Oracle® Solaris Zones 介绍

文件号码 E54013-02
2014 年 12 月

目录

使用本文档

- **概述** – 介绍区域技术以及区域中可用的资源。
- **目标读者** – 系统管理员、技术人员和授权服务提供商。
- **必备知识** – Oracle Solaris 操作系统使用经验，包括网络配置和资源分配知识。

产品文档库

有关本产品的最新信息和已知问题均包含在文档库中，网址为：http://www.oracle.com/pls/topic/lookup?ctx=E56344。

获得 Oracle 支持

Oracle 客户可通过 My Oracle Support 获得电子支持。有关信息，请访问 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info；如果您听力受损，请访问 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs。

反馈

可以在 http://www.oracle.com/goto/docfeedback 上提供有关本文档的反馈。

♦ ♦ ♦ 第 1 章

Oracle Solaris Zones 介绍

Oracle Solaris 操作系统中的 Oracle™ Solaris Zones 功能提供了一个可在其中运行系统上应用程序的隔离环境。

本章概述了区域。

此外，还介绍了以下常规区域主题：

- "区域概述" [9]
- "此发行版支持的区域" [10]
- "关于此版本的 Oracle Solaris Zones" [23]
- "不可编辑区域" [11]
- "关于将 `ipkg` 区域转换为 `solaris` 区域" [11]
- "何时使用区域" [14]
- "区域的工作原理" [16]
- "非全局区域提供的功能" [22]
- "此发行版中的区域标记" [11]

下一章说明了区域配置资源和属性。

如果您已准备就绪，可以开始在系统上创建区域，请跳至《创建和使用 Oracle Solaris 内核区域 》和《创建和使用 Oracle Solaris 区域 》。如果您已准备好将运行 Oracle Solaris 10 的系统（可以包括该系统上的任何非全局 `native` 区域）迁移到 Oracle Solaris 11 系统上的区域中），请参见《创建和使用 Oracle Solaris 10 区域 》。

注 - 有关在 Oracle Solaris Trusted Extensions 系统上使用区域的信息，请参见《Trusted Extensions 配置和管理 》中的第 13 章 "在 Trusted Extensions 中管理区域"。

区域概述

Oracle Solaris Zones 分区技术用于虚拟化操作系统服务，提供安全的隔离环境以便运行应用程序。非全局区域，也称为区域，是在 Oracle Solaris 操作系统的一个单独实例

中创建的一个虚拟化的操作系统环境。操作系统实例称为全局区域。Oracle Solaris 内核区域可以运行支持系统信息库更新 (Support Repository Update, SRU) 或不同于主机的内核版本。

虚拟化的目标是从管理各个数据中心组件转变为管理资源池。成功的服务器虚拟可提高服务器利用率，改善服务器资产利用效率。服务器虚拟对于维护单独系统隔离的成功服务器整合项目也非常重要。

由于将多个主机和服务整合到单台计算机上的需求而产生了虚拟化。虚拟可通过共享硬件、基础结构和管理降低成本。益处具体如下：

- 提高了硬件利用率
- 大大提高了资源分配的灵活性
- 降低了功率要求
- 缩减了管理成本
- 降低了总体拥有成本
- 系统上各应用程序之间可设置管理和资源界限

创建区域时，便创建了一个应用程序执行环境，其中的进程与系统的其余部分相隔离。这种隔离阻止了在一个区域中运行的进程监视或影响在其他区域中运行的进程。对于正在运行的进程，即使具有 root 凭证也不能查看或影响其他区域中的活动。使用 Oracle Solaris Zones，可维护每台服务器一个应用程序的部署模式，同时共享硬件资源。

区域还提供了一个抽象层，用于分隔应用程序和部署这些应用程序的计算机的物理属性。这些属性的示例包括物理设备路径。

可以在任何运行 Oracle Solaris 10 或 Oracle Solaris 11 发行版的计算机上使用区域。系统上 `solaris` 和 `solaris10` 区域的数目上限是 8192。单个系统上可有效托管的区域数量由所有区域中运行的应用程序软件的总资源需求和系统的大小确定。《创建和使用 Oracle Solaris 区域 》中的第 1 章 "如何规划和配置非全局区域"中讨论了这些概念。

如果您要运行 Oracle Solaris 内核区域，有关这些概念的更多信息，请参见《创建和使用 Oracle Solaris 内核区域 》中的"Oracle Solaris 内核区域的硬件和软件要求"。

此发行版支持的区域

Oracle Solaris 11.2 发行版已定义为受支持平台的所有体系结构均支持在单个主机全局区域中运行的非全局 `solaris` 和 `solaris10` 标记区域。

Oracle Solaris 内核区域可在 T4+ 和 M5+ SPARC 计算机、Nehalem+ Intel 计算机以及 Barcelona+ AMD 计算机上运行。有关内核区域系统要求的信息，请参见《创建和使用 Oracle Solaris 内核区域 》中的"Oracle Solaris 内核区域的硬件和软件要求"。

不可编辑区域

不可编辑区域是根目录为只读的 `solaris` 区域。全局和非全局区域均可为不可编辑区域。可通过设置 `file-mac-profile` 属性配置只读区域。提供了多种配置。只读区域根目录扩展了安全运行时界限。

Oracle Solaris 不可编辑全局区域将不可编辑区域功能扩展到了全局区域。对于不可编辑区域和不可编辑内核区域，可以通过 `zlogin` 命令 `zlogin(1)` 来调用可信路径登录。

使用 `zonecfg add dataset` 指定附加数据集的区域仍可对这些数据集进行完全控制。使用 `zonecfg add fs` 指定附加文件系统的区域可对这些文件系统进行完全控制，除非文件系统设置为只读。

有关更多信息，请参见《创建和使用 Oracle Solaris 区域 》中的第 12 章 “配置和管理不可编辑的区域”。

关于将 **ipkg** 区域转换为 **solaris** 区域

为支持 Oracle Solaris 11 Express 发行版客户，配置为 `ipkg` 区域的任何区域都将被转换为 `solaris` 区域，并在 `pkg` 更新或 `zoneadm attach` 时向 Oracle Solaris 11.2 报告为 `solaris`。`ipkg` 名称将映射为 `solaris` 名称（如果在配置区域时使用）。支持导入从 Oracle Solaris 11 Express 主机导出的 `zonecfg` 文件。

对于 Oracle Solaris 11.2 系统上的缺省区域，`zonecfg info` 或 `zoneadm list -v` 等命令的输出会显示 `solaris` 标记。

此发行版中的区域标记

Oracle Solaris 内核区域

Oracle Solaris 内核区域功能可在区域内提供完整的内核和用户环境，并且还会加大主机和区域之间的内核分离。标记名称为 `solaris-kz`。可通过使用现有工具 `zonecfg`、`zoneadm` 和 `zlogin` 从全局区域来管理内核区域。作为内核区域的管理员，相比缺省的 `solaris` 区域管理员，您在配置和管理区域方面具有更大的灵活性。例如，您可以完全更新和修改区域的已安装软件包（包括内核版本），而不会受限于全局区域中安装的软件包。您可以管理区域专属的存储、创建和销毁 ZFS 池，以及配置 iSCSI 和 CIFS。您可以在内核区域内安装 `solaris` 区域以生成分层（嵌套）区域。内核区域支持暂停和恢复。您可以通过在源计算机上暂停区域并在目标计算机上恢复该区域来迁移内核区域。

要使用 Oracle Solaris 内核区域，必须在系统上安装 brand-solaris-kz 软件包。要确定您的计算机是否支持内核区域，请参见“关于此版本的 Oracle Solaris Zones” [23]。如果安装了 Oracle Solaris 11.2，还可以在计算机上运行 virtinfo 命令。有关 Oracle Solaris 内核区域的更多信息，请参见《创建和使用 Oracle Solaris 内核区域 》和 solaris-kz(5) 手册页。有关 virtinfo 命令的更多信息，请参见《创建和使用 Oracle Solaris 内核区域 》中的“如何检验主机上的内核区域支持”和 virtinfo(1M) 手册页。

缺省 Oracle Solaris Zones

Oracle Solaris Zones 功能可为应用程序提供完整的运行时环境。区域提供从应用程序到平台资源的虚拟映射。利用区域可以使应用程序组件彼此隔离，即使这些区域共享单个 Oracle Solaris 操作系统实例也是如此。区域使用资源管理组件控制应用程序如何使用可用系统资源。有关资源管理功能的其他信息，请参见《在 Oracle Solaris 11.2 中进行资源管理 》。

区域建立资源占用（如 CPU）的边界。这些边界可以进行扩展，以适应区域中运行的应用程序不断变化的处理要求。

如需其他隔离，可以配置具有只读根目录的区域，称为不可编辑的区域。

Oracle Solaris 10 Zones

Oracle Solaris 10 Zones（也称为 solaris10 标记非全局区域）使用 BrandZ 技术在 Oracle Solaris 11 操作系统上运行 Oracle Solaris 10 应用程序。应用程序在非全局区域所提供的安全环境中运行，不会被修改。这样，您可使用 Oracle Solaris 10 系统来开发、测试和部署应用程序。在这些标记区域内运行的工作负荷可以利用内核的增强功能以及仅适用于 Oracle Solaris 11 发行版的创新技术。这些区域用于将 Oracle Solaris 10 系统迁移到 Solaris 11 上的区域。solaris 10 标记区域不能是 NFS 服务器。

有关更多信息，请参见《创建和使用 Oracle Solaris 10 区域 》。

区域标记概述

solaris-kz 区域和 solaris 以及 solaris10 标记区域之间的区别如下所示。

表 1-1 Oracle Solaris 区域标记功能比较

组成部分	solaris-kz 标记	solaris 和 solaris10 标记
支持的硬件	在指定硬件上受支持。请参见指向 OTN 站点或 HCL 的链接。	在所有 Oracle Solaris 11.2 系统上受支持。请参见 HCL。

组成部分	solaris-kz 标记	solaris 和 solaris10 标记
内存管理	必须为 solaris-kz 虚拟平台分配固定数量的物理 RAM。	可以共享分配给全局区域的物理 RAM。
内核版本	内核区域可以运行与主机不同的内核版本或 SRU 级别。	内核版本必须与全局区域的版本相同。
存储和设备管理	执行所有存储访问。内核区域不支持 zpool 或 rootzpool 资源。	可通过 fs、zpool 和 dataset zonecfg 资源在文件系统级别提供存储。
联网	仅支持专用 IP 区域。	支持专用 IP 区域和共享 IP 区域。

在 Oracle Solaris Trusted Extensions 系统上使用 Oracle Solaris Zones

有关在 Oracle Solaris Trusted Extensions 系统上使用区域的信息，请参见《Trusted Extensions 配置和管理 》中的第 13 章 “在 Trusted Extensions 中管理区域”。请注意，只能在 Oracle Solaris Trusted Extensions 系统上引导有标签的标记。

Oracle Solaris Cluster 区域群集

区域群集是 Oracle Solaris Cluster 软件的一项功能。区域群集是用作区域群集的节点的一组非全局区域。在使用区域群集配置的每个全局群集节点上创建一个非全局区域。区域群集的节点可以采用 solaris 标记，也可以采用 solaris10 标记，并且使用群集属性。不允许其他标记类型。在区域群集上运行支持服务的方式与全局群集相同，隔离由区域提供。有关更多信息，请参见《Oracle Solaris Cluster 系统管理指南 》。

关于标记区域

缺省情况下，系统上的非全局区域运行与全局区域相同的操作系统软件。Oracle Solaris 操作系统中的标记区域 (branded zone, BrandZ) 功能是 Oracle Solaris Zones 的简单扩展。BrandZ 框架用于创建所含的操作环境与全局区域不同的非全局标记区域。在 Oracle Solaris 操作系统上使用标记区域来运行应用程序。BrandZ 框架通过多种方式扩展了 Oracle Solaris Zones 基础结构。这些扩展可能比较复杂（例如，提供在区域内运行不同操作系统环境的功能），也可能比较简单（例如，增强基础区域命令以便提供新功能）。例如，Oracle Solaris 10 Zones 是一个非全局标记区域，可以模拟 Oracle Solaris 10 操作系统。即使与全局区域共享相同操作系统的缺省区域也要配有标记。

标记定义了可在区域中安装的操作环境并确定系统在该区域内的行为方式，以便在该区域中安装的软件可以正常运行。此外，区域的标记可用于在应用程序启动时识别正确的应用程序类型。所有标记区域管理都通过扩展标准区域结构来执行。所有区域的大多数管理步骤都相同。

标记文档中介绍了此配置中包含的缺省资源，例如，定义的文件系统和特权。

BrandZ 通过以下方式来扩展区域工具：

- 配置区域时，使用 `zonecfg` 命令来设置区域的标记类型。
- 使用 `zoneadm` 命令来报告区域的标记类型并管理区域。

尽管您可以在已启用标签的 Oracle Solaris Trusted Extensions 系统上配置和安装标记区域，但是您不能在此系统配置中引导标记区域，除非所引导的标记是已认证系统配置中的有标签的标记。

可以在已配置状态下更改区域标记。一旦安装了标记区域，就不能更改或删除标记。

注意 - 如果您打算将现有 Oracle Solaris 10 系统迁移到运行 Oracle Solaris 11 发行版的系统上的某个 `solaris10` 标记区域，您必须先将所有现有区域迁移到目标系统。由于 `solaris10` 区域并不嵌套，因此系统迁移过程将使任何现有区域变得不可用。有关更多信息，请参见《创建和使用 Oracle Solaris 10 区域 》中的第 3 章 "将 Oracle Solaris 10 native 非全局区域迁移到 Oracle Solaris 10 区域"。

在标记区域中运行的进程

标记区域在内核中提供了一组插入点，这些插入点只应用于在标记区域中执行的进程。

- 这些点位于 `syscall` 路径、进程装入路径和线程创建路径之类的路径中。
- 在其中每个点处，标记可以选择补充或替换标准 Oracle Solaris 行为。

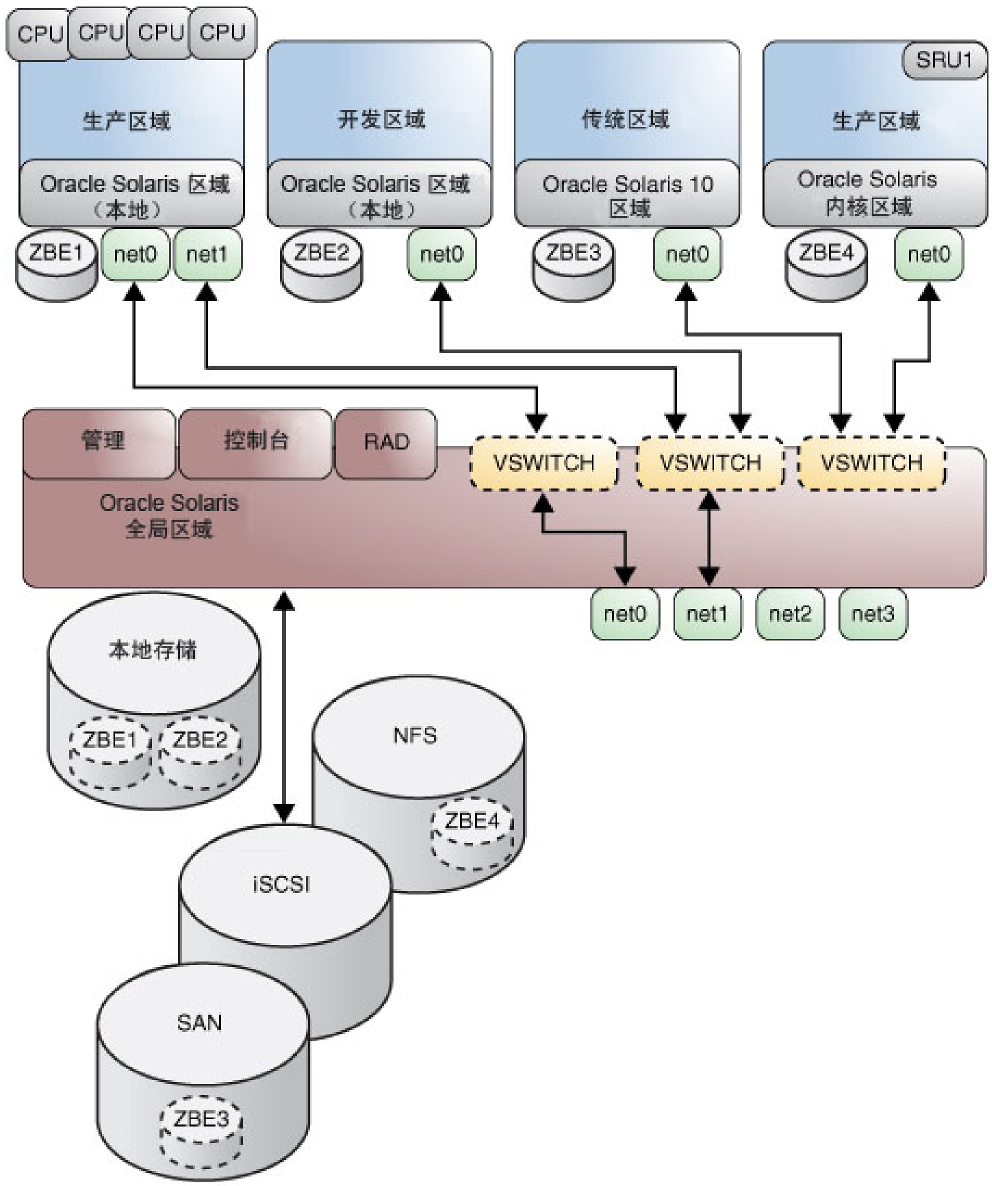
标记还能为 `librtld_db` 提供插件库。通过插件库，Oracle Solaris 工具（如 mdb(1) 中介绍的调试器和 `dtrace`(1M) 中介绍的 DTrace）可以访问在标记区域内运行的进程的符号信息。

请注意，区域不支持静态链接的二进制文件。

何时使用区域

对于将多个应用程序整合在一个服务器中的环境而言，使用区域是明智之举。管理大量计算机所带来的成本和复杂性促使在更大、更具伸缩性的服务器上整合多个应用程序。

图 1-1 区域服务器整合示例



使用区域，可以更有效地利用系统上的资源。使用动态资源重新分配，可以根据需要将未使用的资源转移到其他区域。故障和安全隔离意味着运行欠佳的应用程序不需要一个未充分利用的专用系统。使用区域，可以将这些应用程序与其他应用程序进行整合。

使用区域，可以在维护整体系统安全的同时委托某些管理功能。

区域的工作原理

可以将一个非全局区域想象为一个盒子。一个或多个应用程序可在这个盒子中运行，而不与系统的其余部分交互。区域使用灵活、软件定义的边界将各软件应用程序或服务分隔开来。然后，便可分别管理在 Oracle Solaris 操作系统的同一实例中运行的应用程序。因此，为了符合配置要求，不同版本的同一应用程序可以在不同区域中运行。

指定给某区域的进程可以处理、监视指定给同一区域的其他进程，并可直接与这些进程进行通信。进程不能对指定给系统中其他区域的进程执行这些功能，也不能对未指定给区域的进程执行这些功能。指定给不同区域的进程只能通过网络 API 进行通信。

IP 联网可按两种不同的方式进行配置，具体用哪种方式取决于该区域是具有其自己的专用 IP 实例还是将 IP 层配置和状态与全局区域共享。专用 IP 为缺省类型。有关区域中 IP 类型的更多信息，请参见“区域网络接口” [35]。有关配置信息，请参见《创建和使用 Oracle Solaris 区域 》中的“如何配置区域”。

每个 Oracle Solaris 系统都包含一个全局区域。全局区域具有双重功能。全局区域既是系统的缺省区域，也是用于在整个系统中实施管理控制的区域。如果全局管理员或具有区域安全配置文件的用户没有创建任何非全局区域（简称为区域），则所有进程将在全局区域中运行。

只能从全局区域配置、安装、管理或卸载非全局区域。只有全局区域才可从系统硬件进行引导。只能在物理系统上运行的全局区域中进行系统基础结构（如物理设备）的管理、共享 IP 区域中的路由或动态重新配置 (dynamic reconfiguration, DR)。全局区域中运行的具有适当特权的进程可以访问与其他区域关联的对象。

在某些情况下，全局区域中的非特权进程可以执行非全局区域中不允许特权进程执行的操作。例如，全局区域中的用户可以查看有关系统中每个进程的信息。如果此功能会使站点出现问题，则可以限制对全局区域进行访问。

包括全局区域在内的每个区域都会被指定一个区域名称。全局区域始终命名为 `global`。每个区域还具有唯一的数字标识符，这是引导区域时由系统指定的。全局区域始终会映射到 ID `0`。如果您对内核区域执行 `zlogin`，它也会报告其具有 ID 0，因为它是一个虚拟全局区域。《创建和使用 Oracle Solaris 区域 》中的“如何配置区域”中讨论了区域名称和数字 ID。

每个区域还具有节点名称，此名称完全独立于区域名称。节点名称由区域管理员指定。有关更多信息，请参见《创建和使用 Oracle Solaris 区域 》中的“非全局区域节点名称”。

每个区域都具有一个与全局区域根目录相对的根目录路径。有关更多信息，请参见“使用 zonecfg 命令” [46]。

缺省情况下，非全局区域的调度类设置为系统的调度类。有关在区域中设置调度类的方法讨论，请参见“调度类” [32]。

块设备多路径由 scsi_vhci(7D) 处理。您为配置选择的 lu: storage URI 格式决定了该配置的使用方式。有关将 lu: URI 与多路径配合使用的更多信息，请参见 suri(5) 手册页。

区域摘要（按功能）

下表总结了全局区域和非全局区域的特征。

区域类型	特征
全局	■ 由系统指定 ID 0 ■ 提供正在系统上运行的可引导的 Oracle Solaris 内核的单个实例 ■ 包含 Oracle Solaris 系统软件包的完整安装 ■ 可以包含其他软件包或未通过软件包安装的其他软件、目录、文件以及其他数据 ■ 提供一个完整一致的产品数据库，该数据库包含安装在全局区域中的所有软件组件的有关信息 ■ 仅存放特定于全局区域的配置信息，如全局区域主机名和文件系统表 ■ 是识别所有设备和所有文件系统的唯一区域 ■ 是识别非全局区域存在和配置的唯一区域 ■ 是可以从中配置、安装、管理或卸载非全局区域的唯一区域
非全局	■ 引导区域时由系统指定区域 ID ■ 共享从全局区域引导的 Oracle Solaris 内核下的操作 ■ 包含完整 Oracle Solaris 操作系统软件包中已安装的一部分 ■ 可以包含其他已安装的软件包 ■ 可以包含在非全局区域上创建的，未通过软件包安装的其他软件、目录、文件以及其他数据 ■ 具有一个完整一致的产品数据库，该数据库包含安装在区域中的所有软件组件的相关信息 ■ 不识别其他任何区域的存在 ■ 无法安装、管理或卸载其他区域，包括其本身 ■ 仅具有特定于非全局区域的配置信息，例如非全局区域主机名和文件系统表 ■ 可以具有自己的时区设置

如何管理非全局区域

全局管理员具有超级用户特权或等效的管理权限。当全局管理员登录到全局区域时，可以将系统作为一个整体进行监视和控制。

区域管理员可以管理非全局区域。全局管理员可向区域管理员指定所需的授权，如“admin 资源” [29]中所述。区域管理员的特权仅限于特定的非全局区域。

如何创建非全局区域

您可以在自动安装 (Automated Install, AI) 客户机的安装过程中指定非全局区域的配置和安装。有关更多信息，请参见《安装 Oracle Solaris 11.2 系统 》。Oracle Solaris 内核区域主要使用直接安装方法来创建。《创建和使用 Oracle Solaris 内核区域 》中的“安装内核区域”中介绍了内核区域创建方法。

为在 Oracle Solaris 系统上创建区域，全局管理员将通过为区域的虚拟平台和应用程序环境指定各种参数，使用 `zonecfg` 命令来配置区域。然后，全局管理员安装区域，使用区域管理命令 `zoneadm` 将软件包中的软件安装到为区域建立的文件系统分层结构。使用 `zoneadm` 命令引导区域。然后，全局管理员或授权用户可以使用 `zlogin` 命令登录到已安装的区域。如果使用基于角色的访问控制 (role-based access control, RBAC)，则区域管理员必须具备 `solaris.zone.manage/`*zonename* 授权。

有关区域配置的信息，请参见第 2 章 非全局区域配置概述。有关区域安装的信息，请参见《创建和使用 Oracle Solaris 区域 》中的第 2 章 “关于安装、关闭、停止、卸载和克隆非全局区域”。有关区域登录的信息，请参见《创建和使用 Oracle Solaris 区域 》中的第 4 章 “关于非全局区域登录”。

要配置和安装 Oracle Solaris 内核区域，请参见《创建和使用 Oracle Solaris 内核区域 》。

非全局区域状态模型

非全局区域可以处于以下七种状态之一：

已配置
: 区域配置已完成并提交到稳定存储器。但是，那些必须在初始引导之后指定的区域应用程序环境元素还不存在。

未完成
: 在安装或卸载操作期间，`zoneadm` 将目标区域的状态设置为未完成。成功完成操作之后，便将状态设置为正确的状态。

  可以使用 `zoneadm` 的 `mark` 子命令将被损坏的已安装区域标记为未完成。处于未完成状态下的区域如 `zoneadm list -iv` 的输出所示。

不可用
: 指示区域已安装，但无法验证、就绪、引导、附加或移动。出现以下情况时区域会进入不可用状态：

- 区域的存储不可用而 `svc:/system/zones:default` 已开始，如在系统引导期间
- 当区域的存储不可用时
- 当成功提取归档文件之后基于归档文件的安装失败时
- 当区域的软件与全局区域的软件不兼容时，如在不正确的 `-F`（强制）附加之后

已安装　　已在系统上实例化区域配置。使用 `zoneadm` 命令检验是否可以在指定的 Oracle Solaris 系统上成功使用配置。软件包安装在区域的根路径下。在此状态下，区域没有关联的虚拟平台。

就绪　　已建立区域的虚拟平台。已由内核创建 `zsched` 进程，已设置网络接口且可用于该区域，已挂载文件系统，并且已配置设备。系统会指定唯一的区域 ID。在此阶段，没有启动与区域关联的进程。

正在运行　　正在运行与区域应用程序环境关联的用户进程。创建了与应用程序环境关联的第一个用户进程 (`init`) 之后，区域便会立即进入正在运行状态。

正在关闭和关闭　　这两种状态是停止区域时出现的过渡状态。但是，因某种原因无法关闭的区域将会在这两种状态下停止。

《创建和使用 Oracle Solaris 区域 》中的第 3 章 “安装、引导、关闭、停止、卸载和克隆非全局区域”和 `zoneadm(1M)` 手册页介绍了如何使用 `zoneadm` 命令在这些状态之间进行转换。

此外，Oracle Solaris 内核区域具有三个辅助状态，用于通知主机关于当前区域状态的其他信息。

已暂停　　主状态为已停止，辅助状态为已暂停。

调试　　区域正在运行，但是区域无法响应外部事件，例如联网。`zlogin` 会检查此状态，并等到该状态清除，然后再启动 `zlogin` 会话。

紧急　　区域遇到紧急情况，但区域在重新引导前无法响应外部事件。

有关其他信息，请参见《创建和使用 Oracle Solaris 内核区域 》和 `solaris-kz(5)` 手册页。

表 1-2　　影响区域状态的命令

当前区域状态	适用的命令

已配置	`zonecfg -z` *zonename* `verify`
	`zonecfg -z` *zonename* `commit`
	`zonecfg -z` *zonename* `delete`

当前区域状态	适用的命令

	`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*
	
	您可以使用 `zonecfg` 命令重命名处于已配置状态的区域。请注意，您可以使用 `zoneadm` 命令重命名处于已配置或已安装状态的 Oracle Solaris 区域或 Oracle Solaris 10 区域。

未完成	`zoneadm -z` *zonename* `uninstall`
不可用	`zoneadm -z` *zonename* `uninstall` 可从指定的系统中卸载区域。 `zoneadm -z` *zonename* `attach` `zonecfg -z` *zonename* 可用于更改 `zonepath` 和其他任何处于已安装状态时无法进行更改的属性和资源。

已安装	`zoneadm -z` *zonename* `ready`（可选）
	
	`zoneadm -z` *zonename* `boot`
	
	`zoneadm -z` *zonename* `uninstall` 可从系统中卸载指定区域的配置。
	
	`zoneadm -z` *zonename* `move` *path*
	
	`zoneadm -z` *zonename* `detach`
	
	`zonecfg -z` *zonename* 可用于添加或删除 `attr`、`bootargs`、`capped-memory`、`dataset`、`capped-cpu`、`dedicated-cpu`、`device`、`fs`、`ip-type`、`limitpriv`、`net`、`rctl` 或 `scheduling-class` 属性。您还可以重命名区域。
	
	您可以使用 `zoneadm` 命令重命名处于已配置或已安装状态的 Oracle Solaris 区域或 Oracle Solaris 10 区域。
	
	`zoneadm -z` *zonename* `mark` *incomplete*
	
	`zoneadm -z` *zonename* `mark` *unavailable*

就绪	`zoneadm -z` *zonename* `boot` `zoneadm halt` 加上系统重新引导可使区域从就绪状态恢复为已安装状态。 `zonecfg -z` *zonename* 可用于添加或删除 `attr`、`bootargs`、`capped-memory`、`dataset`、`capped-cpu`、`dedicated-cpu`、`device`、`fs`、`ip-type`、`limitpriv`、`net`、`rctl` 或 `scheduling-class` 属性。

正在运行	`zlogin` *options* `zonename`
	
	`zoneadm -z` *zonename* `reboot`
	
	`zoneadm -z`*zonename* `halt` 可使就绪区域恢复为已安装状态。

当前区域状态	适用的命令
	zoneadm halt 加上系统重新引导可使区域从正在运行状态恢复为已安装状态。 zoneadm - z shutdown 可干净地关闭区域。 zonecfg -z *zonename* 可用于添加或删除 attr、bootargs、capped-memory、dataset、capped-cpu、dedicated-cpu、device、fs、ip-type、limitpriv、anet、net、rctl 或 scheduling-class 属性。不能更改 zonepath 资源。

注 - 通过 zonecfg 更改的参数不会影响正在运行的区域。必须重新引导区域才能使更改生效。

非全局区域特征

区域提供的隔离几乎可细化到您所需的任何程度。区域不需要专用的 CPU、物理设备或部分物理内存。可以在单个域或系统中运行的多个区域之间复用这些资源，也可借助操作系统中可用的资源管理功能为每个区域分别分配这些资源。

每个区域都可提供一组定制的服务。要执行基本进程隔离，一个进程只能看到同一区域中的各个进程，或向这些进程发送信号。区域间的基本通信是通过每个区域的 IP 网络连接来完成的。在某个区域中运行的应用程序看不到其他区域的网络流量。即使各个软件包的流使用同一物理接口，也会维护这种隔离。

每个区域都在文件系统分层结构中拥有一个位置。因为每个区域都只限于文件系统分层结构中的一个子树，所以在某一特定区域中运行的工作负荷不能访问在其他区域中运行的另一个工作负荷的盘上数据。

命名服务使用的文件驻留在区域本身的根文件系统视图中。因此，不同区域的命名服务之间相互分离并可单独配置。

将资源管理功能用于非全局区域

如果您使用资源管理功能，则应当使此功能可以完全控制区域范围。通过指定上述控制范围，可以创建更完整的虚拟机模型，可对其中的名称空间访问、安全隔离和资源使用情况进行完全控制。

对于将各种资源管理功能用于区域的任何特殊要求，将在本手册中介绍这些功能的各章节中介绍。

与区域相关的 SMF 服务

全局区域中与区域相关的 SMF 服务包括以下内容：

svc:/system/zones:default	启动具备 autoboot=true 的每个区域。
svc:/system/zones-install:default	如果需要，首次引导时执行区域安装。
svc:/application/pkg/zones-proxyd:default	包管理系统使用该服务提供对系统信息库的区域访问。
svc:/application/pkg/system-repository:default	高速缓存代理服务器，该服务器用于高速缓存区域安装和其他 pkg 操作期间使用的 pkg 数据和元数据。请参见 pkg(1) 和 pkg(5) 手册页。
svc:/system/zones-monitoring:default	控制 zonestatd。

svc:/application/pkg/zones-proxy-client:default 区域代理客户机 SMF 服务仅在非全局区域运行。包管理系统使用该服务提供对系统信息库的区域访问。

监视非全局区域

有关如何报告当前正在运行的区域的 CPU、内存和资源控制使用情况，请参见《创建和使用 Oracle Solaris 区域 》中的"在非全局区域中使用 zonestat 实用程序"。zonestat 实用程序还可报告专用 IP 区域中的网络带宽使用情况。专用 IP 区域具有其自己的 IP 相关状态以及一个或多个专用数据链路。

可以使用 fsstat 实用程序为非全局区域报告文件操作统计信息。请参见 fsstat(1M) 手册页和《创建和使用 Oracle Solaris 区域 》中的"使用 fsstat 实用程序监视非全局区域"。

非全局区域提供的功能

非全局区域可提供以下功能：

安全性	一旦将进程放入全局区域之外的区域，此进程或其后续子进程便不能更改区域。 可以在区域中运行网络服务。通过在区域中运行网络服务，可限制出现安全违规时可能引起的损坏。如果入侵者成功利用了区域中运行的软件中的安全缺陷，则此入侵者只能在此区域中执行一部分可能的操作。区域中可用的特权是整个系统中可用特权的一部分。
隔离	使用区域，可以在同一计算机上部署多个应用程序，即使这些应用程序运行在不同的信任域中，需要独占访问全局资源或者全局配置出现问题也是如此。应用程序还无法监视或拦截其他应用程序的网络流量、文件系统数据或进程活动。
网络隔离	区域在缺省情况下配置为专用 IP 类型。在 IP 层，这些区域与全局区域隔离，并且相互隔离。出于运行和安全方面的原因而采用了这种隔离。可通过区域来合并必须使用其自己的 LAN 或 VLAN 在不同子网上通信的应用程序。每个区域还可以定义其自己的 IP 层安全规则。
虚拟化	区域提供了一个虚拟环境，此环境可以在应用程序中隐藏详细信息（例如物理设备、系统的主 IP 地址以及主机名）。可以在不同的物理计算机上维护同一应用程序环境。通过虚拟环境，可以单独管理每个区域。区域管理员在非全局区域中执行的操作不会影响系统的其余部分。
粒度	区域提供的隔离几乎可细化到任何程度。有关更多信息，请参见"非全局区域特征" [21]。
环境	区域不更改应用程序的执行环境，但为实现安全和隔离目标而必须更改的情况除外。区域不显示应用程序必须连接的新 API 或 ABI。相反，区域提供具有某些限制的标准 Oracle Solaris 接口和应用程序环境。这些限制主要影响尝试执行特权操作的应用程序。 无论是否配置其他区域，全局区域中的应用程序始终会运行而无需修改。

关于此版本的 Oracle Solaris Zones

本节概述了 Oracle Solaris Zones 功能（包括 Oracle Solaris 内核区域）。

此发行版中的缺省非全局区域为 `solaris`，本指南及 `solaris`(5) 手册页中都有相关介绍。

要检验 Oracle Solaris 发行版本和计算机体系结构，请键入：

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

virtinfo(1M) 手册页中介绍的 virtinfo 命令用于获取以下信息：

- 确定 Oracle Solaris 虚拟化技术系统支持
- 检测运行 Oracle Solaris 的虚拟环境类型，例如 Oracle VM Server for SPARC

solaris 区域使用标记区域框架（如 brands(5) 手册页中所述）运行与全局区域安装了相同软件的区域。使用 solaris 标记非全局区域时，系统软件必须始终与全局区域保持同步。区域中的系统软件包使用映像包管理系统 (Image Packaging System, IPS) 进行管理。IPS 是 Oracle Solaris 11 发行版中的包管理系统，solaris 区域使用这种模式。

在 Oracle Solaris 11 Express 发行版中创建的缺省 ipkg 区域将映射为 solaris 区域。请参见"关于将 ipkg 区域转换为 solaris 区域" [11]。

在自动安装 (Automated Install, AI) 清单中指定的每个非全局区域将在客户机安装过程中进行安装和配置。非全局区域是在安装全局区域后首次重新引导时安装并配置的。当系统第一次引导时，区域自组装 (self-assembly) SMF 服务 svc:/system/zones-install:default 会配置并安装全局区域 AI 清单中定义的每个非全局区域。有关更多信息，请参见《在 Oracle Solaris 11.2 中添加和更新软件 》。也可以在已安装的 Oracle Solaris 系统上手动配置并安装区域。

对于软件包更新，应该通过使用 --proxy 选项在映像中设置持久性代理。如果未使用持久性映像代理配置，则可以设置 http_proxy 和 https_proxy 环境变量。

可以将区域配置为并行更新而不是串行更新。并行更新可大幅缩短更新系统上的所有区域所需的时间。

缺省情况下，使用专用 IP 类型创建区域。如果没有指定联网配置，可以通过 anet 资源将 VNIC 自动包含在区域配置中。有关更多信息，请参见"区域网络接口" [35]。

有关用于获取区域 mac-address 的 auto-mac-address 的信息，请参见"资源类型属性" [53]中的 anet 条目。

共享存储上的 solaris 区域具有 zonecfg rootzpool 资源。将区域封装到专用 zpool。共享存储上的区域访问和管理用于区域的共享存储资源。内核区域没有 zpool 或 rootzpool 资源。solaris 标记区域可使用区域 device 资源以及 zpool 和 rootzpool 资源的以下共享存储。

- iSCSI
- FC LUN
- DAS

用于指定基于 InfiniBand 的 IP (IP over InfiniBand, IPoIB) 数据链路的属性可用于 zonecfg anet 资源。solaris 和 solaris10 标记区域均支持 IPoIB。

专用 IP 和共享 IP 非全局区域都支持可靠数据报套接字 (Reliable Datagram Socket, RDS) IPC 协议。

已扩展 fsstat 实用程序以支持区域。fsstat 实用程序提供每区域统计信息和聚合统计信息。

solaris 区域可以是 NFS 服务器，如《创建和使用 Oracle Solaris 区域 》中的"在区域内运行 NFS 服务器"一节中所述。

试运行（也称为预运行）zoneadm attach -n 提供了 zonecfg 验证，但不执行软件包内容验证。

所有以文件为参数的 zoneadm 选项都需要使用绝对路径。

Oracle Solaris 10 Zones 可在 Oracle Solaris 11 上提供 Oracle Solaris 10 环境。您可以将 Oracle Solaris 10 系统或区域迁移到 Oracle Solaris 11 系统上的 solaris10 区域。请参见《创建和使用 Oracle Solaris 10 区域 》。

zonep2vchk 工具可识别可能会影响将 Oracle Solaris 11 系统或 Oracle Solaris 10 系统迁移到运行 Oracle Solaris 11 发行版系统上的某个区域的问题，包括联网问题。在迁移开始之前，先在源系统上执行 zonep2vchk 工具。此工具还会输出 zonecfg 脚本以便在目标系统上使用。此脚本将创建一个与源系统配置相匹配的区域。有关更多信息，请参见《创建和使用 Oracle Solaris 区域 》中的第 7 章 "关于区域迁移和 zonep2vchk 工具"。

应注意 solaris 区域与 Oracle Solaris 10 发行版中的 native 区域之间存在的以下差异：

- Oracle Solaris 11 系统中创建 solaris 标记，而非 native 标记，后者是 Oracle Solaris 10 系统中的缺省标记。
- solaris 区域仅为完全根类型。

  Oracle Solaris 10 上提供的本机区域的稀疏根类型使用 SVR4 软件包管理系统，但 IPS 不使用这一系统。提供类似于稀疏根类型的只读根区域配置。
- 在本发行版的区域中，与软件管理相关的功能与 Oracle Solaris 10 发行版之间存在以下方面的区别：
  - IPS 与 SVR4 包管理。
  - 安装、分离、附加和物理转换到虚拟功能。
  - 非全局区域根目录是一个 ZFS™ 数据集。

    全局区域中安装的软件包不再安装到所有当前区域和未来的区域中。总体而言，对于 IPS 和 SVR4 包管理，全局区域的软件包内容不再指定每个区域的软件包内容。
- 非全局区域使用引导环境。区域与 beadm 集成在一起，它是用于管理 ZFS 引导环境 (Boot Environment, BE) 的用户界面命令。

  区域支持 beadm 命令，以便用于 pkg 更新，就像在全局区域中一样。beadm 命令可以删除与区域相关联的任何非活动区域 BE。请参见 beadm(1M) 手册页。
- 安装区域时，所有已启用的 IPS 软件包系统信息库都必须可访问。有关更多信息，请参见《创建和使用 Oracle Solaris 区域 》中的"如何安装已配置的区域"。

- 区域软件以最小化形式启动。必须添加区域所需的所有附加软件包。有关更多信息，请参见《在 Oracle Solaris 11.2 中添加和更新软件 》。

区域可以使用 Oracle Solaris 产品和功能，如下所示：

- Oracle Solaris ZFS 加密
- 网络虚拟化和 QoS
- CIFS 和 NFS

不能在 `solaris-kz` 标记区域中配置以下功能：

- FC 服务
- FCoE 服务

实时区域重新配置

使用实时区域重新配置无需重新引导即可重新配置或报告正在运行的 `solaris` 或 `solaris10` 区域的实时配置。可以进行临时性更改，也可以进行持久性更改。

使用实时区域重新配置可报告 `solaris-kz` 标记区域的实时配置信息。

有关更多信息，请参见《创建和使用 Oracle Solaris 区域 》。

♦ ♦ ♦ 第 2 章

非全局区域配置概述

本章介绍非全局区域配置。

本章中的主题包括以下内容：

了解区域配置之后，请转至《创建和使用 Oracle Solaris 区域 》中的第 1 章 "如何规划和配置非全局区域"以配置要在系统上安装的非全局区域。

关于区域中的资源

可以在区域中控制的资源包括：

- 资源池或指定的 CPU，用于对计算机资源进行分区。
- 资源控制，提供了一种系统资源约束机制。
- 调度类，可让您根据资源的重要性在区域中控制可用 CPU 资源的分配。这种重要性通过您为每个区域指定的 CPU 资源份额来表示。

在区域管理中使用权限配置文件和角色

有关配置文件和角色的信息，请参见《Oracle Solaris 11 安全准则 》中的"保护和隔离应用程序"。

zonecfg template 属性

使用 zonecfg template 属性定义以下情况下属性是否变化，以及如何变化：

- 将新资源实例添加到配置中时。
- 在配置克隆期间，当某些属性必须具有唯一值时。使用 template 属性中的令牌提供这些唯一值。

表 2-1　zonecfg template 标记

标记	说明	使用情况
%*zonename*	区域的名称。	可以用在标记的元数据中，以及 zonecfg 中，作为用户或模板值的输入。
%*network-id*	网络资源 net 和 anet 的唯一实例编号。此编号对于全局区域内的 net 和 anet 资源是唯一的。	可以用在标记的元数据中，作为 id 属性 net 和 anet 资源的缺省特性。
%*resource-id*	给定资源全局范围内、全局区域内除 net 和 anet 外的其他所有资源的唯一实例编号。	可以用在标记的元数据中，作为 id 属性的缺省特性。
%*id*	唯一的实例编号，是资源的 *id* 属性值。	可以用在 zonecfg 中作为用户或模板值的输入。应当在支持 id 属性的资源范围内使用。
%%	求值结果为 %。	可以用在标记的元数据中，以及 zonecfg 中作为用户的输入。

区域远程管理守护进程 (remote administration daemon, RAD) 模块配置提供了通过使用属性模板来表示、执行或实施更改的系统方法。请参见 zonemgr(3RAD) 手册页。如果最初未在您的系统上安装 rad-zonemgr 软件包，而是之后使用 pkg install 安装该软件包，则必须重新启动 rad:local。如果 rad:remote 正在运行，也要重新启动。要重新启动，请使用 svcadm(1M)。确保 RAD 守护进程已装入该模块。

安装前配置过程

在系统上安装非全局区域并使用它之前，必须先配置该区域。

zonecfg 命令用于创建配置，并确定指定的资源和属性是否在虚拟系统上有效。zonecfg 对给定配置执行的检查将检验以下内容：

- 确保已指定区域路径.

- 确保已为每个资源指定所有必需的属性。
- 确保配置没有冲突。例如，如果您有一个 `anet` 资源，则区域为专用 IP 类型，不能为共享 IP 区域。此外，如果已有别名的数据集与设备之间有潜在冲突，则 `zonecfg` 命令会发出一个警告。

有关 `zonecfg` 命令的更多信息，请参见 zonecfg(1M) 手册页。

区域组件

本节讨论可以配置的必需区域组件和可选的区域组件。只有区域名称和区域路径是必需的。"区域配置数据" [49]中还提供了附加信息。

区域名称和路径

必须为区域选择名称。如果不指定路径，`zonepath` 的缺省值为 `/system/zones/`*zonename*。

如果为区域选择了名称和路径，则区域必须位于 ZFS 数据集中。在安装或附加区域时，将自动创建 ZFS 数据集。如果无法创建 ZFS 数据集，也无法安装或附加区域。请注意，区域路径的父目录也必须是一个数据集。

如果未指定路径，`zonepath` 的缺省值为 `/system/zones/`*zonename*。

区域自动引导

`autoboot` 属性设置决定了是否在引导全局区域时自动引导该区域。区域服务，`svc:/system/zones:default` 也必须启用。

用于不可编辑区域的 `file-mac-profile` 属性

在 `solaris` 区域中，`file-mac-profile` 用于配置具有只读根目录的不可编辑区域。

有关更多信息，请参见《创建和使用 Oracle Solaris 区域 》中的第 12 章 "配置和管理不可编辑的区域"。

`admin` 资源

`admin` 设置允许您设置区域管理授权。定义授权的首选方法是通过 `zonecfg` 命令。

user 指定用户名。

auths 指定用户名授权。

- solaris.zone.login 如果使用了 RBAC，则交互式登录需要 solaris.zone.login/*zonename* 授权。将在区域中进行口令验证。
- solaris.zone.manage 如果使用 RBAC，则对于非交互式登录或者要跳过口令验证，需要 solaris.zone.manage/*zonename* 授权。
- solaris.zone.clonefrom 如果使用 RBAC，则用于生成其他区域副本的子命令需要 solaris.zone.clonefrom/*source_zone* 授权。

有关授权的更多信息，请参见 auths(1)、auth_attr(4) 和 user_attr(4)。

dedicated-cpu 资源

dedicated-cpu 资源可指定在非全局区域运行时应将系统处理器的某个子集专用于该非全局区域。在引导区域时，系统将动态创建一个临时池，以便在区域运行时使用。

根据 zonecfg 的指定，池设置将在迁移期间进行传播。

dedicated-cpu 资源可为 ncpus 以及 importance（可选）设置限制。

ncpus 指定 CPU 数目或指定一个范围（如 2–4 个 CPU）。如果指定一个范围（因为需要动态资源池行为），则还应执行以下操作：

- 设置 importance 属性。
- 启用 poold 服务。有关说明，请参见《在 Oracle Solaris 11.2 中进行资源管理 》中的“如何使用 svcadm 启用动态资源池服务”。

importance 如果使用 CPU 范围来获取动态行为，还要设置 importance 属性。importance 属性是可选的属性，用来定义池的相对重要性。仅当为 ncpus 指定了范围并且使用由 poold 管理的动态资源池时，才需要此属性。如果 poold 未运行，则会忽略 importance。如果 poold 正在运行并且未设置 importance，那么 importance 将缺省设置为 1。有关更多信息，请参见《在 Oracle Solaris 11.2 中进行资源管理 》中的“pool.importance 属性约束”。

以下属性用于设置 cpus、cores 和 sockets 的持久性 dedicated-cpu 资源。

cpus 将特定 CPU 永久分配给某区域。

cores	将特定核心永久分配给某区域。
sockets	永久分配特定数目的插槽。

注 - capped-cpu 资源与 dedicated-cpu 资源不兼容。cpu-shares rctl 与 dedicated-cpu 资源不兼容。

注 - 针对可用 CPU 数量自动调整大小和自动缩放的应用程序可能无法识别 capped-cpu 限制。将所有 CPU 视为可用可能会对 Oracle 数据库和 Java 虚拟机 (Java virtual machine, JVM) 等应用程序中的缩放和性能产生不利影响。可能会出现应用程序不工作或不可使用的情况。如果性能至关重要，则不应将 JVM 与 capped-cpu 一起使用。受影响类别的应用程序可以使用 dedicated-cpu 资源。

仅限 solaris-kz：virtual-cpu 资源

使用 virtual-cpu 资源可设置内核区域 CPU 的数目。专用于内核区域的主机 CPU 由 ncpus 值定义。缺省内核区域配置具有 1 个 CPU。您可以通过增加 virtual-cpu 属性将更多 CPU 添加到内核区域。

请注意，如果已定义 dedicated-cpu 资源，则虚拟平台中配置的缺省虚拟 CPU 数目与 dedicated-cpu 资源中 ncpus 范围的下限值匹配。没有必要同时设置 dedicated-cpu 和 virtual-cpu 资源。

capped-cpu 资源

capped-cpu 资源对某一项目或区域可占用的 CPU 资源量设立绝对的细粒度限制。在与处理器集结合使用时，CPU 上限将限制某一处理器集内的 CPU 使用。capped-cpu 资源有一个 ncpus 属性，该属性是一个正小数，小数点右侧有两位。该属性与 CPU 的单位相对应。此资源不接受范围值，但接受小数。指定 ncpus 时，值为 1 表示某个 CPU 的 100%。值为 1.25 表示 125%，因为 100% 对应于系统中的一个 CPU。

注 - capped-cpu 资源与 dedicated-cpu 资源不兼容。

注 - 针对可用 CPU 数量自动调整大小和自动缩放的应用程序可能无法识别 capped-cpu 限制。将所有 CPU 视为可用可能会对 Oracle 数据库和 Java 虚拟机 (Java virtual machine, JVM) 等应用程序中的缩放和性能产生不利影响。可能会出现应用程序不工作或不可使用的情况。如果性能至关重要，则不应将 JVM 与 capped-cpu 一起使用。受影响类别的应用程序可以使用 dedicated-cpu 资源。请参见“dedicated-cpu 资源” [30]。

调度类

可以使用公平份额调度器 (fair share scheduler, FSS)，根据区域的重要性控制可用 CPU 资源在区域之间的分配。这种重要性通过您为每个区域指定的 CPU 资源份额来表示。即使您没有使用 FSS 来管理区域之间的 CPU 资源分配，您也可以将区域的调度类设置为使用 FSS，以便您可为区域中的项目设置份额。

在显式设置 `cpu-shares` 属性时，公平份额调度器 (fair share scheduler, FSS) 将用作该区域的调度类。但是，在此情况下使用 FSS 的首选方法是通过 `dispadmin` 命令将 FSS 设置为系统缺省的调度类。这样，所有区域都将从获取系统 CPU 资源的公平份额中受益。如果未为区域设置 `cpu-shares`，区域将使用系统缺省的调度类。以下操作可为区域设置调度类：

- 可以使用 `zonecfg` 中的 `scheduling-class` 属性为区域设置调度类。
- 可以通过资源池功能为区域设置调度类。如果区域与 `pool.scheduler` 属性设置为有效调度类的池相关联，则缺省情况下区域中运行的进程会以该调度类运行。请参见《在 Oracle Solaris 11.2 中进行资源管理 》中的"资源池介绍"和《在 Oracle Solaris 11.2 中进行资源管理 》中的"如何将池与调度类关联"。
- 如果设置了 `cpu-shares` rctl，但未通过其他操作将 FSS 设置为区域的调度类，则 `zoneadmd` 将在区域引导时将调度类设置为 FSS。
- 如果未通过其他任何操作设置调度类，区域将继承系统的缺省调度类。

请注意，您可以使用 `priocntl(1)` 手册页中所述的 `priocntl`，在不更改缺省调度类和不重新引导的情况下将正在运行的进程移至其他调度类。

物理内存控制和 `capped-memory` 资源

`capped-memory` 资源可为 `physical`、`swap` 和 `locked` 内存设置限制。每个限制均是可选的，但至少要设置一个限制。要使用 `capped-memory` 资源，必须在全局区域中安装 `resource-cap` 软件包。另请参见"`capped-cpu` 资源" [31]。

- 如果计划在全局区域中使用 `rcapd` 为区域设置内存上限，请确定此资源的值。`rcapd` 将 `capped-memory` 资源的 `physical` 属性用作区域的 `max-rss` 值。
- `capped-memory` 资源的 `swap` 属性是用于设置 `zone.max-swap` 资源控制的首选方法。
- `capped-memory` 资源的 `locked` 属性是用于设置 `zone.max-locked-memory` 资源控制的首选方法。

注 - 应用程序通常不会锁定大量内存，但是如果已知道区域的应用程序会锁定内存，则您可能会决定设置锁定内存。如果区域信任是一个需要关注的问题，还可以考虑将锁定内存上限设为系统物理内存的百分之十，或区域物理内存上限的百分之十。

有关更多信息，请参见《在 Oracle Solaris 11.2 中进行资源管理 》中的第 10 章 "关于使用资源上限设置守护进程控制物理内存"、《在 Oracle Solaris 11.2 中进行资源管

理 》中的第 11 章 "管理资源上限设置守护进程的任务"和《创建和使用 Oracle Solaris 区域 》中的"如何配置区域"。要临时设置区域的资源上限，请参见《在 Oracle Solaris 11.2 中进行资源管理 》中的"如何为区域指定临时资源上限"。

仅限 solaris 和 solaris10：rootzpool 资源

`zonecfg` 实用程序中的可选 `rootzpool` 资源用于为 `solaris` 和 `solaris10` 标记区域的区域安装创建专用 zpool。区域的根 zpool 可以位于由一个或多个统一资源标识符 (Universal Resource Identifier, URI) 定义的共享存储设备上。必需的 `storage` 属性标识包含区域的根 `zfs` 文件系统的存储对象 URI。对于一个给定区域，只能定义一个 `rootzpool`。引导区域时将自动为区域配置存储。

在执行区域安装或附加操作期间，将自动创建或导入相应的 zpool。对于 rootzpool 和 zpool 资源，一旦安装了区域，就可以自动创建 zpool 镜像。有关更多信息，请参见《创建和使用 Oracle Solaris 区域 》中的第 14 章 "共享存储上的 Oracle Solaris 区域入门"。

卸载或分离区域时，将执行以下操作：

- 自动导出或销毁相应的 zpool。
- 自动取消配置存储资源。

要在区域安装中重用预先创建的 zpool，必须从系统中导出该 zpool。

区域框架支持以下 URI 类型：

- `dev`

  本地设备路径 URI

  格式：

  `dev:`*local-path-under-*`/dev`

  `dev://`*absolute-path-with-dev*

  `dev:`*absolute-path-with-dev*

  示例：

  ```
  dev:dsk/c7t0d0s0
  dev:///dev/dsk/c7t0d0s0
  dev:/dev/dsk/c7t0d0s0
  dev:chassis/SYS/HD1/disk
  ```
- `lu`（逻辑单元）

  光纤通道 (Fibre Channel, FC) 和串行连接 SCSI (Serial Attached SCSI, SAS)

  格式：

  `lu:luname.naa.`*ID*

```
lu:luname.eui.ID
lu:initiator.naa.ID,target.naa.ID,luname.naa.ID
lu:initiator.naa.ID,target.naa.ID,luname.eui.ID
```

示例：

```
lu:luname.naa.5000c5000288fa25
lu:luname.eui.0021280001cf80f6
lu:initiator.naa.2100001d38089fb0,target.naa.2100001d38089fb0,luname.naa.5000c5000288fa25
lu:initiator.naa.2100001d38089fb0,target.naa.2100001d38089fb0,luname.eui.0021280001cf80f6
```

- `iscsi`

  iSCSI URI

  格式：

```
iscsi:///luname.naa.ID
iscsi:///luname.eui.ID
iscsi://host[:port]/luname.naa.ID
iscsi://host[:port]/luname.eui.ID
iscsi:///target.IQN,lun.LUN
iscsi://host[:port]/target.IQN,lun.LUN
```

  示例：

```
iscsi:///luname.eui.0021280001cf80f6
iscsi:///luname.naa.600144f03d70c80000004ea57da10001
iscsi://[::1]/luname.naa.600144f03d70c80000004ea57da10001
iscsi://127.0.0.1/luname.naa.600144f03d70c80000004ea57da10001
iscsi://hostname:1234/luname.eui.0021280001cf80f6
iscsi://hostname:3260/luname.naa.600144f03d70c80000004ea57da10001

iscsi://127.0.0.1/target.iqn.com.sun:02:d0f2d311-f703,lun.0
iscsi:///target.iqn.com.sun:02:d0f2d311-f703,lun.6
iscsi://[::1]:1234/target.iqn.com.sun:02:d0f2d311-f703,lun.2
iscsi://hostname:1234/target.iqn.com.sun:4db41b76-e3d7-cd2f-bf2d-9abef784d76c,lun.0
```

`suriadm` 工具用于根据存储 URI 管理共享目标文件。有关 ID、名称地址机构 (Name Address Authority, NAA) 和获取现有存储对象 URI 的信息，请参见 suriadm(1M) 和 suri(5) 手册页。

系统将根据与 rootzpool 关联的区域为新建或导入的 `rootzpool` 命名。指定的名称采用 *zonename*`_rpool` 形式。

可使用以下命令在 `rootzpool` 资源范围内管理 `storage` 属性：

- `add storage` *URI string*
- `remove storage` *URI string*

自动添加 **zpool** 资源

通过在 zonecfg 实用程序中配置可选的 zpool 资源，可以将 zpool 委托给非全局区域。引导区域时将自动为区域配置 zpool。

在执行区域安装或附加操作期间，将自动创建或导入相应的 zpool。

卸载或分离区域时，将执行以下操作：

- 自动导出或销毁相应的 zpool。
- 自动取消配置存储资源。

必需的 storage 属性标识与该资源关联的存储对象 URI。

可使用以下设置在 zpool 资源范围内管理 storage 属性：

- add storage *URI string*
- remove storage *URI string*

name 属性是 zpool 资源的必需属性。该属性用在委托给区域的 zpool 的名称中。ZFS 文件系统的 name 组件不能包含正斜杠 (/).

新建或导入的 zpool 的指定名称是 name 属性的值。该名称是在非全局区域内可见的 zpool 名称。在全局区域中显示时，新建或导入的 zpool 的指定名称采用 *zonename_name* 形式。

注 - 存储对象包含预先存在的分区、zpool 或 UFS 文件系统时，区域安装会失败。有关更多信息，请参见《创建和使用 Oracle Solaris 区域 》中的"如何安装已配置的区域"中的步骤 4。

区域网络接口

引导区域时，将在其中自动设置并放置通过 zonecfg 实用程序配置的用于提供网络连接的区域网络接口。

Internet 协议 (Internet Protocol, IP) 层可接受和传送网络包。该层包括 IP 路由、地址解析协议 (Address Resolution Protocol, ARP)、Internet 协议安全体系结构 (Internet Protocol Security Architecture, IPsec) 和 IP 过滤器。

可用于非全局区域的 IP 类型有两种：共享 IP 和专用 IP。专用 IP 是缺省 IP 类型。共享 IP 区域与全局区域共享网络接口。要使用共享 IP 区域，必须通过 ipadm 实用程序完成全局区域中的配置。专用 IP 区域必须有专用的网络接口。如果使用 anet 资源配置专用 IP 区域，将自动创建一个专用 VNIC 并将其分配给该区域。通过使用自动的 anet 资源，不必在全局区域中创建和配置数据链路并将数据链路指定给非全局区域。使用 anet 资源可完成以下任务：

- 允许全局区域管理员为指定给非全局区域的数据链路选择特定名称
- 允许多个区域使用同名的数据链路

为了实现向后兼容性，可以向非全局区域指定预配置的数据链路。

有关每种类型的 IP 功能的信息，请参见《创建和使用 Oracle Solaris 区域 》中的"专用 IP 非全局区域中的联网"和《创建和使用 Oracle Solaris 区域 》中的"共享 IP 非全局区域中的联网"。

注 - 《在 Oracle Solaris 11.2 中确保网络安全 》中所述的链路保护可在运行区域的系统上使用。此功能在全局区域中配置。

关于数据链路

数据链路是 OSI 协议栈的第 2 层物理接口，在系统中表示为 STREAMS DLPI (v2) 接口。此类接口可以在 TCP/IP 等协议栈下检测到。数据链路也称为物理接口，例如，网络接口卡 (Network Interface Card, NIC)。数据链路是使用 `zonecfg`(1M) 配置的 `physical` 属性。`physical` 属性可以为 VNIC。

在 Oracle Solaris 11 中，缺省情况下，物理网络设备名称使用通用名称（如 `net0`），而不是设备驱动程序名称（如 `nxge0`）。

有关为 `solaris` 区域使用基于 InfiniBand 的 IP (IP over InfiniBand, IPoIB) 的信息，请参见"资源类型属性" [53]中的 `anet` 说明。

关于弹性虚拟交换机和区域

对于连接至弹性虚拟交换机 (Elastic Virtual Switch, EVS) 的设置了 `evs` 和 `vport` 属性的 `anet` 资源，该 `anet` 资源的属性封装在 `evs` 和 `vport` 对中。您不能更改 EVS `anet` 资源的以下任何属性：

- `mac-address`
- `mtu`
- `maxbw`
- `priority`
- `allowed-address`
- `vlan-id`
- `defrouter`
- `lower-link`

您只可以为 EVS `anet` 资源设置以下属性：

- linkname
- evs
- vport
- configure-allowed-address

您还必须设置 tenant 资源。Tenant 用于名称空间管理。tenant 内定义的 EVS 资源在该租户的命名空间外不可见。

名为 *evszone* 的区域的以下输入会为名为 *tenantA* 的租户设置 tenant 资源。zonecfg anet 资源属性为具有 anet 资源（连接至名为 *evsa* 的 EVS 和名为 *vport0* 的 VPort）的区域创建 VNIC：

```
zonecfg:evszone> set tenant=tenantA

zonecfg:evszone> add anet

zonecfg:evszone> set evs=EVSA

zonecfg:evszone> set vport=vport0
```

有关更多信息，请参见《在 Oracle Solaris 11.2 中管理网络虚拟化和网络资源 》中的第 5 章 "关于弹性虚拟交换机"。

共享 IP 非全局区域

共享 IP 区域使用全局区域中的现有 IP 接口。区域必须有一个或多个专用 IP 地址。共享 IP 区域与全局区域共享 IP 层配置和状态。如果以下两个条件同时成立，则区域应该使用共享 IP 实例：

- 非全局区域使用全局区域使用的相同数据链路，而不管全局区域和非全局区域是否在同一子网中。
- 您不想使用专用 IP 区域提供的其他功能。

使用 zonecfg 命令的 net 资源为共享 IP 区域指定一个或多个 IP 地址。数据链路名称也必须在全局区域中配置。

在 zonecfg net 资源中，必须设置 address 和 physical 属性。defrouter 属性为可选的。

要在全局区域中使用共享 IP 类型联网配置，必须使用 ipadm，而不是自动网络配置。要确定 ipadm 是否正在进行联网配置，请运行以下命令。显示的响应必须为 DefaultFixed。

```
# svcprop -p netcfg/active_ncp svc:/network/physical:default
DefaultFixed
```

指定给共享 IP 区域的 IP 地址与逻辑网络接口相关联。

可以在全局区域中使用 ipadm 命令来在运行的区域中指定或删除逻辑接口。

要添加接口，请使用以下命令：

```
global# ipadm set-addrprop -p zone=my-zone net0/addr1
```

要删除接口，请使用以下命令之一：

```
global# ipadm set-addrprop -p zone=global net0/addr
```

或者：

```
global# ipadm reset-addrprop -p zone net0/addr1
```

有关更多信息，请参见《创建和使用 Oracle Solaris 区域 》中的"共享 IP 网络接口"。

专用 IP 非全局区域

专用 IP 是非全局区域的缺省联网配置。

专用 IP 区域具有其自己的 IP 相关状态以及一个或多个专用数据链路。

可以在专用 IP 区域中使用以下功能：

- DHCPv4 和 IPv6 无状态地址自动配置
- IP 过滤器，包括网络地址转换 (network address translation, NAT) 功能
- IP 网络多路径 (IP Network Multipathing, IPMP)
- IP 路由
- ipadm，用于设置 TCP/UDP/SCTP 和 IP/ARP 级别可调参数
- IP 安全 (IP security, IPsec) 和 Internet 密钥交换 (Internet Key Exchange, IKE)，可自动提供用于 IPsec 安全关联的验证加密材料

有两种配置专用 IP 区域的方式：

- 使用 zonecfg 实用程序的 anet 资源在引导区域时自动为区域创建临时 VNIC，然后在区域停止时删除它。
- 在全局区域中预先配置数据链路，然后使用 zonecfg 实用程序的 net 资源将其指定给专用 IP 区域。数据链路使用 net 资源的 physical 属性指定。physical 属性可以为 VNIC。没有设置 net 资源的 address 属性。

缺省情况下，专用 IP 区域可以在关联接口上配置和使用任何 IP 地址。（可选）可以使用 allowed-address 属性指定逗号分隔的 IP 地址列表。专用 IP 区域不能使用 allowed-address 列表中没有的 IP 地址。此外，将在引导区域时自动为专用 IP 区域永久配置 allowed-address 列表中的所有地址。如果不需要此接口配置，则必须将configure-allowed-address 属性设置为 false。缺省值为 true。

注意，通过指定的数据链路，可使用 snoop 命令。

可以将 dladm 命令与 show-linkprop 子命令一起使用，以显示正在运行的专用 IP 区域的数据链路分配。可以将 dladm 命令与 set-linkprop 子命令一起使用，以将其他数据链路指定给正在运行的区域。有关用法示例，请参见《创建和使用 Oracle Solaris 区域 》中的"在独占 IP 非全局区域中管理数据链路"。

在已指定自己的数据链路集的正在运行的专用 IP 区域中，可以使用 ipadm 命令来配置 IP，包括添加或删除逻辑接口的能力。通过使用 sysconfig(1M) 手册页中所述的 sysconfig 接口，可以按全局区域的设置方式对区域中的 IP 配置进行设置。

专用 IP 区域的 IP 配置仅可在全局区域中使用 zlogin 命令进行查看。

```
global# zlogin zone1 ipadm show-addr
ADDROBJ           TYPE     STATE        ADDR
lo0/v4            static   ok           127.0.0.1/8
nge0/v4           dhcp     ok           10.134.62.47/24
lo0/v6            static   ok           ::1/128
nge0/_a           addrconf ok           fe80::2e0:81ff:fe5d:c630/10
```

非全局区域对可靠数据报套接字的支持

专用 IP 和共享 IP 非全局区域都支持可靠数据报套接字 (Reliable Datagram Socket, RDS) IPC 协议。RDSv3 驱动程序作为 SMF 服务 rds 启用。缺省情况下，安装后禁用此服务。通过区域管理员授予的相应授权，可以在给定非全局区域中启用该服务。在执行 zlogin 后，可以在要运行 rds 的每个区域中启用 rds。

例 2-1 如何在非全局区域中启用 rds 服务

1. 要在专用 IP 或共享 IP 区域中启用 RDSv3 服务，请执行 zlogin 并执行 svcadm enable 命令：

```
# svcadm enable rds
```

2. 验证 rds 是否已启用：

```
# svcs rds
    STATE          STIME    FMRI
    online         22:50:53 svc:/system/rds:default
```

有关更多信息，请参见 svcadm(1M) 手册页。

共享 IP 非全局区域和专用 IP 非全局区域之间的安全差异

在共享 IP 区域中，此区域中的应用程序（包括超级用户）不能发送带有源 IP 地址的包，只能发送通过 zonecfg 实用程序指定给该区域的包。此类型的区域不能发送和接收任意数据链路（第 2 层）包。

但是，对于专用 IP 区域，zonecfg 会将指定数据链路的一切权限都授予该区域。因此，在专用 IP 区域中，超级用户或具有所需权限配置文件的用户可以如同在全局区域中一样，在这些数据链路上发送欺骗性包。可以通过设置 allowed-address 属性来禁用 IP 地址欺骗。对于 anet 资源，可以通过设置 link-protection 属性来启用其他保护（例如，mac-nospoof 和 dhcp-nospoof）。

同时使用共享 IP 和专用 IP 非全局区域

共享 IP 区域总是与全局区域共享 IP 层，而专用 IP 区域总是有其自己的 IP 层实例。共享 IP 区域和专用 IP 区域都可在同一计算机中使用。

在区域中挂载的文件系统

缺省情况下，每个区域都有一个委托给该区域的 ZFS 数据集。这一缺省委托数据集模拟缺省全局区域的数据集布局。名为 .../rpool/ROOT 的数据集包含引导环境。不应直接处理该数据集。rpool 数据集必须存在，缺省情况下挂载在 .../rpool 下。.../rpool/export 和 .../rpool/export/home 数据集挂载在 /export 和 /export/home 下。这些非全局区域数据集与对应的全局区域数据集具有相同的用途，并可以按相同的方式进行管理。区域管理员可以在 .../rpool、.../rpool/export 和 .../rpool/export/home 数据集中创建附加数据集。

不应使用 zfs(1M) 手册页中所述的 zfs 命令创建、删除或重命名以区域的 rpool/ROOT 文件系统开始的分层结构中的文件系统。zfs 命令可用于设置 canmount、mountpoint、sharesmb、zoned、com.oracle.*:*、com.sun:* 和 org.opensolaris.*.*. 以外的属性。

通常，在区域中挂载的文件系统包括：

- 初始化虚拟平台时挂载的文件系统集合
- 在应用程序环境本身中挂载的文件系统集合

例如，这些集合可以包括以下文件系统：

- 具有 mountpoint（none 或 legacy 除外）且 canmount 属性值为 yes 的 ZFS 文件系统。
- 在区域的 /etc/vfstab 文件中指定的文件系统。
- AutoFS 挂载和 AutoFS 触发的挂载。可通过使用 sharectl(1M) 中介绍的 sharectl 设置 autofs 属性。
- 区域管理员明确执行的挂载

  正在运行的区域内的文件系统挂载权限也可通过 zonecfg fs-allowed 属性进行定义。此属性不适用于通过使用 zonecfg add fs 或 add dataset 资源挂载到区域中的文件系统。缺省情况下，区域内只允许挂载区域的缺省委托数据集中的文件系统、hsfs 文件系统和网络文件系统（如 NFS）。

注意 - 将对在应用程序环境中执行的非缺省挂载设定特定限制。这些限制可防止区域管理员拒绝为系统的其余部分提供服务，或者对其他区域产生不良影响。

在区域中挂载特定的文件系统时存在安全限制。其他文件系统在区域中挂载时会显示出特殊行为。有关更多信息，请参见《创建和使用 Oracle Solaris 区域 》中的“文件系统和非全局区域”。

有关数据集的更多信息，请参见 datasets(5) 手册页。有关 BE 的更多信息，请参见《创建和管理 Oracle Solaris 11.2 引导环境 》。

文件系统挂载和更新

不支持会隐藏区域系统映像中的任何文件、符号链接或目录的文件系统挂载方式，如 pkg(5) 手册页中所述。例如，如果安装的软件包都没有在 `/usr/local` 中提供内容，则允许在 `/usr/local` 下挂载文件系统。但是，如果有任何软件包（包括传统 SVR4 软件包）在以 `/usr/local` 开头的路径下提供了文件、目录或符号链接，则不支持在 `/usr/local` 下挂载文件系统。支持在 `/mnt` 下临时挂载文件系统。

由于文件系统在区域中的挂载顺序，如果 `/export` 来自区域的 `rpool/export` 数据集或其他委托数据集，则不能用 `fs` 资源在 `/export/filesys` 下挂载文件系统。

区域中的主机 ID

您可以为非全局区域设置 `hostid` 属性，该属性与全局区域的 `hostid` 属性不同。例如，如果机器迁移到其他系统上的区域，将执行此操作。区域内的现有应用程序可能取决于原始 `hostid`。有关更多信息，请参见“资源类型和属性” [49]。

非全局区域中的 `/dev` 文件系统

`zonecfg` 命令使用与规则匹配的系统来指定应在特定区域中出现的设备。与其中一个规则匹配的设备包括在区域的 `/dev` 文件系统中。有关更多信息，请参见《创建和使用 Oracle Solaris 区域 》中的“如何配置区域”。

非全局区域中的可删除 `lofi` 设备

可在非全局区域中配置可移除的回送文件 `lofi` 设备，其工作方式与 CD-ROM 设备类似。可以更改设备映射到的文件并创建以只读模式使用相同文件的多个 `lofi` 设备。该类

型的 lofi 设备是使用带 -r 选项的 lofiadm 命令创建的。创建时不一定要指定文件名。在可移除 lofi 设备的生命周期内，可以将文件与空设备关联，或取消文件与非空设备的关联。一个文件可以同时与多个可移除 lofi 设备安全关联。可移除 lofi 设备是只读的。不能对已经映射到普通的读写 lofi 设备或可移除 lofi 设备的文件进行重新映射。潜在 lofi 设备的数量受 zone.max-lofi 资源控制的限制，可以在全局区域中使用 zonecfg(1M) 设置该资源控制。

可移除 lofi 设备在创建后是只读的。如果对可移除 lofi 设备执行任何写操作，lofi 驱动程序将返回错误。

lofiadm 命令还可用于列出可移除 lofi 设备。

例 2-2 创建带关联文件的可移除 lofi 设备

```
# lofiadm -r /path/to/file
/dev/lofi/1
```

例 2-3 创建一个空的可移除 lofi 设备

```
# lofiadm -r
/dev/lofi/2
```

例 2-4 将文件插入可移除 lofi 设备

```
# lofiadm -r /path/to/file /dev/lofi/1
/dev/lofi/1
```

有关更多信息，请参见 lofiadm(1M)、zonecfg(1M) 和 lofi(7D) 手册页。另请参见表 2-2 “区域范围的资源控制”。

非全局区域中的磁盘格式支持

可通过 zonecfg 工具启用磁盘分区和使用 uscsi 命令。有关示例，请参见Resource Type Properties中的 “资源类型属性” [53]。有关 uscsi 命令的更多信息，请参见 uscsi(7I)。

- 仅 solaris 区域支持委托。
- 磁盘必须使用通过使用带 -D 选项的 prtconf 命令显示的 sd 目标。请参见 prtconf(1M)。

具有存储 URI 的内核区域设备资源

以下支持可用：

- solaris-kz 支持设备资源中的 bootpri 和 id 属性。
  - 仅对将成为区域根池组成部分的磁盘设置 bootpri。如果对不会成为区域根池组成部分的磁盘设置 bootpri，可能会损坏该磁盘上的数据。
  - id 控制内核区域中磁盘的实例，例如 id=5 表示磁盘将是区域中的 c1d5。
- 在可引导 solaris-kz 磁盘上创建的根 zpool 可在安装过程中导入全局区域中。此时，可通过 zpool 命令显示该根 zpool。有关更多信息，请参见 zpool(1M)。

可配置的特权

引导区域时，配置中包括安全特权的缺省集合。这些特权被视为安全特权，因为它们可以阻止区域中的特权进程影响系统中其他非全局区域或全局区域中的进程。您可使用 zonecfg 命令执行以下操作：

- 将特权添加至缺省特权集，需要了解此类更改可能允许一个区域中的进程通过控制全局资源来影响其他区域中的进程。
- 从缺省特权集中删除特权，需要了解此类更改可能会阻止某些进程正常运行（如果这些进程要求具有特定特权才能运行的话）。

注 - 目前，有些特权不能从区域的缺省特权集中删除，还有一些特权不能添加到缺省特权集中。

有关更多信息，请参见《创建和使用 Oracle Solaris 区域 》中的"非全局区域中的特权"、《创建和使用 Oracle Solaris 区域 》中的"如何配置区域"和 privileges(5)。

资源池关联

如果按《在 Oracle Solaris 11.2 中进行资源管理 》中的第 13 章 "创建和管理资源池的任务"中所述在系统中配置了资源池，则可在配置区域时使用 pool 属性将该区域与其中一个资源池相关联。

您可以使用 dedicated-cpu 资源来指定在某个非全局区域运行时将系统处理器的某个子集专用于该非全局区域。您可以使用 dedicated-cpu 属性将 CPU、核心和插槽分配给区域。系统会动态创建一个临时池，以便在区域运行时使用。根据 zonecfg 的指定，池配置将在迁移期间进行传播。如果要配置 Oracle Solaris 内核区域，另请参见 virtual-cpu 资源。

pool 属性可用于配置共享同一个池的多个区域。

注 - 使用通过 pool 属性设置的永久池的区域配置与通过 dedicated-cpu 资源配置的临时池不兼容。只能设置这两个属性中的其中一个。

设置区域范围的资源控制

全局管理员或具有相应授权的用户可以为区域设置区域范围的特权资源控制。区域范围的资源控制可限制区域内所有进程实体总的资源使用情况。

使用 zonecfg 命令同时为全局区域和非全局区域指定这些限制。请参见《创建和使用 Oracle Solaris 区域 》中的“如何配置区域”。

设置区域范围的资源控制的首选简单方法是使用属性名称或资源（如 capped-cpu），而不使用 rctl 资源（如 cpu-cap）。

zone.cpu-cap 资源控制可以对某个区域可占用的 CPU 资源量设置绝对限制。值 100 表示将一个 CPU 的 100% 用作设置。值 125 表示 125%，因为在使用 CPU 上限时，100% 对应于系统中的一个 CPU。

注 - 设置 capped-cpu 资源时，可以使用小数来表示单位。该值对应于 zone.cpu-cap 资源控制，但设置减小 100 倍。设置为 1 等效于资源控制设置 100。

---

zone.cpu-shares 资源控制可以对区域的公平份额调度器 (fair share scheduler, FSS) CPU 份额数设置限制。CPU 份额首先分配给区域，然后在区域内的项目之间进一步分配，如 project.cpu-shares 项中所述。有关更多信息，请参见《创建和使用 Oracle Solaris 区域 》中的“在安装了区域的 Oracle Solaris 系统上使用公平份额调度器”。此控制的全局属性名称是 cpu-shares。

zone.max-locked-memory 资源控制可以限制某个区域可以使用的锁定物理内存量。可以使用 project.max-locked-memory 资源控制来控制如何在区域中的项目间分配锁定内存资源。有关更多信息，请参见《在 Oracle Solaris 11.2 中进行资源管理 》中的“可用的资源控制”。

zone.max-lofi 资源控制可以限制某个区域可以创建的潜在 lofi 设备的数量。

zone.max-lwps 资源控制通过禁止一个区域中有过多 LWP 影响其他区域，来增强资源隔离功能。对此区域中项目的 LWP 资源的分配可使用 project.max-lwps 资源控制进行控制。有关更多信息，请参见《在 Oracle Solaris 11.2 中进行资源管理 》中的“可用的资源控制”。此控制的全局属性名称是 max-lwps。

zone.max-processes 资源控制通过防止某个区域使用太多的进程表槽并给其他区域造成影响，来增强资源隔离。可以使用《在 Oracle Solaris 11.2 中进行资源管理 》中的“可用的资源控制”中所述的 project.max-processes 资源控制来设置区域内各项目间的进程表槽资源分配。此控制的全局属性名称是 max-processes。zone.max-processes 资源控制还包括 zone.max-lwps 资源控制。如果设置了 zone.max-processes，但未设置 zone.max-lwps，则在引导区域时 zone.max-lwps 将被隐式设置为 zone.max-processes 值的 10 倍。注意，由于常规进程和僵进程都使用进程表槽，因此 max-processes 控制可以防止僵进程用尽进程表。由于僵进程没有定义任何 LWP，因此 max-lwps 无法防止这种可能性。

zone.max-msg-ids、zone.max-sem-ids、zone.max-shm-ids 和 zone.max-shm-memory 资源控制可用于限制区域中的所有进程使用的 System V 资源。对区域中项目的 System V 资源的分配可使用这些资源控制的项目版本来进行控制。这些控制的全局属性名称是 max-msg-ids、max-sem-ids、max-shm-ids 和 max-shm-memory。

zone.max-swap 资源控制可限制区域中的用户进程地址空间映射和 tmpfs 挂载所占用的交换空间。prstat -Z 的输出将显示一个 SWAP 列。报告的交换是区域进程和 tmpfs 挂载所使用的总交换量。此值有助于监视每个区域预留的交换空间，可用于选择适当的 zone.max-swap 设置。

表 2-2　区域范围的资源控制

控制名称	全局属性名称	说明	缺省单位	所用值
zone.cpu-cap		此区域可用的 CPU 资源量的绝对限制	数量（CPU 数目），以百分比表示注 - 设置 capped-cpu 资源时，可以使用小数来表示单位。	
zone.cpu-shares	cpu-shares	此区域的公平份额调度器 (fair share scheduler, FSS) CPU 份额数	数量（份额）	
zone.max-locked-memory		区域可用的锁定物理内存的总量 如果将 priv_proc_lock_memory 指定给某个区域，请考虑同时设置此资源控制，以防止该区域锁定所有内存。	大小（字节）	capped-memory 的 locked 属性
zone.max-lofi	max-lofi	可由区域创建的潜在 lofi 设备的数量限制	数量（lofi 设备的数量）	
zone.max-lwps	max-lwps	此区域可同时使用的最大 LWP 数	数量 (LWP)	
zone.max-msg-ids	max-msg-ids	此区域允许的最大消息队列 ID 数	数量（消息队列 ID）	
zone.max-processes	max-processes	此区域可同时使用的最大进程表槽数	数量（进程表槽数）	
zone.max-sem-ids	max-sem-ids	此区域允许的最大信号量 ID 数	数量（信号量 ID）	
zone.max-shm-ids	max-shm-ids	此区域允许的最大共享内存 ID 数	数量（共享内存 ID）	
zone.max-shm-memory	max-shm-memory	此区域允许的系统 V 共享内存总量	大小（字节）	

控制名称	全局属性名称	说明	缺省单位	所用值
zone.max-swap		可用于此区域的用户进程地址空间映射和 tmpfs 挂载的交换空间总量	大小（字节）	capped-memory 的 swap 属性

可以使用 prctl 命令为正运行的进程指定这些限制。《创建和使用 Oracle Solaris 区域 》中的"如何使用 prctl 命令在全局区域中设置 FSS 份额"中提供了一个示例。通过 prctl 命令指定的限制不是持久的。在重新引导系统后，此限制将失效。

包含区域注释

您可以使用 attr 资源类型为区域添加注释。有关更多信息，请参见《创建和使用 Oracle Solaris 区域 》中的"如何配置区域"。

使用 zonecfg 命令

zonecfg 命令（在 zonecfg(1M) 手册页中介绍）用于配置非全局区域。

也可以使用 zonecfg 命令永久指定全局区域的资源管理设置。例如，可以使用此命令将全局区域配置为通过使用 dedicated-cpu 资源来使用专用 CPU。

zonecfg 命令可以在交互模式、命令行模式或命令文件模式下使用。可以使用此命令执行以下操作：

- 创建或删除（销毁）区域配置
- 将资源添加到特定配置
- 为添加到配置的资源设置属性
- 从特定配置中删除资源
- 查询或检验配置
- 提交到配置
- 恢复到先前配置
- 重命名区域
- 从 zonecfg 会话中退出

zonecfg 提示符的格式如下：

zonecfg:*zonename*>

当您配置特定的资源类型（例如文件系统）时，此资源类型也包含在提示符中：

zonecfg:*zonename*:fs>

有关更多信息（包括说明如何使用本章中所述的 zonecfg 各组成部分的过程），请参见《创建和使用 Oracle Solaris 区域 》中的第 1 章 "如何规划和配置非全局区域"。

zonecfg 模式

范围的概念用于用户界面。范围可以是全局的，也可以是资源特定的。缺省范围为全局。

在全局范围内，add 子命令和 select 子命令用于选择特定资源。然后范围更改为此资源类型。

- 对于 add 子命令，end 或 cancel 子命令用于完成资源指定。
- 对于 select 子命令，end 或 cancel 子命令用于完成资源修改。

然后范围恢复为全局。

某些子命令（例如 add、remove 和 set）在每个范围中都有不同的语义。

zonecfg 交互模式

在交互模式中，支持以下子命令。有关用于这些子命令的语义和选项的详细信息，请参见 zonecfg(1M) 手册页。对于可能会导致破坏性操作或所做工作丢失的任何子命令，系统均要求用户在继续之前进行确认。您可以使用 -F（强制）选项，跳过此项确认操作。

help
列显一般帮助，或者显示有关给定资源的帮助。

```
zonecfg:my-zone:capped-cpu> help
```

create
开始为指定的新区域配置内存中的配置，以实现以下用途之一：

- 将 Oracle Solaris 缺省设置应用于新的配置。此方法为缺省方法。
- 与 -t *template* 选项一起使用时，用于创建与指定模板相同的配置。区域名称从模板名称更改为新区域名称。
- 与 -F 选项一起使用时，用于覆盖现有配置。
- 与 -b 选项一起使用时，用于创建其中未设置任何内容的空配置。

export
采用可以在命令文件中使用的格式，在标准输出或指定输出文件中列显配置。

add
在全局范围中，将指定的资源类型添加到配置。

在资源范围中，添加具有给定名称和给定值的属性。

有关更多信息，请参见《创建和使用 Oracle Solaris 区域 》中的"如何配置区域"和 zonecfg(1M) 手册页。

`set`
: 将给定属性名称设置为给定属性值。请注意，某些属性（例如 zonepath）为全局属性，而其他属性则为资源特定的属性。因此，此命令适用于全局范围和资源范围。

`select`
: 仅适用于全局范围。选择与给定属性名称-属性值对的修改条件相匹配的给定类型资源。将范围更改为此资源类型。您必须为要唯一标识的资源指定足够数量的属性名称-值对。

`clear`
: 清除可选的设置的值。不能清除必需设置。但可以通过指定新值来更改某些必需设置。对属性使用 clear 命令会将该属性的值重置为缺省值。

`remove`
: 在全局范围中，删除指定的资源类型。您必须为要唯一标识的资源类型指定足够数量的属性名称-值对。如果没有指定属性名称-值对，则会删除所有实例。当存在多个属性名称-值对时，如果未使用 -F 选项，则需要进行确认。

在资源范围中，从当前资源中删除指定的属性名称-属性值。

`end`
: 仅适用于资源范围。结束资源指定。

然后，zonecfg 命令将检验是否完全指定当前资源。

- 如果资源完全指定，则可以将其添加到内存中的配置，并且范围将恢复为全局。
- 如果未完全指定，则系统将显示一条描述需要执行何种操作的错误消息。

`cancel`
: 仅适用于资源范围。结束资源指定并将范围重置为全局。系统不会保留任何未完全指定的资源。

`delete`
: 销毁指定的配置。从内存和稳定存储器中删除配置。您必须将 -F（强制）选项与 delete 一起使用。

注意 - 此操作为即时操作。不需要提交，并且无法恢复已删除的区域。

`info`
: 显示有关当前配置或全局资源属性 zonepath、autoboot 和 pool 的信息。如果指定了资源类型，则仅显示有关此类型资源的信息。在资源范围中，此子命令仅应用于要添加或修改的资源。

`verify`
: 检验当前配置是否正确。确保所有资源都指定了所有必需的属性。检验任何 rootzpool 资源组及其属性的语法。不会检验任何用 URI 指定的存储的可访问性。

`commit` 将当前配置从内存提交到稳定存储器。在提交内存中的配置之前，可以使用 `revert` 子命令删除更改。必须提交配置以供 `zoneadm` 使用。完成 `zonecfg` 会话时，便会自动尝试此操作。由于仅可提交正确的配置，因此，提交操作将自动进行检验。

`revert` 将配置恢复到上次提交时的状态。

`exit` 退出 `zonecfg` 会话。您可以将 `-F`（强制）选项与 `exit` 一起使用。

如果需要，会自动尝试 `commit`。请注意，也可以使用 EOF 字符退出会话。

zonecfg 命令文件模式

在命令文件模式中，输入来自文件。可以使用zonecfg Interactive Mode中所述的“zonecfg 交互模式” [47] 子命令生成此文件。可以在标准输出中列显配置，也可以使用 `-f` 选项指定输出文件。

区域配置数据

区域配置数据由两种类型的实体组成：资源和属性。每个资源都有一种类型，并且每个资源还可以有一个包含一个或多个属性的集合。属性具有名称和值。属性集取决于资源类型。

唯一必需的属性是 `zonename` 和 `zonepath`。

资源类型和属性

资源和属性类型如下所述：

`zonename` 区域的名称。以下规则适用于区域名称：

- 每个区域必须具有唯一的名称。
- 区域名称区分大小写。
- 区域名称必须以字母数字字符开头。

  名称可以包含字母数字字符、下划线 (_)、连字符 (-) 和句点 (.)。
- 名称不能超过 63 个字符。
- 名称 `global` 预留给全局区域。

- 以 SYS 开头的名称将预留，无法使用。

zonepath

zonepath 属性指定将在其下安装区域的路径。每个区域都具有一个与全局区域根目录相对的根目录路径。安装时，需要全局区域目录以提供限定的可见性。区域路径必须由 root 拥有，并且模式为 700。如果区域路径不存在，将在安装期间自动创建该路径。如果权限不正确，将自动进行更正。

非全局区域的根路径低一个级别。区域的根目录与全局区域中的根目录 (/) 具有相同的所有权和权限。区域目录必须由 root 所有，并且模式为 755。此分层结构可防止全局区域中的非特权用户遍历非全局区域的文件系统。

区域必须位于 ZFS 数据集中。在安装或附加区域时，将自动创建 ZFS 数据集。如果无法创建 ZFS 数据集，也无法安装或附加区域。

路径	说明
/zones/my-zone	zonecfg zonepath
/zones/my-zone/root	区域的根目录

有关更多信息，请参见《创建和使用 Oracle Solaris 区域 》中的“遍历文件系统”。

在 zonecfg template 属性中，zonepath 的缺省值为 /system/zones/*zonename*。

注 - 通过使用 zoneadm 的 move 子命令指定一个完整的新 zonepath，可将区域移至同一系统上的其他位置。有关说明，请参见《创建和使用 Oracle Solaris 区域 》中的“移动非全局区域”。

---

autoboot

如果此属性设置为 true，则引导全局区域时会自动引导该区域。缺省设置为 false。请注意，如果禁用了区域服务 svc:/system/zones:default，则无论如何设置此属性，区域都不会自动引导。您可以使用 svcadm(1M) 手册页中所述的 svcadm 命令来启用区域服务：

```
global# svcadm enable zones
```

有关 pkg 更新过程中此设置的信息，请参见《创建和使用 Oracle Solaris 区域 》中的“区域包管理概述”。

bootargs

此属性用于为区域设置引导参数。除非被 reboot、zoneadm boot 或 zoneadm reboot 命令覆盖，否则将应用该引导参数。请参见“区域引导参数”。

limitpriv

此属性用于指定缺省特权集之外的特权掩码。请参见《创建和使用 Oracle Solaris 区域 》中的“非全局区域中的特权”。

通过指定特权名称可添加特权，特权名称中可包含或不包含前导 priv_。在特权名称前添加破折号 (-) 或感叹号 (!) 可以排除特权。特权值以逗号分隔，并放在引号 (") 内。

如 priv_str_to_set(3C) 中所述，特殊特权集 none、all 和 basic 对其标准定义进行了扩展。由于区域配置在全局区域内进行，因此不能使用特殊特权集 zone。由于常见用法是通过添加或删除某些特权来更改缺省特权集，因此特殊特权集 default 将映射为缺省特权集。当 default 出现在 limitpriv 属性开头时，它将扩展为缺省权限集。

以下条目增加了使用 DTrace 程序的功能，该程序只要求区域中具有 dtrace_proc 和 dtrace_user 特权：

```
global# zonecfg -z userzone
zonecfg:userzone> set limitpriv="default,dtrace_proc,dtrace_user"
```

如果区域的特权集包含不允许的特权、缺少必需特权或包含未知特权，则检验、准备或引导该区域的尝试都将失败，并将显示错误消息。

scheduling-class

此属性可为区域设置调度类。有关其他信息和提示，请参见“调度类” [32]。

ip-type

必须为所有非全局区域设置该属性。请参见“专用 IP 非全局区域” [38]、“共享 IP 非全局区域” [37]和《创建和使用 Oracle Solaris 区域 》中的“如何配置区域”。

dedicated-cpu

此资源可让系统处理器子集专供某个区域在运行时使用。dedicated-cpu 资源可为 ncpus 以及（可选）importance、ncores、cores 和 sockets 提供限制。有关更多信息，请参见“dedicated-cpu 资源” [30]。

仅限 solaris-kz：virtual-cpu

此 solaris-kz 资源可让系统处理器子集专供某个区域在运行时使用。virtual-cpu 资源可为 ncpus 提供限制。有关更多信息，请参见“仅限 solaris-kz：virtual-cpu 资源” [31]。

capped-cpu

此资源对区域在运行时可占用的 CPU 资源量设置限制。capped-cpu 资源可为 ncpus 提供限制。有关更多信息，请参见“capped-cpu 资源” [31]。

capped-memory

此资源可对为区域设置内存上限时使用的属性分组。capped-memory 资源可为 physical、swap 和 locked 内存提供限制。至少必须指定其中一个属性。要使用 capped-memory 资源，必须在全局区域中安装 service/resource-cap 软件包。

`anet`	`anet` 资源会在区域引导时自动为专用 IP 区域创建临时 VNIC 接口，并在区域停止时删除该接口。
`net`	net 资源可将全局区域中的现有网络接口指定给非全局区域。网络接口资源是接口名称。当区域从已安装状态转换为就绪状态时，每个区域都可以具有可以设置的网络接口。
`dataset`	数据集是描述文件系统、卷或快照的通用术语。添加 ZFS™ 数据集资源可以将存储管理委托给非全局区域。如果委托数据集为文件系统，区域管理员可在该数据集内创建和销毁文件系统以及修改数据集的属性。区域管理员可创建快照、子文件系统和卷以及其后代的克隆。如果委托数据集为卷，则区域管理员可设置属性和创建快照。区域管理员无法影响尚未添加到区域的数据集，也无法超过对指定给区域的数据集设置的任何顶层配额。将数据集委托给非全局区域后，将自动设置 `zoned` 属性。`zoned` 文件系统不能挂载在全局区域中，因为区域管理员可能需要将挂载点设置为不可接受的值。 可以按以下方式将 ZFS 数据集添加到区域中。 ■ 作为一个 `lofs` 挂载文件系统（在目标单独与全局区域共享空间时） ■ 作为一个委托数据集 使用 `zonecfg` `template` 属性时，如果未指定 `rootzpool` 资源，则缺省区域路径数据集为 *rootpool*`/VARSHARE/zones/`*zonename*。该数据集通过具有挂载点 `/system/zones` 的 `svc-zones` 服务创建。其余的属性将会从 *rootpool*`/VARSHARE/zones/` 继承。 请参见《在 Oracle Solaris 11.2 中管理 ZFS 文件系统 》中的第 9 章 “Oracle Solaris ZFS 高级主题”、《创建和使用 Oracle Solaris 区域 》中的“文件系统和非全局区域”和 `datasets`(5) 手册页。 另请参见《创建和使用 Oracle Solaris 区域 》中的第 13 章 “各种 Oracle Solaris 区域问题的故障排除”，了解有关数据集问题的信息。
`fs`	当区域从已安装状态转换为就绪状态时，每个区域都可以拥有已挂载的各种文件系统。文件系统资源指定文件系统挂载点的路径。有关在区域中使用文件系统的更多信息，请参见《创建和使用 Oracle Solaris 区域 》中的“文件系统和非全局区域”。

注 - 要在非全局区域中通过 `fs` 资源使用 UFS 文件系统，必须在安装后或通过 AI 清单脚本将 `system/file-system/ufs` 软件包安装到区域中。

不能使用 `quota`(1M) 中所述的 `quota` 命令来检索通过 `fs` 资源添加的 UFS 文件系统的配额信息。

`fs-allowed` 设置该属性后，区域管理员便能够挂载该类型的任何文件系统（不论是区域管理员创建的文件系统，还是使用 NFS 导入的文件系统），并可以管理该文件系统。正在运行的区域内的文件系统挂载权限也受 `fs-allowed` 属性限制。缺省情况下，区域内仅允许挂载 `hsfs` 文件系统和网络文件系统（如 NFS）。

该属性还可用于块设备或委托给区域的 ZVOL 设备。

`fs-allowed` 属性接受可以在区域中挂载的其他文件系统的逗号分隔列表，例如，`ufs,pcfs`。

```
zonecfg:my-zone> set fs-allowed=ufs,pcfs
```

该属性不会影响全局区域通过 `add fs` 或 `add dataset` 属性管理的区域挂载。

有关安全注意事项，请参见《创建和使用 Oracle Solaris 区域 》中的“文件系统和非全局区域”和《创建和使用 Oracle Solaris 区域 》中的“非全局区域中的设备使用”。

`device` `zonefigdevice` 资源用于将虚拟磁盘添加到非全局区域的平台。设备资源是与设备匹配的说明符。当区域从已安装状态转换为就绪状态时，每个区域都具有应配置的设备。

注 - 要在非全局区域中通过 `device` 资源使用 UFS 文件系统，必须在安装后或通过 AI 清单脚本本将 `system/file-system/ufs` 软件包安装到区域中。

`pool` 此属性用于将区域与系统中的资源池相关联。多个区域可以共享一个池的资源。另请参见“`dedicated-cpu` 资源” [30]。

`rctl` `rctl` 资源用于区域范围的资源控制。当区域从已安装状态转换为就绪状态时，将启用这些控制。

有关更多信息，请参见“设置区域范围的资源控制” [44]。

注 - 要使用 `zonefig` 的 *set* `global_property_name` 子命令而非 `rctl` 资源来配置区域范围的控制，请参见《创建和使用 Oracle Solaris 区域 》中的“如何配置区域”。

`attr` 此通用属性可用于用户注释或其他子系统。`attr` 的 `name` 属性必须以字母数字字符开头。`name` 属性可以包含字母数字字符、连字符 (-) 和句点 (.)。以 `zone.` 开头的属性名称将保留，以供系统使用。

资源类型属性

资源也有要配置的属性。以下属性与所示的资源类型关联。

`admin` 针对给定区域定义该用户的用户名和授权。

```
zonecfg:my-zone> add admin
zonecfg:my-zone:admin> set user=zadmin
zonecfg:my-zone:admin> set auths=login,manage
zonecfg:my-zone:admin> end
```

auths 属性可以采用以下值：

- login (solaris.zone.login)
- manage (solaris.zone.manage)
- clone (solaris.zone.clonefrom)

请注意，不能通过这些 auths 创建区域。该功能包含在区域安全性配置文件中。

仅限 solaris 和 solaris10：rootzpool

storage

标识为区域安装提供专用 ZFS zpool 的存储对象 URI。有关 URI 和 storage 允许值的信息，请参见"仅限 solaris 和 solaris10：rootzpool 资源" [33]。在区域安装期间，将自动创建 zpool，或导入预先创建的 zpool。指定 *my-zone*_rpool 名称。

```
zonecfg:my-zone> add rootzpool
zonecfg:my-zone:rootzpool> add storage dev:dsk/c4t1d0
zonecfg:my-zone:rootzpool> end
```

如果要创建镜像配置，可以添加其他 storage 属性：

```
add storage dev:dsk/c4t1d0
add storage dev:dsk/c4t3d0
```

一个区域只能配置一个 rootzpool 资源。

仅限 solaris 和 solaris10：zpool

storage、name

定义将 zpool 委托给区域的一个或多个存储对象 URI。有关 URI 和 storage 属性允许值的信息，请参见"仅限 solaris 和 solaris10：rootzpool 资源" [33]。zpool(1M) 手册页中定义了 name 属性的允许值。

在此示例中，将一个 zpool 存储资源委托给区域。在安装期间，将自动创建 zpool，或导入以前创建的 zpool。zpool 的名称为 my-zone_pool1。

```
zonecfg:my-zone> add zpool
zonecfg:my-zone:zpool> set name=pool1
zonecfg:my-zone:zpool> add storage dev:dsk/c4t2d0
zonecfg:my-zone:zpool> add storage dev:dsk/c4t4d0
zonecfg:my-zone:zpool> end
```

一个区域可以配置有一个或多个 zpool 资源。

dedicated-cpu

ncpus、importance、cores、cpus、sockets

指定 CPU 个数以及（可选）池的相对重要性。以下示例指定了供区域 my-zone 使用的 CPU 范围，还设置了 importance。

```
zonecfg:my-zone> add dedicated-cpu
zonecfg:my-zone:dedicated-cpu> set ncpus=1-3
zonecfg:my-zone:dedicated-cpu> set importance=2
zonecfg:my-zone:dedicated-cpu> end
```

将核心 0、1、2 和 3 永久分配给区域 my-zone。以下 dedicated-cpu 示例使用了 *cores*，但 cpus=、cores= 和 sockets= 均可使用。

```
zonecfg:my-zone> add dedicated-cpu
zonecfg:my-zone:dedicated-cpu> set cores=0-3
zonecfg:my-zone:dedicated-cpu> end
```

virtual-cpu

ncpus

指定 CPU 数目。以下示例为区域 my-zone 指定了 3 个 CPU。

```
zonecfg:my-zone> add virtual-cpu
zonecfg:my-zone:dedicated-cpu> set ncpus=3
zonecfg:my-zone:dedicated-cpu> end
```

capped-cpu

ncpus

指定 CPU 数目。以下示例指定了供区域 my-zone 使用的 CPU 的 CPU 上限为 3.5 个。

```
zonecfg:my-zone> add capped-cpu
zonecfg:my-zone:capped-cpu> set ncpus=3.5
zonecfg:my-zone:capped-cpu> end
```

capped-memory

physical、swap、locked

为区域 my-zone 指定内存限制。每个限制均是可选的，但至少要设置一个限制。

```
zonecfg:my-zone> add capped-memory
zonecfg:my-zone:capped-memory> set physical=50m
zonecfg:my-zone:capped-memory> set swap=100m
zonecfg:my-zone:capped-memory> set locked=30m
zonecfg:my-zone:capped-memory> end
```

要使用 capped-memory 资源，必须在全局区域中安装 resource-cap 软件包。

fs

dir、special、raw、type、options

fs 资源参数提供的值可确定如何以及在何处挂载文件系统。fs 参数定义如下：

`dir`	为文件系统指定挂载点
`special`	指定要从全局区域挂载的特殊块设备名称或目录
`raw`	指定在挂载文件系统之前运行 `fsck` 所在的原始设备（不适用于 ZFS）
`type`	指定文件系统类型
`options`	指定挂载选项，这些选项类似于使用 `mount` 命令找到的挂载选项

以下示例中的行指定全局区域中名为 `pool1/fs1` 的数据集在所配置的区域中被挂载为 `/shared/fs1`。所使用的文件系统类型为 ZFS。

```
zonecfg:my-zone> add fs
zonecfg:my-zone:fs> set dir=/shared/fs1
zonecfg:my-zone:fs> set special=pool1/fs1
zonecfg:my-zone:fs> set type=zfs
zonecfg:my-zone:fs> end
```

有关参数的更多信息，请参见《创建和使用 Oracle Solaris 区域 》中的"o nosuid 选项"、《创建和使用 Oracle Solaris 区域 》中的"安全限制和文件系统行为"，以及 `fsck`(1M) 和 `mount`(1M) 手册页。另请注意，有关专用于特定文件系统的挂载选项的信息可以在 1M 手册页部分中找到。这些手册页的名称格式为 `mount_`*filesystem*。

注 - 不能使用 `quota`(1M) 中所述的 `quota` 命令来检索通过该资源添加的 UFS 文件系统的配额信息。

`dataset` `name`, `alias`

name

以下示例的几行代码指定数据集 *sales* 将在非全局区域中可见并在该区域中进行挂载，但在全局区域中不再可见。

```
zonecfg:my-zone> add dataset
zonecfg:my-zone> set name=tank/sales
zonecfg:my-zone> end
```

委托数据集可以具有一个下例中所示的非缺省别名。请注意，数据集别名不能含有正斜杠 (/)。

```
zonecfg:my-zone> add dataset
zonecfg:my-zone:dataset> set name=tank/sales
zonecfg:my-zone:dataset> set alias=data
zonecfg:my-zone:dataset> end
```

要恢复缺省别名，请使用 clear alias。

```
zonecfg:my-zone> clear alias
```

anet

linkname、lower-link、allowed-address、auto-mac-address、configure-allowed-address、defrouter、linkmode (IPoIB)、mac-address（非 IPoIB）、mac-slot（非 IPoIB）、mac-prefix（非 IPoIB）、mtu、maxbw、pkey (IPoIB)、priority、vlan-id（非 IPoIB）、rxfanout、rxrings、txrings、link-protection、allowed-dhcp-cids

仅限 solaris：请勿在 zonecfg 中为 IPoIB 数据链路设置以下 anet 属性。

- mac-address
- mac-prefix
- mac-slot
- vlan-id

请勿在 zonecfg 中为非 IPoIB 数据链路设置以下 anet 属性。

- linkmode
- pkey

仅为 EVS anet 资源设置以下属性：

- linkname
- evs
- vport
- configure-allowed-address

anet 资源在区域引导时创建自动 VNIC 接口或 IPoIB 接口，在区域停止时删除 VNIC 或 IPoIB 接口。请注意，solaris-kz 标记不支持 IPoIB。资源属性通过 zonecfg 命令进行管理。有关可用属性的完整信息，请参见 zonecfg(1M) 手册页。

lower-link

为要创建的链路指定底层链路。如果设置为 auto，每次区域引导时，zoneadmd 守护进程都会自动选择用来创建 VNIC 的链路。您可以将可在其上创建 VNIC 的任何链路指定为 anet 资源的 lower-link。

选择了自动创建 VNIC 的数据链路时，引导期间将跳过所有 IPoIB 链路。

linkname

为自动创建的 VNIC 或 IPoIB 接口指定一个名称。请注意，solaris-kz 不支持 IPoIB。

mac-address（不适用于 IPoIB）	根据指定值或关键字设置 VNIC 的 MAC 地址。如果该值不是关键字，则将其解释为单点传送 MAC 地址。有关支持的关键字，请参见 zonecfg(1M) 手册页。如果选择随机 MAC 地址，则区域引导、区域分离和附加操作将保留生成的地址。使用缺省策略 auto-mac-address 时，Oracle Solaris Zones 可获取随机的 mac-address。
pkey（仅限 IPoIB）	设置用于创建 IPoIB 数据链路接口的分区密钥。此属性为强制属性。指定的 pkey 始终作为十六进制数处理，无论其是否有 0x 前缀。
linkmode（仅限 IPoIB）	设置数据链路接口的 linkmode。缺省值为 cm。有效值包括： cm（缺省值）：连接模式。此模式使用缺省 MTU（65520 字节），其支持的最大 MTU 为 65535 字节。 ud：不可靠的数据报模式。如果远程节点无法使用连接模式，则会自动改用不可靠的数据报模式。此模式使用缺省 MTU（2044 字节），其支持的最大 MTU 为 4092 字节。
allowed-address	为专用 IP 区域配置 IP 地址，同时限制专用 IP 区域可以使用的可配置 IP 地址集。要指定多个地址，请使用逗号分隔的 IP 地址列表。
defrouter	当非全局区域和全局区域驻留在单独的网络上时，可使用 defrouter 属性来设置缺省路由。 设置了 defrouter 属性的任何区域必须位于没有为全局区域配置的子网上。

zonecfg 命令使用 SYSdefault 模板创建区域时，如果没有设置其他 IP 资源，将在区域配置中自动包括具有以下属性的 anet 资源。将在物理以太网链路上自动创建 linkname，该名称将设置为第一个可用名称，形式为 net*N*, net*0*。要更改这些缺省值，请使用 zonecfg 命令。

使用缺省策略 auto 时，将会分配相应的 mac-address：

Oracle Solaris 区域	随机 mac-address
Oracle Solaris 内核区域	随机 mac-address
内核区域下的 Oracle Solaris 区域	出厂 mac-address
Oracle VM Server for SPARC 来宾域	出厂 mac-address
Oracle VM Server for SPARC 来宾域上运行的 Oracle Solaris 内核区域	出厂 mac-address

缺省策略通过物理以太网链路（如 net0）创建自动 VNIC，并向 VNIC 分配 MAC 地址。可选的 lower-link 属性设置为要创建的自动 VNIC 的底层链路 (vnic1)。可以使用 zonecfg 命令指定链路名称、底层物理链路、MAC 地址、带宽限制等 VNIC 属性以及其他 VNIC 属性。请注意，还必须指定 ip-type=exclusive。

```
zonecfg:my-zone> set ip-type=exclusive
zonecfg:my-zone> add anet
zonecfg:my-zone:anet> set linkname=net0
zonecfg:my-zone:anet> set lower-link=auto
zonecfg:my-zone:anet> set mac-address=random
zonecfg:my-zone:anet> set link-protection=mac-nospoof
zonecfg:my-zone:anet> end
```

以下示例显示了在物理链路 net5 上配置了 IPoIB 数据链路接口（使用 IB 分区密钥 0xffff）的 solaris 标记区域：

```
zonecfg:my-zone> set ip-type=exclusive
zonecfg:my-zone:anet> add anet
zonecfg:my-zone:anet> set linkname=ib0
zonecfg:my-zone:anet> set lower-link=net5
zonecfg:my-zone:anet> set pkey=0xffff
zonecfg:my-zone:anet> end
```

有关属性的更多信息，请参见 zonecfg(1M) 手册页。有关链路属性的更多信息，请参见 dladm(1M) 手册页。

net	address、allowed-address、physical、defrouter

注 - 对于共享 IP 区域，必须指定 IP 地址和物理设备这两项。或者设置缺省路由器。

对于专用 IP 区域，只需指定物理接口。

- allowed-address 属性可以限制专用 IP 区域可以使用的可配置 IP 地址集。
- 当非全局区域和全局区域驻留在单独的网络上时，可使用 defrouter 属性来设置缺省路由。
- 设置了 defrouter 属性的任何区域必须位于没有为全局区域配置的子网上。
- 来自具有缺省路由器的区域的通信将在回到目标区域之前先进入路由器中。

当共享 IP 区域位于不同的子网上时，请不要在全局区域中配置数据链路。

在以下共享 IP 区域示例中，物理接口 nge0 被添加到 IP 地址为 192.168.0.1 的区域中。要列出系统上的网络接口，请键入：

```
global# ipadm show-if -po ifname,class,active,persistent
lo0:loopback:yes:46--
nge0:ip:yes:----
```

除回送行以外的每一行输出将包含一个网络接口的名称。说明中包含 loopback 的行不适用于卡。46 持久性标志表示该接口已在全局区域中永久配置。yes 活动值表示当前已配置接口，ip 类值表示 nge0 是一个非回送接口。区域的缺省路由设置为 10.0.0.1。defrouter 属性的设置为可选的。请注意，ip-type=shared 为必需项。

```
zonecfg:my-zone> set ip-type=shared
zonecfg:my-zone> add net
zonecfg:my-zone:net> set physical=vnic1
zonecfg:my-zone:net> set address=192.168.0.1
zonecfg:my-zone:net> set defrouter=10.0.0.1
zonecfg:my-zone:net> end
```

在以下专用 IP 区域示例中，将 VNIC 用于物理接口，该接口是 VLAN。要确定哪些数据链路可用，请使用命令 dladm show-link。allowed-address 属性可对区域可以使用的 IP 地址加以限制。defrouter 属性用于设置缺省路由。请注意，还必须指定 ip-type=exclusive。

```
zonecfg:my-zone> set ip-type=exclusive
zonecfg:my-zone> add net
zonecfg:myzone:net> set allowed-address=10.1.1.32/24
zonecfg:my-zone:net> set physical=vnic1
zonecfg:myzone:net> set defrouter=10.1.1.1
zonecfg:my-zone:net> end
```

在 add net 步骤中只会指定物理设备类型。physical 属性可以为 VNIC。

注 - Oracle™ Solaris 操作系统支持所有以太网类型的接口，并且可以使用 `dladm` 命令来管理其数据链路。

`device`

`match`、`allow-partition`、`allow-raw-io`

要匹配的设备名称可以是匹配模式或绝对路径。`allow-partition` 和 `allow-raw-io` 都可以设置为 `true` 或 `false`。缺省值是 `false`。`allow-partition` 可启用分区。`allow-raw-io` 可启用 `uscsi`。有关这些资源的更多信息，请参见 zonecfg(1M)。

可在 `solaris-kz` 区域的 `device:match` 资源属性中指定的内容包括以下限制：

- 每个 LUN 仅允许一个资源。
- 不支持分片和分区。
- 仅提供对原始磁盘设备的支持。
- 支持的设备路径为 `lofi`、`ramdisk`、`dsk` 和 `zvols`。

在以下示例中，`solaris` 区域配置中包括对磁盘设备的 `uscsi` 操作。

```
zonecfg:my-zone> add device
zonecfg:my-zone:device> set match=/dev/*dsk/cXtYdZ*
zonecfg:my-zone:device> set allow-raw-io=true
zonecfg:my-zone:device> end
```

使用 `add device` 将 Veritas 卷管理器设备委托给非全局区域。

在以下示例中，向 `solaris-kz` 区域添加了一个存储设备：

```
zonecfg:my-zone> add device
zonecfg:my-zone:device> set storage=iscsi:///
luname.naa.600144f03d70c80000004ea57da10001
zonecfg:my-zone:device> set bootpri=0
zonecfg:my-zone:device> end
```

注意 - 添加设备前，请参见《创建和使用 Oracle Solaris 区域 》中的“非全局区域中的设备使用”、《创建和使用 Oracle Solaris 区域 》中的“在非全局区域中运行应用程序”和《创建和使用 Oracle Solaris 区域 》中的“非全局区域中的特权”了解有关限制和安全注意事项。

`rctl`

`name`、`value`

以下是可用的区域范围的资源控制。

- `zone.cpu-cap`
- `zone.cpu-shares`（首选：`cpu-shares`）
- `zone.max-locked-memory`

- zone.max-lofi
- zone.max-lwps（首选：max-lwps）
- zone.max-msg-ids（首选：max-msg-ids）
- zone.max-processes（首选：max-processes）
- zone.max-sem-ids（首选：max-sem-ids）
- zone.max-shm-ids（首选：max-shm-ids）
- zone.max-shm-memory（首选：max-shm-memory）
- zone.max-swap

请注意，设置区域范围资源控制的首选的、更简单的方法是使用属性名称，而不是使用 rctl 资源，如《创建和使用 Oracle Solaris 区域 》中的"如何配置区域"中所示。如果区域中的区域范围资源控制条目是使用 add rctl 配置的，则其格式与 project 数据库中的资源控制条目不同。在区域配置中，rctl 资源类型由三个名称/值对组成。名称分别是 priv、limit 和 action。每个名称都有一个简单值。

```
zonecfg:my-zone> add rctl
zonecfg:my-zone:rctl> set name=zone.cpu-shares
zonecfg:my-zone:rctl> add value
 (priv=privileged,limit=10,action=none)
zonecfg:my-zone:rctl> end

zonecfg:my-zone> add rctl
zonecfg:my-zone:rctl> set name=zone.max-lwps
zonecfg:my-zone:rctl> add value
 (priv=privileged,limit=100,action=deny)
zonecfg:my-zone:rctl> end
```

有关资源控制和属性的一般信息，请参见《在 Oracle Solaris 11.2 中进行资源管理 》中的第 6 章 "关于资源控制"和《创建和使用 Oracle Solaris 区域 》中的"在非全局区域中使用的资源控制"。

attr

name、type、value

在以下示例中，添加了有关区域的注释。

```
zonecfg:my-zone> add attr
zonecfg:my-zone:attr> set name=comment
zonecfg:my-zone:attr> set type=string
zonecfg:my-zone:attr> set value="Production zone"
zonecfg:my-zone:attr> end
```

可以使用 export 子命令在标准输出中列显区域配置。通过可以在命令文件中使用的格式保存配置。

Tecla 命令行编辑库

配置中提供了 Tecla 命令行编辑库，可与 `zonecfg` 命令一起使用。此库为命令行历史记录和编辑支持提供了一种机制。

有关更多信息，请参见 tecla(5) 手册页。

词汇表

auxiliary zone state（辅助区域状态）
: 用于将其他状态信息传递给全局区域。另请参见 zone state（区域状态）。

brand（标记）
: BrandZ 功能的实例，提供了包含用于运行应用程序的非本机操作环境的非全局区域。

branded zone（标记区域）
: 一种隔离环境，用于在非全局区域中运行非本机应用程序。

cap
: 针对系统资源使用设定的限制。

capping（上限设置）
: 针对系统资源使用设定限制的过程。

CMT resources（CMT 资源）
: CPU、核心和插槽。

CPU
: 在区域环境中，是指硬件线程。

data-link（数据链路）
: OSI 协议栈的第二层接口，在系统中表示为 STREAMS DLPI (v2) 接口。该接口可以在 TCP/IP 等协议栈下检测到。在 Oracle Solaris 10 Zones 环境中，数据链路为物理接口、集合或带 VLAN 标记的接口。数据链路也称为物理接口，例如，涉及 NIC 或 VNIC 时。

default pool（缺省池）
: 启用池时由系统创建的池。

  另请参见 resource pool（资源池）。

default processor set（缺省处理器集）
: 启用池时由系统创建的处理器集。

  另请参见 processor set（处理器集）。

disjoint（不相交）
: 其成员不重叠并且不重复的一类集合。

dynamic configuration（动态配置）
: 某一时刻，给定系统中资源池框架内的资源部署的相关信息。

dynamic reconfiguration（动态重新配置）
: 在基于 SPARC 的系统上，当系统运行时重新配置硬件的功能。也称为 DR。

extended accounting（扩展记帐）
: 在 Solaris 操作系统中，按任务或进程来记录资源占用情况的一种比较灵活的方法。

fair share scheduler（公平份额调度器）	一个调度类，也称为 FSS，可用于分配基于份额的 CPU 时间。份额定义了分配给某个项目的那一部分系统 CPU 资源。
FSS	请参见 fair share scheduler（公平份额调度器）。
global administrator（全局管理员）	root 用户或具有 root 角色的管理员。登录到全局区域后，全局管理员或被授予相应权限的用户可以将系统作为一个整体进行监视和控制。 另请参见 zone administrator（区域管理员）。
global scope（全局范围）	应用于系统上所有资源控制的资源控制值的操作。
global zone（全局区域）	所有 Oracle Solaris 系统上都包含的区域。使用非全局区域时，全局区域既是系统的缺省区域，也是用于系统范围内管理控制的区域。 另请参见 non-global zone（非全局区域）。
heap（堆）	进程分配的临时内存。
local scope（本地范围）	对试图超越控制值的进程采取的本地操作。
locked memory（锁定内存）	不能执行调页操作的内存。
memory cap enforcement threshold（内存上限执行阈值）	系统中的物理内存使用百分比，该值将触发资源上限设置守护进程执行上限。
naming service database（命名服务数据库）	在本文档的"项目和任务（概述）"一章中，指 LDAP 容器和 NIS 映射。
non-global zone administrator（非全局区域管理员）	请参见 zone administrator（区域管理员）。
non-global zone（非全局区域）	在 Oracle Solaris 操作系统的单个实例中创建的虚拟操作系统环境。Oracle Solaris Zones 软件分区技术用于虚拟化操作系统服务。
Oracle Solaris 10 Zones	一种软件分区技术，为在运行 Oracle Solaris 11 发行版的系统上的 `solaris10` 标记区域中执行的 Solaris 10 应用程序提供完整运行时环境。
Oracle Solaris Kernel Zones（Oracle Solaris 内核区域）	一种软件分区技术，在区域内提供完整的内核和用户环境，并且还会加大主机和区域之间的内核分离。
Oracle Solaris Zones	用于虚拟化操作系统服务的软件分区技术，提供运行应用程序的安全隔离环境。
pool daemon（池守护进程）	需要动态分配资源时处于活动状态的 `poold` 系统守护进程。

pool（池）	请参见 resource pool（资源池）。
processor set（处理器集）	不相交的 CPU 分组。每个处理器集都可以包含零个或多个处理器。在资源池配置中，一个处理器集表示为一个资源元素。也称为 pset。 另请参见 disjoint（不相交）。
project（项目）	相关工作在网络范围内的管理标识符。
read-only zone（只读区域）	配置为只读根的不可编辑区域。
resident set size（驻留集大小）	驻留集的大小。驻留集是驻留在物理内存中的一组页面。
resource capping daemon（资源上限设置守护进程）	一种守护进程，用于调节已定义资源上限的项目中运行的进程所占用的物理内存。
resource consumer（资源使用者）	实际上是指 Solaris 进程。利用进程模型实体（例如项目和任务），可以从总资源占用角度讨论资源占用情况。
resource control（资源控制）	对每个进程、任务或项目设置的资源占用限制。
resource management（资源管理）	可用于控制应用程序如何使用可用系统资源的功能。
resource partition（资源分区）	一个专用的资源子集。资源的所有分区加起来表示正在执行的单个 Solaris 实例中的可用资源总量。
resource pool（资源池）	用于对计算机资源进行分区的配置机制。资源池表示各组可分区资源之间的关联。
resource set（资源集）	可绑定到进程的资源。通常指提供某种分区形式的内核子系统构造的对象。资源集的示例包括调度类和处理器集。
resource（资源）	计算系统的一个方面，可对其进行处理以更改应用程序行为。
RSS	请参见 resident set size（驻留集大小）。
scanner（扫描程序）	标识不常用页面的内核线程。在低内存情况下，扫描程序会回收最近未使用的页面。
static pools configuration（静态池配置）	一种管理员希望如何针对资源池功能对系统进行配置的方法。
task（任务）	在资源管理中，表示一段时间内一组工作的进程集。每项任务都与一个项目关联。
whole root zone（完全根区域）	一种非全局区域类型，在此区域中，所有必需的系统软件和任何附加软件包都安装在该区域的专有文件系统中。

working set size（工作集大小） 工作集的大小。工作集是指在处理项目工作负荷过程中实际使用的一组页面。

workload（工作负荷） 一个或一组应用程序的所有进程的集合。

WSS 另请参见 working set size（工作集大小）。

zone administrator（区域管理员） 区域管理员的特权仅限于某个非全局区域。

另请参见 global administrator（全局管理员）。

zone state（区域状态） 非全局区域的状态。区域状态可以是"已配置"、"未完成"、"已安装"、"就绪"、"不可用"、"正在运行"或"正在关闭"中的一种。

索引

S

V

W

Y

Z