part of a "default deny" policy to block unauthorized communications, both inbound and outbound.

Database Access Control

The available system and network access control technologies are considerable, but ultimately it is the database that controls who has access to what information. In consolidated database architectures,

each database is responsible for managing its own security policy. In this way, security policy can be more easily enforced at a point closest to the asset being protected.

For database administrators, SPARC SuperCluster imposes no restrictions on the traditional security controls employed within the database. Organizations can simply employ database access controls as they do today. That said, it is important to reinforce the security capabilities that are available to customers deploying Oracle Database 11*g* Release 2 as part of the layered security model presented in this paper.

User-Based Access Control

At the simplest level, access to Oracle databases is achieved by supplying the correct password associated with a database user or administrator account. This approach is similar to what is used at the operating system level, but it should be noted that usually operating system users and passwords are separate and distinct from those used by the database.

Oracle End User Security allows organizations to integrate their databases with their existing identity management services in order to support Single Sign-On (SSO) and centralized user and role management. Specifically, Oracle End User Security helps by centralizing (1) provisioning and deprovisioning of database users and administrators, (2) password management and self-service password reset, and (3) management of authorizations using global database roles. Also, organizations requiring multifactor authentication methods, such as Kerberos or PKI, can do so using the Oracle Advanced Security option.

After authentication, the database enforces an access control policy that limits what data and tables a user may access and what operations a user may perform. In Oracle Database, users can be assigned both system privileges and object privileges. System privileges allow users to perform database-wide operations such as creating tablespaces, tables, and users. Object-level privileges are those that apply only to specific database objects. For example, using object-level privileges, a user can be granted access to insert or update information in a specific table, but that same user may not be able to delete rows from the table or insert data into a different table. Again, just as least privilege must be applied at the operating system level so, too, should it be applied here. Database users should have only the permissions that are appropriate to their need.

Role-Based Access Control

In addition to user accounts, Oracle Database supports the notion of roles. Similar to Oracle Solaris roles, database roles allow organizations to group together collections of privileges that can then be

assigned to one or more database users, thereby simplifying the management of database access control policy.

By default, Oracle Database ships with a collection of predefined roles associated with performing administrative functions, gathering system statistics, and integrating with Oracle Enterprise Manager. Organizations can also create custom roles with organization-defined privilege assignments. This allows organizations to create roles that are most relevant to their needs.

View-Based Access Control

Another way in which information access can be managed is through the use of Oracle Virtual Private Database functionality. Oracle Virtual Private Database enables organizations to create security policies that control database access at the row and column level. This is accomplished through the transparent, dynamic assignment of `WHERE` clauses to SQL statements issued against tables, views, and synonyms where an Oracle Virtual Private Database policy has been applied. Since these policies are directly assigned to database objects, they are applied whenever those objects are accessed using statements such as `SELECT`, `INSERT`, `UPDATE`, `INDEX`, and `DELETE`.

For example, database users can be restricted to accessing rows or columns that contain only their or their department's information. Similarly, users can be restricted to read-only access when `INSERT`, `UPDATE`, and `DELETE` actions are not authorized. These scenarios highlight how Oracle Virtual Private Database functionality can be useful for isolating users and data, especially when multiple instances of the same database are consolidated into a single instance. In keeping with recommended security practices, by enforcing policy at the point closest to the data, there is no way to bypass this security protection once it has been properly configured.

Label-Based Access Control

In addition to user, role, and view-based access control policies, Oracle Database supports a multilevel security option whereby data classification labels are assigned to application data allowing data of differing classifications to reside in the same table. This is a very useful option when strong data isolation and security are needed in consolidated database architectures. Oracle Label Security enforces access control by comparing data labels with the label or security clearance of the user requesting access. This ensures that users are able to access only the information to which they have been authorized.

Whereas Oracle Virtual Private Databases effectively limits actions through the use of a `WHERE` clause, Oracle Label Security makes decisions based upon a hidden data label column that is attached to existing application tables. Data labels themselves comprise three components: a mandatory

hierarchical level, an optional compartment, and an optional group. Together, these three elements can be used to easily create both disjoint and hierarchical relationships based upon the needs of the organization.

For example, hierarchical levels can be used to define information sensitivity levels such as public, confidential, and restricted. Similarly, compartments and groups can be used to identify individual tenants, business units, or teams. To simplify use and administration, data labels can be automatically assigned to table rows using a labeling function or using the user's current session label. Further, integration with existing identity management systems allows user label information to be centrally managed across an entire organization.

Administrator Access Control

In the context of a database, access control is not limited to application users and data. As noted above, Oracle End User Security can centralize the management of database administrators and global roles. In addition, it is important to be able to specify security policies that govern actions taken by database administrators. In particular, it is important to ensure that database administrators have the necessary privileges to perform their functions while at the same time not being able to access user or application data to which they are not entitled.

Oracle Database Vault enforces multifactor authorization policies that limit who can access databases, data, and applications, as well as when, where, and how the databases, data, and applications can be accessed. Further, Oracle Database Vault supports separation of duty using out-of-the-box policies for security administration, account management, and day-to-day database administration activities. These policies can be customized and supplemented to meet organizational policies for administrative access and separation of duty.

Database administrators often need very powerful privileges to manage the databases under their control. Oracle Database Vault can be used to ensure that those privileges are used only for legitimate administrative tasks and not to access sensitive data. This is a critical component for consolidated database architectures in which database administrators might have no relation to the databases under their management.

Storage Access Control

Regardless of the database architecture, information will ultimately reside on a storage subsystem, so it is imperative that organizations understand how this information will be protected and how access can be controlled.

In SPARC SuperCluster, information may reside on one of two subsystems: the Oracle Exadata Storage Servers or the Sun ZFS Storage Appliance. Both fixed-purpose subsystems are hardened, storage appliances that do not support customization beyond what is exposed by their management interfaces. For example, these devices do not support the installation of third-party software or services. All of their software updates are managed as part of the SPARC SuperCluster update process.

Administrative access to the Oracle Exadata Storage Servers and the Sun ZFS Storage Appliance should be limited to the SPARC SuperCluster management network whenever possible. Similarly, it is important that these devices be accessed only by using secure communication protocols such as Secure Shell.

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

As noted previously, external NAS and SAN storage can also be optionally integrated with SPARC SuperCluster, but security recommendations for those devices fall outside the scope of this document.

Oracle Exadata Storage Servers

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

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

Organizations adopting a database consolidation strategy are also encouraged to consider the following recommendations as they configure their Oracle Exadata Storage Servers:

- All grid disks that belong to the same Oracle Automatic Storage Management disk group should have the same cell-side grid disk security defined to avoid confusion and errors.
- All Oracle RAC servers in an Oracle Automatic Storage Management or database cluster must have the same content, ownership, and security for the Oracle Automatic Storage Management `cellkey.ora` file.
- If database-scoped security is implemented, ensure it is implemented for all databases accessing the grid disks. Do not mix Oracle Automatic Storage Management–scoped security and database-scoped security.

Sun ZFS Storage Appliance

For database services running on Application domains, database content will be stored on the Sun ZFS Storage Appliance because these domains do not have access to the Oracle Exadata Storage Servers. In this scenario, the Sun ZFS Storage Appliance will provide file system, volume, and disk management services similar to what Oracle Automatic Storage Management provides on Database domains.

Whereas Oracle Automatic Storage Management access control is based upon disk groups, the Sun ZFS Storage Appliance supports access control policies based upon data sets and shares. Typically, each database will have its own data set and share so that security and access control policies can be configured specifically for that database. Further, this ensures that domains and zones are able to mount and access only the share containing their specific database content.

Once mounted, access to directories and files on the share are governed by both POSIX access controls as well as extended access control lists. Together, these capabilities can further limit which users have read, write, and execute access for any content on the share as well as control what kinds of delegated administrative operations can be performed, such as creating a snapshot or clone or changing data set properties.

Cryptographic Services

For most organizations, cryptography is at the heart of their data protection strategy. The use of cryptographic services is systemically applied to ensure the confidentiality and integrity of information as it flows across the network and when it resides on disk.

SPARC SuperCluster has been designed to support the high-performance encryption needs of modern IT environments. For consolidated database architectures, where cryptography figures into nearly every aspect of the architecture, SPARC SuperCluster and its supporting software enable organizations to meet their security and compliance objectives without having to sacrifice performance.

Workload Cryptographic Services

The IT security landscape is filled with tradeoffs. For example, while promoting stronger confidentiality and integrity protections, cryptography can be computationally expensive. The more cryptography that needs to be performed, the less compute resources are available to process transactions, perform queries, and deliver results.

SPARC SuperCluster, however, minimizes this performance impact by accelerating cryptographic operations using capabilities designed into its hardware processors. This strategy yields not only improved cryptographic performance, but also improved overall performance, because more time can be dedicated to servicing workloads.

The compute nodes in SPARC SuperCluster utilize the SPARC T4 processor. This processor builds upon earlier SPARC T-Series designs enabling the acceleration of 16 industry-standard cryptographic algorithms. Together, these algorithms support most modern cryptographic needs including encryption, random number generation, and the calculation and verification of digital signatures and message digests. All of these capabilities are made available to databases and services running on the Oracle Solaris operating system to protect information at rest, in transit, and in use. In consolidated database architectures, each database leverages these capabilities to easily support strong cryptographic protections, including defenses against cache-based and timing side-channel attacks, for its communications and data without having to sacrifice performance.

In addition, at the operating system level, cryptographic hardware acceleration is enabled by default for most core services including Secure Shell, IPsec, and ZFS. This allows organizations to leverage improved security and performance not only for their core database services but also for any administrative or support activities that must be completed on those servers, even when they are run inside an Oracle Solaris Zone.

Network Cryptographic Services

Given the importance of privacy and compliance mandates, organizations considering consolidated database architectures should strongly consider the use of cryptography to protect information flowing to and from their databases. This will ensure that data is not exposed to unauthorized parties while it flows over the network.

Oracle Advanced Security supports both Oracle native and SSL/TLS encryption methods to protect information in transit. Further, using individual SSL certificates for each instance or cluster allows organizations to essentially create isolated, cryptographic boundaries that protect data even when it must flow over a shared network or interface.

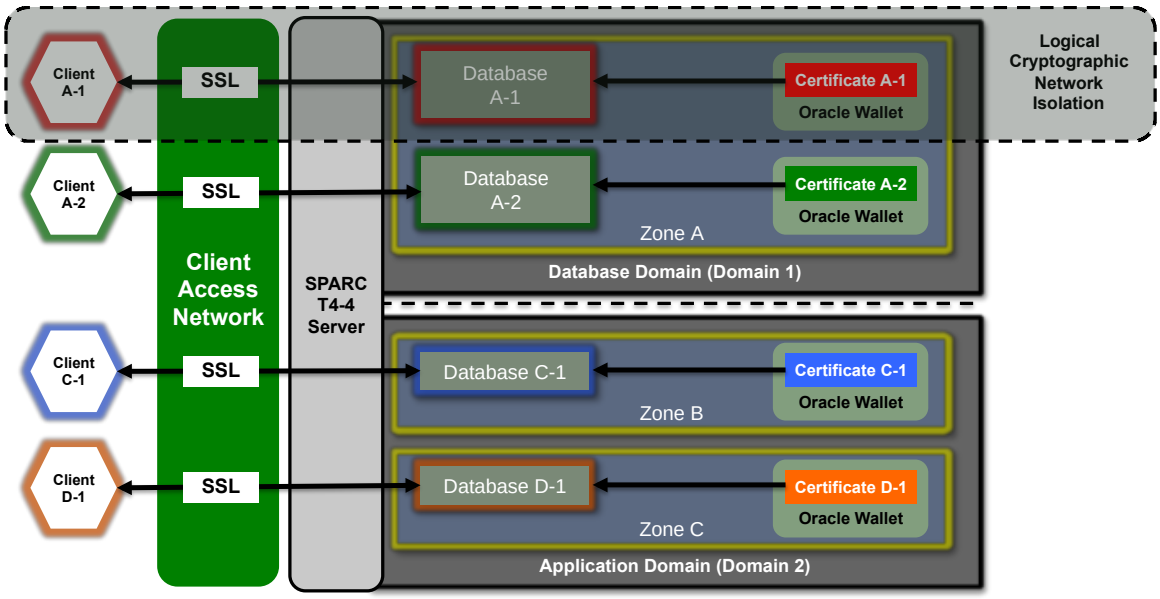

Figure 11. Logical cryptographic network isolation.

It is worth noting that Oracle Advanced Security strong authentication functionality could also be used to ensure that databases and their clients are first able to properly authenticate one another before sharing information.

Client connections to the database are not the only ones that must be protected. For example, organizations are also encouraged to use SSL encryption to protect instance registration in Oracle RAC. In fact, SSL can be used in this scenario to not only protect the confidentiality of communications using encryption, but also to authenticate each endpoint. When integrated with the Oracle End User Security feature, the certificates used for bidirectional authentication can be centrally stored and managed in LDAP.

Further, administrative and support connections to individual Oracle ILOMs, domains, or zones should leverage strong cryptographic protections to avoid accidental disclosure of sensitive information or hijacking of administrative connections. This includes not just interactive sessions but also communications used by management and monitoring tools, backup and recovery solutions, and other similar services.

Database Cryptographic Services

Once information has been received over the network, it is then processed and stored by the database. This information at rest must also be protected to help organizations comply with their security policies and compliance mandates. Oracle Advanced Security, discussed previously, also includes functionality to safeguard information at rest. Specifically, the Transparent Data Encryption capability allows organizations to seamlessly encrypt application data using one of two methods.

- Column-based encryption can be used when encryption should be applied selectively to protect one or more columns within a table. This is most often used when needing to protect personally identifiable information (PII), such as national identification numbers or credit cards.
- Alternatively, tablespace encryption can be used when entire tables or collections of database schema must be protected. Unique column and tablespace keys are used to protect each individual element, and those keys are protected by a single master key that is associated with the database.

Regardless of the approach used, the Transparent Data Encryption feature of Oracle Database helps organizations defend against operating system attacks that might attempt to circumvent the database to gain access to privileged information. This is because any information protected by Transparent Data Encryption is encrypted before being written to disk. Before it can be decrypted, the Oracle Wallet must be unlocked and the master key must be used to decrypt individual table or tablespace keys. Finally, a user must be authenticated and authorized by the database before access to information is granted. This approach is preferred over file system encryption methods that require the content to be accessible at the operating system layer before it can be used by the database.

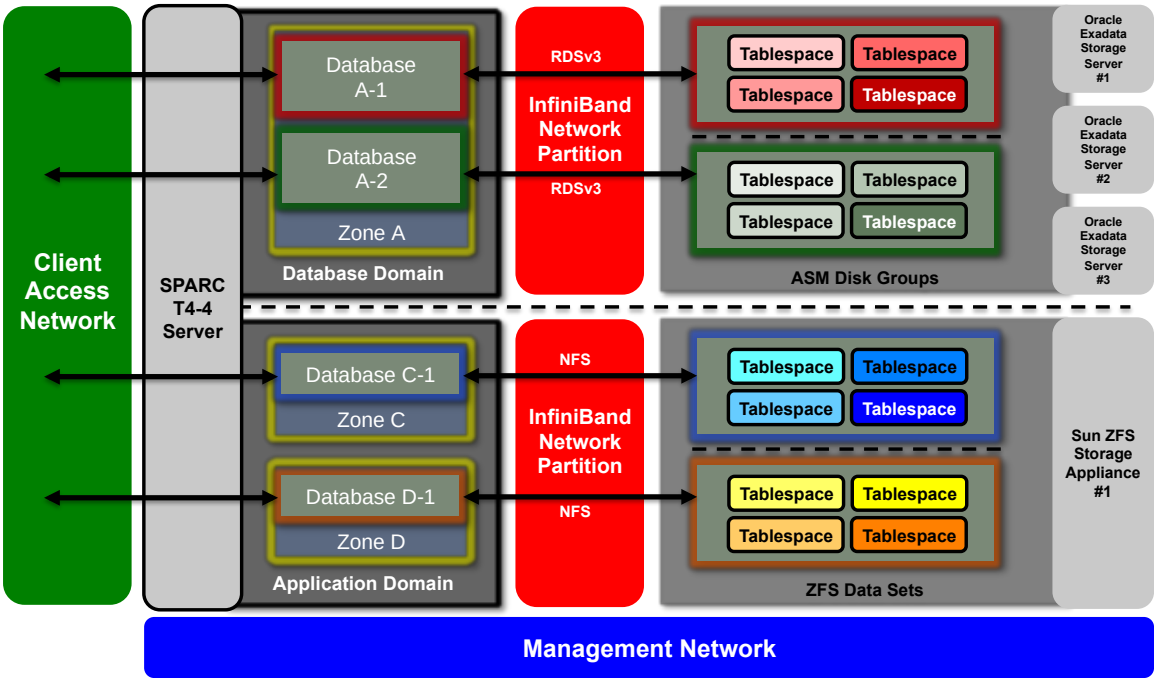

Figure 12. Database cryptographic services.

For versions 11.2.0.3 and newer, Oracle Database automatically identifies the Oracle Solaris operating system and the SPARC T4 processors used by SPARC SuperCluster. When the Oracle Advanced Security Option is licensed, this enables the database to automatically use the hardware cryptographic acceleration capabilities of the platform for tablespace encryption without the need for additional end-user configuration.

Storage Cryptographic Services

As previously noted, the storage subsystems used by SPARC SuperCluster include both Oracle Exadata Storage Servers and the Sun ZFS Storage Appliance. In the context of cryptography, the Sun ZFS Storage Appliance does not currently perform encryption. This is not an issue for database consolidation, because it is expected that organizations will opt for the database-level encryption capabilities of the Oracle Advanced Security option mentioned above. This ensures that any data written to the Sun ZFS Storage Appliance shares is already encrypted by the database and, therefore, no further action is needed by the storage subsystem.

For Oracle Exadata Storage Servers, however, the situation is slightly different, because the Oracle Exadata Storage Servers have the ability to decrypt information before it is passed back to the database servers. This is a useful capability when combined with Exadata Smart Scan, enabling queries to be executed on the storage nodes, thereby reducing the amount of data that must be sent back to the database servers.

To further improve the performance of these operations, the Oracle Exadata Storage Servers are configured by default to use the cryptographic acceleration capabilities of their Intel Xeon processors. As a result, decryption performance is significantly increased, thereby minimizing the performance burden typically associated with the use of cryptography.

It should be noted that decrypting information on the Oracle Exadata Storage Servers is optional and can be disabled. When disabled, the database nodes themselves will encrypt and decrypt application data. Organizations should carefully consider the security and performance tradeoffs before making a decision. Disabling decryption at the Oracle Exadata Storage Server level means that organizations will not be able to leverage Exadata Smart Scan on their encrypted tables. As a result, larger amounts of information might need to be returned to and processed by database servers, thereby impacting their performance and throughput.

Key Management Services

Any discussion of cryptography would be incomplete without also discussing how encryption keys are managed. Generating and managing encryption keys, especially for large collections of services, has traditionally been a major challenge for organizations. Transparent Data Encryption functionality simplifies this problem through the use of a two-tier encryption key architecture that is managed using a built-in key management system.

First, a single master key is created per database instance that is used to encrypt database backups, exports, and redo logs. This master key is also used to protect individual data encryption keys that are used for tablespace and column encryption.

Before encrypted tablespaces or tables with encrypted columns can be accessed, the master key must be obtained. This is typically accomplished by providing a passphrase to unlock the database's external key store, called the Oracle Wallet. Alternatively, the master key can be stored in a hardware security module or an external PKCS#11-compliant key management service, such as Oracle Key Manager. Once the Oracle Wallet has been unlocked, the individual data encryption keys are decrypted using the master key and can then be used by the database.

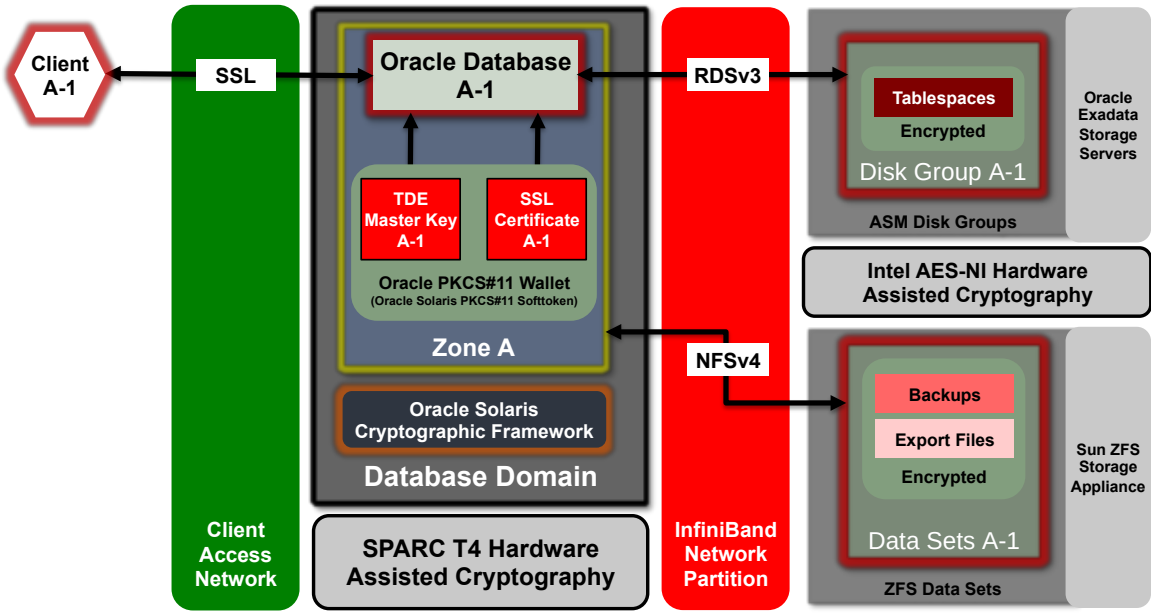

Figure 13. Example of key management services.

On SPARC SuperCluster, Transparent Data Encryption can also leverage an Oracle Solaris PKCS#11 wallet to securely protect the master key. Using the Oracle Solaris PKCS#11 wallet automatically engages the SPARC T4 hardware-assisted cryptographic acceleration for any master key operations. This allows SPARC SuperCluster to significantly improve the performance of encryption and decryption operations associated with database backups (using Oracle Recovery Manager), exports (using the Data Pump feature of Oracle Database), and redo logs (using Oracle Data Guard).

When using a single database instance, there is a one-to-one relationship between that instance and the master key used by Transparent Data Encryption. When using Oracle RAC, however, to support availability and performance objectives, it is necessary to either copy or share the Oracle Wallet so that each database instance in a cluster has access to the same master key. Organizations using a shared-wallet approach can leverage the Sun ZFS Storage Appliance to create a directory that can be shared across all the nodes in a cluster. Using a shared, centralized key store can help organizations better manage, maintain, and rotate the keys in clustered database architectures, because the keys will be synchronized across each of the nodes in the cluster.

Monitoring and Auditing

With the potential for so many individual databases, end users, and administrators operating within consolidated database architectures, it is essential that proper activity monitoring and auditing be implemented. Actions, whether accidental or intentional, must be able to be attributed and records must be kept for troubleshooting, compliance reporting, and incident response.

SPARC SuperCluster supports the ability to monitor actions taken by users and administrators as well as activity detected by system services. More importantly, the comprehensive monitoring capabilities of SPARC SuperCluster enable organizations to obtain monitoring and audit information at the workload, network, database, and storage layers, which helps to ensure that activity can be detected no matter where it happens.

Workload Monitoring and Auditing

Actions taken by users and services on the Oracle Solaris operating system are recorded by the Oracle Solaris audit facility. Enabled by default in the Oracle Solaris 11 operating system, the Oracle Solaris audit facility enables the creation of flexible policies that can track system, administrator, and end-user activity. For example, the Oracle Solaris audit facility can record system boot and shutdown requests, system console and network logins, attempts to perform privileged activities, and even more-granular system level functions such as those related to process and file creation or deletion.

The Oracle Solaris audit facility can be configured at a system or per-user level, allowing organizations to set system-level policies that best reflect their requirements. Organizations can choose to record all actions regardless of the outcome or only those that succeed or fail. This helps organizations to maintain tighter control over the creation of audit records, thereby simplifying the task of analysis and reporting.

Finally, the Oracle Solaris audit facility includes metadata for each record produced, including the real and effective user and group identifier of the actor, the action attempted and whether it was successful, the date and time of the event, and a wealth of other information. Configured well, the Oracle Solaris audit facility is a critical capability for organizations attempting to develop a baseline for normal typical system activity, detect unauthorized activity or attempts to circumvent security controls, and collect evidence in support of audit or incident response requirements. Because Oracle VM Server for SPARC services and Oracle Solaris Zones each run on the Oracle Solaris operating system, events associated with domain and zone configuration, management, and usage are also audited by this facility.

As organizations consider their database consolidation strategy, how and where auditing is used should be carefully considered. For example, in situations in which a common, centralized audit trail is needed, the Oracle Solaris audit facility can be configured to record all system activity, including actions taken in any non-global zones, and store the information centrally in the global zone. This can be useful when security monitoring of a system is managed by a single organization and a single policy is enforced.

There are situations, however, when it might be necessary for each non-global zone to record and store its own events. In consolidated architectures, this situation can arise when individual business units or tenants are responsible for the security monitoring of their own databases. In this scenario, each non-global zone could potentially have a unique policy that drives which events are recorded within each non-global zone.

In addition to system activity auditing, the Oracle Solaris operating system also includes a variety of other tools to help organizations monitor and evaluate the security of their systems. For example, the packaging systems of the Oracle Solaris 10 and Oracle Solaris 11 operating systems support the ability to perform individual and complete package checks on a system to identify when files and directories have been changed from the versions delivered by Oracle.

At the file system level, the Oracle Solaris Basic Audit Reporting Tool enables organizations to detect changes to files, directories, and other file system objects using a flexible policy that can be used across an entire system or just for security-critical files. Again, just as with Oracle Solaris auditing, both the packaging tools and the Oracle Solaris Basic Auditing and Reporting Tool can be used within individual non-global zones or across an entire Oracle VM Server for SPARC domain. As a result, organizations are able to use these capabilities regardless of the actual database consolidation architecture that is deployed.

It is important to reinforce that access to Oracle ILOM functionality can also be audited. Each Oracle ILOM generates its own set of records for all logins, administrative actions, and configuration changes. Just as with Oracle Solaris auditing, all records include timestamps and information about who performed a given action.

Network Monitoring and Auditing

For Oracle VM Server for SPARC domains and Oracle Solaris Zones, the Oracle Solaris audit facility includes information related to network communications. For example, the audit facility can record information related to incoming and outgoing network connections, including when services listen for and accept new connections for system or database services. By centralizing this information within the Oracle Solaris audit facility; this information can be more readily correlated with other system activities to develop a more complete picture of a situation.

In addition, the IP Filter capability of Oracle Solaris can selectively record both inbound and outbound network communications. Each record generated by IP Filter includes a timestamp and the source and destination address and port, as well as whether the communication attempt was permitted or denied by the host-based firewall. For security-critical services, even the logging of permitted requests might be needed to meet security and compliance mandates. As noted previously, IP Filter can be used at both the domain and non-global zone levels so that organizations can segment both their network policies and activity records based upon their deployment scenario.

Database Monitoring and Auditing

Oracle Database includes a native, fine-grained auditing that enables organizations to set auditing policies at the database object level. This is a critical capability allowing organizations to specify policies that can identify potential issues while minimizing the amount of audit data generated.

For example, the Oracle Database fine-grained auditing capability can be configured to generate a record when a specific table is accessed outside of normal business hours, a database connection is received from an unexpected source, a specific column within a table is accessed or updated, or even when a specific value within a column is used. Such levels of fine-grained control over the generation of audit records mean that organizations will not have to sift through a mountain of data to find those few important records. Further, this also means that organizations can minimize the performance impact of auditing by focusing on those activities deemed suspicious or out of the ordinary.

In consolidated database architectures, Oracle Audit Vault and Database Firewall can be used to securely aggregate and analyze audit information from a variety of Oracle and non-Oracle databases as well as audit information from operating systems such as Oracle Solaris. Just as SPARC SuperCluster can support secure consolidation of database services, Oracle Audit Vault and Database Firewall provides the secure consolidation, monitoring, and reporting of audit records, generated from both single-instance or clustered databases.

Once the database audit records have been consolidated onto the Oracle Audit Vault and Database Firewall platform, they are removed from the source databases to better simplify audit record administration and protect the records from tampering. Centralizing audit records from a consolidated database environment provides more complete visibility into user actions that have occurred across multiple databases.

To facilitate audit and compliance reporting, Oracle Audit Vault and Database Firewall also includes dozens of predefined reports that can be used to closely monitor and analyze database activity. Further, Oracle Audit Vault and Database Firewall enables organizations to access its warehouse of audit information using tools such as Oracle Business Intelligence Publisher to create customized reports. Lastly, organizations can also leverage proactive event notification to ensure that sensitive or suspicious activities are quickly identified and escalated.

Beyond activity monitoring, Oracle Database also supports the ability to identify and track configuration changes at the database level. The Oracle Database Lifecycle Management pack integrates with an organization's existing Oracle Enterprise Manager environment and is used to detect, validate, and report on changes to database configurations. The Oracle Database Lifecycle Management pack includes over 250 built-in policy checks and allows organizations to define and customize their own policies. Compliance dashboards are available showing how individual databases comply with the defined policies. Further, notification rules can be implemented, alerting organizations when violations occur. Optionally, corrective actions can be defined and executed whenever a violation is detected.

Storage Monitoring and Auditing

The storage subsystems used by SPARC SuperCluster are hardened appliances. As such, the types of actions that can be taken are severely restricted based upon the role of the user who accesses the device. It is important, therefore, that organizations correctly map users to those administrative roles that best support their function.

That said, the Oracle Exadata Storage Servers and the Sun ZFS Storage Appliance support login, hardware, and configuration auditing. This enables organizations to determine who accessed a device and what actions were taken. While not directly exposed to the end user, Oracle Solaris auditing provides the underlying content for information presented by the Sun ZFS Storage Appliance. Similarly, the Oracle Exadata Storage Servers audit a rich collection of system events that can be used along with hardware and configuration alert information provided by the Exadata Storage Server Software.

Complementary Services

Organizations consolidating database services onto SPARC SuperCluster have an exceptional foundation of security capabilities upon which they can customize and optimize based upon their unique requirements. That said, it is important to understand that SPARC SuperCluster is not a standalone entity. Often, organizations will integrate such platforms with existing, shared security services to more fully comply with their enterprise security requirements. To illustrate this point, this section will introduce three Oracle technologies that can directly support the security needs of consolidated database environments, specifically, Oracle Audit Vault and Database Firewall, Oracle Key Manager, and Privileged Account Manager, which is a feature of Oracle Identity Governance Suite.

Oracle Audit Vault and Database Firewall

While Oracle Database provides a wealth of capabilities to control access to information, there are times when additional support is needed. Oracle Audit Vault and Database Firewall provides the first line of defense for databases helping to protect account misuse, attempted application bypass, and even SQL injection attacks. Its highly accurate SQL grammar-based technology blocks unauthorized transactions, helping to prevent internal and external attacks from ever reaching the database.

Organizations using Oracle Audit Vault and Database Firewall to protect databases operating on SPARC SuperCluster should deploy the software and its management services on separate, physical servers. For example, Oracle's Sun Server X3-2 platforms are ideally suited to support the specific requirements of Oracle Audit Vault and Database Firewall and its management server. Deploying Oracle Audit Vault and Database Firewall in this manner allows organizations to more easily isolate the enforcement and management functions, similar to how other services are deployed on SPARC SuperCluster.

Depending upon an organization's security requirements, Oracle Audit Vault and Database Firewall can operate in one of two modes:

- In Database Activity Monitoring mode, the system can detect and log unusual activity as well as produce warnings and alerts. This can be considered a read-only mode since Oracle Audit Vault and Database Firewall does not actively prevent transactions from completing.
- Organizations seeking a more proactive response to policy violations can use the Database Policy Enforcement mode. In this mode, Oracle Audit Vault and Database Firewall is able to not only detect potential policy violations but also block SQL transactions using a combination of white list, black list, and exception list policies.

In addition, Oracle Audit Vault and Database Firewall can be installed using one of three different deployment architectures: inline blocking and monitoring, active monitoring, and agent-based remote monitoring. The architecture selected impacts whether Oracle Audit Vault and Database Firewall will enforce policy or simply monitor database activity.

Inline Blocking and Monitoring

When used in its Database Policy Enforcement mode, Oracle Audit Vault and Database Firewall must be deployed in between the assets being protected and their respective clients. For databases running on SPARC SuperCluster, this means that Oracle Audit Vault and Database Firewall must be deployed with one interface on a network external to SPARC SuperCluster and another on the platform's client access network.

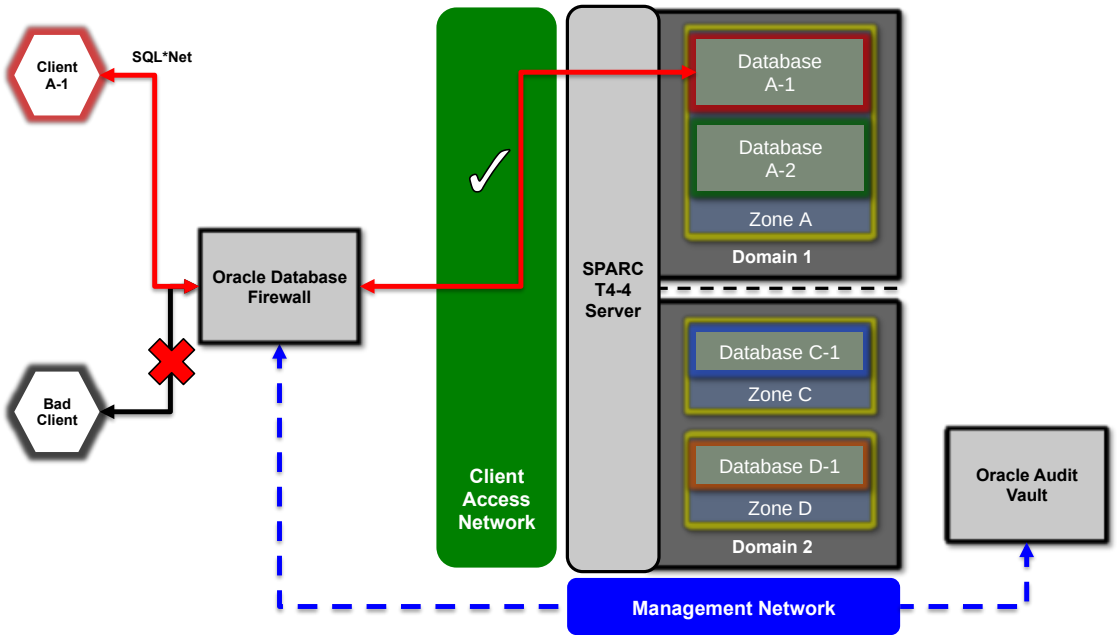

Figure 14. Inline blocking and monitoring architecture.

This architecture allows Oracle Audit Vault and Database Firewall to inspect all incoming connections, evaluate SQL statements using its grammar analysis engine, and make policy-based decisions about how traffic should be handled. When malicious or unapproved SQL statements are detected, Oracle Audit Vault and Database Firewall can either drop the offending statements or substitute them. In addition, Oracle Audit Vault and Database Firewall will trigger an alert ensuring that administrators are aware of the policy violation.

Active Monitoring

When active blocking or substitution of SQL statements is not needed, organizations can deploy Oracle Audit Vault and Database Firewall in an active monitoring configuration. In this scenario, Oracle Audit Vault and Database Firewall is configured to leverage the port-mirroring capabilities of an Ethernet switch, such as Oracle's Sun Network 10 GbE Switch 72p, connected to the SPARC SuperCluster's client access network.

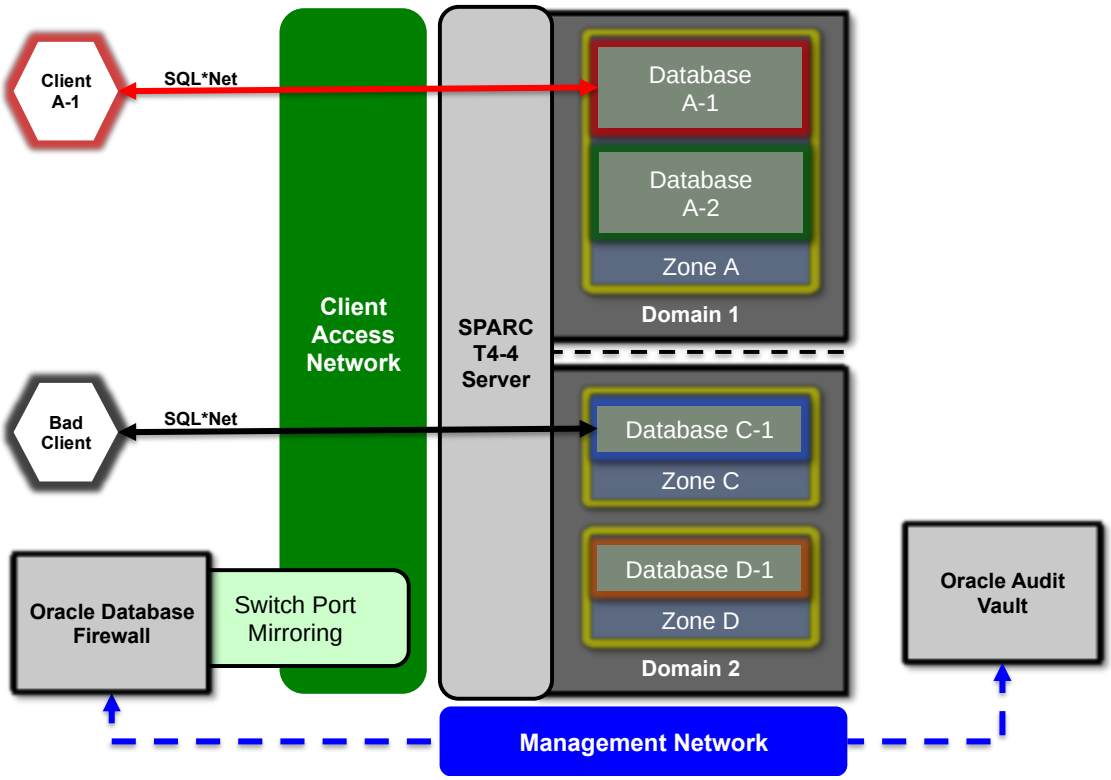

Figure 15. Active monitoring architecture.

This configuration allows Oracle Audit Vault and Database Firewall to transparently inspect any SQL statements flowing into the platform. In this configuration, the client access network switch essentially copies and sends to Oracle Audit Vault and Database Firewall network traffic being sent to any of the databases running on the platform. In SPARC SuperCluster, both inbound and outbound traffic can be mirrored allowing databases running on different domains and zones to be monitored. Just as in the previous scenario, policy violations trigger warnings and alerts ensuring that administrators are notified.

Agent-Based Remote Monitoring

The last deployment scenario leverages software agents that are deployed onto SPARC SuperCluster domains or zones to monitor SQL traffic flowing to and from databases running on the platform. The agent is responsible for capturing SQL traffic and sending it over the SPARC SuperCluster's client access network to Oracle Audit Vault and Database Firewall, which then inspects and processes the SQL traffic, as in the previous scenario, to detect and report on any policy violations.

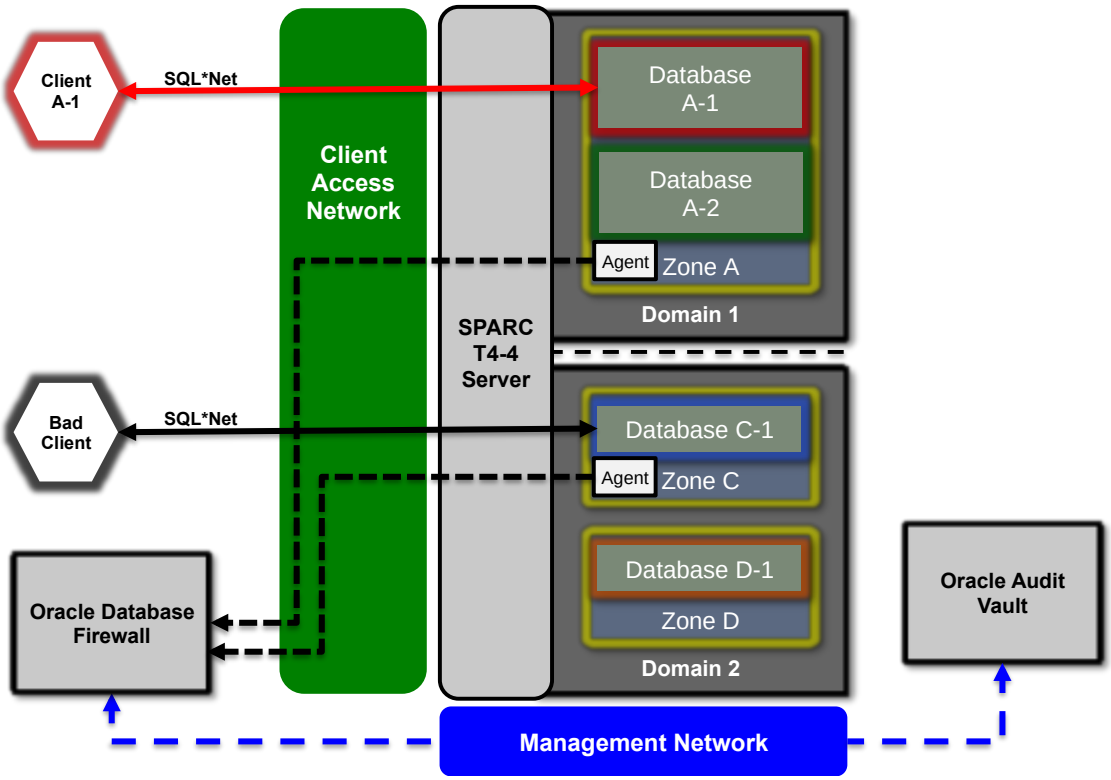

Figure 16. Agent-based remote monitoring architecture.

Oracle Key Manager

Oracle Key Manager centrally authorizes, secures, and manages access to encryption keys used by Oracle Database, the Oracle Solaris operating system, and Oracle's StorageTek encrypting tape drives. Oracle Key Manager is a complete key management appliance that supports lifecycle key management operations and trusted key storage. When configured with Oracle's Sun Crypto Accelerator 6000 PCIe Card, Oracle Key Manager offers FIPS 140-2 Level 3 certified key storage of AES 256-bit encryption keys as well as FIPS 186-2–compliant random number generation.

Within SPARC SuperCluster, Oracle Key Manager can be used to manage keys associated with ZFS encryption, which is available on the Oracle Solaris 11 operating system. This allows organizations to create and use encrypted file systems for their sensitive file-based content. Similarly, Oracle Key Manager can also manage the master keys used by Transparent Data Encryption to encrypt information stored in Oracle Database. In fact, Oracle Key Manager is able to support key management operations associated with individual or multiple database instances, Oracle RAC, Oracle Data Guard, Oracle Recovery Manager, and the Data Pump feature of Oracle Database.

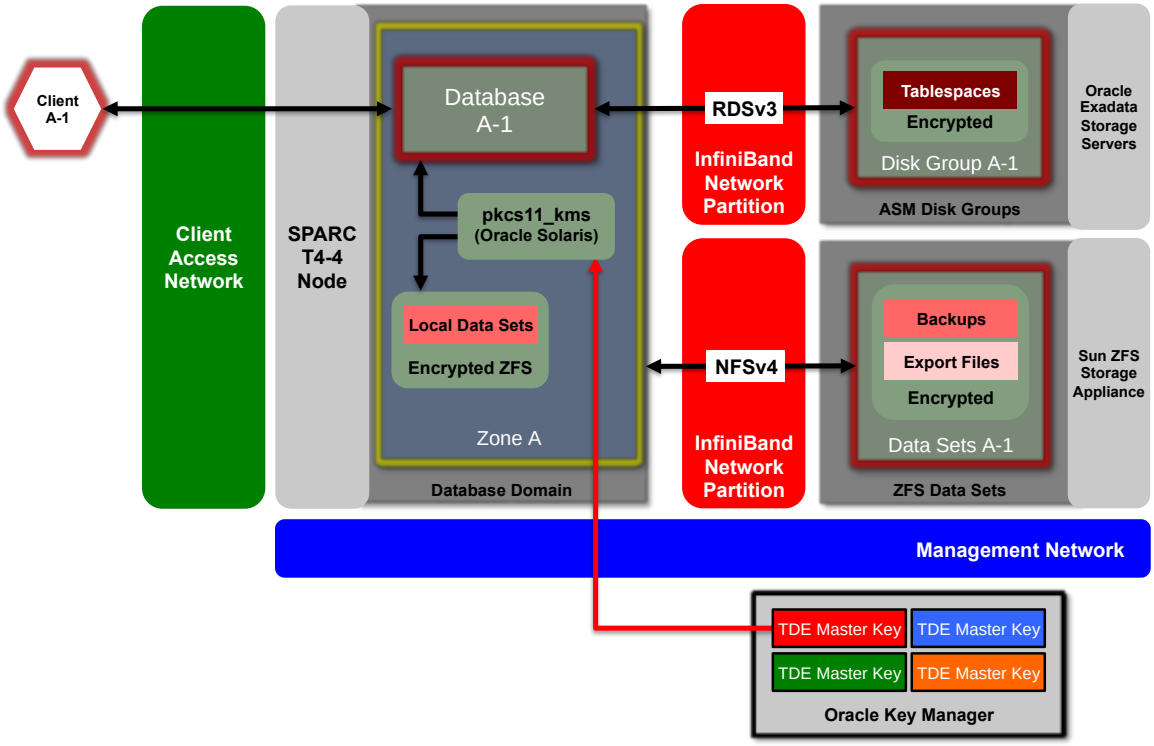

Figure 17. Oracle Key Manager can be used with SPARC SuperCluster.

Recognizing the importance of protecting the key material that it is shared with these services, Oracle Key Manager is configured by default to leverage mutual authentication using X.509 certificates. Further, communications are protected using SSL to ensure that key material is not exposed while in transit.

Finally, separation of duty, enforced by Oracle Key Manager, enables organizations to maintain complete control over their encryption keys with consistent visibility into any key management operations. Given the importance that keys serve in the protection of information, it is critical that organizations implement these necessary levels of role-based access control and auditing to ensure that keys are properly safeguarded throughout their lifetime.

Privileged Account Manager

Part of the Oracle Identity Governance Suite, Privileged Account Manager enables organizations to manage privileged account passwords within a centralized, secure password vault. Using Privileged Account Manager, organizations can generate, provision, and manage passwords for privileged users accessing specific resources. For example, an authorized system administrator could use this service to obtain a `root` or other role password. Similarly, database administrators could use this service to access passwords associated with privileged database roles such as `SYSDBA`.

Using Privileged Account Manager, privileged account credentials are centrally managed and access is governed by a set of policies that specify who can access which resources and for how long. Once properly authenticated, administrators can retrieve credentials to which they have been authorized. All credential access is audited ensuring a high level of accountability, which is especially important since many administrators often must share privileged roles. Optionally, privileged access can be exclusively granted for a time period to further associate actions to specific individuals. Finally, Privileged Account Manager can be configured to automatically change the privileged account password after use to minimize the likelihood of a password being successfully reused.

For database consolidation scenarios, Privileged Account Manager helps to simplify the process of managing access to privileged operating system and database accounts and roles. While this capability can be deployed independently, organizations can expect to gain additional value through its integration with other components of the Oracle Identity Governance Suite, such as Oracle Identity Manager, Oracle Authentication Services for Operating Systems, and Oracle Internet Directory.

Database as a Service

Database consolidation is an important step taken by organizations to rationalize the diversity of vendor products and versions, implement standardized configurations and processes, improve efficiency, and modernize aging hardware platforms. As illustrated previously, SPARC SuperCluster is an ideal architecture upon which organizations can build their consolidated database environment without sacrificing performance, security, or reliability. Increasingly, however, organizations are looking at rationalization and consolidation as simply first steps along a path toward the development of service delivery and cloud computing architectures.

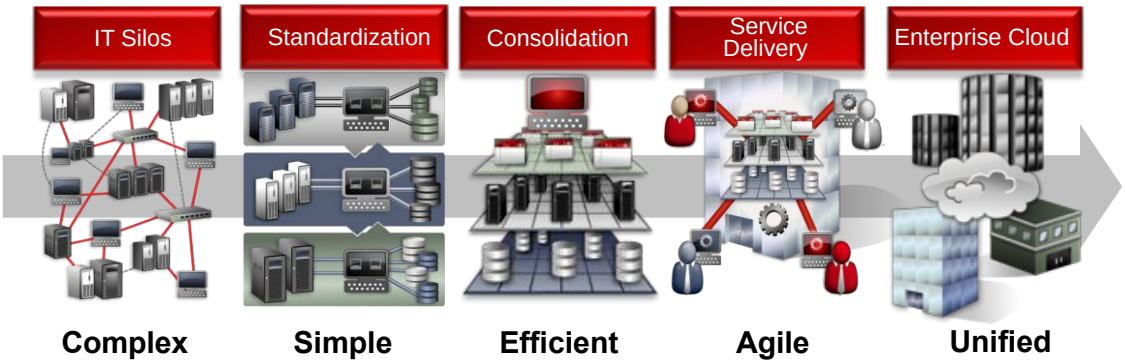

Figure 18. The path toward service delivery and cloud computing architectures.

It is critical that organizations understand that information security and data protection topics such as those discussed in this paper apply equally to cloud computing architectures such as Database as a Service (DBaaS). Regardless of the deployment architecture, organizations must ensure that their information is properly protected and that service levels are maintained at a level commensurate with its value to the organization.

That said, DBaaS and other cloud computing architectures bring new variables into the IT security equation that must be considered. Organizations interested in deploying DBaaS architectures are encouraged to consider the security implications of areas such as cloud operating models, on-demand self-service, elastic growth and contraction, and shared resources and multitenancy.

Cloud Operating Models

One of the most interesting aspects of cloud computing architectures is the division in responsibilities between the consumer and the provider of cloud services. Unlike traditional IT service models, where a consumer of IT services can specify a unique configuration or product combination, cloud consumers are often limited to those services offered by their provider. From the provider perspective, customization is costly and inherently not scalable across multiple tenants. It is important, therefore, for both parties to fully understand their requirements and responsibilities when it comes to securely managing services and information throughout their lifecycle. What might have been traditionally the responsibility of the IT organization might now be transferred to the cloud consumer, depending upon the underlying approach used to implement DBaaS.

This separation in responsibilities should not be viewed as a line of demarcation, however. Rather, consumers must work with their DBaaS providers to ensure that their security, privacy, and compliance requirements can be met in this new architectural model. Through this collaboration, DBaaS providers will be better able to appreciate the needs of their customers and, thereby, develop service offerings that are more closely aligned to their requirements. It is worth noting that approaches to data security that have worked in the past might need to adapt to this new consumer/provider operating model. This is especially true in situations in which providers are not able or permitted to directly access the services or data of their tenants.

SPARC SuperCluster includes a flexible yet complete set of security capabilities that can be tailored based upon a wide array of deployment scenarios including DBaaS. In particular, the fine-grained access control, privileges, and auditing associated with the operating system, database, and related components helps ensure that both providers and consumers have appropriate levels of access.

On-Demand Self-Service

Organizations considering cloud computing architectures are often interested in the ability of consumers to provision, consume, and manage services as needed in a self-service model. While this is certainly empowering to consumers, providers must take care to perform capacity planning, prioritize and isolate services and tenants, and define limits and quotas to ensure that the architecture is able to handle the ad hoc demands of its self-service consumers. In situations in which demand is not properly forecasted or spikes in activity exhaust available resources, organizations should be prepared with policies, processes, and procedures to ensure that business-critical services remain unaffected.

There are many situations in which a database cloud will leverage a variety of different deployment zones based upon either development lifecycle (for example, development, test, unit acceptance test, and production) or other classification criteria. In these situations, it is critical that cloud providers implement policies that are associated with each of these distinct resource pools. This helps to ensure that self-service operations are enabled only for those pools to which a self-service consumer has been authorized. For example, a software developer might be given access to a development pool, but access to production or business-critical resources might be restricted.

Further, DBaaS providers must take care to properly define their service offerings not only in terms of capacity or performance, but also in terms of what security, reliability, and recovery capabilities are available, either by default or as an option. For example, DBaaS providers might want to offer each tenant its own encrypted tablespaces to help protect information at rest. The next obvious question to consider is who is responsible for managing the keys associated with those encrypted tablespaces. While there is no single answer to questions such as this, it is important that a shared understanding be achieved between consumers and providers of cloud services. To facilitate this understanding, security and related capabilities and metrics should be documented as part of the definition of each service offered to consumers.

Through integration with Oracle Enterprise Manager, SPARC SuperCluster is able to support a variety of DBaaS self-service operations. Organizations can define pools of resources, assign pools and quota to individual tenants, identify and publish service catalogs, and monitor the usage of cloud computing resources. Building upon the security capabilities discussed in this paper, Oracle Enterprise Manager provides an abstraction layer offering DBaaS capabilities to consumers without requiring those consumers to have access to the underlying cloud infrastructure.

Elastic Growth and Contraction

Another essential characteristic of cloud computing architectures is the ability to elastically scale resources in response to changes in demand. From a consumer perspective, this is very attractive because excess capacity does not have to be purchased in advance, but rather capacity can be added or removed based upon need. Similarly, from a provider perspective, elasticity is beneficial because it helps ensure more efficient use of available resources across multiple tenants.

From a security perspective, DBaaS providers must be sure to properly implement resource controls and QoS policies to ensure that each tenant is able to access their allotted amount of resources even as the demand for other tenants' resources fluctuates. In this context, resource controls cover the spectrum of resources including compute and storage capacity, network bandwidth, end-to-end performance, and response time. The use of dedicated resource pools might also be leveraged to implement hard divisions between tenants operating at different security tiers or classifications. This could mean isolating development from production or internal services from those exposed to customers, partners, or suppliers.

Another security consideration arising from elastic use of resources is that of data remanence. Resources that can be shared across multiple tenants or even across classifications should be properly sanitized, ensuring data stored by previous tenants is not accessible when those storage resources are allocated to a new tenant. One technique for managing this risk in DBaaS environments is to protect each tenant's information using unique tablespaces that are encrypted when stored on disk. Using Transparent Data Encryption, discussed earlier in this paper, organizations can create cryptographically isolated data sets. When a consumer deprovisions their service, keys associated with those tablespaces can be securely destroyed and the tablespaces removed—effectively eliminating the ability to recover that content.

SPARC SuperCluster is inherently a highly scalable and performant platform upon which database shared services can be offered. Resource controls available at the operating system and database levels offer organizations a fine-grained approach for controlling compute, memory, disk, and network resource utilization. Similarly, the integrated cryptographic acceleration of the SPARC T4 processors utilized by SPARC SuperCluster offset the performance penalties typically associated with widespread use of cryptography, allowing organizations to efficiently protect information at rest and while flowing across the network.

Multitenancy

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

SPARC SuperCluster is uniquely able to support a wide range of isolation strategies depending upon the needs of an organization. Workload isolation can be realized through a combination of techniques at the virtualization, operating system, and database layers. Similarly, storage isolation can be achieved through a combination of techniques including unique Oracle Automatic Storage Management instances and disk groups, use of ZFS data sets, or even existing, external storage services. Network isolation is realized through a combination of physical networks, Ethernet VLANs, and even InfiniBand partitions. In addition to all of this, cryptographic isolation can be employed at both the network and storage layers to offer even stronger protection of confidentiality and integrity.

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

Conclusion

Organizations deploying and consolidating databases on SPARC SuperCluster benefit from a well-rounded security foundation enabled by the underlying server and storage hardware, the virtualization and operating system technologies, the databases themselves, as well as a suite of complementary services. Together, these layers combine to provide a layered, defense-in-depth architecture at every level of the technology stack.

Offering well-integrated security capabilities such as secure isolation, access control, cryptographic services, and monitoring and auditing, SPARC SuperCluster is readily able to meet even the most demanding security requirements. Further, its inherent flexibility allows organizations to customize their architecture to meet their specific workload objectives and security and compliance mandates, without sacrificing reliability, availability, or performance. As a result, SPARC SuperCluster is ideally suited to help organizations securely deploy individual databases, consolidate their database architectures, or even deploy database services as part of a database cloud.

References

General White Papers and Documentation

- "SPARC SuperCluster T4-4 Platform Security Principles and Capabilities": http://www.oracle.com/us/products/servers-storage/servers/sparc-enterprise/supercluster/supercluster-t4-4/ssc-security-pac-1716580.pdf
- "Oracle SPARC SuperCluster Security Technical Implementation Guide (STIG) Validation and Best Practices on the Database Servers": http://www.oracle.com/technetwork/server-storage/hardware-solutions/stig-sparc-supercluster-1841833.pdf
- "A Technical Overview of Oracle's SPARC SuperCluster T4-4": http://www.oracle.com/us/products/servers-storage/servers/sparc-enterprise/supercluster-t4-4-arch-wp-1537679.pdf
- "Delivering Application Performance with Oracle's InfiniBand Technology": http://www.oracle.com/technetwork/server-storage/networking/documentation/o12-020-1653901.pdf

Product Security Guides

- *Oracle Integrated Lights Out Manager Security Guide*: http://docs.oracle.com/cd/E24707_01/pdf/E24526.pdf
- *Sun Datacenter InfiniBand Switch 36 Hardware Security Guide*: http://docs.oracle.com/cd/E19197-01/E26701/E26701.pdf
- *SPARC T4 Series Servers Security Guide*: http://docs.oracle.com/cd/E22985_01/pdf/E24876.pdf
- *Oracle Solaris 10 Security Guidelines*: http://docs.oracle.com/cd/E23823_01/pdf/E23335.pdf
- *Oracle Solaris 11 Security Guidelines*: http://docs.oracle.com/cd/E23824_01/pdf/819-3195.pdf
- *Oracle Database 11g Release 2 Security Guide*: http://www.oracle.com/pls/db112/to_pdf?pathname=server.112/e10575.pdf

Security White Papers and Documentation

Oracle SPARC T4 Processor

- "High Performance Security for Oracle Database and Fusion Middleware Applications Using SPARC T4": http://www.oracle.com/technetwork/server-storage/sun-sparc-enterprise/documentation/o12-021-t4security-1577047.pdf

Oracle Solaris 11 Operating System

- "Oracle Solaris 11 Network Virtualization and Network Resource Management": http://www.oracle.com/technetwork/server-storage/solaris11/documentation/o11-137-s11-net-virt-mgmt-525114.pdf

Oracle VM Server for SPARC

- "Secure Deployment of Oracle VM Server for SPARC": http://www.oracle.com/technetwork/articles/systems-hardware-architecture/secure-ovm-sparc-deployment-294062.pdf

Oracle Database 11*g*

- Oracle Defense-in-Depth Guide home page: http://www.oracle.com/technetwork/database/security/sol-home-086269.html
- "Cost Effective Security and Compliance with Oracle Database 11*g* Release 2": http://www.oracle.com/technetwork/database/security/owp-security-database-11gr2-134651.pdf
- "Oracle Advanced Security with Oracle Database 11*g* Release 2": http://www.oracle.com/technetwork/database/owp-security-advanced-security-11gr-133411.pdf
- "Oracle Advanced Security Transparent Data Encryption Best Practices": http://www.oracle.com/technetwork/database/security/twp-transparent-data-encryption-bes-130696.pdf
- "Oracle Database Vault with Oracle Database 11*g* Release 2": http://www.oracle.com/technetwork/database/security/owp-security-database-vault-11gr2-1-131473.pdf
- "DBA Administrative Best Practices with Oracle Database Vault": http://www.oracle.com/technetwork/database/security/twp-databasevault-dba-bestpractices-199882.pdf
- "Oracle Label Security with Oracle Database 11*g* Release 2": http://www.oracle.com/technetwork/database/security/owp-security-label-security-11gr2-133601.pdf

- "Oracle Database 11*g* Release 2 and the Oracle Sun ZFS Storage Appliance": https://blogs.oracle.com/eSTEP/entry/why_oracle_sun_zfs_storage
- Oracle Database Maximum Availability Architecture home page: http://www.oracle.com/technetwork/database/features/availability/maa-090890.html
- "Oracle Exadata Database Machine Consolidation: Segregating Databases and Roles": http://www.oracle.com/technetwork/database/focus-areas/availability/maa-exadata-consolidated-roles-459605.pdf
- "Security in Private Database Clouds": http://www.oracle.com/technetwork/database/database-cloud/security-in-private-db-clouds-1733933.pdf
- "Isolation in Private Database Clouds": http://www.oracle.com/technetwork/database/database-cloud/isolation-in-pvt-db-clouds-1652083.pdf
- "Network Isolation in Private Database Clouds": http://www.oracle.com/technetwork/database/focus-areas/database-cloud/ntwk-isolation-pvt-db-cloud-1587225.pdf

Oracle Key Manager

- *Oracle Key Manager Administration Guide*: http://docs.oracle.com/cd/E26076_02/en/E26025_01/E26025_01.pdf

Oracle Audit Vault and Database Firewall

- Oracle Audit Vault and Database Firewall documentation: http://docs.oracle.com/cd/E37100_01/index.htm

Privileged Account Manager

- "Protecting Access to Sensitive Resources with Oracle Privileged Account Manager": http://www.oracle.com/technetwork/middleware/id-mgmt/overview/opam-wp-11gr2-1697093.pdf

Secure Database Consolidation Using the
SPARC SuperCluster T4-4 Platform
May 2013, Revision 2.0
Authors: Glenn Brunette, Ramesh Nagappan,
and Joel Weise

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

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200

oracle.com

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

Hardware and Software, Engineered to Work Together