ORACLE

SOLARIS

An Oracle White Paper
March 2012

HP-UX to Oracle Solaris Technology Mapping Guide

Preparing for the Move to Oracle Solaris 11

ORACLE

Chapter 1 Introduction

In many enterprise IT organizations, HP systems running the HP-UX 11i operating system—particularly those based on Intel® Itanium® processors—are failing to keep pace with growing service and application demands. With the future of the platform uncertain, IT managers are looking for alternative platforms that can deliver the functionality, performance, scalability, reliability, availability, and security needed to support business priorities. Oracle's SPARC and x86 systems running the Oracle Solaris operating system provide an obvious alternative and safe platform for running critical business applications. HP-UX and Oracle Solaris share a common UNIX history—and are more alike than they are different—making the transition to Oracle servers running Oracle Solaris an easier task than moving to radically different architectures.

Migrating infrastructure to a new platform can take time and effort, particularly if the technologies used on the new system are unfamiliar. Aimed at technical IT managers, IT architects, and system administrators tasked with moving—or evaluating the move—to Oracle Solaris, this guide compares the key tools and technologies commonly used in HP-UX 11i version 3 environments with those used in Oracle Solaris. Different concepts, processes, and technologies that are essential to successful Oracle Solaris platform deployment are identified. For each topic area, HP-UX features and tools are mapped to their Oracle Solaris 11 counterparts, with discussion centering on similarities and differences in functionality to help technical staff quickly identify where appropriate, equivalent resources (product and technology information, manuals, and training) are needed to support deployment.

- Chapter 2, "Distributing, Installing, and Managing Software," identifies and compares the key tools used for software management.
- Chapter 3, "Managing Data," discusses file system availability, volume management, data backup, swap space considerations and more, as well as whether and how these technologies differ in the two environments.
- Chapter 4, "Virtualizing Infrastructure," maps the key virtualization technologies used in HP-UX to similar Oracle Solaris virtualization mechanisms and highlights similarities and differences that are important to understand before deployment.
- Chapter 5, "Keeping Systems, Applications, and Services Available," compares the commonly used HP-UX and Oracle Solaris tools for maximizing availability.
- Chapter 6, "Keeping Infrastructure Secure," relates the security mechanisms in HP-UX to the extensive defense-in-depth approach in Oracle Solaris.
- Chapter 7, "For More Information," provides a comprehensive list of references to more detailed information. For readers interested in the Oracle Solaris 11 product documentation, see http://www.oracle.com/technetwork/server-storage/solaris11/documentation/index.html.
- Appendix A, "Glossary," defines terms used throughout this document.

Chapter 2 Distributing, Installing, and Managing Software

While HP-UX and Oracle Solaris have similar concepts for software management, the tools used are very different. This chapter discusses several aspects of software management, including software installation, packaging, updates, and upgrades. It identifies which tools are available in Oracle Solaris to perform various tasks, and explains how those tools differ from those commonly used in HP-UX deployments.

Table 2-1 maps tools for managing software in HP-UX 11i v3 to counterpart technologies and tools in Oracle Solaris 11.

TABLE 2-1. SOFTWARE MANAGEMENT MAPPINGS

TASK OR CAPABILITY	HP-UX 11i V3	ORACLE SOLARIS 11
Software packaging model and tools	Software Distributor; GUI, TUI, and command line interfaces provided	Image Packaging System (IPS); GUI and command line interfaces provided
Single system installations	From DVD, virtual media, or using Ignite-UX and software depots	From DVD using Live Media (x86) or interactive text installers (SPARC, x86); USB images available for Live Media and text installer; post-installation customization can be performed using IPS.
Automated installation of multiple systems	Ignite-UX and software depots	Automated Installer and IPS software repositories
Adding software packages to an existing installed system	Software Distributor tools: `swinstall`	IPS tools: `pkg install` (command line) or `packagemanager` (GUI)
Analyzing and applying patches	Software Assistant and Software Distributor	No patching required (package updates applied instead)
Updating software	Ignite-UX or Update-UX tools	IPS tools: `pkg update` (command line); `packagemanager` or `pm-updatemanager` (GUI)
Minimizing downtime and enabling recovery for updates	Dynamic Root Disk (DRD)	Boot Environments (BEs); `beadm` utility for BE management
Creating customized installation images	Example script `make_media_install` provided with Ignite-UX	Distribution Constructor and sample manifests

Cold Installations

When installing a new instance of HP-UX on a single system — a *cold* install — system administrators typically use distribution media or perform virtual media-based networked installations. Oracle Solaris 11 offers similar installation options. Interactive installations from media using Oracle Solaris 11 Live Media

for x86 DVD provide a full desktop environment, while the interactive text-based user interface creates server installations.

In addition, Oracle Solaris 11 supports a hands-off automated installation process called Automated Installer that is analogous to Ignite-UX (see "Automating Installations of Multiple Enterprise Systems" on page 6.) Automated Installer relies on software repositories that loosely resemble HP-UX software depots.

For more information on installation options, see Installing Oracle Solaris 11 Systems.

Software Packaging Model

Oracle Solaris 11 uses a software-packaging model called the Image Packaging System (IPS). IPS provides broad software management functionality that blends and extends the functionality available in HP-UX[1]. Designed to support management tasks for both operating system as well as application software, IPS is a comprehensive framework that spans the full software lifecycle, addressing functions such as installation, patching, upgrades, and software removal. During software package installations, IPS performs automatic dependency checking, adding any additional packages (such as libraries) that might also be required. A snapshot of the system is taken before each package installation, ensuring the system is always in a valid state and enabling a rollback to be performed in the even the package installation fails.

An IPS software package identifies all necessary installable objects in a well-defined format, specifying directories, files, links, drivers, dependencies, groups, users, and license information. IPS packages include attributes such as the package name and a brief description. A Fault Management Resource Identifier (FMRI) uniquely represents each package and consists of a publisher, package name, and version number with the scheme "pkg" as in: *scheme://publisher/package_name@version:dateTtimeZ*. Since the FMRI incorporates an explicit version number and timestamp, IPS can easily determine whether a more up-to-date package release exists. Specifying the package publisher in the FMRI identifies the package developer, supplying a mechanism by which IPS can classify packages, confirm authenticity, and restrict installation.

For more information on the IPS model and tools, see Adding and Updating Oracle Solaris 11 Software Packages.

Managing Software on an Installed System

Similar to the Software Distributor and Ignite-UX, IPS relies on software depots — called software *repositories* in Oracle Solaris 11 — to access software packages for installation and update. IPS supports DVD, CD, and file-based local repositories, as well as network-based remote repositories. Administrators

[1] HP-UX software management tools include Software Distributor, Update-UX, and Software Assistant.

can easily set up and manage local repositories to deploy packages within network-restricted and firewalled environments. The default repository for Oracle Solaris 11 is http://pkg.oracle.com/solaris/release, which is publicly available. Customers with support contracts can access the support repository at My Oracle Support (http://support.oracle.com) to obtain packages with the latest bug fixes and updates.

For more information about setting up local repositories, see Copying and Creating Oracle Solaris 11 Package Repositories.

Both the Software Distributor and IPS provide command-line as well as graphical user interfaces to perform software management tasks. The IPS `pkg(1)` command and its associated subcommands (such as `pkg install`, `pkg uninstall`, and `pkg list`) offer similar functionality to some of the common Software Distributor tools (such as `swinstall`, `swremove`, and `swlist`). While IPS includes two interfaces for software management (one GUI and one command-line interface), there is no Terminal User Interface as with Software Distributor.

- The Package Manager is used to search, install, and remove individual packages or groups of packages. Initiated on the command line by `packagemanager(1)`, it also is used to add, remove, and modify package publishers, or to create, remove, and manage Boot Environments. (Boot Environments are clones of the active boot image.)
- The Update Manager, initiated on the command line by `pm-updatemanager(1)`, is a related GUI used to update all packages in an installation image for which updates are available. The Update Manager is similar to Update-UX. Both the Package Manager and Update Manager GUIs provide descriptive details about each package (including the versions, time stamps, and descriptions to simplify identification), making software management an easy and intuitive process. Package Manager groups packages by category to simplify the task of locating a specific package.

Administrators can use IPS packaging tools in a zones-enabled environment. (Oracle Solaris 11 zones are an operating system virtualization technology used to provide isolated and secure execution environments. Each Oracle Solaris 11 system hosts a global zone in which non-global zones can be created.) With the exception of upgrades, running IPS commands in the global zone impacts only packages in the global zone. For example, executing `pkg install` in the global zone installs the package there; it is not propagated to any other zones. This model allows zones to be independently administered and maintained with their own separate software stacks. A zone administrator can use the same IPS packaging tools to manage software within a non-global zone.

See the Oracle Solaris Administration: Oracle Solaris Zones, Oracle Solaris 10 Zones, and Resource Management manual for more information.

Updating System and Application Software

Patching has traditionally been the means by which software vendors have addressed security issues, bug fixes, performance improvements, and new features. For both HP-UX and earlier versions of Oracle Solaris, patching could sometimes be a complex process that required detailed manual analysis to

understand dependencies before applying the required patches. Oracle Solaris 11, however, eliminates the software maintenance model of patch analysis and application. Instead, the IPS software packaging model releases updated software packages that are already integration-tested before they are made available for download and installation, reducing the risk of incompatibilities between production software modules or problems resulting from human error. As a result, there is no need for a tool such as Software Assistant to stay on top of the latest security bulletins and apply patches accordingly. In addition, package contents that have not changed are not downloaded, resulting in faster updates that minimize network bandwidth consumption.

Update Manager in Oracle Solaris 11 reconciles all installed system software packages, updating packages as needed to bring the base operating system environment to a defined and integration-tested level. Both Update Manager and Package Manager check package versions against packages in a specified repository and identify available updates for installed packages. The "Update All" function in Update Manager updates all installed packages, as does "Update All" in Package Manager. Package Manager, however, allows an administrator to add, remove, or update individual packages in between full system update operations. There is also a command line equivalent (`pkg update`) for updating all packages. If the `pkg update` command (with no Fault Management Resource Indicators (FMRIs) specified) is run in the system's global zone, it updates all software packages in both the global zone and any non-global zones.

Upgrading Software and Boot Environments

When updating HP-UX or installing patches, creating a Dynamic Root Disk (DRD) can be a useful strategy to minimize downtime. Building a DRD allows an administrator to clone the current root volume to an inactive disk and apply updates or patches to the clone, providing a means of recovery in the event there are problems with an update. Once modified, the active image and the clone must be synchronized so that changes made to the active image can be replicated on the clone, and the system rebooted. In Oracle Solaris 11, Boot Environments serve a comparable role. Creating a Boot Environment (BE) takes advantage of the underlying Oracle Solaris ZFS file system technology in Oracle Solaris 11, using its fast snapshot and clone capabilities to replicate the active operating system image. Because Oracle Solaris ZFS uses copy-on-write, cloning a file system takes seconds, even for large disks.

By default, a new BE is created automatically when certain system packages (key drivers and kernel components) are updated or when the administrator updates all packages (via an "Update All" in the GUIs or with "`pkg update`"). In these cases, Oracle Solaris 11 first clones the current BE, applies packaging changes to the clone, and automatically activates the updated BE. If a problem occurs, the administrator can easily roll back to the previous BE image. In this way, Oracle Solaris 11 provides an administrative safety net for upgrades and software changes, helping to improve availability. Because fast reboot is configured as the default, systems can switch to a new BE quickly, often within a few seconds. Administrators can use the Oracle Solaris 11 `beadm(1M)` utility to manage BEs, and the Package Manager GUI also supports the most common BE management tasks.

For more information about creating and managing Boot Environments, see Creating and Administering Boot Environments After Installation.

Automating Installations of Multiple Enterprise Systems

Ignite-UX uses a client-server model to automate the installation of multiple systems across an enterprise. In Oracle Solaris 11, Automated Installer (AI) provides equivalent functionality. AI automates and batches installations based on customized, standardized system profiles, enabling hands-free installation of multiple systems in large-scale enterprises. Similar to Ignite-UX, AI uses a client-server model but leverages other Oracle Solaris 11 technologies, specifically the IPS packaging model and the Service Management Facility (SMF). AI uses networking protocols that are WAN-compatible, such as DHCP, PXE/TFTP, HTTP, and mDNS/DNS, to provide operational flexibility.

The AI installation server houses a SPARC and x86 network boot image, installation instructions (called *AI manifests*), and optional system configuration (SC) profiles. Clients can be customized with installation parameters such as disk layout and software selection, and with system configuration parameters such as host name, network configuration, and user accounts.

An AI client first boots over the network, obtaining its network configuration and the location of the installation server via DHCP. The client is then configured and installed according to the AI manifest that matches client characteristics. AI installs a minimal network boot image on the client and the client subsequently completes the installation by accessing the IPS software repositories specified in the manifest. To customize the system after AI installation, the client applies an SC profile that configures the system using SMF services during the first boot. In addition, virtualized environments are provisioned automatically, with non-global zones configured and installed during the first boot after the AI installation completes.

For more information on the Automated Installer, see Installing Oracle Solaris 11 Systems.

Building a Customized Distribution Image

In some cases, administrators need to build preconfigured, customized ISO installation images. Ignite-UX includes an example script called `make_media_install` that can be used to generate a customized installation image. In a similar vein, Distribution Constructor is a command-line utility in Oracle Solaris 11 for customizing and building installation images. Checkpoints are performed during the construction process using Oracle Solaris ZFS. As a result, portions of the process can be restarted without going back to the beginning each time a change is made.

Distribution Constructor builds an image based on parameters specified in an XML manifest file. Sample manifests define preset, default values for an image and can be edited to further customize the resulting image. Distribution Constructor supplies sample manifests that build customized images similar to the Oracle Solaris Live Media for x86 image, ISO images for an Oracle Solaris 11 text installation, or ISO images for the Automated Installer. It builds an ISO image or a USB image that is based on a generated ISO image. However, a USB image can be used only on x86 systems.

For more information on the Distribution Constructor, see Creating a Custom Oracle Solaris 11 Installation Image.

Chapter 3 Managing Data

When comparing HP-UX 11i v3 to Oracle Solaris, it is important to understand which file systems are supported, which file systems offer new capabilities, and how best to move data from one platform to another. This chapter describes the supported disk-based, network-based, and virtual file systems in HP-UX 11i v3 and Oracle Solaris. Other storage-related topics, including volume managers, data backup and recovery, swap space, and data transformations also are discussed.

Disk-Based File Systems

Table 3-1 lists the disk-based file systems supported on HP-UX 11i v3 and Oracle Solaris. Oracle Solaris supports many of the same file systems as HP-UX 11i, enabling users to simply mount existing file systems rather than migrate them.

FILE SYSTEM	DESCRIPTION	HP-UX 11i v3	ORACLE SOLARIS 11
HFS	High-Performance File System (HP proprietary)	√	—
HSFS	High Sierra File System, ISO 9660, the first CD-ROM file system	√	√
PCFS	Supports read and write access to data and programs on DOS-formatted disks	√	√
Oracle Solaris ZFS	A general-purpose, enterprise-class file system that integrates traditional file system functionality with built-in volume management techniques and data services	—	√ (Default)
UDFS	Universal Disk Format file system, the industry-standard format for storing information on optical media such as DVDs	√	√
UFS	UNIX file system	√	√
VxFS	VERITAS File System	√	Expected in 2012[2]

HP-UX File Systems

HP-UX supports the HP proprietary High-Performance File System (HFS) and VERITAS File System (VxFS) as the primary disk-based file system choices. By default, HFS does not support large files greater than 2 GB in size. HFS can support files and file system sizes up to 128 GB when `largefiles` support is enabled. (The default for HFS file systems is `nolargefiles`.) Starting in the September 2011 HP-UX

[2] As of February 2012, VxFS is not supported on Oracle Solaris 11. Check the Symantec website for the latest information on availability.

update release, VxFS 5.0.1 supports file sizes up to 16 TB and file system sizes up to 256 TB when VERTIAS Volume Manager (VxVM) is used as the volume manager.

HP OnlineJFS extends the functionality of the base VxFS with journaling file system features. HP OnlineJFS is available in the High Availability, Virtual Server, and Data Center Operating Environments for HP-UX 11i v3, and in the Serviceguard Storage Management Suite for HP-UX 11i.

Cross-platform Data Sharing (CDS) support in VxFS enables the sharing and migration of VxFS file systems across heterogeneous platforms such as HP-UX and Oracle Solaris. Currently, VxFS is not supported on Oracle Solaris 11[3].

UFS

The UNIX file system (UFS) is supported in Oracle Solaris 11. As of Oracle Solaris 11, Oracle Solaris ZFS is used for the root file system. HP-UX also supports UFS. However, HP-UX environments running UFS are limited to 1 TB file systems. In contrast, on Oracle Solaris, UFS scales to 16 TB.

Oracle Solaris ZFS

Oracle Solaris includes the Oracle Solaris ZFS file system. In Oracle Solaris 11, Oracle Solaris ZFS always is used as the root file system. (Other file systems are supported as data file systems.) The move to Oracle Solaris ZFS as the root file system enables fast root file system snapshots and easy roll back to previous states. Oracle Solaris 11 also includes support for a read-only root file system, which can be used to lock down an environment for added security.

This 128-bit file system, with a theoretical limit of 16 exabytes for a single file and file systems up to 21 billion Yottabytes, provides the scalability to store and manage virtually unlimited amounts of data. Complicated storage administration is automatic and simplified, reducing administrative overhead. For example, a redundant file system spanning multiple disks can be created with a single command, and Oracle Solaris ZFS file systems are mounted automatically when created and remounted automatically when systems are rebooted.

Unlike traditional file systems that require a separate volume manager, Oracle Solaris ZFS integrates volume management functions such as virtualized storage resources and redundant data protection. Oracle Solaris ZFS implements RAID-Z, which uses parity, striping, and atomic operations to ensure reconstruction of corrupted data. All data is protected by 256-bit checksums, and a self-healing feature automatically repairs corrupt data. Because the file system is always consistent, time-consuming recovery procedures such as `fsck` are not required if the system is shut down in an unclean manner.

[3] VxFS support is expected in 2012. Check the Symantec website for the latest information on availability.

- **Integrated volume management and storage pools.** Oracle Solaris ZFS uses a storage pool model of the underlying physical storage devices. Space from a single storage pool, comprising multiple physical devices, is shared dynamically between multiple file systems and parceled out as file systems request it. Physical storage can be added to storage pools dynamically, without interrupting services, providing new levels of flexibility, availability, scalability, and performance. When capacity no longer is required by a file system in the pool, it is made available to other file systems.
- **Hybrid Storage Pools.** Oracle Solaris ZFS provides the ability to optimize data placement for fast access with Hybrid Storage Pools. Flash technology can be placed in a new storage tier to assist hard disk drives by holding frequently accessed data to minimize the impact of disk latencies and improve application performance. By using Flash devices to handle certain types of I/O, and hard disk drives to store massive data sets, a Hybrid Storage Pool delivers significant application performance gains without sacrificing capacity (Figure 3-1).

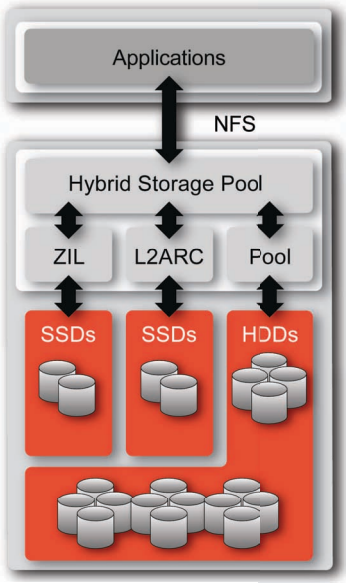

Figure 3-1. Hybrid Storage Pools optimize data placement to improve I/O performance.

Hybrid Storage Pool technology is designed to exceed the performance of Fibre Channel technologies without the additional management complexity of a SAN. Several Oracle Solaris ZFS components are key to Hybrid Storage Pool operation and help accelerate application performance. The Oracle Solaris ZFS Adaptive Replacement Cache (ARC) is the main file system memory cache and is stored in DRAM. The Level Two Adaptive Replacement Cache (L2ARC) extends the ARC into read-optimized Flash devices to provide a large read cache to accelerate reads. The Oracle Solaris ZFS Intent Log (ZIL) is transactional and uses write-based Flash devices to provide a large cache to accelerate writes.

Sophisticated file system algorithms in Oracle Solaris ZFS use the ARC in memory and the L2ARC on Flash devices to determine pre-fetch or data placement during sustained read operations. Flash devices accelerate write throughput for Oracle Solaris ZFS synchronous write I/O operations, helping to boost write performance.

See Oracle Solaris Administration: ZFS File Systems manual for detailed information on how to set up and administer Oracle Solaris ZFS file systems.

Network-Based File Systems

Both HP-UX 11i v3 and Oracle Solaris provide support for the Network File System (NFS) and Common Internet File System (CIFS) network-based file systems (Table 3-2).

TABLE 3-2. NETWORK-BASED FILE SYSTEMS

FILE SYSTEM	DESCRIPTION	HP-UX 11i v3	ORACLE SOLARIS 11
NFS	Network File System	√	√
SMB (CIFS)	Server Message Block (SMB) service provides distributed resources to Windows and Mac OS systems and supports Common Internet File System (CIFS)	√	√

Both Oracle Solaris and HP-UX 11i include support for the NFS version 4 distributed file access protocol.

The Server Message Block (SMB) service provides access to distributed files and directories to Windows, Mac OS, and Oracle Solaris clients. The Oracle Solaris kernel provides a built-in Server Message Block (SMB) protocol server, and a client implementation supports numerous SMB dialects, including NT LM 0.12 and Common Internet File System (CIFS). While Oracle Solaris offers a fast, kernel-level CIFS implementation, HP-UX provides CIFS support through the HP CIFS Client and Server suite.

See the Managing Network File Systems section of the Oracle Solaris Administration: Network Services guide for detailed information on how to set up and administer NFS file systems. See the Oracle Solaris Administration: SMB and Windows Interoperability guide for detailed information on the SMB server and client in Oracle Solaris.

Virtual File Systems

Table 3-3 lists common virtual file systems and details their availability on HP-UX 11i and Oracle Solaris.

TABLE 3-3. ADDITIONAL SUPPORTED FILE SYSTEMS

FILE SYSTEM	DESCRIPTION	HP-UX 11i v3	ORACLE SOLARIS 10	ORACLE SOLARIS 11
CTFS	Contract file system, used to create, control, and observe contracts (primarily used by SMF)	—	√	√
FDFS	File Descriptor File Systems, provides explicit names for opening files using file descriptors	√	√	√
FIFOFS	First-in, first out file system, provides named pipe files that give processes common access to data	√	√	√
LOFS	Loopback file system, allows the creation of a virtual file system so that files can be accessed using an alternative path name	√	√	√
MNTFS	Provides read-only access to the table of mounted file systems for the local system	√	√	√
NAMEFS	Used mostly by STREAMS for dynamic mounts of file descriptors on top of files	√	√	√
OBJFS	Object file system, describes the state of modules currently loaded by the kernel (used by debuggers to access information about kernel symbols without having to access the kernel directly)	—	√	√
SHAREFS	Provides read-only access to the table of shared file systems for the local system	—	√	√
SPECFS	Special file system, provides access to character special devices and block devices	√	√	√
SWAPFS	Used by the kernel for swapping	√	√	√
TMPFS	Uses local memory for file system reads and writes, which is typically faster than a UFS file system	—	√	√

The majority of these virtual file systems do not require administration. One exception is the memory-based file systems: MemFS on HP-UX and TMPFS in Oracle Solaris. Both of these file systems provide similar functionality, using the system's physical memory to store the file system to provide fast access to temporary files. Administrators can create a MemFS or TMPFS file to provide increased performance as

compared to the disk-based file systems. While these file systems can be used for the storage of temporary files, they cannot be used as a replacement for disk-based file systems since they do not preserve data across system reboots or file system remounts.

See the Oracle Solaris Administration: Devices and File Systems guide for information on memory-based file systems in Oracle Solaris.

Volume Managers

Oracle Solaris ZFS eliminates the need for separate volume management altogether. Instead of creating virtualized data volumes, Oracle Solaris ZFS aggregates devices into a storage pool. The storage pool describes the physical characteristics of the storage and acts as an arbitrary data store from which file systems can be created. File systems are no longer constrained to individual devices.

Redundant storage pools can be created easily with a single command. Oracle Solaris ZFS provides two types of redundant configurations: mirrored pools and RAID-Z pools. RAID-Z configurations include RAID-Z (distributed parity), RAID-Z2, and RAID-Z3. Oracle Solaris ZFS dynamically stripes data across all non-redundant, mirrored, and RAID-Z configurations.

Oracle Solaris supports the legacy Solaris Volume Manager (SVM) product, although you cannot boot from an SVM root device in Oracle Solaris 11. While SVM is supported, using Oracle Solaris ZFS is generally a better alternative as it decreases the administration overhead and provides increased functionality as compared to SVM.

HP-UX 11i v3 supports Logical Volume Manager (LVM) and VERITAS Volume Manager (VxVM), with LVM used as the default volume management option. The VxVM that ships with HP-UX is a subset of the full version, which requires an additional license. Currently, VxVM is not supported on Oracle Solaris 11[4]. Where feasible, Oracle recommends that organizations transition from VxVM to using Oracle Solaris ZFS to take advantage of built-in functionality.

[4] VxVM support is expected in 2012. Check the Symantec website for the latest information on availability.

Data Backup and Restore

Both HP-UX and Oracle Solaris support a wide range of backup utilities, as listed in Table 3-4.

TABLE 3-4. BACKUP UTILITIES

UTILITY	DESCRIPTION	HP-UX 11i v3	ORACLE SOLARIS 10	ORACLE SOLARIS 11
cpio	Saves and restores archives; copies files and directories while replicating the directory tree structure	√	√	√
fbackup/ frecover	HP-UX specific backup utility	√	—	—
pax	Extracts, writes, and lists archive files; copies files and directories (newer version of `cpio` and `tar`)	√	√	√
tar	Extracts, writes, and lists archive files; copies files and directories (newer version of `cpio` and `tar`)	√	√	√
vxdump	Copies files in a VxFS file system to magnetic tape	√		
ufsdump /ufsrestore	Provides a UFS incremental file system dump	—	√	√

While some backup utilities such as `fbackup` and `ufsdump` are specific to only HP-UX or Oracle Solaris, many backup utilities are common to both systems. For example, the newer `pax` utility is POSIX-conformant and is compatible with both HP-UX and Oracle Solaris. The `pax` utility supports a wide variety of archive formats, including `tar` and `cpio`, and can be used for data migration from one system to another. Data backed up using the `pax` utility on an HP-UX system can be imported on an Oracle Solaris system, and vice versa. Backup utilities can also be used to migrate data from one file system type to another on the same system.

In addition to these backup utilities, Oracle Solaris ZFS includes snapshot capabilities—the ability to create a read-only copy of an Oracle Solaris ZFS file system or volume and restore it at a later time, if needed. Snapshots can be created almost instantly, and initially consume no additional disk space within the storage pool. Replicated streams of descendant file systems can be sent to named snapshots, preserving properties, snapshots, file systems, and clones. With snapshots, developers can save the state of a file system at a particular point in time, and recreate it on another machine to simplify data migration.

Oracle Solaris ZFS also provides support for *shadow migration*, a new feature in Oracle Solaris 11. Shadow migration enables the migration of data from an existing locale or remote Oracle Solaris ZFS or UFS file system to a new Oracle Solaris ZFS file system. A shadow file system is created that pulls data from the source and uses the native file system once a file is migrated.

See the man pages for detailed information on user commands and utilities, such as `cpio` and `tar`. For information on Oracle Solaris ZFS snapshots, see the Overview of ZFS Snapshots section of the Oracle Solaris Administration: ZFS File Systems guide.

Additional Storage Software

In addition to the built-in file system support described in the previous sections, the following data storage software and file systems are available to fill specific storage and data requirements for Oracle Solaris and HP-UX environments.

- Oracle's Sun Storage Archive Manager (SAM) software offers tiered data storage capabilities such as data classification, centralized meta-data management, policy-based data placement and migration. Oracle's SAM-FS is a self-protecting file system that offers continuous backup and fast recovery features.
- Oracle's Sun QFS software is a robust file system intended for environments that share large data volumes. Sun QFS provides nearly raw device access to information and data consolidation for read/write file sharing.
- The Lustre File System is an open-source parallel file system, designed to enable I/O performance and scaling beyond the limits of traditional storage technology. The Lustre file system is developed and maintained as open source software with an open networking protocol, and provides support for heterogeneous networking environments. This highly scalable distributed file system scales to tens of petabytes and thousands of clients.
- In HP-UX, VxFS 5.0 includes a multi-volume file system (MVS), which enables a file to exist in multiple volumes. In addition, HP-UX offers Dynamic Storage Tiers and Quality of Storage Service (QoSS) built on top of MVS. These features enable administrators to configure relocation policies to place data on the storage tier that is most appropriate. While not included in the base HP-UX 11iv3 release, MVS and QoSS are available as part of HP Serviceguard Storage Management Suite products.

See the Sun StorageTek QFS documentation and the Lustre File System Software documentation for more information on these file systems.

Swap Space

HP-UX supports three types of swap space: device swap, file system swap, and pseudo swap. Device swap is a disk partition or logical volume that is dedicated for system paging. File system swap space enables a file system to be allocated and used as additional swap space. In addition, HP-UX provides pseudo swap functionality. Pseudo swap space capitalizes on the fact that not all swap space that is reserved is actually used. HP-UX acts as if the pseudo swap space, which does not actually exist, is available, allowing more processes to run in memory that can be supported by the actual physical swap space.

Similar to HP-UX, Oracle Solaris 10 also uses device swap and file system swap devices. In Oracle Solaris 11, Oracle Solaris ZFS is used for the root file system. In an Oracle Solaris ZFS root file system, the disk

space reserved for swap is an Oracle Solaris ZFS volume. In an Oracle Solaris ZFS root pool, swap devices are not pre-allocated to fixed-size slices, so the swap size can be modified later as needed. Additional swap volumes can be added to increase the amount of available swap space.

See the Oracle Solaris Administration: ZFS File Systems guide and Adding or Changing Swap Space in an Oracle Solaris ZFS Root Environment for more information.

Data Transformation

Data transformation is the process of converting data from one format to another, and is an important component of any migration effort if data is to be readable on the target system. Data transformation can involve file systems, file content, applications, and database content.

Encoded Data Transformations

Encoded data transformations are necessary when data is stored in a different or incompatible file format than the receiving system anticipates. Fortunately, HP-UX and Oracle Solaris both use ASCII to store textual data, as well as a standard text file format. As a result, issues stemming from the use of other character sets, such as EBCDIC, and differences in text file formatting, such as the use of control-linefeed (CR/LF) versus carriage return (CR) characters to delimit lines in a file, are avoided.

Application Data Transformation

HP-UX and Oracle Solaris provide many common applications and utilities for managing data. For example, the tape archive utility (`tar`) uses a similar data format and provides many common options in both environments. This commonality is true for many other applications and utilities, and can yield significant benefits both during and after the data migration. For those applications that differ between HP-UX and Oracle Solaris, most provide a utility to convert standard data interchange formats, such as comma-separated values or tab delimited files, into their format.

Database Transformation

Many enterprise applications depend on large databases. If an older version of a database is in use in the HP-UX environment, licenses may or may not be available for those versions on Oracle Solaris. IT organizations should be prepared to acquire a current version of the database software. It is important to note that changes to the infrastructure may be needed to support the new database and its configuration, however existing data should be immediately accessible. Table 3-5 lists the popular databases and their support availability on HP-UX 11i v3 and Oracle Solaris.

TABLE 3-5. SUPPORTED DATABASES (TYPICALLY INSTALLED SEPARATELY)

DATABASE	HP-UX 11I v3		ORACLE SOLARIS	
	PA-RISC	ITANIUM	SPARC	X86
Oracle Database 11*g* Release 2	√	√	√	√
Oracle Database 11*g* Release 1	√	√	√	√
Oracle Database 10*g* Release 2	√	√	√	√
MySQL Database 5.6	√	√	√	√
MySQL Database 5.5	√	√	√	√
MySQL Database 5.1	√	√	√	√
MySQL Database 5.0	√	√	√	√
Sybase IQ Enterprise Edition 15.3	√	√	√	√
Sybase IQ Enterprise Edition 15.2	√	√	√	√
Sybase IQ Enterprise Edition 15.1	√	√	√	√
PostgreSQL Database	√	√	√	√

While there are many similarities between a database running on HP-UX and one running on Oracle Solaris, simply moving a database from one to the other likely requires some data transformation. In the case of the same database vendor in both environments, this may be as simple as exporting the database running on HP-UX to a standardized file format, followed by an import into a new database on Oracle Solaris. When the port also involves a change in database vendors, more extensive data transformations may be required.

Because database transformations are usually such a large part of the overall migration effort, many specialized utilities have been created to address them. These programs, called Extract, Transform, and Load (ETL) utilities, take a wide array of formats and convert them into Structured Query Language (SQL) for relational database management systems (RDBMS). Most RDBMSs provide a basic set of utilities to convert SQL or standard interchange formats into their data storage format.

Chapter 4 Virtualizing Infrastructure

As IT organizations continue to consolidate infrastructure and move to cloud computing, having a robust virtualized environment is essential. While both HP-UX and Oracle Solaris provide hard partitioning, virtual machines, and operating system virtualization capabilities, Oracle Solaris extends virtualization throughout the technology stack. Oracle Solaris 11 is a completely virtualized operating environment, with technologies that span server, network, and storage virtualization to help IT organizations optimize enterprise infrastructure resources. Because no two deployment environments have exactly the same needs, Oracle's virtualization technologies provide varying degrees of isolation, resource granularity, and flexibility, and can be used separately or together to tackle specific deployment environment challenges.

Table 4-1 maps HP-UX virtualization technologies to their Oracle Solaris counterparts.

TABLE 4-1. VIRTUALIZATION TECHNOLOGY MAPPINGS

TYPE	HP-UX 11i V3	ORACLE SOLARIS 11
Hard partitions	HP nPars	Dynamic Domains (Oracle's SPARC Enterprise M-Series servers only)
Virtual machines	HP vPars Integrity VM	Oracle VM Server for SPARC (Oracle's SPARC T-Series servers only) Oracle VM Server for x86 (x86 systems only) Oracle VM VirtualBox (x86 systems only)
Operating system virtualization	HP-UX Containers	Oracle Solaris Zones (also useful in situations where HP vPars were used)
Network virtualization	N/A	Network Virtualization
Storage virtualization	N/A	Oracle Solaris ZFS

Hard Partitioning

IT organizations that use HP nPars to maximize isolation can use the hard partitioning capabilities provided by Dynamic Domains. Available on Oracle's SPARC Enterprise M-Series servers, Dynamic Domains technology enables a single system to be divided into multiple electrically isolated partitions for maximum workload isolation. Each domain runs its own instance of Oracle Solaris—even different versions of the operating system—on dedicated hardware. A high-performance system, network, and I/O architecture eliminates overhead and delivers bare-metal performance to applications. Hardware and software failures are contained within a domain, increasing availability and providing a reliable, secure platform for running multiple applications simultaneously. These hard partitions also support the physical insertion or removal of system boards from a running domain without stopping the server or operating system.

- **Isolation.** HP nPars and Dynamic Domains both offer complete electrical isolation. While HP nPars permit CPU boards to be split into multiple domains, Dynamic Domains prohibit this action to maintain full electrical isolation.
- **Reconfiguration.** While only some HP nPars can be reconfigured dynamically, Dynamic Domains offer online reconfiguration of CPUs, memory, and I/O subsystems. System administrators can perform maintenance, live upgrades, and physical changes to hardware system resources while the server continues to execute applications. The ability to remove and add components from a running system helps to reduce system downtime, and simplify maintenance and upgrades by eliminating the need for system reboots after hardware configuration changes.
- **Configuration options.** HP nPars have configuration limits on some systems. For example, only half of the blades in the system can be configured into an nPar when using HP nPars on HP Superdome 2 systems. In contrast, Dynamic Domains allow the entire system to be configured as a single partition or divided into as many as 24 domains that can support thousands of Oracle Solaris Zones for further consolidation, isolation, and resource granularity.
- **Resource flexibility.** Unlike HP nPars, Dynamic Domains support CPUs with different clock speeds on the same system. System administrators can mix and match up to 32 or 64 quad-core SPARC 64 VII/VII+ processors and/or dual-core SPARC64 VI processors in the same system.
- **Migration.** Migration from HP nPars to Dynamic Domains requires few architectural changes. If HP nPars are used to host HP vPars or Integrity VM guests, the guests are required to use separate Dynamic Domains or Oracle VM Server for SPARC domains. Alternatively, they can be consolidated using Oracle Solaris Zones to maintain workload isolation.

More information on Dynamic Domains can be found in the Oracle SPARC M-Series Servers documentation.

Virtual Machines

IT organizations that use HP vPars or HP Integrity Virtual Machines (Integrity VM) can achieve similar levels of partitioning and isolation using Oracle VM Server for SPARC (previously called Sun Logical Domains). Purpose-built for Oracle's servers with chip multithreading technology, Oracle VM Server for SPARC provides a full virtual machine that runs an independent operating system instance and contains a wide range of virtualized devices. Unlike Integrity VM that uses an operating system as a hypervisor, Oracle VM Server for SPARC uses a hypervisor that largely resides in a chip on the server. Because the software is tightly integrated with the hardware, virtual machines can take advantage of underlying system advancements and reduce the overhead typically associated with software-based solutions such as Integrity VM.

Key differences between Oracle VM Server for SPARC and Integrity VM and HP vPars include:

- **Scalability.** Oracle VM Server for SPARC provides better scalability than HP vPars, making it ideal for small workloads. While HP vPars are limited to eight partitions per system, Oracle VM Server for SPARC supports up to 128 domains on a single server.
- **Virtualized resources.** HP vPars do not permit add-on networking or cryptographic devices to be partitioned, shared, or abstracted. Oracle VM Server for SPARC supports virtualized CPU, memory, storage, I/O, console, and cryptographic devices, and redundant I/O paths, to maximize resource utilization.
- **Dynamic configuration.** Integrity VM supports the dynamic configuration of vCPUs and adjustment of RAM size. On Oracle's SPARC Enterprise M-Series servers, dynamic reconfiguration of hardware is provided by Dynamic Domains, while Oracle VM Server for SPARC allows computing resources (CPUs, virtual I/O, cryptographic units, and memory) to be dynamically added, removed, and reconfigured on an active domain on Oracle's SPARC T-Series servers.
- **Virtual I/O.** Integrity VM supports virtual disks, DVDs and tape drives, and virtual network components such as vNICs, vSwitches, and VLANS. In Oracle Solaris, network virtualization is built into the operating system.
- **Additional tools.** Integrity VM includes tools to configure, create, start, stop, and migration virtual machines. Both offline and online (live) migration can be performed but require shared storage. In Oracle Solaris, system administrators can use physical to virtual (P2V) and virtual to virtual (V2V) migration tools in addition to higher-level management tools such as Oracle Enterprise Manager Ops Center. In addition, Oracle VM Server for SPARC supports the live migration of an active domain to another physical machine, with on-chip cryptographic accelerators providing secure, wire-speed encryption capabilities for the live migration process.
- **Performance.** Because Integrity VM uses and operating system as a hypervisor, it experiences significant performance overhead. In contrast, Oracle VM Server for SPARC uses a hypervisor that largely resides in hardware to reduce overhead and deliver more predictable performance. A large number of threads are supported, eliminating the need to share CPUs and create virtual CPUs that complicate scheduling, can cause resource contention, and add overhead.
- **Migration.** When migrating from Integrity VM guests to Oracle Solaris 11, few architectural changes are necessary. HP-UX guests can be deployed in Oracle VM Server for SPARC domains, or consolidated using Oracle Solaris Zones to maintain workload isolation.

More information can be found in the Oracle VM Server for SPARC Documentation.

Operating System Virtualization

IT organizations that use HP-UX Containers (formerly HP-UX Secure Resource Partitions) to consolidate and virtualize servers can take advantage of similar capabilities in Oracle Solaris Zones. Built into the operating system, Oracle Solaris Zones provision many secure, isolated runtime environments for individual applications using flexible, software-defined boundaries. Oracle Solaris Zones run under a single operating system kernel, enabling fine-grained control over rights and resources within a consolidated server without increasing the number of operating system instances to manage. Computing resources—CPUs, physical memory, network bandwidth, and more—can be dedicated to a single application one moment and shared with others in an instant, without moving applications or rebooting the system, dynamic domain, or logical domain where the Oracle Solaris Zone resides.

Because Oracle Solaris Zones are built into the operating system, they can be used on Oracle's entire range of SPARC and x86 processor-based servers—SPARC Enterprise M-Series, SPARC T-Series, and Sun Fire X-Series servers—enabling IT organizations to standardize on a virtualization technology across server architectures. Oracle Solaris 11 adds new capabilities to Oracle Solaris Zones, including:

- **Simplified consolidation.** A Preflight checker, `zonep2vchk(1M)`, can help system administrators identify identifies issues that could affect the migration from physical to virtual servers, and creates zone configuration output for the target zone.
- **Oracle Solaris 10 Zones on Oracle Solaris 11.** Oracle Solaris 10 Zones provide an Oracle Solaris 10 environment on Oracle Solaris 11. Organizations can use this feature to reap the benefits of Oracle Solaris 11 without disrupting existing applications, run legacy Oracle Solaris 10 applications, or test them on Oracle Solaris 11 platforms.
- **Immutable Zones.** Immutable zones allow the creation of a read-only copy of a zone and related Oracle Solaris ZFS file system, including the boot and root file systems. The ability to deploy read-only zones provides an additional security barrier to lock down applications and data resident to that zone. Providing read-only access to an application and its data further secures it and prevents unauthorized access or hacking. In addition, Oracle Solaris 11 network services are disabled by default in an immutable zone, or set to listen only for local system communications, to limit opportunities for unapproved access. Unless performed as specific maintenance operations, modifications to system binaries or system configurations are blocked.

Key differences between HP-UX Containers and Oracle Solaris Zones include:

- **Isolation.** Oracle Solaris Zones provide a better and more scalable multi-tenancy framework with extremely low overhead. This is made possible by a more complete set of isolation features, including zone-specific instances of the Service Management Facility, limited root access, read-only access support, assurance that zones cannot communicate or interfere with other zones, and more.
- **Scalability.** Oracle Solaris Zones running on Oracle's SPARC servers scale to more CPUs and cores than HP-UX running on HP's servers with Intel Itanium processors. In addition, the HP environment assumes that each HP-UX Container has its own physical network interface card, severely limiting

virtualization scalability on the system. Oracle Solaris Zones can take advantage of built-in network virtualization to share networking resources. Finally, Oracle Solaris Zones are included with the operating system at no additional cost, resulting in lower licensing costs that enable more workloads to be handled per hardware, energy, and power dollar spent.

- **Workloads.** Existing Oracle Solaris 10 workloads can be moved to Oracle Solaris 11 simply by placing them in an Oracle Solaris 10 Zone. In contrast, HP-UX Containers running on HP-UX 11i v3 can only run HP-UX 11i v3 workloads. In addition, users can install third-party software in Oracle Solaris Zones, something that is discouraged in HP-UX Containers. (System administrator installation is recommended.)
- **Security.** The security mechanisms inherent in Oracle Solaris Zones are stronger than those in HP-UX Containers. For example, HP-UX Containers do not permit the delegation of a container to a department unless users are given an account in the original container. In addition, users cannot be given root access to an HP-UX Container without also giving them root access to the complete HP-UX environment, creating potential security risks. Furthermore, every HP-UX Container has read/write access to system binaries, while Oracle Solaris Zones support read-only access (immutable zones) to limit what users and applications can do to the system and its applications. Finally, preventing HP-UX Containers from seeing or modifying files in other containers relies on file permissions, a mechanism that can be difficult to get right to ensure optimal protection. In fact, an HP-UX Container can be given permission to communicate directly with other compartments via inter-process communication (IPC), introducing the potential for one container to compromise another one—something that is not possible with Oracle Solaris Zones.
- **Availability and manageability.** In the event a service in an Oracle Solaris Zone fails, it is automatically restarted by the Service Management Facility rather than requiring manual intervention by system administrators. This is made possible by the fact that each zone contains its own instance of SMF, including a per-zone SMF repository and set of daemons. In addition, managing a zone is very similar to managing a physical Oracle Solaris system. In contrast, the tasks involved in managing an HP-UX Container are different from those used to manage physical HP-UX systems.
- **Rollback.** In Oracle Solaris 11, Oracle Solaris ZFS is the default file system. As a result, zones in the Oracle Solaris ZFS pool each have their own Boot Environment (BE). Updates to the operating system result in alternate BEs (ABEs). A zone can be booted into the old BE or the new ABE, enabling system administrators to undo configuration changes or software updates and revert to a previous version of the operating system with a simple zone reboot. HP-UX Containers do not offer a similar capability.
- **System observability.** Oracle Solaris includes the Oracle Solaris Dynamic Tracing (DTrace) facility, a tool that provides observability of application and operating system behavior. Hundreds of thousands of tracing points, or probes, are embedded in the Oracle Solaris kernel, utilities, and other software components to enable dynamic instrumentation of user-specified probes for recording data and examining the system in-depth. Trace points are completely passive until enabled for data collection, and can be disabled when observation no longer is required. DTrace can be used in a zone to examine applications, identify performance bottlenecks, and quantify application resource requirements.

- **Oracle Solaris Zones observability.** The `zonestat` command makes it easy to identify resource bottlenecks or misbehaving applications on a zone. With `zonestat`, administrators can monitor CPU, memory, and network utilization, compare utilization rates to resource control limits, and determine how these resources are used in the zone over specified periods of time.

For more information on Oracle Solaris Zones, see Oracle Solaris Administration: Oracle Solaris Zones, Oracle Solaris 10 Zones, and Resource Management.

Network Virtualization

While HP-UX requires third-party solutions to support network virtualization, Oracle Solaris 11 brings network virtualization and resource control into the operating system architecture to eliminate layered functionality with heavy overhead and undue complexity. Within the operating system, Network Virtualization virtualizes the network stack and allows fine-grained monitoring and control to let applications take advantage of improved network performance. It supports the parallelization of network workloads across multiple processor threads and cores. In addition, the use of on-NIC hardware acceleration enables dedicated bandwidth and resources to be provided to separate services and protocols without a performance penalty.

- **Virtual network interface cards.** In Oracle Solaris 11, a physical network card can be presented to applications as multiple VNICs. Each VNIC acts like any networking device on which an IP interface can be plumbed. The network stack and network interface card can be virtualized around any service protocol, such as HTTP, HTTPS, FTP, and NFS, or virtual environments created with Oracle VM Server for SPARC or Oracle Solaris Zones.
- **Automatic VNIC creation for Oracle Solaris Zones.** Automatic VNIC creation automatically creates a temporary virtual network interface controller for exclusive-IP non-global zones. The VNIC is created when the zone boots, and is deleted when the zone halts. Since VNIC configuration information resides in the zone, administrators do not need to recreate VNICs when moving zones between systems.
- **Network bandwidth sharing.** Multiple VNICs can be created on a physical NIC to maximize bandwidth utilization. Using the basic building blocks of VNICs, virtual switches, virtual interconnects, virtual LANs, virtual routing and virtual firewalls, high-bandwidth physical network connections can be carved up to enhance network utilization or aggregated as needed to meet peak workload demands. Similarly, multiple Gigabit Ethernet connections can be aggregated to offer a single, larger network connection with greater bandwidth to applications.
- **Bandwidth management.** Each virtual stack can be assigned its own bandwidth on a shared NIC without degrading performance. Traffic for one VNIC can be isolated from other traffic and assigned limits or guarantees on the amount of bandwidth it can use. Placing limits on bandwidth consumption improves network utilization and performance rates, and supports operating system virtualization, server consolidation, and cloud computing efforts. The architecture dynamically manages bandwidth resources, and can provide a better defense against denial of service attacks directed at a particular service or virtual

machine by isolating the impact to that entity. As a result, administrators can ensure key applications are not starved of network resources, keep critical backup operations from impacting network performance, and control the resources users receive more effectively.

- **Single-root I/O virtualization.** The trend toward greater server consolidation and virtualization is exposing software emulated I/O as a limiting factor. Similar to HP-UX, Oracle Solaris 11 supports the single-root I/O virtualization (SR-IOV) framework, defining extensions to the PCI Express (PCIe) specification to support the efficient sharing of PCIe devices among virtual machines in hardware and software.

For more information on Network Virtualization, see Oracle Solaris System Administration: Network Interfaces and Network Virtualization.

Summary of Comparable Virtualization Technologies

Table 4-2 summarizes the key differences between HP-UX and Oracle Solaris virtualization technologies.

TABLE 4-2. COMPARISON SUMMARY OF HP-UX AND ORACLE SOLARIS VIRTUALIZATION TECHNOLOGIES

VIRTUALIZATION TECHNOLOGIES		
TYPE	**HP-UX**	**ORACLE SOLARIS**
Hard Partitions	• HP nPars	• Dynamic Domains (Oracle's SPARC Enterprise M-Series servers) • Up to 24 domains per system
Virtual Machines	• HP vPars	• Oracle VM Server for SPARC (Oracle's SPARC T-Series servers) • Oracle VM VirtualBox (x86 servers only)
Operating System Virtualization	• HP-UX Containers	• Oracle Solaris Zones (Oracle's SPARC and x86 servers)
Network Virtualization	• Third-party add-ons • SR-IOV framework	• Built into the operating system • SR-IOV framework

VIRTUALIZATION TECHNOLOGY CHARACTERISTICS							
	HP-UX			**ORACLE SOLARIS**			
	NPARS	**VPARS**	**HP-UX CONTAINERS**	**DYNAMIC DOMAINS**	**ORACLE VM SERVER FOR SPARC**	**ORACLE SOLARIS ZONES**	**ORACLE VM VIRTUALBOX**
Electrical Isolation	√	—	—	√	—	—	—
Logical Isolation	√	√	√	√	√	√	√

TABLE 4-2. COMPARISON SUMMARY OF HP-UX AND ORACLE SOLARIS VIRTUALIZATION TECHNOLOGIES							
Mix CPU Speeds	—	—	—	√	—	√ (on Dynamic Domain)	—
Dynamic Reconfiguration	√	—	—	√	√	√	—
Resource Management	√	√	√	√	√	√	√
Built-in Network Bandwidth Sharing	—	—	—	√	√	√	√
Built-in Bandwidth Management	—	—	—	√	√	√	√
Shared SAN, iSCSI, NAS Storage	—	—	—	√	√	√	√
Physical to Virtual Migration Tools				√	√	√	
Virtual to Virtual Migration Tools			√	√	√	√	
Templates for Rapid Deployment					√	√	√
High Availability	HP Serviceguard	HP Serviceguard	HP Serviceguard	Oracle Solaris Cluster	Oracle Solaris Cluster	Oracle Solaris Cluster	

Chapter 5 Keeping Systems, Applications, and Services Available

Understanding the need to deliver reliable infrastructure, HP-UX and Oracle Solaris include tools for monitoring and managing systems and processes, as well as handling automatic failover, restart, and recovery in the event of a disruption in service due to hardware or software malfunction. Table 2-1 maps technologies for maximizing availability in HP-UX 11i v3 deployments to counterpart technologies for deploying highly available Oracle Solaris systems.

TABLE 5-1. AVAILABILITY TECHNOLOGY MAPPINGS

FUNCTIONALITY	HP-UX 11I V3	ORACLE SOLARIS
Fault detection, reporting, and recovery	System Fault Management (SFM)	Fault Management Architecture (FMA)
Configuring and managing system services	`init` run levels and `/etc/rc` start and stop scripts	Service Management Framework (SMF) in addition to `init` run levels
Clustering	HP Serviceguard	Oracle Solaris Cluster
Infrastructure and system monitoring and management	HP System Insight Manager, HP Insight Control, and HP Insight Dynamics	Oracle Enterprise Manager and Oracle Enterprise Manager Ops Center

Predictive Self Healing

Predictive Self Healing technologies proactively monitor and manage system components to help organizations optimize IT service availability. These technologies are built into Oracle Solaris to leverage hardware diagnostics, allowing business-critical applications and essential system services to continue uninterrupted in the event of software defects, major hardware component failures, and even misconfigured software. The Oracle Solaris Service Management Facility (SMF) and Oracle Solaris Fault Management Architecture (FMA) are the two main components of Predictive Self Healing.

Oracle Solaris Service Management Facility (SMF)

HP-UX uses System V UNIX `init` run levels and the `/etc/rc` model for configuring services and system daemons. Oracle Solaris 11 includes a standardized infrastructure for controlling system services — the Service Management Facility (SMF) — that augments the traditional `/etc/rc` start and stop scripts, `init` run levels, and configuration files.

SMF provides a framework that simplifies the management of system services and delivers improved ways to manage them. Services are treated as objects that administrators can consistently configure, enable, control, observe, and manage in a uniform way. Relationships and dependencies between services are easily defined and managed — an advantage over `/etc/rc` scripts. Information needed to manage each service is stored in a service repository. In the event of a failure, services are restarted automatically (along

with any dependent services), whether accidentally terminated by an administrator, aborted as the result of a software programming error, or interrupted by an underlying hardware problem. Administrators can be notified of service state transitions and fault management events via SNMP traps or email messages, providing better visibility into errors and improving debugging capabilities to help resolve service-related problems quickly.

Along with the installation and packaging technologies in Oracle Solaris, SMF is at the heart of initial system configuration tasks and a key part of the underlying software installation architecture. Different SMF services are activated on first reboot as a part of the operating system installation process, applying system configuration profiles to configure and activate services. During software package installations on a running system, SMF services can apply or refresh configuration caches as an alternative to post-installation scripts, at the same time taking into account defined service dependencies. SMF helps to apply configuration changes in a reliable and repeatable fashion, enabling more seamless and error-free software installations and upgrades.

Fault Management Diagnosis and Recovery

To increase system availability, the Fault Management Architecture (FMA) in Oracle Solaris helps to detect system problems, similar to the way System Fault Management (SFM) does in HP-UX. FMA goes further than simple detection and reporting by diagnosing faults and initiating recovery measures that can help to prevent outages. FMA tries to configure problem components out of a system before a failure occurs. In the event of a failure, it initiates automatic recovery using SMF. FMA builds a suspect list of root causes based on error patterns and identifies the likely associated system resources. Following this diagnosis step, FMA provides fault information to agents that know how to respond to specific faults.

At a high level, the FMA stack contains error detectors, diagnosis engines, and response agents. A Fault Management daemon (itself a service under SMF control) connects FMA components and acts as a multiplexor between them. FMA error detectors sense errors in the system and report them to a diagnosis engine. The diagnosis engine interprets the report, determines whether a fault or defect is present, and identifies a probable cause. The source of the problem may have an associated Automatic System Reconfiguration Unit (ASRU) or a Field-Replaceable Unit (FRU). An ASRU is a system resource that an FMA agent can disable to isolate the problem and suppress further error reports. In many cases an FRU can immediately be removed from the service, mitigating the problem until replacement is possible.

Oracle Solaris notifies administrators of FMA fault management events as well as SMF service state changes. Administrators can configure Simple Network Management Protocol (SNMP) trap notifications and Simple Mail Transport Protocol (SMTP) email notifications to watch for certain events or services. Systems often can automatically configure around a failed component and notify the system administrator of such an event. Notifications also can be sent directly to Oracle with Automated Service Requests (ASR), providing automatic telemetry for customers who have active Oracle support agreements and enabling a proactive response from Oracle service and support engineers.

For more information on SMF and FMA, see Oracle Solaris Administration: Common Tasks.

Clustering Technology

Strategic business applications demand continuous availability, so IT departments often configure clustering technologies when deploying data center systems to meet strict service-level agreements. Because organizations can implement geographically dispersed clusters, clustering technologies also are implemented to meet requirements for disaster recovery. For organizations that deploy local, campus, metropolitan, or worldwide clusters, Oracle Solaris Cluster extends high availability features built into the core Oracle Solaris 11 operating system, providing clustering functionality similar to HP Serviceguard.

Oracle Solaris Cluster is a comprehensive clustering framework that encompasses the core Oracle Solaris Cluster software, Oracle Solaris Cluster Geographic Edition, Oracle Solaris Cluster agents, and developer tools and support for clustering commercial and open-source applications. To optimize the availability of mission-critical applications and services in traditional or virtualized environments, Oracle Solaris Cluster provides load balancing, automatic fault detection, and failover.

Overview of Oracle Solaris Cluster

At its simplest, Oracle Solaris Cluster monitors the health of cluster components, including the stack of applications, middleware, operating system, servers, storage, network interconnects, and even Oracle Solaris Zones. Any failure executes a policy-based, application-specific recovery action. Recovery is enabled through redundant infrastructure and intelligent software algorithms.

From a physical perspective, an Oracle Solaris Cluster system consists of two or more nodes that work together as a single entity to cooperatively provide applications, system resources, and data to users (Figure 5-1). Each node provides some level of redundancy. Data is stored on highly available redundant disk systems, which may be mirrored, supporting data access in the event of a service interruption on a single disk or storage subsystem. Redundant connections are provided to disk systems so that data is not isolated in the event of a server, controller, or cable failure. A high-speed, redundant, private interconnect provides access to resources across the server set. Redundant connections to the public network also provide each node with multiple paths for access to outside systems, helping ensure continued access in the event of a network connection or node failure.

No single hardware, software, storage, or network failure can cause the cluster to fail. Loss of service is prevented through hardware redundancy, hardware and software failure detection, automatic recovery of services, and application failover. In addition, a single management view enables the entire cluster to be managed as a single entity, reducing the risk of errors.

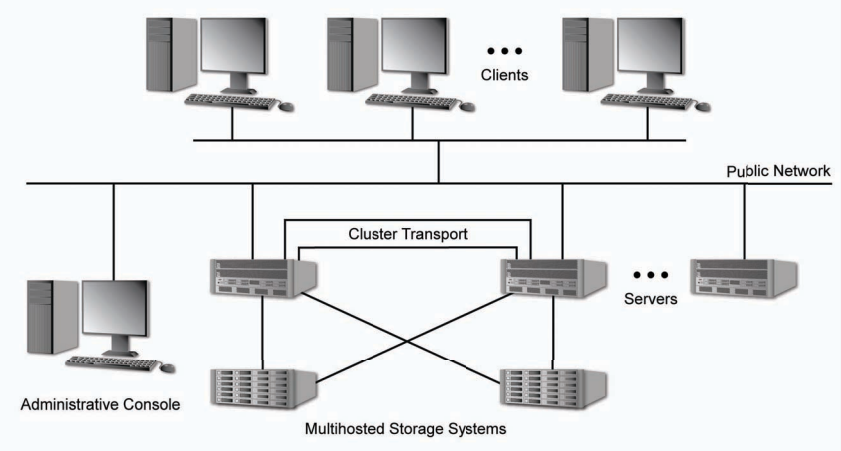

Figure 5-1. Oracle Solaris Cluster enables multiple servers and storage systems to act as a single system.

Oracle Solaris Cluster includes capabilities to detect, isolate, and contain failing cluster nodes. It accomplishes this using a robust, kernel-based membership monitor. Each node in the cluster sends out low-level Data Link Provider Interface (DLPI) packets once per second (a heartbeat) to each of its peers on each of the private networks. These packets are sent in the kernel interrupt context, making them very resilient to peaks in system load. A network, or path, between two nodes is declared down only if a heartbeat message does not complete the round trip between nodes over that specific path within the timeout period.

Network Availability

Oracle Solaris Cluster leverages Oracle Solaris IP network multipathing (IPMP) as public network interfaces for monitoring local failures, and for performing automatic failover from one failed network adapter to another. IP network multipathing enables a server to have multiple network ports connected to the same subnet. First, IP network multipathing software provides resilience from network adapter failure by detecting the failure or repair of a network adapter. The software simultaneously switches the network address to and from the alternate adapter. When more than one network adapter is functional, IP network multipathing increases data throughput by spreading outbound packets across multiple adapters.

For scalable data services, requests go through a round-robin load-balancing scheme for a balanced load distribution to the various instances of the distributed application running within the cluster. Scalable data services can be made more secure through the use of Internet Protocol security (IPsec) services in combination with Oracle Solaris Cluster load balancing services.

Data Integrity

Because cluster nodes share data and resources, Oracle Solaris Cluster works to ensure a cluster never splits into separate, active partitions that continue to access and modify data. Similar to HP Serviceguard, Oracle Solaris Cluster applies fencing techniques and a quorum to protect data integrity. Failing nodes are

isolated from the cluster and prevented from accessing clustered data. The fencing protocol can be chosen per storage device.

In a more complex situation where all paths across the private interconnect fail and the cluster breaks into multiple partitions, Oracle Solaris Cluster uses a quorum mechanism to recreate the cluster and resolve partitions or split brain syndrome, and to protect data integrity. The quorum also prevents amnesia by detecting and rejecting the use of outdated configuration information that could lead to data corruption.

The quorum can be tailored to the storage and system topology, enabling disk-based and software quorum solutions. A quorum device protocol permits the use of different types of disks, such as high-capacity 2 TB disk drives, SATA, and Flash as quorum devices. All quorum devices are continuously monitored to enhance availability.

Virtual Clustering

Oracle Solaris Cluster software also supports virtual clustering, allowing Oracle Solaris Zones to function in the role of cluster nodes. Virtual clusters allow organizations to deploy multiple applications or multi-tiered workloads on a single physical cluster configuration. Applications can run within a specific zone cluster under separate zone policy-based management. In the event of a zone failure, individual zones can be restarted or failed over. In this way, Oracle Solaris Cluster can protect applications that run in Oracle Solaris Zones, or Oracle Solaris 10 zones hosted on Oracle Solaris 11 systems.

Key Components

Key components of Oracle Solaris Cluster include:

- **High availability framework.** The framework detects node failures quickly and activates resources on another node in the cluster. It includes a Cluster Membership Monitor, a distributed set of algorithms and agents that exchange messages over the cluster interconnect to enforce a consistent membership view, synchronize reconfiguration, handle cluster partitioning, and help maintain full connectivity among all cluster members. Inter-node message delivery and responses are handled in an atomic manner that accounts for delivery failures, node membership, and software revision level to provide for rolling upgrades.
- **Failover, scalable, and cluster-aware agents.** Failover and scalable agents are software programs that enable Oracle or third-party applications to take full advantage of Oracle Solaris Cluster features. Cluster-aware applications have direct knowledge of Oracle Solaris Cluster systems, such as Oracle Real Application Clusters (RAC) software. Oracle Solaris Cluster agents specify the actions to be taken should an application fail. Many agents for Oracle and third-party enterprise applications are available, as shown in Table 5-2. Oracle Solaris Cluster includes built-in support for Oracle Solaris 11 services such as Apache, Apache Tomcat, DHCP, DNS, NFS, as well as additional Oracle software such as Oracle WebLogic Server and Oracle Database (single instance and Oracle RAC). If an agent does not exist for an application, one can be built using provided tools.

- **Highly available private interconnect.** Multiple types of interconnect technologies are supported by Oracle Solaris Cluster to establish a private communication channel between cluster nodes. Support for multiple interconnects helps to ensure high availability and improve performance of private inter-node communication. Heartbeats monitor cluster nodes over the private interconnect. If a server goes offline and ceases its heartbeat, it is isolated. Applications and data are failed over to another server quickly and transparently to users.

Key Features

Oracle Solaris Cluster extends Oracle Solaris to provide enhanced availability of hosted applications. Using the advanced capabilities in Oracle Solaris, Oracle Solaris Cluster offers:

- **Flexible configurations.** While HP Serviceguard supports N+1 clusters, Oracle Solaris Cluster supports pair, pair+N, N*1, N*N for flexible topologies, as well as clustering support for Oracle Solaris Zones.
- **Global devices, files, and networking.** All global devices, files, and network interfaces can be seen as local resources. Cluster nodes can access and utilize devices that are attached to another node within the cluster. These facilities create improved resource availability and simplified administration.
- **Virtualization support.** Oracle Solaris Cluster supports Oracle's virtualization portfolio — Oracle Solaris Zones, Oracle VM Server for SPARC available on Oracle's SPARC T-Series servers), and Dynamic Domains (available on Oracle SPARC Enterprise M-Series servers) — for flexible configurations that support consolidation efforts. Applications can run unmodified in virtualized environments.
- **Flexible storage support.** Oracle Solaris Cluster deployments can take advantage of a wide range of storage technologies, such as Fibre Channel, SCSI, iSCSI, and NAS storage solutions from Oracle and other vendors. Support for a broad range of file systems eases the data migration process.
- **Oracle RAC 10*g* and 11*g* integration and administration.** Automated installation and wizard-led configuration enable faster setup of Oracle RAC with Oracle Solaris Cluster. Specific Oracle RAC integration points enable improved coordination and simplified administration.
- **Campus and geographic clusters.** Oracle Solaris Cluster supports the creation of clusters across a campus or metropolitan area (campus cluster) or over large distances (geographic cluster) to support multi-site disaster recovery.

For more information on Oracle Solaris Cluster, see the Oracle Solaris Cluster Technical Information and Oracle Solaris Cluster Product Documentation.

Differences Between HP Serviceguard and Oracle Solaris Cluster

Table 5-2 summarizes the key differences between HP Serviceguard and Oracle Solaris Cluster.

TABLE 5-2. COMPARISON SUMMARY OF HP SERVICEGUARD AND ORACLE SOLARIS CLUSTER

ITEM	HP SERVICEGUARD	ORACLE SOLARIS CLUSTER
Configuration	• 2 to 16 nodes • Active/active, active/standby, rolling standby • N+1	• 2 to 16 nodes (SPARC), 2 to 8 (x86) • Active/active, active/standby, rolling standby • Pair, pair+N, N*1, N*N • Oracle Solaris Zones
Interconnects	• Ethernet, Fast Ethernet, Gigabit Ethernet • FDDI, Token Ring, HyperFabric2, Serial	• Ethernet, Fast Ethernet, Gigabit Ethernet • 10 Gigabit Ethernet, InfiniBand
Networking Protocols	• IPv4, IPv6, RDS	• IPMP, Trunking, Jumbo Frames, VLAN • IPv4, IPv6, SCTP, RDS
Disk Fencing	• Only when using VxFS	• Yes
File Systems	• Veritas VxFS	• Root: UFS, Oracle Solaris ZFS • Failover: UFS, Oracle Solaris ZFS, NFS • Cluster: PxFS, Oracle ASM • Support for Cluster File System (ACFS) and QFS coming soon
Volume Management	• Veritas Volume Manager • HP-UX Logical Volume Manager	• Oracle Solaris Volume Manager • Oracle Automatic Storage Management (ASM) • Oracle Solaris ZFS
Virtualization Support	• vPars	• Oracle Solaris Zones • Oracle VM Server • Dynamic Domains (on supported systems)
Monitoring	• System (heartbeat) • Network • Application	• System (heartbeat) • Network • Application • Quorum • Disk path • Storage resources
Workload Management	• Yes	• Yes
Cluster Management	• HP Event Monitoring Service • HP Serviceguard Manager	• Web-based GUI • Configuration Wizards • Object-oriented command line interface • Integrated with Oracle Enterprise Manager Ops Center • Integrated with SMF
Applications Support	• HP Serviceguard Extension for RAC	• Apache

	• HP Serviceguard Extension for SAP R/3	• Apache Tomcat
	• IBM DB2	• DHCP
	• Informix	• DNS
	• NFS	• NFS
	• Oracle Database	• Oracle E-Business Suite
	• Oracle RAC	• Oracle Database 11.2.0.3 single instance
	• Sybase	• Oracle Database 11.2.0.3 Real Application Clusters
		• Oracle WebLogic Server
		• Additional applications pending

System Monitoring and Management

For business-critical systems to achieve high service levels, proactive monitoring and management help to prevent system errors and faults from impacting application response time and user productivity. By closely monitoring performance metrics and system health, administrators can take action before a problem escalates, service delivery deteriorates, and unplanned downtime occurs. In large heterogeneous datacenters, streamlining administration also helps to lower operational costs and speed deployment. HP System Insight Manager, HP Insight Control, and HP Insight Dynamics are tools that aid in deploying and monitoring HP-UX systems in the enterprise.

To provide end-to-end IT management that extends from applications to systems, virtual machines, software, and storage, Oracle offers an integrated set of tools in the Oracle Enterprise Manager product line. The family of Oracle Enterprise Manager products enables management of the entire Oracle stack. Rich monitoring features support proactive application and systems management across the infrastructure for both Oracle and non-Oracle components.

A key part of the product family is Oracle Enterprise Manager Ops Center, which controls data center assets and simplifies physical and virtual server lifecycle management. The Ops Center software enables provisioning, patching, monitoring, administration, and configuration management via a Web-based user interface. As a result, it helps to reduce the complexity and cost associated with managing Oracle Solaris, Oracle VM Server, Linux, Unix, and Windows operating system environments. The tool helps administrators to gain insight into Oracle server, storage, and network components, helping them to manage large numbers of systems in a more scalable manner.

Oracle Enterprise Manager Product Family

The Oracle Enterprise Manager family of products provides comprehensive solutions for testing, deploying, operating, monitoring, diagnosing, and resolving problems in complex IT environments. Administrators can manage the entire application life cycle with comprehensive application quality management and compliance solutions.

- **Cloud Lifecycle Management.** Oracle Enterprise Manager is a complete cloud management solution that includes self-service provisioning using centralized, policy-based resource management, integrated chargeback and capacity planning, and visibility into the physical and virtual environment from applications to disk.
- **Application Management.** Oracle Enterprise Manager provides the most complete management solution for Oracle Fusion Middleware applications, Oracle E-Business Suite, and Oracle's Siebel PeopleSoft, and JD Edwards applications. It provides unique capabilities such as real user monitoring, zero-overhead instrumentation, and testing accelerators.
- **Middleware Management.** Delivering capabilities such as production diagnostics, model-driven topology mapping and business transaction management, Oracle Enterprise Manager is an end-to-end middleware management solution for Oracle Fusion Middleware environments.
- **Database Management.** From a single console, Oracle Enterprise Manager enables database manageability with real-time Automatic Database Diagnostic Monitor (ADDM) and Active Session History (ASH) analytics.
- **Application Performance Management.** Oracle Enterprise Manager provides a complete Application Performance Management (APM) solution for custom and Oracle applications, including Oracle E-Business Suite, Oracle Fusion Middleware, and Oracle's Siebel, PeopleSoft, and JD Edwards applications.
- **Application Quality Management.** Oracle Application Quality Management products provide a complete testing solution for Oracle Database, Oracle packaged applications, and custom Web applications.
- **Lifecycle Management.** Lifecycle Management is a comprehensive solution that helps database, system, and application administrators automate the processes needed to manage the lifecycle of Oracle technologies. It eliminates the manual and time-consuming tasks related to discovery, initial provisioning, patching, configuration management, and ongoing change management. In addition, it provides compliance frameworks for reporting and managing industry and regulatory compliance standards.
- **Exadata and Exalogic Management.** Oracle Enterprise Manager supports comprehensive and centralized health monitoring and management of hardware and software components in Oracle engineered systems, including Oracle Exadata Database Machine and Oracle Exalogic Elastic Cloud.
- **Hardware and Virtualization Management.** Described in more detail below, Oracle Enterprise Manager Ops Center combines the management of servers, operating systems, firmware, virtual machines, storage, and network fabrics into a single console. It delivers an integrated solution for physical and virtual server lifecycle management, providing comprehensive provisioning, patching, monitoring, administration, and configuration management.
- **Heterogeneous Management.** Oracle Enterprise Manager provides an extensible and customizable IT management framework. System Monitoring Plug-ins, developed both by Oracle and third-party vendors, add visibility into the underlying database, middleware, applications software, and hardware components. Oracle Enterprise Manager can be integrated with legacy third-party management tools

and help desk systems, either by forwarding monitoring events or through the customized actions of Management Connectors. Management Connectors provide the bi-directional exchange of alerts, automatic help desk ticket creation, and seamless workflow for incident management and resolution. An HP OpenView Operations Connector, for example, enables bi-directional, end-to-end event and alert sharing between HP OpenView and Oracle Enterprise Manager, streamlining the correlation of availability and performance problems.

Oracle Enterprise Manager Ops Center

Designed to simplify the management of large numbers of IT systems, Oracle Enterprise Manager Ops Center is a comprehensive tool for managing Oracle Solaris, Oracle VM Server, Linux, and Windows servers — from firmware, server status, energy use, and operating systems, to virtual machines, storage, and network fabrics. Administrators use a centralized dashboard to gain cross-stack visibility into infrastructure resources (Figure 5-2). Capabilities include asset discovery, firmware and operating system provisioning, automated patch and configuration management, virtualization management, and compliance reporting.

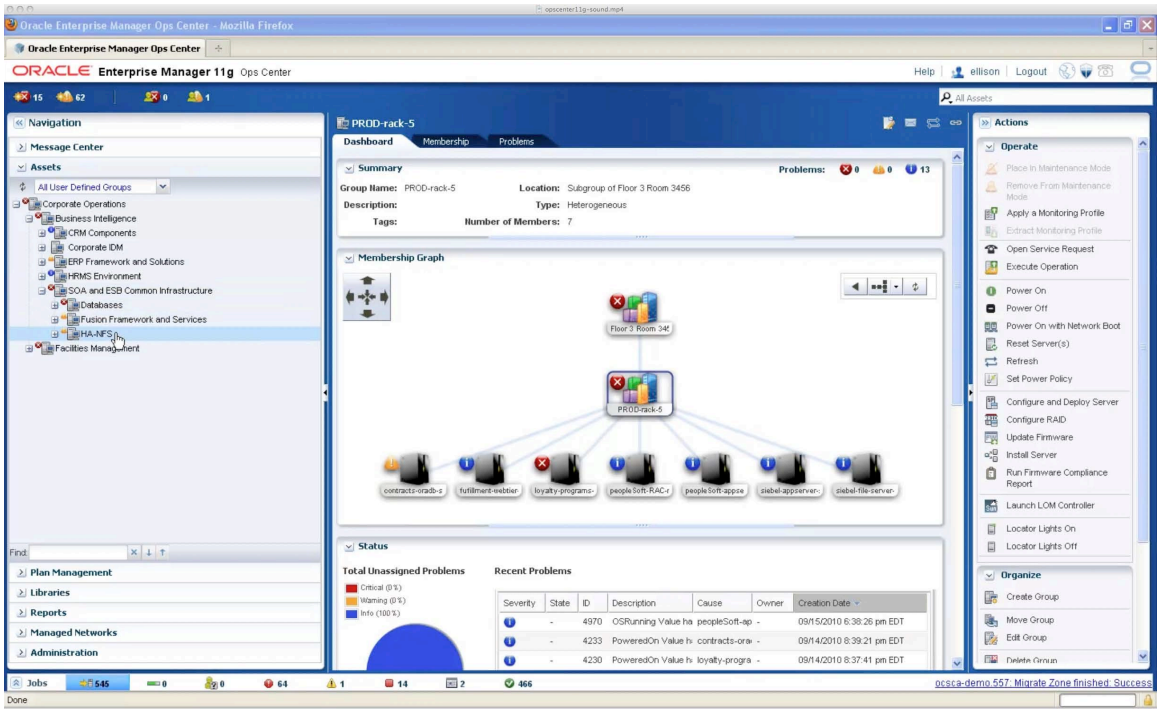

Figure 5-2. The Oracle Enterprise Manager Ops Center dashboard provides a comprehensive view of managed assets.

Oracle Enterprise Manager Ops Center includes these capabilities:

- **Systems monitoring.** Oracle Enterprise Manager Ops Center provides data about potential faults, performance metrics, and system health so that operational staff can resolve issues and take action, helping to prevent downtime.
- **Energy monitoring.** Modern servers use built-in service processors to monitor power consumption, making it possible for Oracle Enterprise Manager Ops Center to monitor and report on energy use for individual or logical groups of systems.
- **Operating system software monitoring.** Oracle Enterprise Manager Ops Center automatically installs lightweight software agents that track operating system performance characteristics, displaying collected data in easy-to-understand graphs and tables. Administrators can set site-specific thresholds to limit the amount of reported data, reducing administrative overhead and improving an operator's ability to detect problems.
- **Point-in-time provisioning.** Oracle Enterprise Manager Ops Center can discover new datacenter assets and access service processors on these systems to capture location identifiers, power states, network boot configurations, and firmware versions. Administrators can trigger firmware updates as needed. To expedite the deployment of new systems in the datacenter, Oracle Enterprise Manager Ops Center streamlines network configuration, automatically identifying MAC addresses, tracking ports, and maintaining this information in the DHCP configuration. Once the network is configured, Oracle Enterprise Manager Ops Center can use operating provisioning technologies such as the Oracle Solaris 11 Automated Installer, Oracle Solaris 10 JumpStart, Kickstart, or AutoYaST tools. Administrators can save common installation profiles and install new systems from them.
- **Software lifecycle management.** Operating system vendors commonly offer software updates to address security concerns, fix defects, or add new features. Oracle Enterprise Manager Ops Center creates dependency trees across software components, including trees for Oracle Solaris, Oracle Linux, Red Hat Enterprise Linux, Attachmate/Novell SUSE Linux, and Microsoft Windows distributions. By scanning patch readme files, package dependency files, RPM package manager header files, and other sources, Oracle Enterprise Manager Ops Center performs periodic baseline analysis on software update recommendations. Software updates to Oracle Solaris 11 take advantage of its Image Packaging System technology and Boot Environment capabilities, allowing administrators to update a clone of the active boot image, minimizing downtime for system upgrades and kernel package updates.
- **Virtualization management.** Oracle Enterprise Manager Ops Center allows administrators to manage the full lifecycle of virtual machines defined with Oracle Solaris Zones, Oracle VM Server for x86, or Oracle VM Server for SPARC. Administrators can create, delete, stop, start, clone, and change the configuration of a virtual machine, and perform all of these actions on logical system groupings for efficient virtual machine management and provisioning.

For more information, see the Oracle Enterprise Manager Ops Center resources page.

Chapter 6 Keeping Infrastructure Secure

HP-UX and Oracle Solaris are two of the most secure enterprise-grade UNIX environments. A wide range of security features are available in both operating systems, from role-based access controls (RBAC) that provide fine-grained permission management, to trusted extensions for labeling and containing data when working in highly sensitive and secure environments. While HP-UX provides extensive security tools for protecting host systems, Oracle Solaris takes security further with a defense-in-depth approach that protects physical and virtual systems, networks, and data. These security capabilities, combined with built-in virtualization technologies, are essential as IT organizations move to the multiple tenant environments of cloud computing.

Table 2-1 maps key security technologies in HP-UX 11i v3 deployments to associated technologies in Oracle Solaris systems.

TABLE 6-1. SECURITY TECHNOLOGY MAPPINGS

FUNCTIONALITY	HP-UX 11I V3	ORACLE SOLARIS
Fine-grained privilege management	Role-based access control	Role-based access control Root account replaced with root role
Secure remote login	Secure Shell	Secure Shell with X.509 certificate extensions
On-disk encryption	HP-UX Encrypted Volume and File System (EVFS)	Oracle Solaris ZFS dataset encryption Oracle Solaris Cryptographic Framework
System hardening	HP-UX Bastille	Oracle Solaris Secure By Default configurations Basic Audit Reporting Tool (BART)
Trusted computing	HP-UX Trusted Computing Base	Oracle Solaris Trusted Extensions Labeled IPsec Labeled Oracle Solaris ZFS datasets
Firewall	IP Filter	IP Filter with SMF integration
Application isolation	HP-UX Secure Resource Partitions	Oracle Solaris Zones Optional private IP stack per zone without dedicated hardware

More information on these security topics can be found in the Oracle Solaris 11 Security Guidelines and Oracle Solaris Administration: Security Services manuals.

Role-Based Access Control

Many traditional UNIX systems have limited protection mechanisms. For example, the commonly used superuser (`root`) account has long been an issue when trying to keep UNIX systems secure. Without fine-grained controls, providing access to the root account is an all or nothing step. Even the most junior administrators have complete access. Anyone with the root password can log in directly, leaving no audit trail or indication of who is using this wide-open access mechanism.

Oracle Solaris offers unique user and process rights management technology that reduces security risks by granting users and applications only the minimum capabilities needed to perform tasks. Process rights management enables processes to be restricted at the command, user, role, or system level. In Oracle Solaris, process rights management is implemented through a privilege mechanism. Privileges decrease the security risk that is associated with a user or process having full superuser capabilities on a system.

Privileges and role-based access control (RBAC) provide a compelling alternative to the traditional superuser model. In the RBAC model on Oracle Solaris, users log in as themselves and assume roles when needed that enable them to perform tasks that require elevated privileges. In Oracle Solaris 11, even root access follows this model. By making root a role, users cannot log in as root directly. Administrators must first log in under their regular user ID. When root privileges are needed, administrators must enter a password to assume to root role. Removing direct access to the root account provides better audit trails that are tied to a specific user and makes the system more secure.

Most UNIX systems include a `setuid` mechanism that can be set on a command to enable any user who runs it to run as specific user — usually `root` — to perform a specific task. A `setuid` root executable has complete access to the system and network when the command is running. As a result, compromising a `setuid` executable can give an attacker unrestricted access to the system. Oracle Solaris uses a privilege framework that allows fine-grained control of what a process can do, such as read or write files, gain network access, or manipulate processes. These controls can be used to limit the capabilities granted to any privileged executable to only the specific rights that are needed for the task. This can significantly limit potential vulnerabilities associated with `setuid` executables.

More information on RBAC in Oracle Solaris can be found in the Roles, Rights Profiles, and Privileges section of the Oracle Solaris Administration: Security Services guide.

On-Disk Encryption

Keeping data secure when it is at rest is just as important as keeping it safe as it travels over networks. Using encryption to protect files can help protect information from being stolen or manipulated in the event of a network security breach. Similar to the HP-UX Encrypted Volume and File System (EVFS) capabilities that enable files, file systems, or volumes to be encrypted, Oracle Solaris ZFS supports encrypted datasets. The ability to encrypt datasets helps protect against the theft of devices, man-in-the-

middle attacks on the SAN, and dataset-level secured deletion. In addition, just as HP-UX EVFS is integrated with HP Serviceguard, Oracle Solaris ZFS is integrated with Oracle Solaris Cluster to support highly available, secure infrastructure deployments.

Because data is encrypted at the dataset level rather than on a per-disk basis, users can place a mix of encrypted and unencrypted information on the same storage pool. Whether or not to encrypt data in a dataset is determined at dataset creation, and user data and file system metadata are encrypted using a sophisticated encryption key management facility to support different key management strategies.

Oracle Solaris ZFS uses the cryptographic framework built into the operating system to enable cryptographic protection of data on a per-dataset basis. Based on the PKCS#11 public key cryptography standard created by RSA Security, Inc., the framework provides a mechanism and API whereby both kernel- and user-based cryptographic functions can transparently use software encryption modules and hardware accelerators configured on the system. Applications that run on Oracle's SPARC T-Series servers and use the cryptographic framework gain an added benefit: cryptographic operations are offloaded automatically to an on-chip cryptographic accelerator in the server for improved performance.

The framework provides various services, including message encryption and message digest, message authentication, and digital signing. It also includes APIs for accessing cryptographic services, and SPIs for providing cryptographic services. New cryptographic enhancements in Oracle Solaris 11 include support for FIPS 140-2 of the Federal Information Processing Standard, and the implementation of ECC and other NSA Suite B protocols to meet stringent government standards. These highly-optimized routines are used automatically by Oracle Solaris ZFS, the Java Cryptography Extension (JCE), Kerberos, IPsec, and other components in Oracle Solaris.

More information on the cryptographic framework can be found in the Cryptographic Services section of the Oracle Solaris Administration: Security Services guide.

Host Security

HP-UX and Oracle Solaris contain mechanisms for ensuring host security. In HP-UX, this is accomplished through the HP-UX Bastille configuration tool for managing security settings. Oracle Solaris takes a different approach, building many security features directly into the operating system. The system can be hardened and minimized by installing reduced configurations with fewer software packages, no active networking, and a minimum number of running services. In addition, Oracle Solaris 11 provides a *secure-by-default* environment that disables network services by default, or sets them to listen only for local system communication, to limit opportunities for unauthorized access.

The security management capabilities provided by HP-UX Bastille — hardening capabilities, firewall management, account policies, and assessment reports — are largely built into Oracle Solaris. Additional facilities are handled by a combination of Solaris IP Filter, the Basic Auditing Reporting Tool (BART), and the Service Management Facility. In addition, many tools are available to query the information kept by the operating system and modify settings.

- **Basic Auditing Reporting Tool.** This tool validates systems by performing file-level checks of a system over time. By creating a baseline manifest for a newly installed and configured system, it is possible to gather information about installed software. This baseline information can be compared to a snapshot of the system at a later time. A generated report lists file-level changes that have taken place since system installation, enabling administrators to verify that no accidental or malicious changes have been made to the environment.
- **Image Packaging System.** The manifest maintained by the Imaging Packaging System describes all package files and their permissions. This information can be used to verify the integrity of installed packages by using the `pkg verify` command. In addition, Oracle Solaris 11 digitally signs all packages to ensure authenticity can be verified.
- **Audit access.** The Oracle Solaris audit feature provides the ability to log system activity for any auditable Oracle Solaris event—such as system calls on the server machine, packets sent over the network, or a sequence of bits written to disk—at a granular level. Starting with Oracle Solaris 11, auditing is a service that is managed by SMF, and auditing records are stored in binary files on an Oracle Solaris ZFS file system. System reboots are not required to enable auditing. The */etc/security/audit_user* and */etc/security/audit_control* files, and the *bsmconv/unconv* script, no longer are used.

See Using the Basic Audit Reporting Tool, Verifying Package Installation, and Monitoring SMF Services for more information.

Network Security

A key component of the defense-in-depth approach to security in Oracle Solaris is extensive network security. Designed to protect physical and virtual systems and networks, Oracle Solaris creates a fully virtualized and secure network that provides protection even if intruders gain access to physical or virtual systems.

- **Secure by default configuration.** When Oracle Solaris is installed, a large set of network services are disabled by default. In this Secure by Default configuration, the only network service that accepts network requests is the `sshd` daemon. All other network services are disabled or only handle local requests. These services are managed just like all other services, using the Service Management Facility (SMF). As a result, administration is simplified. Individual network services, such as `ftp`, can be enabled through the SMF interface.
- **Integrated firewall.** Both HP-UX and Oracle Solaris include an integrated firewall that is based on the open source IP Filter software. IP Filter provides basic firewall services and network address translation (NAT). In Oracle Solaris 11, the IP Filter software is configured and managed using SMF. The `pfil` module is replaced by packet filter hooks, streamlining the procedure to enable the IP Filter software. Through these hooks, IP Filter uses pre-routing (input) and post-routing (output) filter taps to control packet flow into and out of the Oracle Solaris system. The results are improved performance and the ability to filter traffic between Oracle Solaris Zones.

- **Secure Shell with X.509 certificate extensions.** Both HP-UX and Oracle Solaris include the Secure Shell (`ssh`) for secure remote login. In Oracle Solaris 11, the `ssh` utility is extended to allow the use of X.590 certificates for authenticating users and hosts. This makes the use and administration of the `ssh` utility more straightforward and secure. Users do not need to populate authorized key files on each host or answer prompts to verify a host's authenticity since it can be verified using the host's X.509 certificate.

For more information on the IP Filter implementation in Oracle Solaris, see the "IP Filter in Oracle Solaris (Overview)" section of the Oracle Solaris Administration: IP Services guide.

Server Virtualization Security

HP-UX and Oracle Solaris include virtualization capabilities. At the server virtualization level, HP-UX Containers (formerly called HP-UX Secure Resource Partitions) are similar to Oracle Solaris Zones. Both technologies give administrators a richer set of options for securing and isolating applications than is available using physical hosts. While similar in concept and functionality, Oracle Solaris Zones provide more comprehensive security features, such as the ability to delegate administration for individual zones without giving away administrative access to the host system.

- **Delegated administration.** Oracle Solaris enables the delegation of common administrative tasks for specific zones to specific administrators using role-based access controls. This is particularly powerful in a shared environment where it is desirable to allow specific users to only manage zones that are relevant to their role.
- **Zone link protection.** In many virtualized environments, it is common for the host administrator to grant exclusive access of a physical link or a virtual network interface card (NIC) to a guest virtual machine. Doing so enables guests to benefit from traffic isolation and improved performance. On the other hand, guests can generate any type of traffic, even harmful packets, and send it over the network. Oracle Solaris 11 provides a new link protection mechanism for preventing potentially malicious or misbehaving guest virtual machines from sending harmful packets to the network. This feature provides protection against basic threats, including IP, DHCP, MAC, and L2 frame spoofing.
- **Exclusive IP Zones.** In many virtualization environments, a dedicated physical network interface controller is needed to achieve network separation between virtual environments. Exclusive-IP Zones in Oracle Solaris give administrators the ability to assign a separate IP stack for each zone. The stack is completely separate from all other zones yet does not require the expense or complexity of a dedicated network connection.
- **Immutable Zones (read-only root).** Oracle Solaris supports the creation of Immutable Zones — zones that have read-only file systems. Using mandatory write access control, read-only file systems cannot be modified by processes running in the zone, even those with root privileges. Writes can take place only in the system's global zone.

Trusted Computing

Oracle Solaris includes Trusted Extensions, an optional layer of secure labeling technology that enables data security policies to be separated from data ownership. These capabilities are similar to the Trusted Computing Base (TCB) extensions that are available for HP-UX. In the past, both HP-UX and Oracle Solaris offered these security extensions as separate products with separate release schedules, which complicated support for the secure versions of the operating system. Over time many security features, including trusted extensions, were integrated into the Oracle Solaris and HP-UX base operating systems, eliminating the need to install add-on products.

The following highlight the key aspects of security extensions and how they work in Oracle Solaris.

- **Enforced policies and labels.** In HP-UX, compartments are used to isolate resources. When used, everything related to an application—binaries, processes, files, and communication channels—has limited access to resources outside the compartment to minimize system damage in the event the application is compromised. In Oracle Solaris, Trusted Extensions enforce a mandatory policy based on security labels. Going a step further than HP-UX compartments, Trusted Extensions enforce labeled separation for desktop clients, labeled networking, and file system labeling.
- **Labels and access control.** Trusted Extensions supports traditional discretionary access control (DAC) policies based on ownership, as well as label-based mandatory access control (MAC) policies. When the label-based MAC policies are enabled, all data flows are restricted based on a comparison of the labels associated with the processes (subjects) requesting access and the objects containing the data. Unlike most other multi-level operating systems, Oracle Solaris includes a multi-level desktop.
- **Network traffic.** When labeled processes in a multi-level secure operating system communicate across system boundaries, their network traffic must be labeled and protected. Typically this requirement is met by using physically separate network infrastructure to ensure that data belonging to different labeled domains stays in separate physical infrastructures. In Oracle Solaris 11, security labels on packets received from remote hosts and labeled IPsec/IKE, enables organizations to reuse the same physical network infrastructure for labeled communications by transferring labeled data within separate labeled IPsec security associations, removing the need for redundant and expensive physical network infrastructure.
- **Credentials.** To enable greater flexibility and security, the Trusted Extensions feature in Oracle Solaris 11 enables per-label and per-user credentials. As a result, administrators can require a unique password for each label. Since this password is in addition to the session login password, administrators can set a per-security zone encryption key for each label of every user's home directory.
- **Datasets.** In Oracle Solaris 11, Trusted Extensions enables security labels to be set on Oracle Solaris ZFS datasets. When used, the security labels ensure that Oracle Solaris ZFS file systems used for a specific security label cannot be mounted on a physical or virtual system with a different security label. This restriction helps to avoid the inadvertent upgrade or downgrade of the classification of data.

- **Certification.** Oracle Solaris Trusted Extensions meet the requirements of the Common Criteria Labeled Security Protection Profile (LSPP), the Role-Based Access Protection Profile (RBACPP), and the Controlled Access Protection Profile (CAPP). What makes the Oracle Solaris implementation unique is its ability to provide high assurance while maximizing compatibility and minimizing overhead.
- **Trusted Platform Module.** HP-UX provides a kernel driver for communication with an optional microcontroller, called a Trusted Platform Module (TPM), that stores digital certificates, keys, and passwords. Software based on TrouSerS, the open source Trusted Computing Group (TCG) Software Stack, provides access to RSA key pair generation, encryption, decryption, and storage. Oracle Solaris provides similar functionality. It includes the TrouSerS package, a PKCS#11 provider for using the TPM to store keys, and a `tpmadm` utility for performing administrative functions and viewing the state of TPM registers.

For more information, see the Oracle Solaris Trusted Extensions User's Guide.

Chapter 7 For More Information

Additional information and resources can be found in the references listed in Table 7-1.

TABLE 7-1. ADDITIONAL READING

ORACLE SOLARIS	
Oracle Solaris	http://www.oracle.com/solaris
Oracle Solaris 11 Documentation	http://docs.oracle.com/cd/E23824_01/
Oracle Solaris 11 How-To Articles	http://www.oracle.com/technetwork/server-storage/solaris11/documentation/how-to-517481.html
Oracle Solaris 11 What's New	http://www.oracle.com/technetwork/server-storage/solaris11/documentation/solaris11-whatsnew-201111-392603.pdf
DATA MANAGEMENT	
Oracle Solaris Administration: Devices and File Systems	http://download.oracle.com/docs/cd/E23824_01/html/821-1459/index.html
Oracle Solaris Administration: ZFS File Systems	http://download.oracle.com/docs/cd/E23824_01/html/821-1448/index.html
Oracle Solaris Administration: SAN Configuration and Multipathing	http://docs.oracle.com/cd/E23824_01/html/E23097/index.html
HIGH AVAILABILITY AND SYSTEM MANAGEMENT	
Oracle Solaris 11 Administration: Common Tasks	http://docs.oracle.com/cd/E23824_01/html/821-1451/toc.html
Oracle Solaris Cluster	http://www.oracle.com/technetwork/server-storage/solaris-cluster/index.html
Oracle Solaris Cluster Technical Information	http://www.oracle.com/technetwork/server-storage/solaris-cluster/overview/index.html
Oracle Solaris Cluster Product Documentation	http://www.oracle.com/technetwork/server-storage/solaris-cluster/documentation/index.html
Oracle Solaris Cluster Training	http://www.oracle.com/technetwork/server-storage/solaris-cluster/training/index.html
Oracle Enterprise Manager 12c	http://www.oracle.com/technetwork/oem/grid-control/overview/index.html
Oracle Enterprise Manager Extensions Exchange	http://www.oracle.com/technetwork/oem/extensions/index.html
Oracle Enterprise Manager 12c Cloud Control Documentation	http://docs.oracle.com/cd/E24628_01/index.htm

NETWORKING	
Oracle Solaris Administration: IP Services	http://docs.oracle.com/cd/E23824_01/html/821-1453/index.html
Oracle Solaris Administration: Naming and Directory Services	http://docs.oracle.com/cd/E23824_01/html/821-1455/index.html
Oracle Solaris Administration: Network Interfaces and Network Virtualization	http://docs.oracle.com/cd/E23824_01/html/821-1458/index.html
Oracle Solaris Administration: Network Services	http://docs.oracle.com/cd/E23824_01/html/821-1454/index.html
Oracle Solaris Administration: IP Services	http://docs.oracle.com/cd/E23824_01/html/821-1453/index.html
SECURITY	
Oracle Solaris 11 Security Guidelines	http://docs.oracle.com/cd/E23824_01/html/819-3195/index.html
Oracle Solaris Administration: Security Services	http://docs.oracle.com/cd/E23824_01/html/821-1456/index.html
Oracle Solaris Trusted Extensions User's Guide	http://docs.oracle.com/cd/E23824_01/html/821-1484/index.html
Trusted Extensions Configuration and Administration	http://docs.oracle.com/cd/E23824_01/html/821-1482/index.html
Trusted Extensions Label Administration	http://docs.oracle.com/cd/E23824_01/html/821-1481/index.html
SERVICES	
"How to Create an Oracle Solaris Service Management Facility Manifest" white paper	http://www.oracle.com/technetwork/server-storage/solaris/solaris-smf-manifest-wp-167902.pdf
"Management of Systems and Services Made Simple with the Oracle Solaris Service Management Facility" white paper	http://www.oracle.com/technetwork/server-storage/solaris/solaris-smf-wp-167901.pdf
"Managing Services"	http://docs.oracle.com/cd/E23824_01/html/821-1451/dzhid.html
SOFTWARE MANAGEMENT	
Installing Oracle Solaris 11 Systems	http://docs.oracle.com/cd/E23824_01/html/E21798/index.html
Creating and Administering Boot Environments After Installation	http://docs.oracle.com/cd/E23824_01/html/E21801/index.html
Creating a Custom Oracle Solaris 11 Installation Image	http://docs.oracle.com/cd/E23824_01/html/E21800/index.html
Adding and Updating Oracle Solaris 11 Software Packages	http://docs.oracle.com/cd/E23824_01/html/E21802/index.html
Copying and Creating Oracle Solaris 11 Package Repositories	http://docs.oracle.com/cd/E23824_01/html/E21803/index.html

Oracle Solaris 11 Installation Man Pages	http://docs.oracle.com/cd/E23824_01/html/E21797/index.html
Image Packaging System Map Pages	http://docs.oracle.com/cd/E23824_01/html/E21796/index.html
VIRTUALIZATION	
Oracle Solaris Administration: Oracle Solaris Zones, Oracle Solaris 10 Zones, and Resource Management	http://docs.oracle.com/cd/E23824_01/html/821-1460/index.html
Oracle Solaris Administration: Network Interfaces and Network Virtualization	http://docs.oracle.com/cd/E23824_01/html/821-1458/index.html
OTHER ADMINISTRATION	
HP-UX to Oracle Solaris 11 Evaluation Page	http://www.oracle.com/technetwork/server-storage/solaris11/overview/hp-ux-mapping-guide-1557285.html
Oracle Solaris Tunable Parameters Reference Guide	http://docs.oracle.com/cd/E23824_01/html/821-1450/index.html
Oracle Solaris Administration: SMB and Windows Interoperability	http://docs.oracle.com/cd/E23824_01/html/821-1449/index.html
How to Perform System Archival and Recovery Procedures with Oracle Solaris 11	http://www.oracle.com/technetwork/articles/servers-storage-admin/o11-091-sol-dis-recovery-489183.html
International Language Environment Guide	http://docs.oracle.com/cd/E23824_01/html/E26033/index.html
TRAINING	
Oracle Solaris 11 Training and Support	http://www.oracle.com/technetwork/server-storage/solaris11/training/index.html
Oracle University	http://education.oracle.com/

Appendix A Glossary

Access Control List (ACL)
A file containing a list of principals with certain access permissions. Typically, a server consults an access control list to verify that a client has permission to use its services.

Agent Builder
A component of Oracle Solaris Cluster that automates the creation of a data service.

API
Application programming interface.

appcert
A utility that examines an application's conformance to the Oracle Solaris Application Binary Interface. Use of the appcert utility can help identify potential binary compatibility issues when porting applications to Oracle Solaris.

Authentication
A security service that verifies a claimed identity.

Authorization
The process of determining whether a user can use service, which objects the user can access, and the type of access allowed.

Big Endian
An architecture that stores the most-significant byte of data first. Oracle Solaris uses a Big Endian architecture on SPARC processor-based systems and a Little Endian architecture on x86 platforms.

Bourne shell
The default shell in Oracle Solaris 10. The shell is found in `/usr/bin/sh`.

Chip-Multithreading Technology
Multithreaded processor technology that enables each processor core to switch between multiple threads on each clock cycle.

CMT
Chip-Multithreading Technology.

Data transformation
The process of converting data from one format to another.

DTrace
See Oracle Solaris DTrace.

ETL utilities
Extract, Transform, and Load utilities, tools that take a wide array of formats and convert them into Structured Query Language (SQL) for relational database management systems.

Hybrid Storage Pool
A combination of disk drives and Flash devices that work together to minimize the impact of disk latencies and improve application performance. Flash devices handle certain types of I/O while hard disk drives store massive data sets. Hybrid Storage Pools are enabled by Oracle Solaris ZFS.

Korn shell
Oracle Solaris 10 supports `ksh88` (located in `/usr/bin/ksh`). Oracle Solaris 11 provides ksh93 as the default shell (located in `/usr/bin/ksh`), as well as `ksh88` (located in `/usr/sunos/bin/ksh`) for compatibility.

Little Endian
An architecture that stores the least-significant byte of data first. Oracle Solaris uses a Little Endian architecture on x86 systems and a Big Endian architecture on SPARC processor-based platforms.

Oracle Solaris Cluster
A high availability solution for Oracle Solaris that is integrated at the kernel level. It monitors servers, storage, network components, operating system, virtual machines, and applications. Recovery actions are based on policies and application specifications.

Oracle Solaris Cryptographic Framework
A framework built into Oracle Solaris that provides kernel-level and user-level consumers with access to software-based or hardware-based cryptographic capabilities.

Oracle Solaris DTrace
A dynamic tracing facility built into Oracle Solaris that lets developers observe operating system and application behavior in real time.

Oracle Solaris Key Management Framework
A framework that provides tools and programming interfaces for managing PKI objects.

Oracle Solaris Service Management Facility
A facility introduced in Oracle Solaris 10 that simplifies service management and control.

Oracle Solaris Studio
A free, comprehensive C, C++, and Fortran tool suite for Oracle Solaris and Linux operating systems that accelerates the development of scalable, secure, and reliable enterprise applications.

Oracle Solaris ZFS
A 128-bit file system that integrates volume management and provides virtually unlimited file system scalability.

Oracle VM
Scalable server virtualization software that supports Oracle and non-Oracle applications.

Package
A collection of files and directories required for a software product. On Oracle Solaris, applications are distributed for deployment in packages.

PKI
Public Key Infrastructure.

POSIX
Portable Operating System Interface for UNIX. A set of standards that provide a well-defined system call interface for kernel facilities, as well as shell and utilities interfaces.

Privilege
A discrete right that can be granted to an application.

SMF
See Oracle Solaris Service Management Facility.

Trusted Extensions
An optional layer of secure label technology in Oracle Solaris that allows data security policies to be separated from data ownership. Multilevel data access policies support compliance goals.

UFS
UNIX File System, the default file system in Oracle Solaris 10.

ZFS
See Oracle Solaris ZFS.

HP-UX to Oracle Solaris
Technology Mapping Guide
March 2012, Version 1.0

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

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200

oracle.com

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

Hardware and Software, Engineered to Work Together