ORACLE
OPTIMIZED SOLUTIONS

Oracle Optimized Solution for Secure Backup and Recovery

Oracle SuperCluster Backup and Recovery

ORACLE WHITE PAPER | OCTOBER 2015

Table of Contents

Introduction

Oracle SuperCluster is Oracle’s most powerful Oracle Database and application consolidation platform. This engineered system is optimized for Oracle Database and Oracle applications and is ideal for private cloud implementations of a wide range of enterprise application and database deployments. Oracle SuperCluster is a pretested, optimized, and integrated server, storage, networking, and software system that includes: Oracle’s SPARC servers; Oracle Exadata Storage Servers and Oracle ZFS Storage Appliance; high-speed, low-latency InfiniBand fabric; and the Oracle Solaris operating system with built-in virtualization. With massive capacity and extreme performance, Oracle SuperCluster requires a new way of thinking about backup and recovery.

Oracle Optimized Solution for Secure Backup and Recovery on Oracle SuperCluster accelerates data-protection processing and management while providing breakthrough cost structures and industry-leading performance. Using components from Oracle's end-to-end hardware and software technology stack, the solution delivers virtually unlimited scalability with centralized management. This solution provides options for traditional disk and tape backups as well as cloud-based backups. Complementary technologies—including Oracle Recovery Manager (Oracle RMAN), Data Guard, and Oracle’s Zero Data Loss Recovery Appliance—provide next-generation data protection that more than meets enterprise requirements.

Solution Overview

Oracle Optimized Solution for Secure Backup and Recovery on Oracle SuperCluster is designed as a complete solution for performing backups of Oracle SuperCluster systems. Leveraging built-in integration of Oracle hardware and software, it provides pretested, recommended solutions for the backup and recovery of Oracle SuperCluster.

A comprehensive solution for Oracle Database backups as well, Oracle Optimized Solution for Secure Backup and Recovery provides support for Oracle Database 11*g* Release 2 or higher. With complete end-to-end data protection for Oracle SuperCluster, the solution enables IT staff to create backups to disk or tape. Using Oracle RMAN and the Data Guard feature of Oracle Database, administrators can take backups residing on Oracle ZFS Storage Appliance and copy them to high-performing encrypted tape for cost-effective, long-term storage.

A unique offering that is low cost and high performance, the solution is a clear industry leader in terms of price/performance for backup and recovery. Using disk-only solutions that do not rely on tape backups can save on the costs of licensing tape management software. For example, backups to Oracle ZFS Storage Appliances or Oracle’s Exadata Storage Expansion Racks are disk-only solutions that do not incur additional software licensing costs for backup and recovery use.

When the solution is deployed to back up Oracle SuperCluster, it dramatically simplifies backup and recovery processing and management. Third-party deduplication technologies are typically deployed for space savings or to replicate backups, but they can be needlessly complex. When Oracle Optimized Solution for Secure Backup and Recovery is deployed in replicated configurations, it eliminates the need for third-party deduplication, because simple tape and disk backups can be performed at one or both sites for complete data protection.

Creating More Secure Backup and Recovery Environments

Protecting data is an essential business concern for all enterprises. Enterprise-level backup environments typically use a centralized backup and recovery model, which simplifies administration as the size of the data continues to grow. However, this centralization also presents a potential security threat: If an intruder gains access to a centralized backup or media server, data for many systems across the enterprise can be compromised. Physical security is, of course, fundamental, and access to servers and media libraries must be protected and audited. Backup servers, clients, networks, storage, and tape libraries should all be configured following recommended security guidelines to provide end-to-end security. Data encryption is also recommended to protect data at rest and while in transit across networks and to/from storage media.

The following steps can help create a more secure backup and recovery environment:

- **Simplify the infrastructure.** Most backup and recovery environments are based on a complex infrastructure, making implementation and management complicated. This complexity increases the risk of security vulnerabilities. A backup and recovery implementation as a whole is only as secure as its most vulnerable component, and it can be challenging to securely configure the myriad interacting components and products in a heterogeneous system. Oracle Optimized Solutions simplify backup and recovery implementations through the use of consolidation and virtualization technologies. Oracle also offers security guidelines and recommendations, and many Oracle components have security built-in by default.
- **Reduce implementation flaws.** Secure software is important but not sufficient by itself. Most security vulnerabilities arise from flawed implementation and architecture, including improper configuration and access control, lack of patch management, unencrypted communications, and inadequate security policies and processes. Based on current security best practices, Oracle Optimized Solutions provide proven and tested architecture recommendations for increased backup and recovery solution protection.

- **Eliminate performance and cost penalties.** Many security processes, such as on-the-fly encryption/decryption, can have a significant negative impact on the performance and cost of a backup and recovery solution. Oracle Optimized Solutions leverage Oracle's SPARC-based systems, which offer high-performance security using cryptographic instruction accelerators that are directly integrated into the processor cores. By providing wire-speed security capabilities, Oracle systems eliminate the performance and cost penalties typically associated with real-time, secure computing.

Architecture Overview

Oracle Optimized Solution for Secure Backup and Recovery features a flexible, scalable architecture (see Figure 1) that supports all Oracle SuperCluster models, as well as older SPARC SuperCluster T4-4 systems from Oracle. This solution provides options for traditional disk and tape backups as well as cloud-based backups, and includes Oracle ZFS Storage Appliance and Oracle's StorageTek tape libraries. In addition, Oracle's Zero Data Loss Recovery Appliance can optionally be deployed to revolutionize database protection with its incremental-forever backup strategy, which eliminates potential loss and dramatically decreases backup overhead.

Designed to be software agnostic, the solution can work with Oracle RMAN, Oracle Secure Backup, Symantec NetBackup, or other third-party backup software. For illustration purposes, this paper refers to the use of Oracle Secure Backup software throughout for the tape management component of the solution. Note that in disk-only environments—such as those using Oracle Exadata storage, Exadata Storage Expansion Racks, or Oracle ZFS Storage Appliance—no additional backup software is required. Disk backups can be completed using the operating system and Oracle Database tools (such as Oracle RMAN) alone.

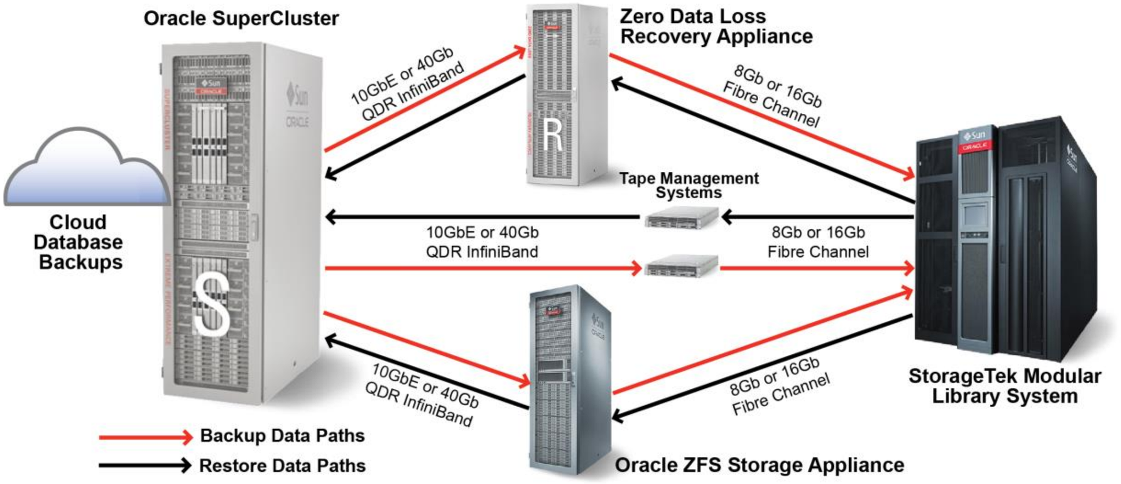
Oracle SuperCluster
Zero Data Loss Recovery Appliance
10GbE or 40Gb QDR InfiniBand
8Gb or 16Gb Fibre Channel
Cloud Database Backups
Tape Management Systems
10GbE or 40Gb QDR InfiniBand
8Gb or 16Gb Fibre Channel
10GbE or 40Gb QDR InfiniBand
8Gb or 16Gb Fibre Channel
StorageTek Modular Library System
Backup Data Paths
Restore Data Paths
Oracle ZFS Storage Appliance

Figure 1. Oracle Optimized Solution for Secure Backup and Recovery on Oracle SuperCluster supports different backup target devices.

For more information on the architecture and components in Oracle Optimized Solution for Secure Backup and Recovery, refer to the Oracle web site oracle.com/solutions/optimized-solutions/backup-and-recovery.

Private Cloud Deployment

Oracle Optimized Solution for Secure Backup and Recovery on Oracle SuperCluster supports cloud-based backups. When deploying backup and recovery solutions in private cloud environments, isolation technologies throughout the solution's cloud infrastructure provide comprehensive security and data protection. For example, the following hardware and software isolation features help provide end-to-end data security:

- Zero Data Loss Recovery Appliance: User ID ownership of all resources isolates databases and helps protect against unauthorized access from other databases on the cloud-based backup.
- Oracle ZFS Storage Appliance: Virtualized networking and ZFS storage pools provide isolation and protection of resources. Encryption supplies an additional layer of protection for data resources.
- StorageTek Tape libraries: Hardware and software virtualization options can be used to logically or physically isolate both tapes and media. Encryption supplies an additional layer of protection for data resources.

Disk and Tape Backup and Recovery Options

Oracle Optimized Solution for Secure Backup and Recovery on Oracle SuperCluster provides a choice of backup and restore methods:

- Tape-based backup (using Oracle's StorageTek modular library systems)
- Disk-based backup (using Oracle ZFS Storage Appliance or Exadata Storage Expansion Racks)
- Zero Data Loss Recovery Appliance
- Disk-to-disk-to-tape backups

Disk and tape backups each have their advantages. Disk backups can provide backed-up data immediately in the event of a disaster, while a restore operation from tape can take far too long to be a viable recovery solution. Disk-only backups provide faster recovery times for data and logical corruptions and some tablespace point-in-time recovery (TSPITR) scenarios. Backups to disk also provide the ability to use backups directly—with no restore needed—by switching to a copy of the database, tablespace, or data file after performing image backups.

Tape backups can provide cost-effective, long-term storage for valuable enterprise data. Economical for archiving, tape media are also portable, enabling off-site storage for purposes such as disaster recovery (DR) protection and regulatory compliance.

Disk-to-disk-to-tape backups combine both disk and tape backups: Data is initially backed up to disk and then copied again to tape. Performing disk-to-disk-to-tape backups enables administrators to leverage the advantages of both disk and tape backups and provide for various contingencies.

Oracle Optimized Solution for Secure Backup and Recovery on Oracle SuperCluster includes two disk-based options: Oracle ZFS Storage Appliance or Exadata Storage Expansion Racks. The different configurations are designed to meet a variety of backup solution requirements. In general, Exadata Storage Expansion Racks provide the highest performance and serviceability, while Oracle ZFS Storage Appliances provide flexibility and a lower-cost option.

Optionally, Zero Data Loss Recovery Appliance can be used for database protection. This engineered system can be used to provide a centralized backup strategy for hundreds to thousands of databases in the enterprise, using fully fault-tolerant hardware and storage.

Requirements for Complete Oracle SuperCluster Recovery

To provide complete protection against loss of data and operations in Oracle SuperCluster, the backup and recovery plan must include the cluster infrastructure, unstructured data—including the operating system and applications, and Oracle Database (see Table 1).

TABLE 1. ORACLE SUPERCLUSTER BACKUP AND RECOVERY FREQUENCY

Category	Components	Backup Frequency
Infrastructure	» Control domain configurations » Switch configurations » Internal Oracle ZFS Storage Appliance configuration	Backed up less frequently, based upon upgrades and system changes
Unstructured data	» Infrastructure backups » Operating system » Applications » iSCSI zones » NFS shares	Backed up daily and after upgrades and system changes
Database	» Oracle Database	Backed up daily and after upgrades and system changes

The following list provides more details about the backup requirements for the three categories:

- **Oracle SuperCluster infrastructure.** Oracle SuperCluster infrastructure configuration information, including the networking configuration, must be backed up to preserve the settings and provide for a quick recovery process in the event of a disaster.
- **Unstructured data.** Backups of the operating system on the Oracle SuperCluster nodes, including Oracle Solaris domains and Oracle Solaris Zones, are required. Applications and other data stored on the internal Oracle ZFS Storage Appliance must also be backed up regularly. These backups are similar to standard backups for any server in an enterprise environment.
- **Oracle Database.** Oracle Database is a vital element of Oracle SuperCluster and must be backed up to ensure against loss of business- or mission-critical data.

The infrastructure data requires less-frequent backups; these backups are based primarily on upgrades and changes to the Oracle SuperCluster system. The unstructured data and database are typically backed up daily and upon upgrades and system changes. The following sections discuss backup and recovery of Oracle SuperCluster and include best practices designed for high availability, optimal performance, and maximum data protection.

Protecting Oracle SuperCluster Infrastructure

Oracle SuperCluster configuration information, including switch configurations for the InfiniBand fabric, is created when Oracle SuperCluster is first deployed. This configuration information must be backed up to preserve the settings and enable quick recovery in case of human error or a disaster.

Bare-metal backups capture a snapshot of the entire Oracle SuperCluster infrastructure configuration. These backups can be used to restore the complete system from “bare metal” in the event of a catastrophic failure. Typically, bare-metal backups are performed after installation and upon major system updates or configuration changes.

Bare-Metal Backups of Oracle SuperCluster Infrastructure

The Oracle SuperCluster backup tool, `osc-backup`, is used to create a snapshot of the entire Oracle SuperCluster infrastructure. The built-in `osc-backup` tool is included with the Oracle SuperCluster software and provided at no additional cost. It is intended for bare-metal backups of the system rather than for daily backups. It is recommended to perform bare-metal backups using this tool in the following events:

- After initial deployment to provide an initial backup snapshot of the Oracle SuperCluster infrastructure
- Before and after reconfiguration of significant operating parameters

- Before and after installation of each quarterly full stack download patch (QFSDP) for Oracle SuperCluster
- As part of a regular maintenance schedule, at a frequency that is practical and feasible (monthly, for example)

The `osc-backup` tool automates the process of backing up configuration information for all components in Oracle SuperCluster, including networking configuration, and Oracle Solaris domains and Oracle Solaris Zones on the compute notes. This tool performs multiple steps sequentially to prepare the environment and capture the configuration information. Specifically, the following Oracle SuperCluster components are backed up by the `osc-backup` tool:

- Logical Domains (LDoms) on the Oracle SuperCluster compute nodes
- Cisco and InfiniBand switch configuration information
- ZFS data sets and iSCSI mirrors of `rpool`/`u01-pool` on database and application domains
- Oracle Explorer Data Collector information from each LDom running either a database or application
- Oracle SuperCluster configuration information
- Oracle ZFS Storage Appliance configuration information

It is equally important to note that the following are *not* backed up by the `osc-backup` tool: Oracle Database and information stored on NFS shares on the internal Oracle ZFS Storage Appliance including iSCSI zones, applications, and other data. For complete bare-metal protection of Oracle SuperCluster, backups of this information are also required.

The backups created by the `osc-backup` tool are stored on the Oracle ZFS Storage Appliance that is internal to Oracle SuperCluster. It is critical that this storage be backed up as part of an enterprise backup and recovery strategy to safeguard against catastrophic failures and disasters. Replication, tape backups, and disk-to-disk-to-tape backups are strategies that can be used to back up the information on the internal Oracle ZFS Storage Appliance.

For more information on using the `osc-backup` tool, refer to My Oracle Support Document 1903189.1, “SuperCluster–How to back up a SuperCluster using the `osc-backup` tool.”

Bare-Metal Restores of Oracle SuperCluster Infrastructure

Information on how to restore Oracle SuperCluster from backups performed by the `osc-backup` tool is contained in My Oracle Support Document 1903364.1, “SuperCluster–Recovery Guide.” The `osc-backup` tool saves the Oracle SuperCluster infrastructure information on the internal Oracle ZFS Storage Appliance. In addition to having a good backup from the `osc-backup` tool, a proxy system on the network is required to access the Oracle ZFS Storage Appliance and the compute node that is being restored.

The following steps provide a high-level overview of the recovery process:

1. **Configure the primary node to boot from the iSCSI LUN on the internal Oracle ZFS Storage Appliance**. As part of the backup procedure, a working Oracle Solaris image from the primary domain was copied onto an iSCSI LUN on the internal Oracle ZFS Storage Appliance. Using the proxy host, discover the settings needed to successfully boot from the iSCSI LUN and set the network boot arguments on the primary node accordingly.
2. **Boot the primary cluster node using the iSCSI LUN from the internal Oracle ZFS Storage Appliance.** Make sure the Service Processor and the target initiator groups are configured correctly, and then power on the system.
3. **Fix storage pools on the cluster node.** After the system boots, log in and fix any faulted storage pools on the node, and verify and fix the mirrored root pool (`rpool`).
4. **Boot the system using the repaired `rpool`.** Shut down the system, set the boot device, and boot from the `rpool` created in the previous step.
5. **Restore any additional storage pools configured on this node.**

6. **Prepare the guest domains.** Configuration information for the guest domains was saved by the `osc-backup` tool to the internal Oracle ZFS Storage Appliance. Use this information to reconfigure the domains and assign resources.
7. **Restore the operating system from iSCSI disk.** Use the above steps to restore the operating system on the guest domains using the iSCSI LUNs on the internal Oracle ZFS Storage Appliance.

To completely restore Oracle SuperCluster, this procedure should be followed on all nodes in the cluster.

Protecting Local Backups

Bare-metal backups of the Oracle SuperCluster infrastructure created using the `osc-backup` tool are stored on the internal Oracle ZFS Storage Appliance. The internal Oracle ZFS Storage Appliance can also be used for daily backups of the Oracle SuperCluster operating system and applications. For greater protection in the event of local failures or disasters, these backups should be protected with remote replication to an off-site copy, be backed up to a tape device, or both.

» **Remote replication**. Data that is stored on the internal Oracle ZFS Storage Appliance can be protected using Oracle ZFS Storage Appliance replication (see Figure 2). With Oracle ZFS Storage Appliance replication, a copy of the backup data is copied from the internal Oracle ZFS Storage Appliance (the source) to an external Oracle ZFS Storage Appliance (the target) through an interconnecting TCP/IP network. This storage appliance can be a standalone appliance or an internal Oracle ZFS Storage Appliance in a separate Oracle SuperCluster. The target appliance can be located virtually any distance from the source, as long as the interconnecting network has sufficient bandwidth to carry the data. Data on the source system is periodically replicated to the target at user-defined intervals. Data can be transmitted securely using SSL.

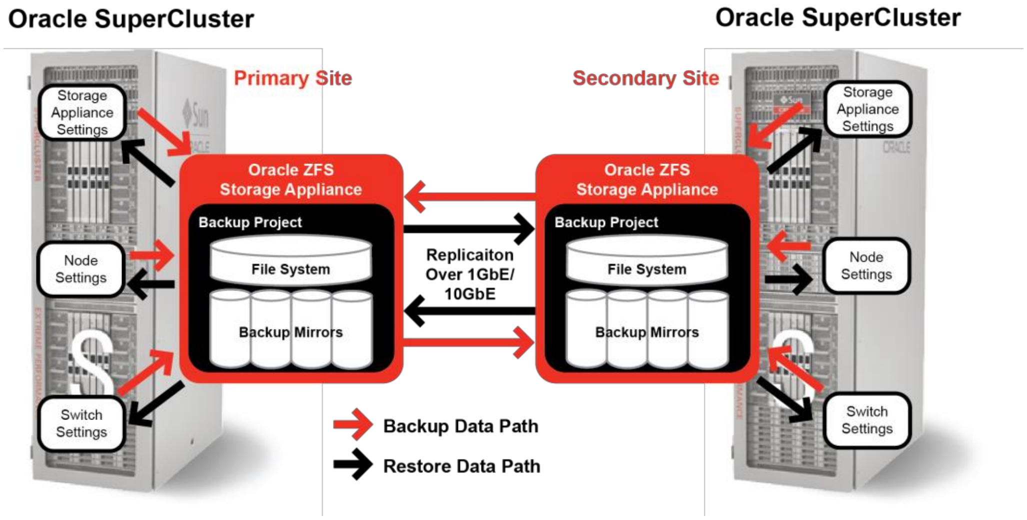

Figure 2. Backup using replication to another Oracle ZFS Storage Appliance.

For more information on replication implementation details, see the Oracle white paper "Architecture Principles and Implementation Practices for Remote Replication Using Oracle ZFS Storage Appliance."

- **Tape backups**. In configurations that use tape-based backups, backup and recovery software such as Oracle Secure Backup can be used to perform Network Data Management Protocol (NDMP) backups of the internal Oracle ZFS Storage Appliance to tape (see Figure 3).

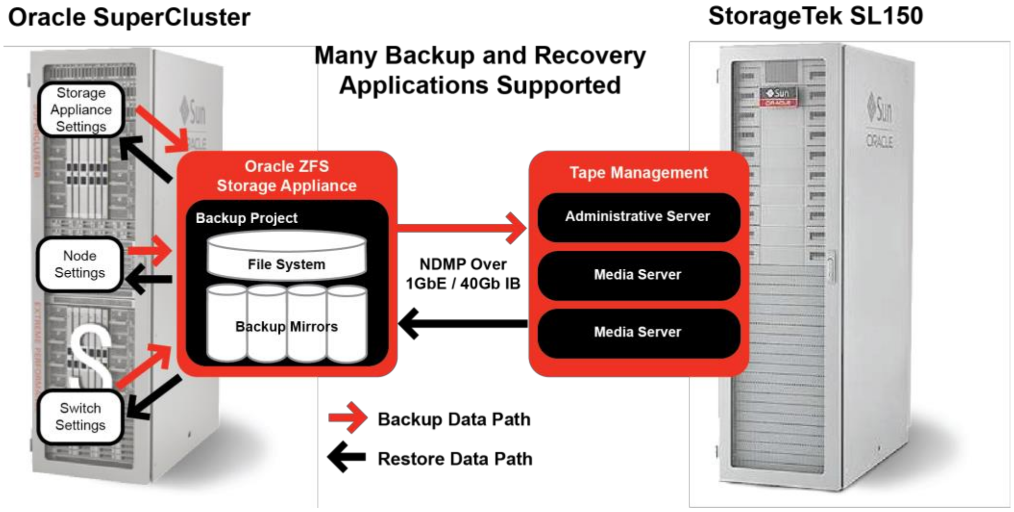

Figure 3. Tape-based backups using Oracle's StorageTek SL150 modular tape library.

- **Disk-to-disk-to-tape backups**. Data can also be protected using disk-to-disk-to-tape backups (see Figure 4), with the data replicated to an Oracle ZFS Storage Appliance and also backed up to tape. More information on disk-to-disk-to-tape backups is included later in this paper (see "Disk-to-Disk-to-Tape Backups" on page 15).

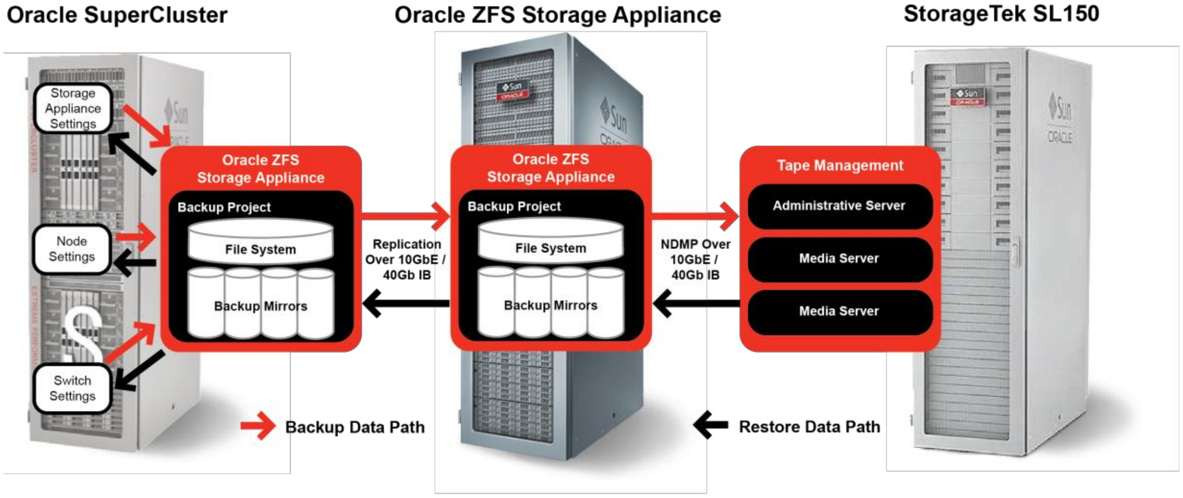

Figure 4. Disk-to-disk-to-tape backup and recovery of Oracle SuperCluster.

Protecting Unstructured Data

In addition to the bare-metal backups of the Oracle SuperCluster infrastructure provided by the `osc-backup` tool, day-to-day backups are required to provide ongoing protection of the unstructured data including the Oracle SuperCluster operating system environment and applications. The operating system on cluster nodes, Oracle Solaris domains, Oracle Solaris Zones, and iSCSI zones within Oracle SuperCluster must be backed up to provide for recovery in the event of a disaster. In addition, applications and other unstructured data installed on NFS shares on the internal Oracle ZFS Storage Appliance must be backed up.

Daily Oracle SuperCluster backups (that is, non-database backups) are similar to backups for other Oracle Solaris servers. Systems are backed up and restored in normal operations using backup and recovery software clients on the operating systems (Oracle Solaris domains and Oracle Solaris Zones) in the system.

Note: The operating system on the internal Oracle Exadata Storage Servers does not have to be backed up. Recovery of those servers is accomplished in a similar manner to restoring the firmware on a switch.

Backing Up the Operating System on Compute Nodes

The conventional method for backing up an operating system is to install backup software and back up the operating system to disk or tape. Operating system backups are critical and should be made regularly as well as before and after every significant change to Oracle SuperCluster software. In Oracle Solaris 10 and Oracle Solaris 11, ZFS file system snapshots can also be used for fast backup of the operating system. Daily backups provide the usual protection from unintentional file deletion, unexpected problems, and administrator error, and they are required to provide point-in-time recovery past the latest bare-metal backup.

Operating system backups should be performed regularly (typically daily) and before and after the following procedures:

- Installation or reconfiguration of significant software or applications
- Reconfiguration of significant operating parameters
- Before and after each quarterly full stack download patch (QFSDP) for Oracle SuperCluster

Backing Up Applications and Oracle Solaris Zones on iSCSI

Backup and recovery of applications is supported in NFS, and backup and recovery procedures remain the same for snapshots and replication of NFS shares, as well as for backup to tape using NDMP. To back up NFS shares, use the internal Oracle ZFS Storage Appliance with NDMP using the `dump` backup type. The `dump` backup type provides high-performance, block-level backups. For more information on using NDMP with Oracle ZFS Storage Appliance, please refer to the Oracle white paper “NDMP Implementation Guide for the Sun ZFS Storage Appliance” at oracle.com/technetwork/articles/systems-hardware-architecture/ndmp-whitepaper-192164.pdf.

Within Oracle SuperCluster, Oracle Solaris Zones typically contain applications or databases for different use cases. Oracle Solaris Zones can be installed on Oracle SuperCluster internal drives or on iSCSI LUNs.

To back up the iSCSI LUNs, use the Oracle ZFS Storage Appliance with NDMP using the `zfs` backup type. The `zfs` backup type does not support file history or direct access recovery (DAR), but it might be faster for some data sets. The iSCSI zones can also be backed up with ZFS snapshots and replication on the internal Oracle ZFS Storage Appliance, providing a high-performance method that works well for restoring an entire zone. Any zones stored on the internal hard drives of the Oracle SuperCluster compute nodes are backed up by the daily operating system backups and by the `osc-backup` tool bare-metal backup.

Protecting Oracle Database 11*g* Release 2 or Higher

A complete strategy for high availability and disaster recovery requires proven and dependable data backup, restore, and recovery procedures. Oracle RMAN provides a comprehensive foundation for efficiently backing up and recovering Oracle Database. Designed to work intimately with the database server, Oracle RMAN provides block-level corruption detection during backup and restore. It also optimizes performance and space consumption during backups through the use of file multiplexing and backup set compression.

Oracle RMAN takes care of all underlying database procedures before and after backup or restore operations, eliminating a dependency on operating system and SQL*Plus scripts. Oracle RMAN provides a common interface, by means of the command line and Oracle Enterprise Manager, for backup tasks across different host operating systems. Oracle RMAN offers features—such as parallelization of backup and restore data streams, retention policies for backup files, and detailed backup histories—that are not available through user-managed methods. Oracle RMAN integrates with Oracle Secure Backup as well as third-party media management products for tape backup.

Best Practice: Always Use a Fast Recovery Area

The following sections include best practices for Oracle Database backup and recovery in Oracle SuperCluster when using Exadata Storage Expansion Racks, Oracle ZFS Storage Appliance, tape-based backups, or Zero Data Loss Recovery Appliance. One best practice recommendation applies to all use cases: Always use a fast recovery area (FRA).

One vital database backup and recovery best practice is to deploy the database with an FRA, the location where the database stores all of its information for Oracle Flashback technologies, snapshots, database backups, rollbacks, and more. The FRA enables the database to protect itself, rolling the database back to a certain point in time and restoring it within a matter of seconds instead of minutes or hours using conventional backup and recovery methods. Consequently, database recovery time is limited only by the speed of the device on which the FRA resides, and the FRA should be located on the fastest performing storage possible. Oracle engineered systems such as Oracle SuperCluster are designed with the FRA built in, because placing the FRA on anything but Oracle Exadata internal storage or an external Exadata Storage Expansion Rack will lengthen the amount of time it takes for recovery. Exadata Storage Expansion Racks can be used for extra space for the FRA, as needed.

Database backups can, if desired, be excluded from the FRA and stored instead on Oracle ZFS Storage Appliance. In this case, the FRA on Oracle Exadata can be configured to be much smaller, because space for the full and incremental backups is not required in the FRA. This configuration can provide cost savings, because lower-cost storage can be used for database backup, without sacrificing system performance.

Using Exadata Storage Expansion Racks to Protect Oracle Database

Using Exadata Storage Expansion Racks for Oracle Database backups provides the highest performance and service levels, and this configuration is the general recommendation for performing Oracle SuperCluster database backups to disk. Oracle Database backup technologies—Oracle RMAN and Oracle Secure Backup—perform especially well on Oracle Exadata with its high-bandwidth InfiniBand network and Oracle Exadata Storage Server grid.

The Oracle Maximum Availability Architecture operational and configuration practices for Oracle Exadata provide the most-comprehensive high availability solution for Oracle Database. The following references provide additional information on Oracle Exadata backup and recovery of Oracle Database:

- “Deploying Oracle Maximum Availability Architecture with Exadata Database Machine,” oracle.com/au/products/database/exadata-maa-131903.pdf
- “Backup and Recovery Performance and Best Practices for Exadata Cell and Oracle Exadata Database Machine,” oracle.com/au/products/database/maa-tech-wp-sundbm-backup-11202-183503.pdf
- My Oracle Support Document 1558851.1, “Oracle Optimized Solution for Secure Backup and Recovery”

- My Oracle Support Document 13549801.1, “Oracle ZFS Storage: FAQ: Exadata RMAN Backup with the Oracle ZFS Storage Appliance”

Best Practices Using Exadata Storage Expansion Racks

General best practices for Oracle SuperCluster configurations using Exadata Storage Expansion Racks include the following:

- Scale backup rates for disk:
  - Use all instances and start with two Oracle RMAN channels per instance.
  - Continue to add an additional two Oracle RMAN channels for performance.
- Utilize the automatic configuration of the Oracle Exadata Storage Server grid disk group layout during deployment for better performance. This approach assigns the faster (outer) 40 percent of the disk to the DATA area and the slower (inner) 60 percent of the disk to the FRA (RECO) area.
- An alternative strategy is to purchase additional serial ATA (SATA) Oracle Exadata storage specifically for storing the FRA. This configuration allows the application to leverage the full Oracle SuperCluster storage grid, allows the use of lower-cost storage for backups, and provides better failure isolation by using separate backup hardware. To reserve more space and bandwidth for the DATA disk group, Oracle recommends using a tape-based backup solution or, at the very least, a hybrid approach where full database backups are written to tape and incremental disk backups are written to the FRA. Note, however, that the FRA should never be placed on Oracle ZFS Storage Appliances. For optimal performance, the FRA should remain on the Oracle Exadata Storage Servers internal to the Oracle SuperCluster or on Exadata Storage Expansion Racks.
- Configure a high-redundancy DATA disk group to contain the Oracle Cluster Registry file, Oracle SuperCluster voting disk, spfiles, data files, redo log groups, and control files for any disk-based backup solution.

Best Practices for Performing Local Disk-Based Backups with Oracle RAC

Scale backup rates written to local disk in the FRA on an Oracle Database Appliance by using an Oracle Real Applications Clusters (Oracle RAC) configuration, as follows:

- Use multiple instances and start with one Oracle RMAN channel per instance.
- Continue to add Oracle RMAN channels for performance per instance. Optimal backup rates were observed with all Oracle RAC instances and one to four Oracle RMAN channels.

Best Practices for Performing Local Disk-Based Backups with Oracle RAC One Node

Scale backup rates written to local disk in the FRA on an Oracle Database Appliance by using a single-instance and Oracle RAC One Node configuration, as follows:

- Start with one Oracle RMAN channel.
- Continue to add Oracle RMAN channels to the single database instance to increase performance. Optimal backup rates were observed with two to four Oracle RMAN channels.

Using Oracle ZFS Storage Appliance to Protect Oracle Database

Oracle ZFS Storage Appliance can be connected with a 10 GbE connection or directly to the InfiniBand network of Oracle SuperCluster to provide a high-performance backup solution for Oracle SuperCluster. Coengineered with Oracle Database, Oracle ZFS Storage Appliance benefits from features such as Oracle Hybrid Columnar Compression and Oracle Intelligent Storage Protocol, which are not available to third-party storage systems. These storage appliances can be specifically tuned for Oracle engineered systems to provide optimum performance.

This solution uses Oracle RMAN with the storage array, eliminating the need for additional backup software or a media server and associated software licenses. License-free data services, including snapshots and compression, reduce costs; and with built-in snapshot and cloning capabilities, Oracle ZFS Storage Appliance can be used for value-added work such as test, development, and quality assurance (QA). Oracle Snap Management Utility for

Oracle Database is supported with Oracle SuperCluster, automating the creation and management of snapshots and clones on Oracle ZFS Storage Appliances.

The QDR InfiniBand fabric provides a direct high-bandwidth connection between Oracle ZFS Storage Appliance and the Oracle SuperCluster InfiniBand backplane. Backup and restore operations can be parallelized, significantly reducing backup and recovery times compared to a traditional NAS storage system. Example testing has shown that Oracle ZFS Storage Appliance can perform a backup of an Oracle SuperCluster T5-8 half-rack configuration at a data rate of up to 14 TB/hour, and it can perform a restore at a data rate of up to 7 TB/hour. Configurations that use 10 GbE network connectivity can provide nearly equal performance to those using InfiniBand connections.

The following references provide additional information on using Oracle ZFS Storage Appliance for backup and recovery of Oracle Database:

- Oracle technical white paper “Configuring an Oracle ZFS Storage ZS3-BA with an Oracle SuperCluster for Oracle Database Backup and Recovery,” oracle.com/technetwork/server-storage/sun-unified-storage/documentation/zs3ba-supercluster-config-2014-2227429.pdf
- My Oracle Support Document 1517107.1, “RMAN Backup from SPARC SuperCluster to Sun ZFS Backup Appliance”
- My Oracle Support Document 1354980.1, “Oracle ZFS Storage: FAQ: Exadata RMAN Backup with the Oracle ZFS Storage Appliance”
- Oracle white paper “NDMP Implementation Guide for the Sun ZFS Storage Appliance,” oracle.com/technetwork/articles/systems-hardware-architecture/ndmp-whitepaper-192164.pdf

Configuring Oracle ZFS Storage Appliance with Oracle SuperCluster

Correct configuration of Oracle ZFS Storage Appliance is required for the best performance of Oracle SuperCluster backups. This section provides an overview of the configuration process. For complete details, see the Oracle technical white paper “Configuring an Oracle ZFS Storage ZS3-BA with an Oracle SuperCluster for Oracle Database Backup and Recovery,” oracle.com/technetwork/server-storage/sun-unified-storage/documentation/zs3ba-supercluster-config-2014-2227429.pdf.

- **Physically connect the Oracle ZFS Storage Appliance**. If InfiniBand connectivity is used, the Oracle ZFS Storage Appliance must be physically connected to each Oracle SuperCluster system’s InfiniBand infrastructure. Both primary and failover paths for Oracle ZFS Storage Appliance must be configured to allow for data availability. Oracle ZFS Storage Appliance can be connected directly to the Oracle SuperCluster InfiniBand switches (if it is the only device connected to the infrastructure), or it can be connected to external InfiniBand leaf switches (if additional appliances or devices will be connected). Once the connections are made, the ports on the Oracle ZFS Storage Appliance must be activated and then configured on the InfiniBand switches.
- **Configure the Oracle ZFS Storage Appliance**. After the storage appliance is physically connected, it must be properly configured. This configuration includes the following tasks:
  - **Set up InfiniBand/10GbE networking**. Key steps for InfiniBand connectivity include configuring the Oracle ZFS Storage Appliance InfiniBand data links; reconfiguring the Oracle SuperCluster InfiniBand switches to include the GUIDs of the Oracle ZFS Storage Appliance InfiniBand HBA ports; and configuring Oracle ZFS Storage Appliance networking for either a single IP connection or active-active IPMP connection (for configurations with external leaf switches).
  - **Configure Oracle ZFS Storage Appliance storage pools**. A pool configuration assigns physical disk drive resources to logical storage pools for backup data storage. To maximize system throughput, configure two equally sized storage pools by assigning half of the physical drives in each drive tray to each storage pool.
- **Use Oracle Engineered Systems Backup Utility for Oracle ZFS Storage Appliance**. Lastly, the Oracle Engineered Systems Backup Utility for Oracle ZFS Storage Appliance is run to complete the configuration on the Oracle Solaris 11–based Oracle Database 11*g* Release 2 database server nodes. This tool, which can be used to configure the Oracle ZFS Storage Appliance that is internal to the Oracle SuperCluster and any additional

external Oracle ZFS Storage Appliance for backup, verifies the system configuration and automates the necessary configuration steps, including the following:

- Configuring Oracle ZFS Storage Appliance. This includes creating a project and shares for Oracle RMAN.
- Configuring the Oracle SuperCluster database nodes. This includes enabling direct NFS (dNFS), creating mount points, and adding backup services.
- Creating the final Oracle RMAN scripts. (Note: The Oracle RMAN run block scripts are intended for samples only, and should be reviewed and modified as necessary to meet site-specific requirements.)

Although these configuration steps can be performed manually, use of the Oracle Engineered Systems Backup Utility is recommended to reduce the risk of accidental misconfiguration.

The Oracle Engineered Systems Backup Utility for Oracle ZFS Storage Appliance can be downloaded from the Oracle ZFS Storage Appliance Plug-in Downloads web page, oracle.com/technetwork/server-storage/sun-unified-storage/downloads/zfssa-plugins-1489830.html.

Recommended Best Practices for Database Backup and Restore Using Oracle ZFS Storage Appliance

Oracle recommends using a combination of level-0 and level-1 backup sets when backing up Oracle Database to the internal Oracle ZFS Storage Appliance. The frequency of backups is dictated by recovery time objectives (RTOs) and recovery point objectives (RPOs). Note that when using Oracle ZFS Storage Appliance, Oracle recommends testing an incrementally updated backup strategy using a combination of data file copies and incremental backup sets that are subsequently merged into the data file copies before deployment into production. When an incrementally updated backup strategy is selected, the backup solution becomes I/O bound during the merge process, and alleviating this bottleneck requires a significant number of available disk spindles in order to achieve the required IOPS rate.

For most IT departments, the following recommendations should be sufficient:

- The Oracle Database FRA should remain on the Oracle Exadata Storage Servers that are part of Oracle SuperCluster and should not be put on Oracle ZFS Storage Appliance.
- The weekly full level-0 backup should be written to Oracle ZFS Storage Appliance.
- A daily incremental level-1 backup should be written to Oracle ZFS Storage Appliance. A maximum of 16 Oracle RMAN channels should be allocated and configured for both weekly level-0 and daily level-1 backups to write to one of the 16 Oracle ZFS Storage Appliance shares created using the Oracle Engineered Systems Backup Utility (or created manually).
- Two separate backup jobs should be submitted if Oracle RMAN compression is used to preserve space on Oracle ZFS Storage Appliance but the database consists of a mixture of uncompressed data and compressed data or data that cannot be compressed further. One of the backup jobs will create an uncompressed backup, and the second will create a compressed backup. Otherwise, compressing data that does not typically yield good compression ratios lengthens the backup window significantly, consumes unnecessary CPU resources, and results in very little space savings.
- Oracle RMAN offers an option to amortize the backup over a given time period and minimize the performance impact to critical applications (the Oracle RMAN `BACKUP DURATION` command with the `MINIMIZE LOAD` option). For example, if there is an eight-hour backup window available for the weekly level-0 backup of a 20 TB database, but critical database functions are still running during that backup window, Oracle RMAN can spread the work over the entire backup window.
- The use of Oracle RMAN options such as `sectionsize` is recommended. These options are included in the backup scripts generated by the Oracle Engineered Systems Backup Utility. The `sectionsize` parameter breaks `BIGFILE` tablespaces into more manageable amounts. Oracle recommends that the largest tablespaces be broken into equal sized sections for each Oracle RMAN channel. For instance, if there are two tablespaces of 10 TB and 14 TB, and there are 16 Oracle RMAN channels, the `sectionsize` parameter should be set to approximately 320 GB.

- The Oracle Engineered Systems Backup Utility does not enable Oracle RMAN or Oracle ZFS Storage Appliance compression, because this capability is dependent on the data to be backed up and the database licensing options purchased. Enabling Oracle RMAN compression increases CPU utilization.
- Although use of the Oracle ZFS Storage Appliance that is internal to the Oracle SuperCluster is supported, using an external Oracle ZFS Storage Appliance is a recommended best practice. Backups inherently consume bandwidth and latency. If the internal storage appliance is used, response time of other executables reading and writing to this storage will be impacted during backup and recovery. Regardless of the storage appliance model that is used, the Oracle Engineered Systems Backup Utility should be used to do the final configuration.

Using Tape to Protect Oracle Database

Tape-based backups provide cost-effective data protection for Oracle SuperCluster. Tape backups employ the lowest-cost tape storage media, which is ideal for older backup copies and long-term data retention. Oracle's StorageTek tape libraries and Oracle's StorageTek tape drives work in combination with InfiniBand fabric to provide a high-performance, cost-effective tape-based backup solution for Oracle SuperCluster (see Figure 5). Oracle Optimized Solution for Oracle SuperCluster Backup and Recovery is software agnostic, and it supports the use of Oracle Secure Backup, Symantec NetBackup, and other third-party backup software.

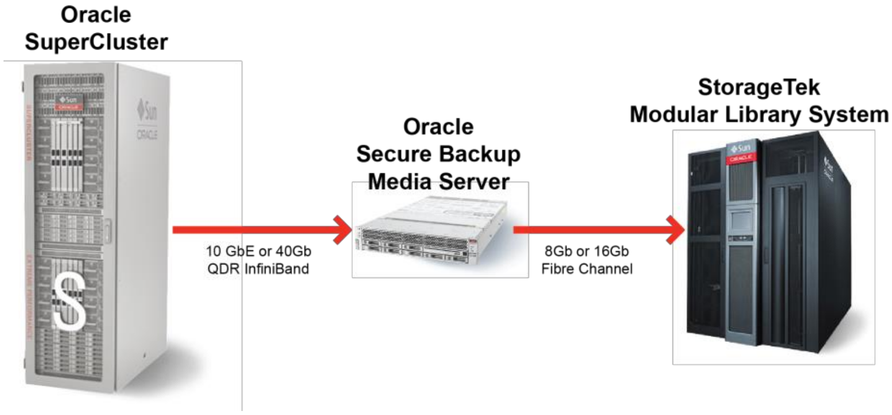
Oracle SuperCluster
Oracle Secure Backup Media Server
StorageTek Modular Library System
10 GbE or 40Gb QDR InfiniBand
8Gb or 16Gb Fibre Channel

Figure 5. Oracle SuperCluster uses backup and recovery software such as Oracle Secure Backup to perform tape-based backups.

Backup and Recovery Software

Organizations have a choice of backup and recovery software with Oracle Optimized Solution for Secure Backup and Recovery on Oracle SuperCluster. However, Oracle recommends using Oracle Secure Backup for low-cost, fast tape backups. This tape management software component from Oracle carries a low-cost, one-time software licensing fee per tape drive, resulting in significant savings over the cost of most competing products. Oracle Secure Backup provides the fastest database backup to tape due to its tight integration with Oracle products, including Oracle RMAN and Oracle Database. Using Oracle Secure Backup enables the unused-block optimization capability. However, if the backup is made directly to tape using a third-party media management product, this capability does not have any effect, because unused-block optimization is available only with Oracle Secure Backup.

Media management software such as Oracle Secure Backup uses a client/server architecture with one administrative server, one or more media servers, and the backup clients. Any server in the domain can act as the administrative server. Note, however, that the media server cannot be configured on Oracle SuperCluster itself; a separate server must be configured. Although installing backup software on Oracle SuperCluster is permitted and necessary, installing additional hardware (such as Fibre Channel cards on an Oracle SuperCluster database node) is not supported. All Oracle SuperCluster backups to tape must use the InfiniBand or 10 GbE network connections through a separate media server to the tape library.

Although Figure 5 shows a single media server, multiple media servers can be used for increased performance. A single server can be used for both the administrative server and media server roles; however, for optimal performance and availability, these roles should not be provided by a single server. Oracle's x86-based systems and Oracle's SPARC servers are recommended as administrative and media servers because of their I/O bandwidth, performance, and scalability.

Database Best Practices for Tape-Based Backups

In addition to the general best practices for Oracle Database backups, best practices for tape-based backups include the following:

- Keep the number of archive logs to a minimum to avoid adversely impacting backup rates.
- Remember that heavy loads on an active database and fully consumed CPUs will affect backup rates.
- Configure persistent bindings for tape devices. It is very important that the environment maintains consistent device addresses.
- Perform daily backups of the Oracle Secure Backup or third-party backup and recovery software catalog. This catalog maintains backup metadata, scheduling, and configuration details for the backup domain, and should be backed up on a regular basis. For more information, see My Oracle Support Document 1558851.1.
- Configure one Oracle RMAN channel per tape drive and add tape drives to scale backup rates. Backup performance scales when more tape drives and Oracle RMAN channels are added, assuming there is available throughput on the media server.
- Configure dedicated 10 gigabit Ethernet (GbE) or InfiniBand. Using a dedicated interface for the transport eliminates the impact on the client access network. Use InfiniBand for the best backup rates, especially for larger databases that require fast backup rates and low CPU overhead. When not using InfiniBand, use 10 GbE.
- Configure an Oracle RAC service for backups running on all database instances. This step reduces CPU utilization on the database and media server nodes and load balances the backups.
- Use SQL*Net service load balancing to distribute Oracle RMAN channels evenly among the allocated instances.

More Information

For more information on tape backups, see the Oracle white paper "Protecting SPARC SuperCluster—Tape Backup with Symantec NetBackup," oracle.com/technetwork/server-storage/sun-tape-storage/documentation/o13-016-1900890.pdf.

Disk-to-Disk-to-Tape Backups

The disk-to-disk-to-tape approach first backs up data to disk and then copies the data to tape, providing the combined advantages of both disk and tape backups. As with tape-only backups, disk-to-disk-to-tape backups in Oracle SuperCluster are software agnostic: Oracle Secure Backup, Symantec NetBackup, and other third-party backup software are supported. When not using Oracle Secure Backup, additional licensing might be required for third-party backup software.

There are two general methods for performing disk-to-disk-to-tape backups. The first method uses Oracle RMAN to first perform a database backup to Oracle ZFS Storage Appliance or Exadata Storage Expansion Rack (see Figure 6). The administrator then uses Oracle RMAN to perform a `backup BACKUPSET`, which copies the backup set from disk to tape. Oracle Secure Backup or third-party backup and recovery software such as Symantec NetBackup handles the tape management portion of the backup. Oracle RMAN can restore the database from either disk or tape in a single restore process. (Note: the Oracle Engineered Systems Backup Utility tool does not create example disk-to-disk-to-tape scripts. Details on making copies of the backup sets from disk to tape can be found in the Oracle RMAN documentation.)

With this approach, Oracle RMAN is aware of all backups and manages the retention periods for all backups. For example, Oracle RMAN can set tape retention periods for all tape backups, and then each day delete obsolete backups from disk based on the number of days of backups that should be retained. This method does push the data through the database server twice. However, the process of database servers performing a `backup BACKUPSET` operation is not resource intensive; therefore, this method has a very low impact on CPU utilization and I/O bus traffic, and it does not significantly affect database performance.

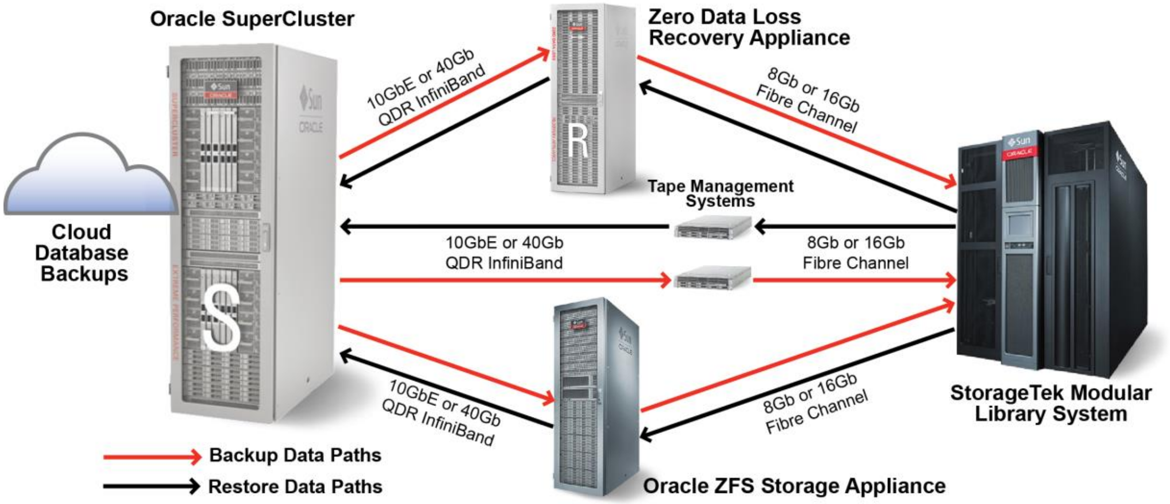
Oracle SuperCluster
Zero Data Loss Recovery Appliance
10GbE or 40Gb QDR InfiniBand
8Gb or 16Gb Fibre Channel
Cloud Database Backups
Tape Management Systems
10GbE or 40Gb QDR InfiniBand
8Gb or 16Gb Fibre Channel
10GbE or 40Gb QDR InfiniBand
8Gb or 16Gb Fibre Channel
StorageTek Modular Library System
Backup Data Paths
Restore Data Paths
Oracle ZFS Storage Appliance

Figure 6. Disk-to-disk-to-tape backups with Oracle RMAN.

The second method for disk-to-disk-to-tape backup first uses Oracle RMAN to perform a database backup to an Oracle ZFS Storage Appliance, and then it uses Network Data Management Protocol (NDMP) to back up the Oracle ZFS Storage Appliance to tape (see Figure 7). With this method, it is not necessary for the data to be pushed back through the database server during the NDMP process. The downside of this method, however, is that Oracle RMAN is not aware of all the copies, because Oracle RMAN is not used to back up the Oracle ZFS Storage Appliance to tape.

When using this second method, restoring backup data requires an intermediate step. The administrator must first restore the backup from tape to the Oracle ZFS Storage Appliance, and then use Oracle RMAN to restore the data from there back to the database. This procedure can take a long time if the database is very large, and it requires sufficient available space on the Oracle ZFS Storage Appliance. The frequency and time sensitivity of restores from tape should be considered when choosing this backup method.

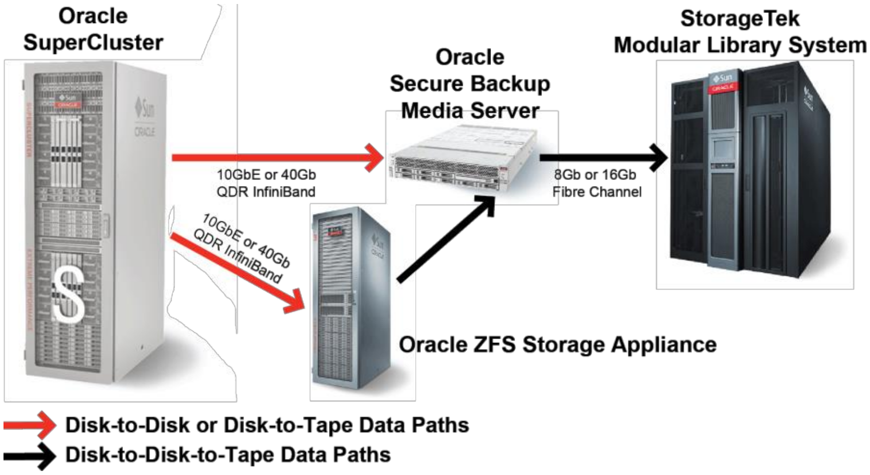
Oracle SuperCluster
Oracle Secure Backup Media Server
StorageTek Modular Library System
10GbE or 40Gb QDR InfiniBand
8Gb or 16Gb Fibre Channel
10GbE or 40Gb QDR InfiniBand
Oracle ZFS Storage Appliance
Disk-to-Disk or Disk-to-Tape Data Paths
Disk-to-Disk-to-Tape Data Paths

Figure 7. Disk-to-disk-to-tape backups using NDMP.

Both methods of disk-to-disk-to-tape backup are supported in Oracle Optimized Solution for Secure Backup and Recovery on Oracle SuperCluster. Each approach has its advantages and might be preferred for certain scenarios (see Table 2). The choice of method should take the database characteristics and recovery requirements into account. For example, if tape backups are performed primarily for archive and compliance reasons and restoration from tape is expected to occur rarely, the second method using NDMP to perform tape backups might be preferred for its simplicity and reduced load on the database servers during backup. Conversely, if a fast recovery option from tape is required, the first method using Oracle RMAN to copy the backup set to tape might be the better choice.

TABLE 2. DISK-TO-DISK-TO-TAPE BACKUP OPTIONS

Method	Advantages	Disadvantages
1. Oracle RMAN database backup to Oracle ZFS Storage Appliance or Exadata Storage. 2. Use Oracle RMAN to copy backup set from disk to tape.	» Faster and easier to restore from tape (can restore directly from tape) » Oracle RMAN aware of all copies of the backup set	» Additional load on database servers when performing tape backup
1. Oracle RMAN database backup to Oracle ZFS Storage Appliance. 2. Use NDMP to back up the Oracle ZFS Storage Appliance to tape.	» No additional load on database servers when performing tape backup	» Requires two-step procedure to restore from tape » Longer recovery time from tape » Oracle RMAN catalog would not be updated by the NDMP backup of the backup set files on the Oracle ZFS Storage Appliance

Offload Database Backups with Data Guard

Data Guard—a feature included in Oracle Database, Enterprise Edition—is the recommended disaster recovery solution to protect mission-critical databases residing on Oracle SuperCluster. Data Guard physical standby databases support all Oracle data types and features, including Exadata Hybrid Columnar Compression, and they are able to support the very high transaction volume driven by Oracle SuperCluster.

Data Guard standby databases are also used to offload backups from a primary production database. Both disk-based and tape-based backups can be performed using a physical standby database. Oracle Active Data Guard, a priced option that extends Data Guard functionality, can be used to offload fast incremental backups

(Oracle RMAN block change tracking), further reducing backup times and the impact on the primary database. Additional benefits of Oracle Active Data Guard include offloading read-only queries and reports from the primary database to a synchronized physical standby database and performing automatic block repair if the software detects a block corruption. All Data Guard standby databases can also be used to detect lost write corruptions and for database rolling upgrades and other maintenance while also providing disaster protection.

For more information, please see the Oracle white paper “Oracle Data Guard: Disaster Recovery for Oracle Exadata Database Machine” at oracle.com/technetwork/database/features/availability/maa-wp-dr-dbm-130065.pdf. The Oracle web site oracle.com/solutions/optimized-solutions/disaster-recovery also provides additional information.

Oracle’s Zero Data Loss Recovery Appliance

Oracle’s Zero Data Loss Recovery Appliance—an engineered system for database backup that eliminates data loss exposure without impacting the performance of production environments—is an option that should be considered when traditional backup and recovery approaches are not sufficient to meet enterprise requirements. Compute, network, and storage are integrated into a massively scalable appliance with a cloud-scale architecture that provides fully automated database backup and recovery for multiple databases.

Featuring an incremental-forever backup strategy, the Recovery Appliance provides minimal impact backups. The databases send only changes, and all backup and tape processing is offloaded from the production servers to the appliance for improved system performance. Real-time database redo block information is transmitted, eliminating potential data loss and providing instant protection of new transactions. Database recoverability is improved with end-to-end reliability, visibility, and control of the database as a whole, rather than as a disjoint set of files.

Zero Data Loss Recovery Appliance is a complementary technology to other backup and recovery options such as Oracle ZFS Storage Appliance and Oracle Active Data Guard. For example, an enterprise backup and recovery solution could use Zero Data Loss Recovery Appliance to provide a centralized backup service for all databases, use the snapshot and cloning capabilities of Oracle ZFS Storage Appliance for development/test environments, and use Oracle Active Data Guard to provide fast failover capabilities for critical databases.

Oracle Secure Backup Cloud Module

Oracle Secure Backup Cloud Module provides the flexibility to back up databases to cloud-based storage services offered by Amazon Simple Storage Service (Amazon S3). It is compatible with Oracle Database version 9*i* Release 2 and later. Oracle Secure Backup Cloud Module is implemented using the Oracle RMAN System Backup to Tape (SBT) interface, which enables external backup libraries to be seamlessly integrated with Oracle RMAN. With this cloud offering, local disk backups are sent directly to Amazon S3 for offsite storage and are fully integrated with Oracle RMAN.

Oracle Secure Backup Cloud Module provides the following advantages over traditional offsite tape-based backups:

- **Continuous accessibility.** Backups stored in the cloud are always accessible—in much the same way local disk backups are. As such, there is no need to call anyone and no need to ship or load tapes before a restore can be performed. Administrators can initiate restore operations using their standard tools (Oracle Enterprise Manager, scripts, and so on) exactly as if the offsite backup were stored locally. This process can restore data faster and reduce downtime from days to hours or even minutes in many cases.
- **Better reliability.** Storage clouds are disk-based and, thus, inherently more reliable than tape media. Additionally, cloud vendors typically keep multiple redundant copies of data for availability and scalability purposes.
- **Cost savings**. Cloud storage backups can reduce or eliminate upfront capital expenditures, as well as tape backup licensing and offsite storage costs.

Securing data, especially when stored off premises, is critical. To ensure data is properly secured, Oracle RMAN backup encryption is recommended as a standard part of the cloud-based backup process.

Provide Efficiency Savings and High Availability with Remote DR Sites

Figure 8 shows the ultimate solution for providing the ability to restore IT operations while spending less for backup and recovery. Traditional solutions require expensive backup and recovery equipment to restore the production system as quickly as possible. An alternative solution is to have a second, remote site with replicated applications and data. Using a primary site and a remote secondary sites eliminates the need for high-performance systems to recover production operations. Instead of deploying Oracle SuperCluster and a high-performance disk array to back it up, a secondary Oracle SuperCluster with lower cost Oracle ZFS Storage Appliance or tape can be deployed. In the event of a failure, production can be switched over immediately to the remote site. The primary site's recovery time is irrelevant because production continues on the secondary systems. This approach provides better business continuance and results in significant savings because backup and recovery system costs are lower.

When not running production operations as part of a business continuance effort, the remote replicated location can be used for testing, development, and other functions. The ability to generate reports from a copy of the secondary site's production database—a capability for which Oracle continues to add support—enables IT staff to offload work from the production system and keep the secondary database current. This solution provides savings for backup and recovery and maximizes system availability. Many organizations distribute their recovery systems in this manner, with applications that can fail over from city to city. In fact, this design can be used almost universally, with the exception of firms that are required to have large and elaborate backup and recovery systems for compliance reasons.

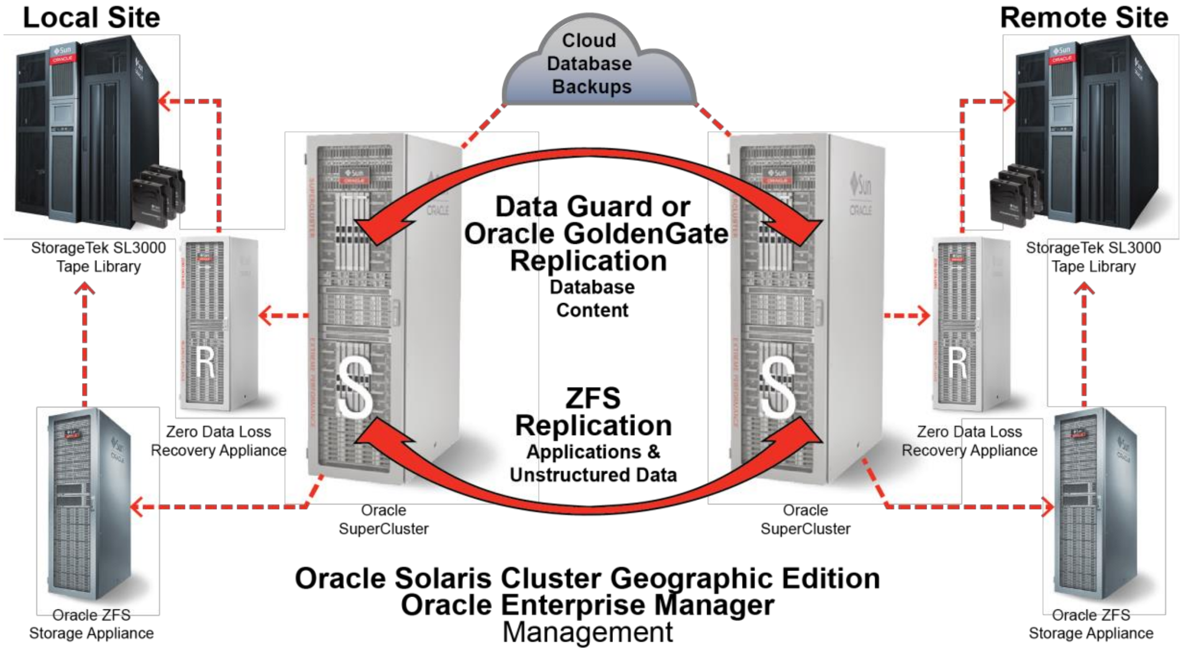
Local Site
Remote Site
Cloud Database Backups
StorageTek SL3000 Tape Library
StorageTek SL3000 Tape Library
Data Guard or Oracle GoldenGate Replication
Database Content
ZFS Replication
Applications & Unstructured Data
Zero Data Loss Recovery Appliance
Zero Data Loss Recovery Appliance
Oracle SuperCluster
Oracle SuperCluster
Oracle ZFS Storage Appliance
Oracle ZFS Storage Appliance
Oracle Solaris Cluster Geographic Edition
Oracle Enterprise Manager
Management

Figure 8. Oracle technologies enable maximum protection plus cost savings.

Best Practices for Secure Backup and Recovery Implementation

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

Oracle highly recommends leveraging existing recommendations and guidelines from product security guides, Center for Internet Security (CIS) benchmarks, ISACA publications, and Department of Defense (DoD) Security Technical Implementation Guides (STIGs) when designing a backup and recovery environment.

Security Technical Implementation Guides

STIGs are continually updated and currently available for many Oracle products. A list of STIGs relevant to this solution is shown in Table 3.

TABLE 3. EXAMPLES OF RELEVANT STIGS

STIG	Location
Oracle Solaris	iase.disa.mil/stigs/os/unix-linux/Pages/solaris.aspx
Oracle Database 11*g* Release 2	iasecontent.disa.mil/stigs/zip/Apr2015/U_Oracle_Database_11-2g_V1R3_STIG.zip
Oracle Integrated Lights Out Manager	iase.disa.mil/stigs/app-security/database/Pages/exadata_lights.aspx
Oracle Exadata Storage Server	iase.disa.mil/stigs/app-security/database/Pages/exadata_storage.aspx
Oracle's Sun Datacenter InfiniBand Switch 36	iase.disa.mil/stigs/app-security/database/Pages/exadata_infiniband.aspx
Oracle ZFS Storage Appliance	iase.disa.mil/stigs/app-security/database/Pages/exadata_zfs.aspx
Oracle WebLogic Server 12*c*	iase.disa.mil/stigs/Documents/u_oracle_weblogic_server_12c_v1r1_stig.zip
DoD Secure Telecommunications	iase.disa.mil/stigs/net_perimeter/telecommunications/Pages/index.aspx
Oracle Linux 6 Manual STIG	iasecontent.disa.mil/stigs/zip/Apr2015/U_Oracle_Linux_6_V1R2_STIG.zip
Storage Area Network (SAN)	iase.disa.mil/stigs/Documents/u_storage_area_network_v2r2_stig.zip

For more STIGs, please see the website iase.disa.mil/stigs/Pages/index.aspx.

Component-Level Security Recommendations

Oracle recommends the following component-level security guidelines.

- **Change system default passwords.** Using known vendor-provided default passwords is a common way cyber criminals gain unauthorized access to infrastructure components. Changing all default passwords to stronger, custom passwords is a mandatory step during infrastructure deployment.
- **Keep component patching current.** Ensure that all components are using the most recent firmware and software versions to the extent possible. This tactic ensures that each component is protected by the latest security patches and vulnerability fixes.
- **Leverage isolated, purpose-based network interfaces** Network interfaces, virtual or physical, should be used to separate architectural tiers, such as client access and management. In addition, consider using network interfaces to separate tiers within a multitier architecture. This enables per-tier security policy monitoring and

enforcement mechanisms including network, application, and database firewalls as well as intrusion detection and prevention systems.

- **Enable encrypted network communications.** Ensure all endpoints use encrypted network-based communications, including secure protocols, algorithms, and key lengths. For Oracle WebLogic, use the UCrypto provider to ensure that cryptography leverages the hardware assist capabilities of the SPARC platform.
- **Enable encrypted data-at-rest protections.**
  - Use encrypted swap, `/tmp`, and ZFS data sets for any locations that could potentially house sensitive or regulated data. This automatically takes advantage of cryptographic acceleration in Oracle Solaris.
  - Use tape drive encryption to protect data that must leave the data center for off-site storage.
  - For databases, use Transparent Data Encryption (TDE) to protect tablespaces that might store sensitive or regulated data. TDE automatically takes advantage of cryptographic acceleration in Oracle Solaris on SPARC systems.
- **Secure the database.** Refer to Oracle Optimized Solution for Secure Oracle Database security best practices and recommendations.
- **Deploy application services in Oracle Solaris non-global zones.** Deploying applications within Oracle Solaris non-global zones has several security advantages, such as kernel root kit prevention, prevention of direct memory and device access, and improved control over security configuration (via `zonecfg(1M)`). This approach also enables higher assurance auditing, because audit data is not stored in the Oracle Solaris non-global zone, but rather in the Oracle Solaris global zone.
- **Implement a baseline auditing policy.** Use audit logs and reports to track user activity—including individual transactions and changes to the system—and to flag events that fall out of normal parameters. These should be implemented at both the Oracle Solaris and database levels. The baseline security audit policy should include login/logout activity, administrative actions, and security actions, as well as specific command executions for Oracle Solaris. This tactic enables auditing of a core set of security critical actions without overburdening the system or database.
- **Follow the rule of least privilege**. Increase access control by granting only those privileges that a given individual needs. This should be implemented at both the ERP system level and the infrastructure level.
- **Use strong authentication.** Many intellectual property attacks use stolen credentials. Implementing strong authentication methods, such as Kerberos, RADIUS, and SSL, can help prevent unauthorized access.
- **Leverage role-based access control.** As the number of applications and users increases, user-based identity management can quickly become time consuming and labor intensive for IT staff. Consequentially, many users are granted inappropriate authorities. Though it requires increased efforts during the design and implementation phases, role-based access control (RBAC) is a popular option for low-maintenance, scalable access control, and it can help alleviate the burden of identity management.

Table 4 lists Oracle SuperCluster security recommendations. A full list of relevant component security recommendations is shown in Table 5.

TABLE 4. ORACLE SUPERCLUSTER SECURITY RECOMMENDATIONS

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

TABLE 5. EXAMPLES OF COMPONENT SECURITY RECOMMENDATIONS

Resource	Location
Oracle Solaris 11 Security Guidelines	docs.oracle.com/cd/E36784_01/html/E36837/index.html
Oracle Solaris 11.2 Security Compliance Guide	docs.oracle.com/cd/E36784_01/pdf/E39067.pdf
“Secure Deployment of Oracle VM Server for SPARC”	oracle.com/technetwork/articles/systems-hardware-architecture/secure-ovm-sparc-deployment-294062.pdf
Oracle Solaris Cluster Security Guide	docs.oracle.com/cd/E39579_01/html/E39649/index.html
“User Authentication on the Solaris OS: Part 1”	oracle.com/technetwork/server-storage/solaris/user-auth-solaris1-138094.html
Oracle ILOM Security Guide	docs.oracle.com/cd/E37444_01/html/E37451/index.html
Database Advanced Security Administrator's Guide	docs.oracle.com/cd/E11882_01/network.112/e40393/toc.htm
“Oracle Database 12*c* Security and Compliance”	oracle.com/technetwork/database/security/security-compliance-wp-12c-1896112.pdf
“Best Practices for Deploying Encryption and Managing Its Keys on the Oracle ZFS Storage Appliance”	oracle.com/technetwork/server-storage/sun-unified-storage/documentation/encryption-keymgr-1126-2373254.pdf
Securing the Network in Oracle Solaris 11.2	docs.oracle.com/cd/E36784_01/html/E36838/index.html
Securing Users and Processes in Oracle Solaris 11.2	docs.oracle.com/cd/E36784_01/html/E37123/index.html
Securing Systems and Attached Devices in Oracle Solaris 11.2	docs.oracle.com/cd/E36784_01/html/E37121/index.html
Securing Files and Verifying File Integrity in Oracle Solaris 11.2	docs.oracle.com/cd/E36784_01/html/E37122/index.html
Managing Encryption and Certificates in Oracle Solaris 11.2	docs.oracle.com/cd/E36784_01/html/E37124/index.html
Developer's Guide to Oracle Solaris 11 Security	docs.oracle.com/cd/E36784_01/html/E36855/index.html
“Configuring Oracle GoldenGate Security”	docs.oracle.com/goldengate/1212/gg-winux/GWUAD/wu_security.htm#GWUAD354
“Managing Security for Backup Networks”	docs.oracle.com/cd/E26569_01/doc.104/e21477/network_security.htm#OBINS277
Oracle Key Manager documentation library	docs.oracle.com/cd/E26076_02/index.html

Backup Schedules

When planning backup schedules for Oracle SuperCluster, both bare-metal backups and day-to-day backups must be considered.

Bare-metal backups enable the entire Oracle SuperCluster to be recovered from a “bare metal” state. These backups can be performed less frequently than day-to-day backups: typically monthly and after significant changes to the configuration. A complete bare-metal backup includes the following:

- Backups of the Oracle SuperCluster configuration (performed by the `osc-backup` tool)
- Unstructured data stored in the internal Oracle ZFS Storage Appliance (applications and Oracle Solaris Zones with iSCSI root drives)
- Databases stored on internal Oracle Exadata storage or on external storage

Day-to-day backups are performed regularly to provide ongoing protection for Oracle SuperCluster. In general, it is recommended to perform either two full backups and five incremental backups, or one full backup and six incremental backups, each week. These day-to-day backups include the following:

- Operating systems in physical domains (PDoms), logical domains (LDoms), and Oracle Solaris Zones
- Unstructured data stored in the internal Oracle ZFS Storage Appliance: `osc-backup` tool backups, applications, and Oracle Solaris Zones with iSCSI root drives
- Databases using internal Oracle Exadata storage and external storage

Recommended Backup Schedule for Oracle SuperCluster

Figure 9 shows the recommended monthly backup schedule for Oracle SuperCluster. A full system (bare-metal) backup—including the Oracle SuperCluster configuration, unstructured data stored on the internal Oracle ZFS Storage Appliance, and databases—is performed once a month. Daily backups—including the operating system, unstructured data stored on the internal Oracle ZFS Storage Appliance, and databases—are performed on the remaining days of the month. Each week, two full and five incremental daily backups are performed.

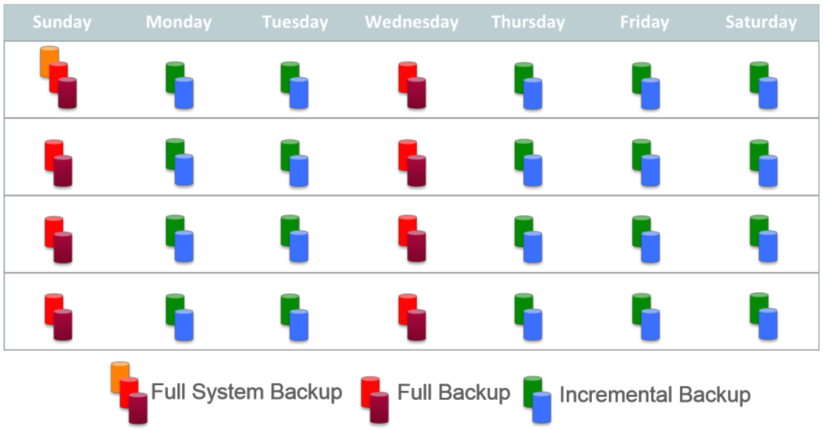

Figure 9. The recommended backup schedule includes a monthly full system backup and a mix of full and incremental daily backups.

An alternative backup schedule for Oracle SuperCluster is shown in Figure 10. This schedule is essentially the same as the previous schedule, with a single full system (bare-metal) backup each month and a mix of full and incremental daily backups. However, in this schedule only one full daily backup is performed per week. On the remaining days of the week, an incremental daily backup is performed.

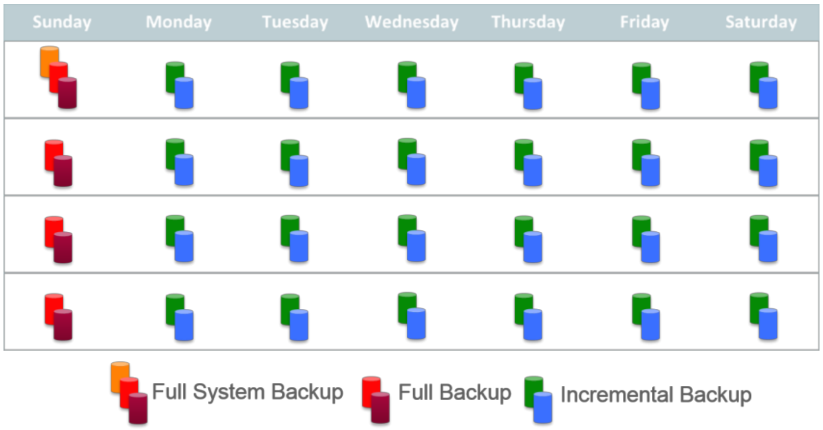

Figure 10. Alternative backup schedule with maximum incremental backups.

The backup schedule used for Oracle SuperCluster will depend on the specific backup and recovery requirements for that deployment. Full backups are more time consuming and space intensive than incremental backups, but they simplify restoration: Only the full backup file is required to restore the system, making restoration faster and simpler. On average, Oracle SuperCluster customers are reporting backup speeds that are five times faster than previous backups. This performance improvement enables more full backups to be performed each month.

Incremental backups are faster and less space intensive than full backups. However, during restoration, each incremental backup since the last full backup must be processed, lengthening the restoration process. Having fewer incremental backups simplifies the restoration process. Oracle does not recommend stretching incremental backups for more than seven days between full backups.

Monitoring and Troubleshooting

Monitoring and troubleshooting capabilities can help if a problem arises. There are several areas for which monitoring provides valuable insight into backup problems.

» Monitoring the media server and client operating systems

For Oracle Solaris and Oracle Linux, use the monitoring tools that are built into the operating system to monitor the system, whether it is a media server or a client. Please see My Oracle Support Document 1558851.1 for more details.

» Monitoring Oracle ZFS Storage Appliances

To monitor Oracle ZFS Storage Appliances, use the Oracle ZFS Storage Appliance analytics feature to monitor the network, block and file protocols, CPU, cache, and physical disk analytics. Please see My Oracle Support Document 1558851.1 for more details.

» Monitoring StorageTek tape devices

Oracle's StorageTek Tape Analytics Software simplifies tape storage monitoring and troubleshooting, taking a proactive approach to eliminate library, drive, and media errors through an intelligent monitoring application.

» Monitoring Oracle RMAN

When the Oracle RMAN job is executed, the job transcript is written to `stdout` by default, but the output can be redirected to a log file that can be analyzed for errors and warnings. The log file can also be used to review backup piece names that are written to. Additionally, Oracle RMAN uses the `NLS_DATE_FORMAT` environment variable to report times in hours, minutes, and seconds, which is a useful feature when monitoring run times.

- Monitoring and troubleshooting Oracle Secure Backup

  The particular backup problem that is reported determines where to begin troubleshooting. If the problem concerns primary Oracle Secure Backup resources, look at the following:

  - The backup and restore job transcript and job properties
  - Daemon (process) logs
  - Device logs

  If the problem concerns external environmental areas, then do the following:

  - Review the operating system configuration settings
  - Confirm that the Oracle Secure Backup user has the correct operating system privileges to perform backup and restore operations
  - Confirm that the tape device is accessible to the host

- Monitoring TCP/IP traffic

  Oracle Secure Backup sends data across the TCP/IP stack. To verify backup rates, view output from the `sar` command in real time or historically to see the data transfer rates achieved between the database servers and the media servers.

Key Performance Observations and Backup and Restore Rates

Example testing by Oracle engineers has demonstrated that the combination of an Oracle SuperCluster protected by an Oracle ZFS Storage Appliance is capable of backing up an Oracle Database 11*g* Release 2 database at a rate of 14.06 TB per hour. This testing was performed on Oracle's SPARC SuperCluster T4-4 half-rack configuration, with two SPARC T4-4 compute nodes and three Exadata Storage Server X3-2 servers. Restore operations for that same database achieved rates of 5.16 TB per hour. Performance of newer Oracle SuperCluster models is expected to easily exceed these example test results in many environments.

Oracle ZFS Storage Appliance can be specifically tuned for the backup and recovery of Oracle engineered systems such as Oracle SuperCluster. When used with Oracle RMAN and other backup and recovery software, Oracle ZFS Storage Appliance safeguards against data corruption. The appliance can be directly connected to the Oracle SuperCluster's built-in InfiniBand fabric, delivering extremely fast backup and restore throughputs for narrow backup windows, and meeting recovery time objectives by providing timely recovery in the event of a disaster.

The Oracle RMAN configuration that was found by Oracle engineers to deliver the best all-around performance consisted of eight file systems on the Oracle ZFS Storage Appliance with four Oracle RMAN channels allocated per file system (for a total of 32 channels). Additional performance improvements can be achieved by the following:

- Using a database that has a tablespace that comprises an even number of data files divisible by the number of channels to be used.
- Using an Oracle Automatic Storage Management configuration with standard redundancy for the database storage. This step increases the number of disk spindles while reducing the performance penalty caused by configuring additional redundancy.
- Adding an Exadata Storage Expansion Rack to increase the number of disk spindles.

For up-to-date details on performance, please see My Oracle Support Document 1558851.1, "Oracle Optimized Solution for Secure Backup and Recovery."

Connecting Backup and Recovery Devices to Oracle SuperCluster

There are four common scenarios for connecting backup and recovery devices to Oracle SuperCluster:

- Multiple 10 GbE links
- Multiple 40 Gb InfiniBand links
- A hybrid of multiple 10 GbE and 40 Gb InfiniBand links
- Shared storage for two InfiniBand fabrics

These common scenarios are briefly described in the following sections. For details on external device connectivity, see the *Oracle SuperCluster Administration Guide*.

Multiple 10 GbE Links

In this scenario, multiple 10 GbE links are used to provide sufficient network bandwidth over an external data center network to external disk and tape resources for backup and recovery (see Figure 11). Using multiple 10 GbE links provides nearly equal performance to using InfiniBand connections. This scenario simplifies the connection of multiple engineered systems to a single backup and recovery infrastructure. In addition, this configuration provides less shared infrastructure between production systems and backup and recovery systems.

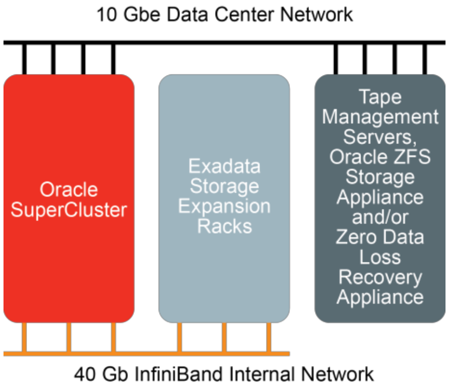
10 Gbe Data Center Network
Oracle SuperCluster
Exadata Storage Expansion Racks
Tape Management Servers, Oracle ZFS Storage Appliance and/or Zero Data Loss Recovery Appliance
40 Gb InfiniBand Internal Network

Figure 11. Connecting backup and recovery devices with multiple 10 GbE links.

Multiple 40 Gb InfiniBand Links

In this scenario, multiple 40 Gb InfiniBand links are used to directly connect external disk and tape resources for backup and recovery (see Figure 12). Solutions that require only external disk or tape (but not both) generally have sufficient free InfiniBand ports on the Oracle SuperCluster and can connect directly to these backup devices using these ports. Solutions that require both external InfiniBand disk and tape devices must use external InfiniBand switches. Adding external InfiniBand switches adds up to 72 more InfiniBand ports for multiple device connections; however, these ports are only supported for backup and recovery uses.

This configuration provides the highest performing connectivity to external disk and tape for backup and recovery, and it offloads tremendous amounts of backup and recovery traffic from the corporate network infrastructure. This is also the connectivity solution that is most integrated with remote direct memory access (RDMA), Hybrid Columnar Compression, and other technologies built only for Oracle hardware.

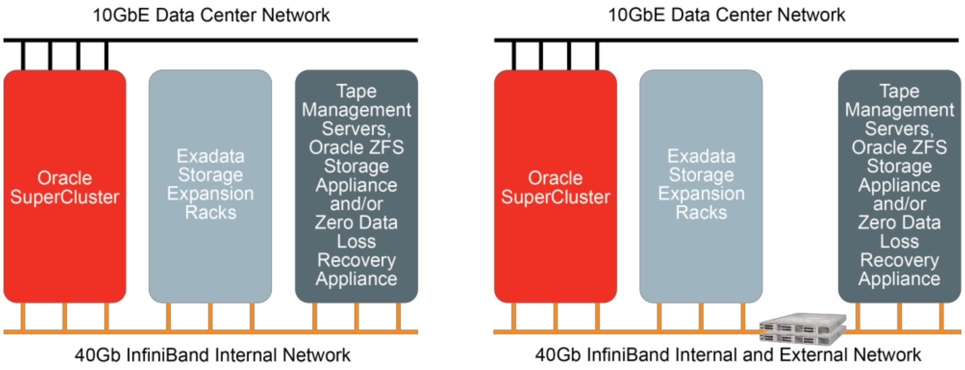
10GbE Data Center Network
Oracle SuperCluster
Exadata Storage Expansion Racks
Tape Management Servers, Oracle ZFS Storage Appliance and/or Zero Data Loss Recovery Appliance
40Gb InfiniBand Internal Network
10GbE Data Center Network
Oracle SuperCluster
Exadata Storage Expansion Racks
Tape Management Servers, Oracle ZFS Storage Appliance and/or Zero Data Loss Recovery Appliance
40Gb InfiniBand Internal and External Network

Figure 12. Connecting backup and recovery devices with multiple 40 Gb InfiniBand links provides the highest performance.

A Hybrid of Multiple 10 GbE and 40 Gb InfiniBand Links

In this scenario, multiple 10 GbE and 40 Gb InfiniBand links are used to connect external disk and tape resources for backup and recovery (see Figure 13). This configuration is the most flexible networking configuration for the backup and recovery infrastructure for Oracle SuperCluster. This option simplifies attachment to existing backup and recovery infrastructure and enables the sharing of storage systems between Oracle SuperCluster and external systems on the corporate network.

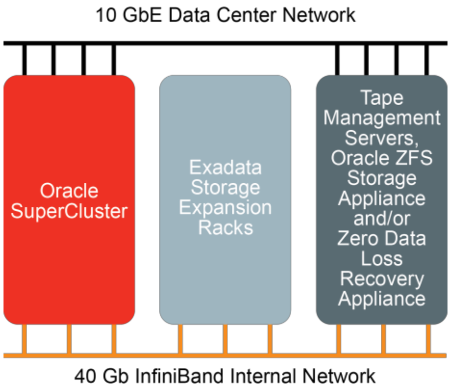
10 GbE Data Center Network
Oracle SuperCluster
Exadata Storage Expansion Racks
Tape Management Servers, Oracle ZFS Storage Appliance and/or Zero Data Loss Recovery Appliance
40 Gb InfiniBand Internal Network

Figure 13. A hybrid of multiple 10 GbE and 40 Gb InfiniBand links provides the greatest flexibility.

Shared Storage for Two InfiniBand Fabrics

In this scenario, a single Oracle ZFS Storage Appliance is connected to two separate InfiniBand fabrics providing shared storage between separate Oracle SuperCluster systems (see Figure 14). This configuration offloads tremendous amounts of backup and recovery traffic from the corporate network infrastructure and keeps backup and recovery data secured on a private network.

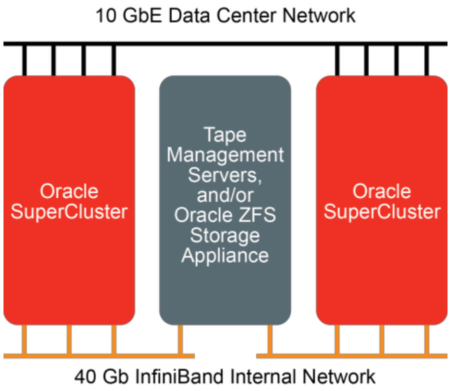
10 GbE Data Center Network
Oracle SuperCluster
Tape Management Servers, and/or Oracle ZFS Storage Appliance
Oracle SuperCluster
40 Gb InfiniBand Internal Network

Figure 14. A single Oracle ZFS Storage Appliance can provide shared storage for separate Oracle SuperCluster systems.

Conclusion

Oracle SuperCluster delivers extreme compute power, unmatched scalability, accelerated processing, and database optimization with integrated components taken from the tiers of Oracle's technology stack. These features of Oracle SuperCluster demand comparable functionality in a backup and recovery solution.

Oracle Optimized Solution for Secure Backup and Recovery matches the innovation built into Oracle SuperCluster, providing higher capacity and performance with greater operational efficiency at a lower cost. The data protection features of the solution provide backup and recovery capabilities for the network switching infrastructure, operating system, domains, zones, and database. The result is an end-to-end solution that ensures the fastest, most reliable backup and recovery for Oracle SuperCluster.

References

For more information, please see the following resources:

- Oracle Optimized Solution for Secure Backup and Recovery.
  oracle.com/solutions/optimized-solutions/backup-and-recovery
- Oracle Optimized Solution for Secure Disaster Recovery
  oracle.com/solutions/optimized-solutions/disaster-recovery
- Oracle ZFS Storage Appliance Plug-in Downloads web page.
  oracle.com/technetwork/server-storage/sun-unified-storage/downloads/zfssa-plugins-1489830.html.
- Oracle Maximum Availability Architecture—MAA web page.
  oracle.com/technetwork/database/features/availability/maa-090890.html.
- Oracle white papers:
  - “NDMP Implementation Guide for the Sun ZFS Storage Appliance”
    oracle.com/technetwork/articles/systems-hardware-architecture/ndmp-whitepaper-192164.pdf
  - “Deploying Oracle Maximum Availability Architecture with Exadata Database Machine”
    oracle.com/au/products/database/exadata-maa-131903.pdf
  - “Backup and Recovery Performance and Best Practices for Exadata Cell and Oracle Exadata Database Machine”
    oracle.com/au/products/database/maa-tech-wp-sundbm-backup-11202-183503.pdf
  - “Configuring an Oracle ZFS Storage ZS3-BA with an Oracle SuperCluster for Oracle Database Backup and Recovery”

  oracle.com/technetwork/server-storage/sun-unified-storage/documentation/zs3ba-supercluster-config-2014-2227429.pdf

  - “Architecture Principles and Implementation Practices for Remote Replication Using Oracle ZFS Storage Appliance” oracle.com/technetwork/server-storage/sun-unified-storage/documentation/zfssa-replication-2014-1-2120969.pdf
  - “Protecting SPARC SuperCluster—Tape Backup with Symantec NetBackup” oracle.com/technetwork/server-storage/sun-tape-storage/documentation/o13-016-1900890.pdf
  - “Oracle Data Guard: Disaster Recovery for Oracle Exadata Database Machine” oracle.com/technetwork/database/features/availability/maa-wp-dr-dbm-130065.pdf.
- Oracle support documents:
  - My Oracle Support Note 1354980.1, “Oracle ZFS Storage: FAQ: Exadata RMAN Backup with the Oracle ZFS Storage Appliance”
  - My Oracle Support Document 1517107.1, “RMAN Backup From SPARC SuperCluster to Sun ZFS Backup Appliance”
  - My Oracle Support Note 1558851.1, “Oracle Optimized Solution for Secure Backup and Recovery”
  - My Oracle Support Note 1903189.1, “SuperCluster–How to Backup a SuperCluster using the `osc-backup` tool”
  - My Oracle Support Document 1903364.1, “SuperCluster–Recovery Guide”

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

Oracle Optimized Solution for Secure Backup and Recovery: Oracle SuperCluster Backup and Recovery
October 2015
Author: Dean Halbeisen