Introduction to Oracle® Solaris Zones

Part No: E54762
November 2016

ORACLE

Introduction to Oracle Solaris Zones

Part No: E54762

Référence: E54762

Accessibilité de la documentation

Pour plus d'informations sur l'engagement d'Oracle pour l'accessibilité à la documentation, visitez le site Web Oracle Accessibility Program, à l'adresse `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Accès aux services de support Oracle

Les clients Oracle qui ont souscrit un contrat de support ont accès au support électronique via My Oracle Support. Pour plus d'informations, visitez le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` ou le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` si vous êtes malentendant.

Contents

Using This Documentation

- **Overview** – Describes the zones technology.
- **Audience** – System administrators, technicians, and authorized service providers.
- **Required knowledge** – Experience with the Oracle Solaris operating system, including knowledge of network configuration and resource allocation.

Product Documentation Library

Documentation and resources for this product and related products are available at http://www.oracle.com/pls/topic/lookup?ctx=E53394.

Feedback

Provide feedback about this documentation at http://www.oracle.com/goto/docfeedback.

♦ ♦ ♦ CHAPTER 1

Oracle Solaris Zones Introduction

The Oracle™ Solaris Zones feature in the Oracle Solaris operating system provides an isolated environment in which to run applications on your system.

The chapter provides an overview of zones covering the following topics:

Comprehensive documentation about zones is listed in the section "For More Information" on page 33.

Zones Concepts Overview

Oracle Solaris Zones is a virtualization technology that enables you to consolidate multiple physical machines and services on a single system. Virtualization reduces costs through the sharing of hardware, infrastructure, and administration. Benefits include the following:

- Increased hardware utilization
- Greater flexibility in resource allocation
- Reduced power requirements
- Fewer management costs

- Lower cost of ownership
- Administrative and resource boundaries between applications on a system

The Oracle Solaris Zones partitioning technology is used to virtually divide the resources of a physical machine and its Oracle Solaris operating system to simulate multiple machines and operating systems. Each system that is created in a zone is dedicated to the programs running inside. Zones technology is used to provide an isolated and secure environment for running applications.

Oracle Solaris Zones provides two main types of zones, each having attributes that control how its operating system behaves and how it can be used. The instance of the operating system that is running directly on a machine is called the *global zone*. An instance of a virtual system running inside the global zone is called a *non-global zone*, or simply a *zone*.

A *kernel zone* is a non-global zone that runs a kernel and operating system that is separate from the global zone. The separate kernel and OS installation in a kernel zone provide for greater independence and enhanced security of operating system instances and applications. Oracle Solaris Kernel Zones can run an Oracle Solaris release, Support Repository Update (SRU), or kernel version that is different from that of the host system. The Oracle Solaris release in a kernel zone must be at least Oracle Solaris 11.2.

Every zone is configured with an associated *brand*. The brand is used to determine behavior when a zone is installed and booted. In addition, a zone's brand is used to identify the correct application type at application launch time. The default brand is `solaris`. The brand for a kernel zone is `solaris-kz`. The brand for a zone running Oracle Solaris 10 is `solaris10`.

When you create a zone, you produce an application execution environment in which processes are isolated from the rest of the system. This isolation prevents processes that are running in one zone from monitoring or affecting processes that are running in other zones. Even a process running with root credentials cannot view or affect activity in other zones. Use Oracle Solaris Zones to maintain the deployment model of one-application-per-server while simultaneously sharing hardware resources.

A zone also provides an abstract layer that separates applications from the physical attributes of the system on which they are deployed. Examples of these attributes include physical device paths.

Zones can be used on any system that is running the Oracle Solaris 10 or Oracle Solaris 11 release. The upper limit for the number of `solaris` and `solaris10` zones on a system is 8192. The number of zones that can be effectively hosted on a single system is determined by the total resource requirements of the application software running in all of the zones, and the size of the system. System requirement concepts for zones are discussed in Chapter 1, “How to Plan and Configure Non-Global Zones” in *Creating and Using Oracle Solaris Zones*.

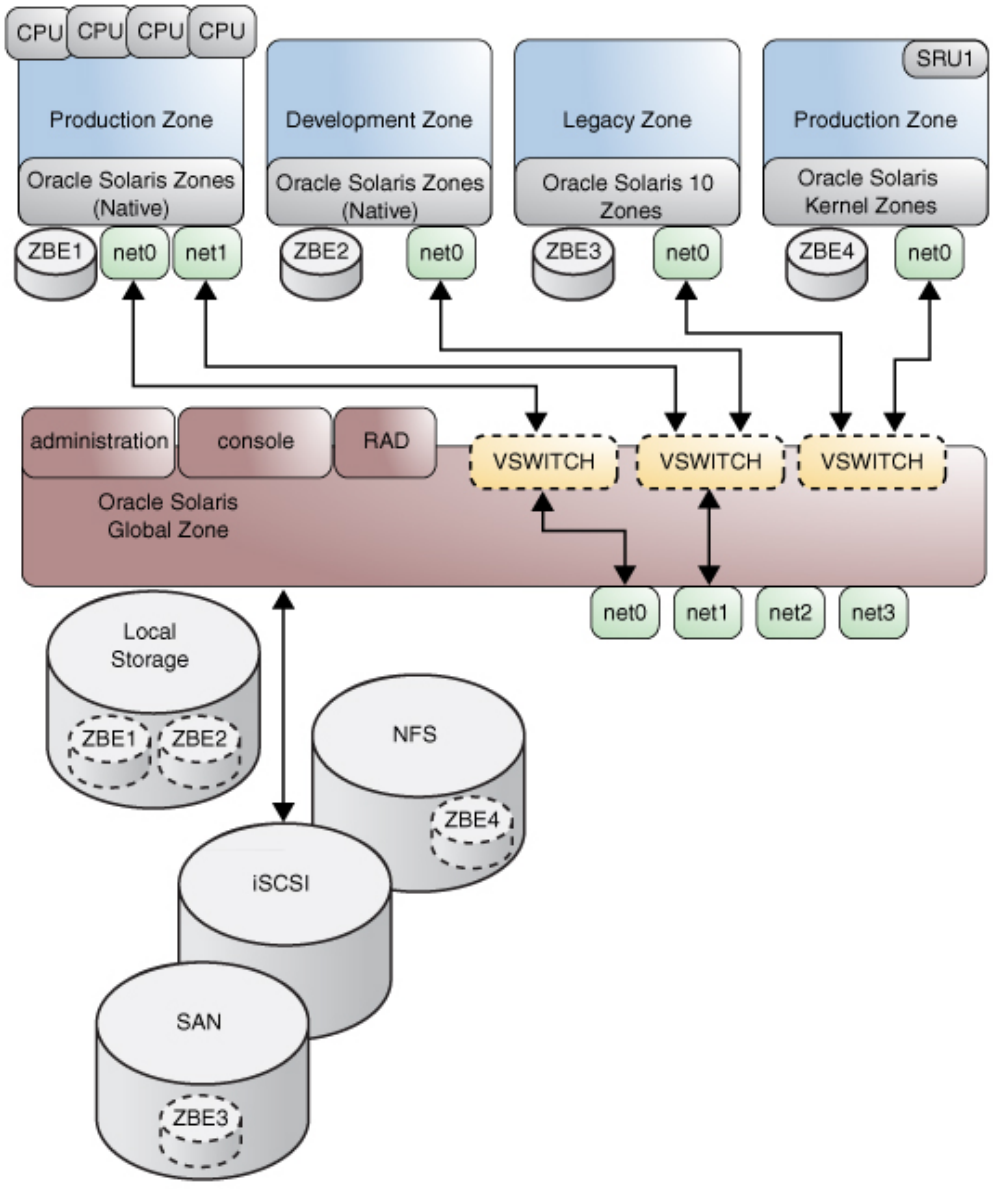
System requirement concepts for Oracle Solaris Kernel Zones are discussed in “Hardware and Software Requirements for Oracle Solaris Kernel Zones” in *Creating and Using Oracle Solaris Kernel Zones*.

When to Use Zones

Zones are ideal for environments that consolidate a number of applications on a single server. The cost and complexity of managing numerous physical machines make it advantageous to consolidate several applications on larger, more scalable servers.

The following figure shows zones that create separate execution environments for running an application in a production environment in a native zone and a kernel zone running a different SRU. Another native zone is used for developing the application. An additional zone maintains an environment to run legacy versions on Oracle Solaris 10. All zones run on the same server that is running an Oracle Solaris 11 global zone.

FIGURE 1 Zones Server Consolidation Example



Zones enable more efficient resource utilization on your system. Dynamic resource reallocation permits unused resources to be shifted to other zones as needed. Fault and security isolation

mean that poorly behaved applications do not require a dedicated and underutilized system. With the use of zones, these applications can be consolidated with other applications.

Zones allow you to delegate some administrative functions while maintaining overall system security.

How Zones Work

One or more applications can run in a zone without interacting with the rest of the system. Zones isolate software applications or services by using flexible, software-defined boundaries. Applications that are running in the same instance of the Oracle Solaris operating system can then be managed independently of each other. Thus, different versions of the same application can be run in different zones, to match the requirements of your configuration.

A process assigned to a zone can manipulate, monitor, and directly communicate with other processes that are assigned to the same zone. The process cannot perform these functions with processes that are assigned to other zones in the system or with processes that are not assigned to a zone. Processes that are assigned to different zones are only able to communicate through network APIs.

IP networking can be configured in two different ways, depending on whether the zone has its own exclusive IP instance or shares the IP layer configuration and state with the global zone. Exclusive-IP is the default type. For more information about IP types in zones, see "Zone Network Interfaces" in *Oracle Solaris Zones Configuration Resources*. For zone configuration information, see "How to Configure the Zone" in *Creating and Using Oracle Solaris Zones*.

Every Oracle Solaris system contains a *global zone*. The global zone has a dual function. The global zone is both the default zone for the system and the zone used for system-wide administrative control. All processes execute in the global zone if no *non-global* zones, referred to simply as zones, are created by the *global administrator* or a user with the Zone Security profile.

The global zone is the only zone from which a non-global zone can be configured, installed, managed, or uninstalled. Only the global zone is bootable from the system hardware. Administration of the system infrastructure, such as physical devices, routing in a shared-IP zone, or dynamic reconfiguration (DR), is only possible in the global zone running on a physical system. Appropriately privileged processes running in the global zone can access objects associated with other zones.

In some cases, unprivileged processes in the global zone might be able to perform operations not allowed to privileged processes in a non-global zone. For example, users in the global zone can view information about every process in the system. If this capability presents a problem for your site, you can restrict access to the global zone.

Each zone, including the global zone, is assigned a zone name. The global zone always has the name `global`. Each zone is also given a unique numeric identifier, which is assigned by the

system when the zone is booted. The global zone is always mapped to ID `0`. if you `zlogin` to a kernel zone, it also reports that it has ID 0, because it is a virtual global zone. Zone names and numeric IDs are discussed in "How to Configure the Zone" in *Creating and Using Oracle Solaris Zones*.

Each zone also has a node name that is completely independent of the zone name. The node name is assigned by the administrator of the zone. For more information, see "Non-Global Zone Node Name" in *Creating and Using Oracle Solaris Zones*.

Each zone has a path to its root directory that is relative to the global zone's root directory. For more information, see "About Using the zonecfg Command" in *Oracle Solaris Zones Configuration Resources*.

The scheduling class for a non-global zone is set to the scheduling class for the system by default. See "Scheduling Class" in *Oracle Solaris Zones Configuration Resources* for a discussion of methods used to set the scheduling class in a zone.

Block device multipathing is handled by `scsi_vhci(7D)`. The form of the `lu: storage` URI you select for your configuration determines how the configuration is used. For more information about using `lu:` URIs with multipathing, see the `suri(5)` man page.

Comparison of Global and Non-Global Zones

The following table summarizes the operating system characteristics of global and non-global zones along with the differences in the non-global zones that are kernel zones.

TABLE 1 Comparison of Zone Characteristics

Characteristic	Global Zone	Non-Global Zone	Kernel Zone
ID	Assigned ID `0` by the system	Assigned a zone ID by the system when the zone is booted	Assigned a zone ID by the system when the zone is booted
Kernel status	Provides the main instance of the Oracle Solaris kernel that is bootable and running on the system	Shares operation under the Oracle Solaris kernel booted from the global zone	Provides its own kernel
OS packages	Contains a complete installation of the Oracle Solaris system software packages	Contains an installed subset of the complete Oracle Solaris operating system software packages	Contains a complete installation of the Oracle Solaris system software packages
Additional software permitted	Can contain additional software packages or additional software, directories, files, and other data that is not installed through packages	Can contain additional software, directories, files, and other data created on the non-global zone that are not installed through packages	Can contain additional software, directories, files, and other data created on the non-global zone that are not installed through packages
		Can contain additional installed software packages	Can contain additional installed software packages

Characteristic	Global Zone	Non-Global Zone	Kernel Zone
		Might require software to be installed in the global zone in order to provide some functionality.	
Product database	Provides a complete and consistent product database that contains information about all software components installed in the global zone	Has a complete and consistent product database that contains information about all software components installed on the non-global zone	Has a complete and consistent product database that contains information about all software components installed on the kernel zone
Configuration information access	Holds configuration information specific to the global zone only, such as the global zone host name and file system table	Has configuration information specific to that non-global zone only, such as the non-global zone host name and file system table	Has configuration information specific to that kernel zone only, such as the kernel zone host name and file system table
Awareness of devices and file systems	Is the only zone that is aware of all devices and all file systems	Is aware of its own file systems only	Is aware of some devices but not file systems of the global zone
Awareness of other zones on system	Is the only zone with knowledge of non-global zone existence and configuration	Is not aware of the existence of any other zones	Is not aware of the existence of any other zones
Zone installation and management capabilities	Is the only zone from which a non-global zone can be configured, installed, managed, or uninstalled	Cannot install, manage, or uninstall zones on its hosting global zone.	Cannot install, manage, or uninstall zones on its hosting global zone. Can act as a global zone and contain non-global zones.
Time zone information	Has its own time zone that does not need to be used by non-global zones	Can have its own time zone setting that is different from the global zone	Can have its own time zone setting that is different from the global zone
Immutable read-only capability	Can be configured as an immutable zone with read-only access to the root	Can be configured as an immutable zone with read-only access to the root	Can be configured as an immutable zone with read-only access to the root

Capabilities Provided by Non-Global Zones

Non-global zones provide the following features:

Security

Once a process has been placed in a zone other than the global zone, neither the process nor any of its subsequent children can change zones.

Network services can be run in a zone. By running network services in a zone, you limit the damage possible in the event of a security violation. An intruder who successfully exploits a security flaw in software running within a zone is confined to the restricted set

of actions possible within that zone. The privileges available within a zone are a subset of those available in the system as a whole.

Isolation

Zones allow the deployment of multiple applications on the same system, even if those applications operate in different trust domains, require exclusive access to a global resource, or present difficulties with global configurations. The applications are also prevented from monitoring or intercepting each other's network traffic, file system data, or process activity.

Network Isolation

Zones are configured as exclusive-IP type by default. The zones are isolated from the global zone and from each other at the IP layer. This isolation is useful for both operational and security reasons. Zones can be used to consolidate applications that must communicate on different subnets using their own LANs or VLANs. Each zone can also define its own IP layer security rules.

Virtualization

Zones provide a virtualized environment that can hide details such as physical devices and the system's primary IP address and host name from applications. The same application environment can be maintained on different physical machines. The virtualized environment allows separate administration of each zone. Actions taken by a zone administrator in a non-global zone do not affect the rest of the system.

Granularity

A zone can provide isolation at almost any level of granularity. See “Non-Global Zone Isolation” on page 25 for more information.

Environment

Zones do not change the environment in which applications execute except when necessary to achieve the goals of security and isolation. Zones do not present a new API or ABI to which applications must be ported. Instead, zones provide the standard Oracle Solaris interfaces and application environment, with some restrictions. The restrictions primarily affect applications that attempt to perform privileged operations.

Applications in the global zone run without modification, whether or not additional zones are configured.

Zone Brands Overview

This section describes the types of brands available in this release, compares their features, and describes the BrandZ technology that enables branding.

Native Oracle Solaris Zones

The Oracle Solaris Zones feature is a complete runtime environment for applications. The default `solaris` branded zone is also known as the native zone. Native zones are managed from the global zone by using the tools `zonecfg`, `zoneadm`, and `zlogin`.

A zone provides a virtual mapping from the application to the platform resources. Zones allow application components to be isolated from one another even though the zones share a single instance of the Oracle Solaris operating system. Zones use resource management components to control how applications use available system resources. For additional information on resource management features, see *Administering Resource Management in Oracle Solaris 11.3*.

The zone establishes boundaries for resource consumption, such as CPU. These boundaries can be expanded to adapt to changing processing requirements of the application running in the zone.

Native `solaris` zones cannot contain any other zones within them.

For additional isolation, you can configure zones with a read-only root, called Immutable Zones. See “Immutable Zones” on page 27 later in this document for more information.

Oracle Solaris Kernel Zones

The Oracle Solaris Kernel Zones feature provides a full kernel and user environment within a zone, and also increases kernel separation between the host system and the zone. The brand name is `solaris-kz`. Kernel zones are managed from the global zone by using the existing tools `zonecfg`, `zoneadm`, and `zlogin`. The administrator of a kernel zone has greater flexibility in configuring and managing the zone than the administrator of a default `solaris` zone. For example, you can fully update and modify the zone's installed packages, including the kernel version, without being limited to the packages installed in the global zone. You can manage storage private to the zone, create and destroy ZFS pools, and configure iSCSI and CIFS. You can install `solaris` and `solaris10` zones within the kernel zone.

A `solaris-kz` installation is independent of that of the global zone; it is not a `pkg(5)` linked image and can be modified regardless of the global zone content. A `solaris-kz` zone can be installed in the same manner as other brands: Directly from the global zone, or by using a boot media.

When specifying a manifest for installation, use a manifest that is suitable for a global zone installation.Because kernel zones always install into a known location for the root pool, an installation target disk should not be specified.

Boot environment (BE) management is independent of the global zone.

Kernel zones support live migration and warm migration using suspend and resume. You can migrate a kernel zone by suspending the zone on the source system and resuming the zone on the target system.These zones also support cold migration.

To use Oracle Solaris Kernel Zones, the package `brand-solaris-kz` must be installed on your system. To determine whether your system supports kernel zones, see "Hardware and Software Requirements for Oracle Solaris Kernel Zones" in *Creating and Using Oracle Solaris Kernel Zones*. You can also run the `virtinfo` command on your system. For more information about Oracle Solaris Kernel Zones, see *Creating and Using Oracle Solaris Kernel Zones* and the `solaris-kz`(5) man page. For more information about the `virtinfo` command, see "How to Verify Kernel Zone Support on a Host" in *Creating and Using Oracle Solaris Kernel Zones* and the `virtinfo`(1M) man page.

Oracle Solaris 10 Zones

Oracle Solaris 10 Zones, also known as `solaris10` branded non-global zones, use BrandZ technology to run Oracle Solaris 10 applications on the Oracle Solaris 11 operating system. Applications run unmodified in the secure environment provided by the non-global zone. This enables you to use the Oracle Solaris 10 system to develop, test, and deploy applications. Workloads running within these branded zones can take advantage of the enhancements made to the kernel and utilize some of the innovative technologies available only on the Oracle Solaris 11 release. These zones are used to convert Oracle Solaris 10 systems into zones on Oracle Solaris 11. A `solaris10` branded zone cannot be an NFS server.

Oracle Solaris 10 Zones cannot contain any other zones within them.

For more information, see *Creating and Using Oracle Solaris 10 Zones*.

Zone Brand Comparison

Differences between `solaris-kz` branded zones and `solaris` and `solaris10` branded zones are shown below.

TABLE 2 Comparison of Oracle Solaris Zone Brand Features

Component	`solaris-kz` Brand	`solaris` and `solaris10` Brands
Supported Hardware	Supported on specified hardware. See "Hardware and Software Requirements for	Supported on all systems that support the Oracle Solaris 11.3 release.

Component	`solaris-kz` Brand	`solaris` and `solaris10` Brands
	Oracle Solaris Kernel Zones" in *Creating and Using Oracle Solaris Kernel Zones*.	
Memory Management	A fixed amount of physical RAM must be allocated to the `solaris-kz` virtual platform.	Can share the physical RAM allocated to the global zone.
Kernel Version	A kernel zone can run a different kernel version or SRU level than the host.	Kernel version must be the same as that of the global zone.
Storage and Device Management	Performs all storage access. Kernel zones do not support `zpool` or `rootzpool` resources.	Storage can be made available at the file system level though the `fs`, `zpool`, and `dataset` `zonecfg` resources.
Networking	Only exclusive-IP zones are supported.	Exclusive-IP and shared-IP zones are supported.
Migration	Supports live, warm, and cold migration.	Supports cold migration.

About the Branded Zones Framework

By default, a non-global zone on a system runs the same operating system software as the global zone. The branded zone (BrandZ) facility in the Oracle Solaris operating system is a simple extension of Oracle Solaris Zones. The BrandZ framework is used to create non-global branded zones that contain operating environments that are different from that of the global zone. Branded zones are used on the Oracle Solaris operating system to run applications. The BrandZ framework extends the Oracle Solaris Zones infrastructure in a variety of ways. These extensions can be complex, such as providing the capability to run different operating system environments within the zone, or simple, such as enhancing the base zone commands to provide new capabilities. For example, Oracle Solaris 10 Zones are branded non-global zones that can emulate the Oracle Solaris 10 operating system. Even default zones that share the same operating system as the global zone are configured with a *brand*.

The brand defines the operating environment that can be installed in the zone, and determines how the system will behave within the zone so that the software installed in the zone functions correctly. In addition, a zone's brand is used to identify the correct application type at application launch time. All branded zone management is performed through extensions to the standard zones structure. Most administration procedures are identical for all zones.

The resources included in the configuration by default, such as defined file systems and privileges, are covered in the documentation for the zone brands referenced in "For More Information" on page 33.

BrandZ extends the zones tools in the following ways:

- The `zonecfg` command is used to set a zone's brand type when the zone is configured.
- The `zoneadm` command is used to report a zone's brand type as well as administer the zone.

Although you can configure and install branded zones on an Oracle Solaris Trusted Extensions system that has labels enabled, you cannot boot branded zones on this system configuration, *unless* the brand being booted is the `labeled` brand on a certified system configuration.

You can change the brand of a zone that is in the `configured` state. Once a branded zone has been *installed*, the brand cannot be changed or removed.

Caution - If you plan to migrate your existing Oracle Solaris 10 system into a `solaris10` branded zone on a system running the Oracle Solaris 11 release, you must migrate any existing zones to the target system first. Because `solaris10` zones do not nest, the system migration process renders any existing zones unusable. See Chapter 3, "Migrating an Oracle Solaris 10 native Non-Global Zone Into an Oracle Solaris 10 Zone" in *Creating and Using Oracle Solaris 10 Zones* for more information.

Processes Running in a Branded Zone

Branded zones provide a set of interposition points in the kernel that are only applied to processes executing in a branded zone.

- These points are found in such paths as the `syscall` path, the process loading path, and the thread creation path.
- At each of these points, a brand can choose to supplement or replace the standard Oracle Solaris behavior.

A brand can also provide a plug-in library for `librtld_db`. The plug-in library allows Oracle Solaris tools such as the debugger, described in `mdb(1)`, and DTrace, described in `dtrace(1M)`, to access the symbol information of processes running inside a branded zone.

Note that zones do not support statically linked binaries.

Zone Brands In Related Oracle Solaris Products

This section provides information about Oracle Solaris Zones used in other Oracle Solaris family products.

Oracle Solaris Zones on an Oracle Solaris Trusted Extensions System

Oracle Solaris Trusted Extensions use a zone brand called `labeled`.

For information about using zones on an Oracle Solaris Trusted Extensions system, see Chapter 13, "Managing Zones in Trusted Extensions" in *Trusted Extensions Configuration and Administration*. Note that only the `labeled` brand can be booted on an Oracle Solaris Trusted Extensions system.

Oracle Solaris Cluster Zone Clusters

Zone clusters are a feature of Oracle Solaris Cluster software. A zone cluster is a group of non-global zones that serve as the nodes of the zone cluster. One non-global zone is created on each global cluster node that is configured with the zone cluster. The nodes of a zone cluster can be of either the `solaris` brand or the `solaris10` brand, and use the cluster attribute. No other brand type is permitted except `labeled` if the cluster is using Oracle Solaris Trusted Extensions. You can run supported services on the zone cluster in the same way as on a global cluster, with the isolation that is provided by zones. For more information, see the *Oracle Solaris Cluster 4.3 System Administration Guide*.

Zone Administration Overview

This section provides an overview of zone administration information for non-global zones.

How Non-Global Zones Are Created

You can specify the configuration and installation of non-global zones as part of an Automated Install (AI) client installation. See *Installing Oracle Solaris 11.3 Systems* for more information. Oracle Solaris Kernel Zones primarily are created using the direct installation method. Kernel zone creation methods are documented in "Installing a Kernel Zone" in *Creating and Using Oracle Solaris Kernel Zones*.

To create a zone on an Oracle Solaris system, the global administrator uses the `zonecfg` command to configure a zone by specifying various parameters for the zone's virtual platform and application environment. The zone is then installed by the global administrator, who uses the zone administration command `zoneadm` to install software at the package level into the file system hierarchy established for the zone. The `zoneadm` command is used to boot the zone. The global administrator or authorized user can then log in to the installed zone by using the `zlogin` command. If role-based access control (RBAC) is in use, the zone administrator must have the authorization `solaris.zone.manage/`*zonename*.

For information about zone configuration, see Chapter 1, "Non-Global Zone Configuration" in *Oracle Solaris Zones Configuration Resources*. For information about zone installation, see Chapter 2, "About Installing, Shutting Down, Halting, Uninstalling, and Cloning Non-Global Zones" in *Creating and Using Oracle Solaris Zones*. For information about zone login, see Chapter 4, "About Non-Global Zone Login" in *Creating and Using Oracle Solaris Zones*.

To configure and install Oracle Solaris Kernel Zones, see *Creating and Using Oracle Solaris Kernel Zones*.

How Non-Global Zones Are Administered

A global administrator has superuser privileges or equivalent administrative rights. When logged in to the global zone, the global administrator can monitor and control the system as a whole.

A non-global zone can be administered by a *zone administrator*. The global administrator assigns the required authorizations to the zone administrator as described in "admin Resource" in *Oracle Solaris Zones Configuration Resources*. The privileges of a zone administrator are confined to a specific non-global zone.

Non-Global Zone State Model

A non-global zone can be in one of the following seven states:

`Configured` — The zone's configuration is complete and committed to stable storage. However, those elements of the zone's application environment that must be specified after initial boot are not yet present.

`Incomplete` — During an install or uninstall operation, `zoneadm` sets the state of the target zone to incomplete. Upon successful completion of the operation, the state is set to the correct state.

A damaged installed zone can be marked incomplete by using the `mark` subcommand of `zoneadm`. Zones in the incomplete state are shown in the output of `zoneadm list -iv`.

`Unavailable` — Indicates that the zone has been installed, but cannot be verified, made ready, booted, or moved. A zone enters the unavailable state at the following times:

- When the zone's storage is unavailable and `svc:/system/zones:default` begins, such as during system boot
- When the zone's storage is unavailable
- When archive-based installations fail after successful archive extraction
- When the zone's software is incompatible with the global zone's software, such as after an improper `-F` (force) attach

`Installed` — The zone's configuration is instantiated on the system. The `zoneadm` command is used to verify that the configuration can be successfully used on the designated Oracle Solaris system. Packages are installed under the zone's root path. In this state, the zone has no associated virtual platform.

`Ready`	The virtual platform for the zone is established. The kernel creates the `zsched` process, network interfaces are set up and made available to the zone, file systems are mounted, and devices are configured. A unique zone ID is assigned by the system. At this stage, no processes associated with the zone have been started.
`Running`	User processes associated with the zone application environment are running. The zone enters the running state as soon as the first user process associated with the application environment (`init`) is created.
`Shutting down` and `Down`	These states are transitional states that are visible while the zone is being halted. However, a zone that is unable to shut down for any reason will stop in one of these states.

Chapter 3, "Installing, Booting, Shutting Down, Halting, Uninstalling, and Cloning Non-Global Zones" in *Creating and Using Oracle Solaris Zones* and the `zoneadm`(1M) man page describe how to use the `zoneadm` command to initiate transitions between these states.

Auxiliary States for Kernel Zones

In addition to the states available to all non-global zones, Oracle Solaris Kernel Zones have *auxiliary states* which provide the host system with additional information about the current zone state. Auxiliary states are set during migration, debugging, and kernel maintenance operations.

`Suspended`	When a kernel zone is suspended with the `zoneadm suspend` command, the zone is in the installed state with the suspended auxiliary state. In the case of warm migration, `zoneadm detach` clears the suspended auxiliary state on the source system. The `zoneadm attach` command on the target system brings the zone from configured to installed with the suspended auxiliary state. The zone will resume on the next boot.
`Debugging`	The zone is in the kernel debugger, `kmdb`. The zone is running, but the zone cannot respond to external events, such as networking. The `zlogin` command checks for this state and waits until the state is cleared before starting a `zlogin` session.
`Panicked`	The zone has panicked. The zone cannot respond to external events until it is shut down or rebooted. You must use the console login to log into a zone in this state.
`Migrating-out`	The zone is running and being live migrated to another host system.
`Migrating-in`	The zone has been booted on the target host and the zone is receiving the migrated image. The zone will be running when migration is complete.

For additional information, see *Creating and Using Oracle Solaris Kernel Zones* and the `solaris-kz`(5) man page.

Zone States and Zone Commands

The zone state determines which `zonecfg`, `zoneadm`, and `zlogin` commands can be used on the zone.

TABLE 3 Commands That Affect Zone State

Current Zone State	Applicable Commands

`Configured`	`zonecfg -z` *zonename* `verify`
	
	`zonecfg -z` *zonename* `commit`
	
	`zonecfg -z` *zonename* `delete`
	
	`zoneadm -z` *zonename* `attach`
	
	`zoneadm -z` *zonename* `verify`
	
	`zoneadm -z` *zonename* `install`
	
	`zoneadm -z` *zonename* `clone`
	
	`zoneadm -z` *zonename* `mark incomplete`
	
	`zoneadm -z` *zonename* `mark unavailable`
	
	You can use the `zonecfg` command to rename a zone in the configured state. Note that you can use the `zoneadm` command to rename an Oracle Solaris Zone or Oracle Solaris 10 Zone in either the configured or installed state.

`Incomplete`	`zoneadm -z` *zonename* `uninstall`
`Unavailable`	`zoneadm -z` *zonename* `uninstall` uninstalls the zone from the specified system. `zoneadm -z` *zonename* `attach` transitions a zone from the unavailable state to the installed state. If the `attach` subcommand is unable to perform such a transition, the zone will remain in the unavailable state. `zonecfg -z` *zonename* can be used to change `zonepath` and any other property or resource that cannot be changed when in the installed state.

`Installed`	`zoneadm -z` *zonename* `ready` (optional)
	
	`zoneadm -z` *zonename* `boot`
	
	`zoneadm -z` *zonename* `uninstall` uninstalls the configuration of the specified zone from the system.
	
	`zoneadm -z` *zonename* `move` *path*
	
	`zoneadm -z` *zonename* `detach`

Current Zone State	Applicable Commands

	`zonecfg -z` *zonename* can be used to add or remove an `attr`, `bootargs`, `capped-memory`, `dataset`, `capped-cpu`, `dedicated-cpu`, `device`, `fs`, `ip-type`, `limitpriv`, `net`, `rctl`, or `scheduling-class` property. You can also rename a zone.
	
	You can use the `zoneadm` command to rename an Oracle Solaris Zone or Oracle Solaris 10 Zone in the configured or installed state.
	
	`zoneadm -z` *zonename* `mark incomplete`
	
	`zoneadm -z` *zonename* `mark unavailable`

`Ready`	`zoneadm -z` *zonename* `boot` `zoneadm halt` and system reboot return a zone in the ready state to the installed state. `zonecfg -z` *zonename* can be used to add or remove `attr`, `bootargs`, `capped-memory`, `dataset`, `capped-cpu`, `dedicated-cpu`, `device`, `fs`, `ip-type`, `limitpriv`, `net`, `rctl`, or `scheduling-class` property.
`Running`	`zlogin` *options zonename* `zoneadm -z` *zonename* `reboot` `zoneadm -z`*zonename* `halt` returns a ready zone to the installed state. `zoneadm halt` and system reboot return a zone in the running state to the installed state. `zoneadm -z shutdown` cleanly shuts down the zone. `zonecfg -z` *zonename* can be used to add or remove an `attr`, `bootargs`, `capped-memory`, `dataset`, `capped-cpu`, `dedicated-cpu`, `device`, `fs`, `ip-type`, `limitpriv`, `anet`, `net`, `rctl`, or `scheduling-class` property. If set, the `zonepath` resource cannot be changed.

Non-Global Zone Isolation

A zone provides isolation at almost any level of granularity you require. A zone does not need a dedicated CPU, a physical device, or a portion of physical memory. These resources can either be multiplexed across a number of zones running within a single domain or system, or allocated on a per-zone basis using the resource management features available in the operating system.

Each zone can provide a customized set of services. To enforce basic process isolation, a process can see or signal only those processes that exist in the same zone. Basic communication between zones is accomplished by giving each zone IP network connectivity. An application running in one zone cannot observe the network traffic of another zone. This isolation is maintained even though the respective streams of packets travel through the same physical interface.

Each zone is given a portion of the file system hierarchy. Because each zone is confined to its subtree of the file system hierarchy, a workload running in a particular zone cannot access the on-disk data of another workload running in a different zone.

Files used by naming services reside within a zone's own root file system view. Thus, naming services in different zones are isolated from one other and the services can be configured differently.

Resource Management With Non-Global Zones

If you use resource management features, you should align the boundaries of the resource management controls with those of the zones. This alignment creates a more complete model of a virtual machine, where namespace access, security isolation, and resource usage are all controlled.

Any special requirements for using the various resource management features with zones are addressed in the individual chapters of this manual that document those features.

Zones-Related SMF Services

Zones-related Service Management Facility (SMF) services in the global zone include the following:

`svc:/system/zones:default`

Starts each zone that has `autoboot=true`.

`svc:/system/zones-install:default`

Performs zone installation on first boot, if needed.

`svc:/application/pkg/zones-proxyd:default`

Used by the packaging system to provide zones access to the system repository.

`svc:/application/pkg/system-repository:default`

Caching proxy server that caches `pkg` data and metadata used during zone installation and other `pkg` operations. See the `pkg(1)` and `pkg(5)` man pages.

`svc:/system/zones-monitoring:default`

Controls `zonestatd`.

The `svc:/application/pkg/zones-proxy-client:default` zones proxy client SMF service runs only in the non-global zone. The service is used by the packaging system to provide zones access to the system repository.

Monitoring Non-Global Zones

To report on the CPU, memory, and resource control utilization of the currently running zones, see "Using the zonestat Utility in a Non-Global Zone" in *Creating and Using Oracle Solaris Zones*. The `zonestat` utility also reports on network bandwidth utilization in exclusive-IP zones. An exclusive-IP zone has its own IP-related state and one or more dedicated datalinks.

The `fsstat` utility can be used to report file operations statistics for non-global zones. See the `fsstat`(1M) man page and "Monitoring Non-Global Zones Using the fsstat Utility" in *Creating and Using Oracle Solaris Zones*.

Immutable Zones

Immutable Zones are `solaris` zones with read-only roots. Both global and non-global zones can be Immutable Zones. A read-only zone can be configured by setting the `file-mac-profile` property. Several configurations are available. A read-only zone root expands the secure runtime boundary.

Oracle Solaris Immutable Global Zones extended the Immutable Zones feature to the global zone. For Immutable Zones and Immutable Kernel Zones, the Trusted Path login can be invoked through the `zlogin` command `zlogin`(1).

Zones that are given additional datasets using `zonecfg add dataset` still have full control over those datasets. Zones that are given additional file systems using `zonecfg add fs` have full control over those file systems, unless the file systems are set read-only.

See Chapter 11, "Configuring and Administering Immutable Zones" in *Creating and Using Oracle Solaris Zones* for more information.

Live Zone Reconfiguration

Use Live Zone Reconfiguration to report live configuration information or to reconfigure running zones without rebooting. Changes can be made on a temporary or persistent basis.

For more information, see Chapter 6, "Live Zone Reconfiguration" in *Creating and Using Oracle Solaris Zones*.

About Zone Conversion

Zone conversion is used in the following processes:

- Transforming global zones into non-global zones, also known as physical to virtual (P2V) conversion
- Transforming non-global zones into global zones
- Transforming Oracle Solaris 10 `native` zones to `solaris10` branded zones on an upgraded system by using an archive

On Oracle Solaris 11, zone conversions using archives can be part of a zone migration strategy. Migration can also involve data transfer using archives.

About Zone Migration

A zone migration transfers an existing zone or global zone into a zone on another system. The three types of zone migrations are live migration, warm migration, and cold migration.

Live and warm migration are supported only for kernel zones. A native non-global zone uses the global zone's kernel and its software packages are linked to those of the global zone, so it cannot be migrated to a different global zone unless it is first shut down.

solaris-kz Only: About Live Migration

In a kernel zone *live migration*, the memory state of the migrated zone is copied to the migrated guest. Live zone migration has a brief outage time that is not noticeable to most applications or end-users. Kernel zone live migration can also be used to load balance services.

Live migration is recommended for situations where downtime must be minimized and applications must remain in a running state. The migration process can have a performance impact that might negatively affect heavy workloads. In cases such as this, use warm migration or cold migration during the outage window.

Live migration during an off-peak time can be an option as well. Live migration with a quiesced application and sufficient network bandwidth can be faster than warm migration.

See "Using Live Migration to Migrate a Kernel Zone" in *Creating and Using Oracle Solaris Kernel Zones* for more information on live migration.

solaris-kz Only: About Warm Migration

In a kernel zone *warm migration*, the migrated zone memory state is written to disk. The zone is moved from the source host to the destination host and restarted. This zone migration type is also known as *migration using suspend and resume*.

For applications where live migration is not suitable, use a warm migration. A warm migration does not require a full system reboot and restart of the application while the kernel zone is running. All networking connections are lost to the zone during a warm migration, but outage times are reduced to seconds or minutes.

Some database applications can take several hours to warm up after a system reboot. A warm migration captures the database running state and significantly decreases the outage time.

For more information, see "Using Warm Migration to Migrate a Kernel Zone" in *Creating and Using Oracle Solaris Kernel Zones*.

About Cold Migration

All zone brands support cold migration.

In a *cold migration*, a zone is shut down on the source host and rebooted on a target host. Use cold migration for applications that provide time-critical services or applications that have a large memory footprint. Cold migration is recommended for transferring existing zones or systems.

See Chapter 7, "Migrating and Converting Oracle Solaris Zones" in *Creating and Using Oracle Solaris Zones* for more information.

About Oracle Solaris Zones in This Release

This section lists changes in Oracle Solaris Zones features, including Oracle Solaris Kernel Zones, for this release.

The default non-global zone in this release is `solaris`, described in this guide and in the `solaris`(5) man page.

To verify the Oracle Solaris release and the physical machine architecture, type:

```
# uname -r -m
```

The `virtinfo` command described in the `virtinfo`(1M) man page is used to obtain the following information:

- Determine system support for Oracle Solaris virtualization technologies
- Detect the type of virtual environment Oracle Solaris is running in, such as Oracle VM Server for SPARC

The `solaris` zone uses the branded zones framework described in "About the Branded Zones Framework" on page 19 and in the `brands`(5) man page to run zones installed with the same

software that is installed in the global zone. The system software must always be in sync with the global zone when using a `solaris` brand non-global zone. The system software packages within the zone are managed using the Image Packaging System (IPS). IPS is the packaging system on the Oracle Solaris 11 release, and `solaris` zones use this model.

Default `ipkg` zones created on the Oracle Solaris 11 Express release will be mapped to `solaris` zones. See "About Converting `ipkg` Zones to `solaris` Zones" on page 32.

Each non-global zone specified in the Automated Install (AI) manifest is installed and configured as part of a client installation. Non-global zones are installed and configured on the first reboot after the global zone is installed. When the system first boots, the zones self-assembly SMF service, `svc:/system/zones-install:default`, configures and installs each non-global zone defined in the global zone AI manifest. See *Adding and Updating Software in Oracle Solaris 11.3* for more information. It is also possible to manually configure and install zones on an installed Oracle Solaris system.

For package updates, persistent proxies should be set in an image by using the `--proxy` option. If a persistent image proxy configuration is not used, `http_proxy` and `https_proxy` environment variables can be set.

Zones can be configured to be updated in parallel instead of serially. The parallel update provides a significant improvement in the time required to update all the zones on a system.

By default, zones are created with the exclusive-IP type. Through the `anet` resource, a VNIC is automatically included in the zone configuration if networking configuration is not specified. For more information, see "Zone Network Interfaces" in *Oracle Solaris Zones Configuration Resources*.

For information on the `auto-mac-address` used to obtain a `mac-address` for a zone, see the entry `anet` in "Resource Type Properties" in *Oracle Solaris Zones Configuration Resources*.

A `solaris` zone on shared storage has a `zonecfg rootzpool` resource. A zone is encapsulated into a dedicated zpool. Zones on shared storage access and manage shared storage resources for zones. Kernel zones do not have `zpool` or `rootzpool` resources. A `solaris` brand zone can use the following shared storage for zone `device` resources, and for `zpool` and `rootzpool` resources.

- iSCSI
- FC LUNs
- DAS

Properties used to specify IP over InfiniBand (IPoIB) datalinks are available for the `zonecfg anet` resource. IPoIB is supported for `solaris` and `solaris10` brand zones.

The Reliable Datagram Sockets (RDS) IPC protocol is supported in both exclusive-IP and shared-IP non-global zones.

The `fsstat` utility has been extended to support zones. The `fsstat` utility provides per-zone and aggregate statistics.

`solaris` zones can be NFS servers, as described in the section "Running an NFS Server in a Zone" in *Creating and Using Oracle Solaris Zones*.

Trial-run, also called dry-run, `zoneadm attach -n`, provides `zonecfg` validation, but does not perform package contents validation.

All `zoneadm` options that take files as arguments require absolute paths.

Oracle Solaris 10 Zones provide an Oracle Solaris 10 environment on Oracle Solaris 11. You can migrate an Oracle Solaris 10 system or zone into a `solaris10` zone on an Oracle Solaris 11 system. See *Creating and Using Oracle Solaris 10 Zones*.

The `zonep2vchk` tool identifies issues, including networking issues, that could affect the migration of an Oracle Solaris 11 system or an Oracle Solaris 10 system into a zone on a system running the Oracle Solaris 11 release. The `zonep2vchk` tool is executed on the source system before migration begins. The tool also outputs a `zonecfg` script for use on the target system. The script creates a zone that matches the source system's configuration. For more information, see Chapter 7, "Migrating and Converting Oracle Solaris Zones" in *Creating and Using Oracle Solaris Zones*.

The following differences between `solaris` zones on the Oracle Solaris 11 release and `native` zones on the Oracle Solaris 10 release should be noted:

- The `solaris` brand is created on Oracle Solaris 11 systems instead of the `native` brand, which is the default on Oracle Solaris 10 systems.
- `solaris` zones are whole-root type only.

  The sparse root type of native zone available on Oracle Solaris 10 uses the SVR4 package management system, and IPS does not use this system. A read-only root zone configuration that is similar to the sparse root type is available.
- Zones in this release have software management related functionality that is different from the Oracle Solaris 10 release in these areas:
  - IPS versus SVR4 packaging.
  - Install, detach, attach, and physical to virtual capability.
  - The non-global zone root is a ZFS™ dataset.

    A package installed in the global zone is no longer installed into all current and future zones. In general, the global zone's package contents no longer dictate each zone's package contents, for both IPS and SVR4 packaging.
- Non-global zones use boot environments. Zones are integrated with `beadm`, the user interface command for managing ZFS Boot Environments (BEs).

  The `beadm` command is supported inside zones for `pkg` update, just as in the global zone. The `beadm` command can delete any inactive zones BE associated with the zone. See the `beadm(1M)` man page.

- All enabled IPS package repositories must be accessible while installing a zone. See "How to Install a Configured Zone" in *Creating and Using Oracle Solaris Zones* for more information.
- Zone software is minimized to start. Any additional packages the zone requires must be added. See *Adding and Updating Software in Oracle Solaris 11.3* for more information.

Zones can use Oracle Solaris products and features such as the following:

- Oracle Solaris ZFS encryption
- Network virtualization and QoS
- CIFS and NFS

The following functions cannot be configured in a `solaris` branded zone:

- DHCP address assignment in a shared-IP zone
- `ndmpd`
- SMB server
- SSL proxy server
- FC services
- FCoE services
- iSCSI services
- ZFS pool administration through `zpool` commands cannot be used

The following functions cannot be configured in a `solaris-kz` brand zone:

- FC services
- FCoE services

Zones Support in This Release

Non-global `solaris` and `solaris10` brand zones running within a single host global zone are supported on all architectures that are defined as supported platforms for the Oracle Solaris 11.3 release. See the Oracle Solaris Hardware Compatibility List (HCL).

For information about Oracle Solaris Kernel Zones physical machine support and system requirements, see "Hardware and Software Requirements for Oracle Solaris Kernel Zones" in *Creating and Using Oracle Solaris Kernel Zones*.

About Converting `ipkg` Zones to `solaris` Zones

To support Oracle Solaris 11 Express release customers, any zone configured as an `ipkg` zone is converted to a `solaris` zone and reported as `solaris` upon `pkg` update or `zoneadm attach`

to Oracle Solaris 11.3. The `ipkg` name will be mapped to the `solaris` name if used when configuring zones. Import of a `zonecfg` file exported from an Oracle Solaris 11 Express system will be supported.

The output of commands such as `zonecfg info` or `zoneadm list -v` displays a brand of `solaris` for default native zones on an Oracle Solaris 11.3 system.

For More Information

For more in-depth information about zones see the following documentation:

Creating and Using Oracle Solaris Zones

To start creating zones on your system.

Creating and Using Oracle Solaris Kernel Zones

To learn more about kernel zones and kernel zone migration.

Creating and Using Oracle Solaris 10 Zones

To convert a system running Oracle Solaris 10 into a zone on an Oracle Solaris 11 system.

Oracle Solaris Zones Configuration Resources

To learn more about zone configuration resources and properties.

Chapter 13, “Managing Zones in Trusted Extensions” in *Trusted Extensions Configuration and Administration*

To learn about using zones on an Oracle Solaris Trusted Extensions system.

Glossary of Zones Terminology

auxiliary zone state For Oracle Solaris Kernel Zones, used to communicate additional state information about the zone state to the host. See also zone state.

brand An instance of the BrandZ functionality, which provides non-global zones that contain non-native operating environments used for running applications.

branded zone An isolated environment in which to run non-native applications in non-global zones.

cap A limit that is placed on system resource usage.

capping The process of placing a limit on system resource usage.

CMT resources CPUS, cores, and sockets.

conversion Transform global zones into non-global zones,non-global zones into global zones, Oracle Solaris 10 `native` zones to `solaris10` branded zones on an upgraded host by using an archive. See also migration.

CPU In the zones context, refers to a hardware thread.

datalink An interface at Layer 2 of the OSI protocol stack, which is represented in a system as a STREAMS DLPI (v2) interface. This interface can be plumbed under protocol stacks such as TCP/IP. In the context of Oracle Solaris 10 zones, datalinks are physical interfaces, aggregations, or VLAN-tagged interfaces . A datalink can also be referred to as a physical interface, for example, when referring to a NIC or a VNIC.

default pool The pool created by the system when pools are enabled.

See also resource pool.

default processor set The processor set created by the system when pools are enabled.

See also processor set.

disjoint A type of set in which the members of the set do not overlap and are not duplicated.

dynamic configuration Information about the disposition of resources within the resource pools framework for a given system at a point in time.

dynamic reconfiguration	On SPARC based systems, the ability to reconfigure hardware while the system is running. Also known as DR.
extended accounting	A flexible way to record resource consumption on a task basis or process basis in the Solaris operating system.
fair share scheduler	A scheduling class, also known as FSS, that allows you to allocate CPU time that is based on shares. Shares define the portion of the system's CPU resources allocated to a project.
FSS	See fair share scheduler.
global administrator	The root user or an administrator with the root role. When logged in to the global zone, the global administrator or a user granted the appropriate authorizations can monitor and control the system as a whole. See also zone administrator.
global scope	Actions that apply to resource control values for every resource control on the system.
global zone	The zone contained on every Oracle Solaris system. When non-global zones are in use, the global zone is both the default zone for the system and the zone used for system-wide administrative control. See also non-global zone.
heap	Process-allocated scratch memory.
Immutable Zone	A zone configured with a read-only root.
Live Zone Reconfiguration	Reconfigure or report on the live configuration of non-global zones while the zones are running.
local scope	Local actions taken on a process that attempts to exceed the control value.
locked memory	Memory that cannot be paged.
memory cap enforcement threshold	The percentage of physical memory utilization on the system that will trigger cap enforcement by the resource capping daemon.
migration	Transfers an existing zone or global zone into a zone on another system. Also see conversion.
naming service database	In the Projects and Tasks (Overview) chapter of this document, a reference to both LDAP containers and NIS maps.
non-global zone	A virtualized operating system environment created within a single instance of the Oracle Solaris operating system. The Oracle Solaris Zones software partitioning technology is used to virtualize operating system services.

non-global zone administrator See zone administrator.

Oracle Solaris 10 Zones A software partitioning technology that provides a complete runtime environment for Solaris 10 applications executing in a `solaris10` branded zone on a system running the Oracle Solaris 11 release.

Oracle Solaris Kernel Zones A software partitioning technology that provides a full kernel and user environment within a zone, and also increases kernel separation between the host and the zone.

Oracle Solaris Zones A software partitioning technology used to virtualize operating system services and provide an isolated, secure environment in which to run applications.

partitioning A software technology that is used to dedicate a subset of system resources to a defined workload.

pool See resource pool.

pool daemon The `poold` system daemon that is active when dynamic resource allocation is required.

processor set A disjoint grouping of CPUs. Each processor set can contain zero or more processors. A processor set is represented in the resource pools configuration as a resource element. Also referred to as a pset.

See also disjoint.

project A network-wide administrative identifier for related work.

resident set size The size of the resident set. The resident set is the set of pages that are resident in physical memory.

resource An aspect of the computing system that can be manipulated with the intent to change application behavior.

resource capping daemon A daemon that regulates the consumption of physical memory by processes running in projects that have resource caps defined.

resource consumer Fundamentally, a Solaris process. Process model entities such as the project and the task provide ways of discussing resource consumption in terms of aggregated resource consumption.

resource control A per-process, per-task, or per-project limit on the consumption of a resource.

resource management A functionality that enables you to control how applications use available system resources.

resource partition	An exclusive subset of a resource. All of the partitions of a resource sum to represent the total amount of the resource available in a single executing Solaris instance.
resource pool	A configuration mechanism that is used to partition system resources. A resource pool represents an association between groups of resources that can be partitioned.
resource set	A process-bindable resource. Most often used to refer to the objects constructed by a kernel subsystem offering some form of partitioning. Examples of resource sets include scheduling classes and processor sets.
RSS	See resident set size.
scanner	A kernel thread that identifies infrequently used pages. During low memory conditions, the scanner reclaims pages that have not been recently used.
static pools configuration	A representation of the way in which an administrator would like a system to be configured with respect to resource pools functionality.
task	In resource management, a process collective that represents a set of work over time. Each task is associated with one project.
whole root zone	A type of non-global zone in which all of the required system software and any additional packages are installed into the private file systems of the zone.
working set size	The size of the working set. The working set is the set of pages that the project workload actively uses during its processing cycle.
workload	An aggregation of all processes of an application or group of applications.
WSS	See also working set size.
zone administrator	The privileges of a zone administrator are confined to a non-global zone. See also global administrator.
zone state	The status of a non-global zone. The zone state is one of configured, incomplete, installed, ready, unavailable, running, or shutting down.

Index