

创建和使用 Oracle Solaris 内核区域

ORACLE®

文件号码 E54023-03
2014 年 12 月

版权所有 © 2014, Oracle 和/或其附属公司。保留所有权利。

本软件和相关文档是根据许可证协议提供的，该许可证协议中规定了关于使用和公开本软件和相关文档的各种限制，并受知识产权法的保护。除非在许可证协议中明确许可或适用法律明确授权，否则不得以任何形式、任何方式使用、拷贝、复制、翻译、广播、修改、授权、传播、分发、展示、执行、发布或显示本软件和相关文档的任何部分。除非法律要求实现互操作，否则严禁对本软件进行逆向工程设计、反汇编或反编译。

此文档所含信息可能随时被修改，恕不另行通知，我们不保证该信息没有错误。如果贵方发现任何问题，请书面通知我们。

如果将本软件或相关文档交付给美国政府，或者交付给以美国政府名义获得许可证的任何机构，必须符合以下规定：

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

本软件或硬件是为了在各种信息管理应用领域内的一般使用而开发的。它不应被应用于任何存在危险或潜在危险的应用领域，也不是为此而开发的，其中包括可能会产生人身伤害的应用领域。如果在危险应用领域内使用本软件或硬件，贵方应负责采取所有适当的防范措施，包括备份、冗余和其它确保安全使用本软件或硬件的措施。对于因在危险应用领域内使用本软件或硬件所造成的一切损失或损害，Oracle Corporation 及其附属公司概不负责。

Oracle 和 Java 是 Oracle 和/或其附属公司的注册商标。其他名称可能是各自所有者的商标。

Intel 和 Intel Xeon 是 Intel Corporation 的商标或注册商标。所有 SPARC 商标均是 SPARC International, Inc 的商标或注册商标，并应按照许可证的规定使用。AMD、Opteron、AMD 徽标以及 AMD Opteron 徽标是 Advanced Micro Devices 的商标或注册商标。UNIX 是 The Open Group 的注册商标。

本软件或硬件以及文档可能提供了访问第三方内容、产品和服务的方式或有关这些内容、产品和服务的信息。对于第三方内容、产品和服务，Oracle Corporation 及其附属公司明确表示不承担任何种类的担保，亦不对其承担任何责任。对于因访问或使用第三方内容、产品或服务所造成的任何损失、成本或损害，Oracle Corporation 及其附属公司概不负责。

目录

使用本文档	5
1 规划和配置 Oracle Solaris 内核区域	7
关于 Oracle Solaris 内核区域	7
内核区域和一般的区域概念	8
Oracle Solaris 内核区域的硬件和软件要求	8
检验内核区域主机上的硬件和软件支持	9
调整内核区域主机上的主机 ZFS ARC 高速缓存	10
配置 Oracle Solaris 内核区域	10
▼ 如何配置内核区域	10
配置和定制内核区域资源	12
管理内核区域 CPU	12
管理内核区域内存	13
管理内核区域存储设备和 bootpri 资源属性	14
管理内核区域网络设备和配置	15
2 安装、关闭、克隆和迁移 Oracle Solaris 内核区域	19
安装内核区域	19
直接安装内核区域	19
在内核区域安装中使用 AI 清单和 sysconfig 配置文件	22
从安装介质安装内核区域	24
卸载内核区域	25
关闭、重新引导和停止内核区域	26
克隆内核区域	26
挂起和恢复内核区域	28
使用挂起和恢复迁移内核区域	28
▼ 如何迁移内核区域	29
3 管理 Oracle Solaris 内核区域	31
在内核区域环境中工作	31

区域中的进程 ID 可见性	31
内核区域中的重复进程 ID	32
内核区域的区域路径	32
内核区域中的资源管理功能	32
使用内核区域和不可编辑的区域	32
配置不可编辑的区域	32
▼ 如何将内核区域配置为不可编辑的（只读）区域	32
维护和管理只读内核区域	33
管理内核区域中的可移除设备	33
▼ 如何将虚拟 CD-ROM 设备添加到内核区域	34
使用内核区域辅助状态	36
管理嵌套区域	37
▼ 如何将多个 MAC 地址添加到内核区域	37
嵌套区域和新的非全局区域配置	38
内核区域主机数据和主机 ID	38
使用内核区域引导装载程序	39
▼ 如何指定内核区域中的备用引导环境	40
 索引	 43

使用本文档

- 概述 – 介绍如何规划、配置、安装和管理 Oracle Solaris 内核区域
- 目标读者 – 技术人员、系统管理员和授权服务提供商
- 必备知识 – 具有 Oracle Solaris 环境管理经验。另外，需要具有虚拟化环境经验。

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。

规划和配置 Oracle Solaris 内核区域

本章讨论如何规划和配置 Oracle Solaris 内核区域（也称为 solaris-kz 标记区域）。其中提供了特定于内核区域的检验硬件支持、区域配置和应用区域资源的过程。

本章包含以下规划和配置主题：

- “关于 Oracle Solaris 内核区域” [7]
- “Oracle Solaris 内核区域的硬件和软件要求” [8]
- “配置 Oracle Solaris 内核区域” [10]
- “配置和定制内核区域资源” [12]

关于 Oracle Solaris 内核区域

Oracle Solaris 内核区域也称为 solaris-kz 标记区域，使用标记区域框架运行内核和操作系统 (OS) 安装独立于全局区域的区域。独立的内核和 OS 安装可为操作系统实例和应用程序提供更大的独立性和增强的安全性。

内核区域的管理和结构内容完全独立于全局区域。例如，内核区域不会与全局区域或内核区域主机共享系统封装。内核区域主机上的软件包更新并非链接映像，且不会影响内核区域。同样，封装命令（如 pkg update）可在内核区域中完全正常工作。有关封装命令的其他信息，请参见《在 Oracle Solaris 11.2 中使用映像包管理系统打包和交付软件》中的第 3 章“安装、删除和更新软件包”。

系统进程将在内核区域的独立进程 ID 表中进行处理且不会与全局区域共享。内核区域中的资源管理也有所不同。配置内核区域时，max-processes 等资源控制不可用。

使用现有 zlogin、zonecfg 和 zoneadm 命令管理全局区域中的内核区域。

有关标记区域框架的更多信息，请参见 [brands\(5\)](#) 手册页。

有关内核区域概念的其他概述，请参见《Oracle Solaris Zones 介绍》中的第 1 章“Oracle Solaris Zones 介绍”。



注意 - 如果 Oracle VM VirtualBox 和 Oracle Solaris 内核区域同时在 Oracle Solaris x86 系统上运行，则该系统可能会出现紧急情况。

内核区域和一般的区域概念

本书假设您熟悉以下资源管理和区域概念：

- 资源控制，确定应用程序如何使用可用的系统资源
- 用于配置、安装和管理区域的命令，主要包括 zonecfg、zoneadm 和 zlogin
- zonecfg 资源和属性类型
- 全局区域和非全局区域
- 完全根非全局区域模型
- 通过 zonecfg 实用程序授予的授权
- 全局管理员和区域管理员
- 区域状态模型
- 区域隔离特性
- 网络概念和配置
- 区域共享 IP 和专用 IP 类型

有关这些概念的更多信息，请参见《[Oracle Solaris Zones 介绍](#)》和《[创建和使用 Oracle Solaris 区域](#)》。

Oracle Solaris 内核区域的硬件和软件要求

要使用内核区域，必须在主机操作系统上运行 Oracle Solaris 11.2。

物理主机系统必须具有以下组件：

- SPARC 系统：
 - 至少带有系统固件 8.5.1 的 SPARC T4 系统。
 - 至少带有系统固件 9.2.1 的 SPARC T5、SPARC M5 或 SPARC M6 系统。
 - 至少带有 XCP Firmware 2230 的 Fujitsu M10/SPARC M10 系统。
- 您可以下载最新的系统固件，方法是登录 [My Oracle Support](#)，然后单击 "Patches & Updates" (补丁程序和更新) 链接。使用 "Search" (搜索) 找到适用于您的系统类型的固件下载。
- x86 系统：
 - 基于 Nehalem+ (Intel) 或 Barcelona+ (AMD) 的 x86 计算机，已在 BIOS 中启用 CPU 虚拟化 (例如，VT-x)。具体来说，x86 上的内核区域需要扩展/嵌套页表支持，也称为 EPT、NPT 或 RVI (Rapid Virtualization Indexing, 快速虚拟化索引)。

此外，SPARC 和 x86 系统都需要满足以下条件：

- 物理 RAM 至少为 8 GB

- 内核区域标记软件包 `brand/brand-solaris-kz`。
有关获取和安装软件包的信息，请参见《在 Oracle Solaris 11.2 中使用映像包管理系统打包和交付软件》中的第 3 章“安装、删除和更新软件包”。
- 充分调整主机上的 ZFS 自适应替换高速缓存 (Adaptive Replacement Cache, ARC) 以防止出现内存错误。请参见“调整内核区域主机上的主机 ZFS ARC 高速缓存” [10]。

Oracle Solaris 内核区域可在 Oracle VM Server for SPARC 上的来宾域中运行。每个 Oracle VM Server for SPARC 域对可以运行的内核区域数量的限制是独立的。对于 SPARC T4 或 SPARC T5 系统，此限制为 768，对于 SPARC M5 或 SPARC M6 系统，此限制为 512。

内核区域不能在 Oracle VM Server for x86 来宾域或 Oracle VM VirtualBox 中运行。

检验内核区域主机上的硬件和软件支持

在规划和部署内核区域之前，您必须检验内核区域主机是否满足“Oracle Solaris 内核区域的硬件和软件要求” [8]中所述的硬件和软件要求。您可以使用 `virtinfo` 命令检验内核区域主机上的硬件要求、固件或 BIOS 要求以及内核区域标记软件包软件要求。

▼ 如何检验主机上的内核区域支持

1. 成为内核区域主机的管理员。
有关更多信息，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全》中的“使用所指定的管理权限”。
2. 检验 Oracle Solaris 操作系统版本是否至少为 11.2。

```
# uname -a
```

例如，在主机 `global` 上：

```
global# uname -a
SunOS global 5.11 11.2 sun4v sparc sun4v
```

3. 检验是否已安装内核区域标记软件包 `brand/brand-solaris-kz`。

```
# pkg list brand/brand-solaris-kz
```

以下示例说明在主机 `global` 上安装了内核区域标记软件包。

```
global# pkg list brand/brand-solaris-kz
NAME (PUBLISHER)                VERSION                                IFO
system/zones/brand/brand-solaris-kz 0.5.11-0.175.2.0.0.36.22321         i--
```

4. 运行 `virtinfo` 命令。

```
# virtinfo
```

以下示例输出说明主机 `global` 支持内核区域。

```
global# virtinfo
NAME                CLASS
logical-domain     current
non-global-zone    supported
kernel-zone        supported
```

另请参见 有关详细信息，请参见 [virtinfo\(1M\)](#) 手册页。

调整内核区域主机上的主机 ZFS ARC 高速缓存

要确保高效性能，则必须配置内核区域主机以限制系统 ZFS 自适应替换高速缓存 (Adaptive Replacement Cache, ARC)。规划内核区域配置时，只需在主机上设置此值一次。



注意 - 如果未限制主机 ZFS ARC 高速缓存，则会导致内存不足故障。

要限制主机上的 ZFS ARC 高速缓存，请以管理员身份将 `zfs_arc_max` 值设置为 ZFS ARC 高速缓存值（字节）。建议值是要使用的主机 ZFS 资源的一半。例如，如果希望 ZFS 使用少于 2 GB 的内存，则将 ARC 高速缓存设置为 1 GB 或 `0x40000000`。有关详细信息，请参见《[Oracle Solaris 11.2 可调参数参考手册](#)》中的“ZFS ARC 参数”和《[在 Oracle Solaris 11.2 中管理 ZFS 文件系统](#)》中的第 11 章“建议的 Oracle Solaris ZFS 做法”。

必须重新引导内核区域主机以使更改生效。

配置 Oracle Solaris 内核区域

本节介绍如何配置 Oracle Solaris 内核区域。

▼ 如何配置内核区域

以下过程说明如何使用内核区域模板 `SYSsolaris-kz` 配置内核区域。有关区域模板属性的概述，请参见《[Oracle Solaris Zones 介绍](#)》中的“`zonecfg template` 属性”。有关区域

配置的一般信息，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](#)”。

开始之前 开始配置内核区域之前，您必须确认主机系统上的内核区域硬件支持、软件支持以及内存配置。请参见“[检验内核区域主机上的硬件和软件支持](#)” [9]和“[调整内核区域主机上的主机 ZFS ARC 高速缓存](#)” [10]。

1. 成为管理员。

有关更多信息，请参见《[在 Oracle Solaris 11.2 中确保用户和进程的安全](#)》中的“[使用所指定的管理权限](#)”。

2. 创建新的内核区域配置。

solaris-kz 标记区域模板为 SYSsolaris-kz。例如，在主机 global 上，要为内核区域 kzone1 创建新的内核区域配置：

```
global# zonecfg -z kzone1
Use 'create' to begin configuring a new zone.
zonecfg:kzone1> create -t SYSsolaris-kz
```

此过程中的其余配置步骤使用内核区域 kzone1。

3. 添加任何其他内核区域资源。

您可以现在或在配置区域后设置某些内核区域资源。有关更多信息，请参见“[配置和定制内核区域资源](#)” [12]。

4. 提交区域配置。

```
zonecfg:kzone1> commit
```

5. 退出 zonecfg。

```
zonecfg:kzone1> exit
```

6. (可选) 检验区域配置。

可以在安装区域之前对其进行检验。如果您跳过此步骤，则会在安装区域时自动执行检验。请参见《[创建和使用 Oracle Solaris 区域](#)》中的“[\(可选\) 如何在安装已配置的区域之前检验该区域](#)”。

```
# zoneadm -z zonename verify
```

例如，检验主机 global 上的内核区域 kzone1：

```
global# zoneadm -z kzone1 verify
```

如果显示错误消息并且无法检验区域，请执行消息中指定的更正操作，并再次尝试执行此命令。如果未显示错误消息，则可以安装区域。

配置和定制内核区域资源

区域资源是用于管理计算机、系统和 CPU 资源的机制。规划区域配置时设置资源。请注意，内核区域中的部分资源不同于 solaris 和 solaris10 区域中提供的资源。例如，不支持 solaris-kz 区域中 max-processes、fs-allowed 和 ip-type 资源。

本节介绍如何配置资源以便为以下组件添加其他支持：

- 内核区域 CPU。请参见“[管理内核区域 CPU](#)” [12]。
- 内核区域内存。请参见“[管理内核区域内存](#)” [13]。
- 内核区域存储设备。请参见“[管理内核区域存储设备和 bootpri 资源属性](#)” [14]。
- 内核区域网络设备和网络配置。请参见“[管理内核区域网络设备和配置](#)” [15]。

可在全局区域中使用 zonecfg 命令设置或修改内核区域资源。

注 - 您必须是全局管理员或在全局区域中具有相应授权的用户才能使用 zonecfg 命令。

有关内核区域资源的其他信息，请参见《[Oracle Solaris Zones 介绍](#)》中的“[关于区域中的资源](#)”和 [solaris-kz\(5\)](#) 手册页。

管理内核区域 CPU

缺省情况下，在创建内核区域时将为其指定一个虚拟 CPU。您可以通过添加和修改 virtual-cpu 资源以修改虚拟 CPU 的数量。

使用 dedicated-cpu zonecfg 资源属性将主机 CPU 专用于内核区域。

请注意，如果已定义 dedicated-cpu zonecfg 资源，则虚拟平台中配置的缺省虚拟 CPU 数量与 dedicated-cpu zonecfg 资源内 ncpus 范围的下限值匹配。如果同时存在上述两种资源，则会交叉检查两者是否一致。有关详细信息，请参见 [zonecfg\(1M\)](#) 手册页。

有关如何设置 virtual-cpu 和 dedicated-cpu 区域资源的一般信息，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](#)”。

例 1-1 将其他虚拟 CPU 添加到内核区域

本示例说明如何将其他虚拟 CPU 添加到内核区域 kzone1。

```
global# zonecfg -z kzone1
zonecfg:kzone1> info virtual-cpu
zonecfg:kzone1> add virtual-cpu
zonecfg:kzone1:virtual-cpu> set ncpus=8
zonecfg:kzone1:virtual-cpu> end
```

```
zonecfg:kzone1> info virtual-cpu
virtual-cpu:
    ncpus: 8
zonecfg:kzone1> exit
```

例 1-2 将专用 CPU 添加到内核区域

本示例说明如何将专用 CPU 添加到内核区域 kzone1。

```
global# zonecfg -z kzone1
zonecfg:kzone1> info dedicated-cpu
zonecfg:kzone1> add dedicated-cpu
zonecfg:kzone1:dedicated-cpu> set ncpus=8
zonecfg:kzone1:dedicated-cpu> end
zonecfg:kzone1> info dedicated-cpu
    ncpus: 8
zonecfg:kzone1> exit

zonecfg:kzone1> info dedicated-cpu
dedicated-cpu:
    ncpus: 8
```

管理内核区域内存

您必须将固定数量的物理 RAM 分配给内核区域虚拟平台。您可以通过设置内核区域 capped-memory 资源定义此数量。

指定给内核区域的物理内存存在配置内核区域时已全部分配。分配的内存仅供内核区域专用。例如，引导内核区域后，capped-memory 资源中指定的所有内存将用于主机操作系统。

在 x86 系统上，必须以 2 兆字节 (MB) 为增量设置 capped-memory 资源。

在 SPARC 系统上，必须以 256 兆字节 (MB) 为增量设置 capped-memory 资源。

引导区域后，区域会分配 capped-memory 资源。区域运行时，此数量将保持不变。

有关如何设置 capped-memory 区域资源的一般信息，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”。

如果在安装之前增大内核区域内存大小，则您还必须增加内核区域根磁盘大小以容纳较大的交换和转储设备。如果内核区域没有显式添加的磁盘，则会创建 zvol 并将其用作根磁盘。缺省情况下，zvol 的大小为 16GB。如果需要不同的根磁盘大小，则使用 zoneadm install -x install-size 命令修改磁盘大小。例如，要在内核区域 kzone1 上指定 32GB 根磁盘大小：

```
global# zoneadm -z kzone1 install -x install-size=32G
```

有关设置 capped-memory 区域资源的其他信息，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”。有关使用 zoneadm 命令修改磁盘大小的信息，请参见 [zoneadm\(1M\)](#) 手册页。

例 1-3 在 SPARC 系统上设置 capped-memory 资源

本示例说明如何在 SPARC 系统上设置 capped-memory 资源。

```
global# zonecfg -z kzone1
zonecfg:kzone1> select capped-memory
zonecfg:kzone1:capped-memory> set physical=2048m
zonecfg:kzone1:capped-memory> end
zonecfg:kzone1> exit
```

例 1-4 在 x86 系统上设置 capped-memory 资源

本示例说明如何在 x86 系统上设置 capped-memory 资源。

```
global# zonecfg -z kzone1
global# zonecfg -z kzone1
zonecfg:kzone1> select capped-memory

zonecfg:kzone1:capped-memory> set physical=16g
zonecfg:kzone1:capped-memory> end
zonecfg:kzone1> exit
```

管理内核区域存储设备和 bootpri 资源属性

内核区域根目录始终可供访问。可以使用 add device 资源将其他存储设备添加到内核区域。其他内核区域存储设备需满足以下要求：

- 必须指定完整的存储设备路径（如 /dev/rdisk/c9t0d0）。
- 只能通过以下方式之一定义存储设备：
 - add device match 资源属性如果为 add device match 资源属性指定存储设备，则必须指定存在于 /dev/rdisk、/dev/zvol/rdisk 或 /dev/did/rdisk 中的设备。
 - 有效的存储 URI。
- 存储设备必须是整个磁盘或 LUN。

使用 bootpri 资源属性指定每个存储设备的引导顺序。必须将 bootpri 资源属性设置为任何正整数值。



注意 - 只有在设备将用作引导设备时，才必须设置 bootpri 资源属性。如果在引导设备以外的设备上设置 bootpri 资源属性，则可能会导致数据损坏。

要取消设置 `bootpri` 资源属性，请使用 `clear bootpri` 资源属性。

如果在安装过程中存在多个可引导的设备，则这些设备将用于区域中的镜像 ZFS 池。

每个设备的缺省引导顺序由以下设备排序方式确定：先按 `bootpri` 排序，如果多个设备具有相同的 `bootpri`，再按 `id` 排序。

例 1-5 将其他存储设备添加到内核区域

本示例说明如何将其他存储设备 `/dev/rsk/c9t0d0` 添加到内核区域 `kzone1`。

```
global# zonecfg -z kzone1
zonecfg:kzone1> add device
zonecfg:kzone1:device> set match=/dev/rdisk/c9t0d0
zonecfg:kzone1:device> set bootpri=4
zonecfg:kzone1:device> end
```

例 1-6 更改内核区域缺省引导设备以使用存储 URI：

本示例说明如何更改内核区域 `kzone1` 中的缺省引导设备，以使用位于 `iscsi://zfssa/lunname.naa.600144F0DBF8AF19000052E820D60003` 的存储 URI。

```
global# zonecfg -z kzone1
zonecfg:kzone1> select device id=0
zonecfg:kzone1:device> set storage=iscsi://zfssa/
lunname.naa.600144F0DBF8AF19000053482CC00029
zonecfg:kzone1:device> end
zonecfg:kzone1> info device
device:
  match not specified
  storage: iscsi://zfssa/lunname.naa.600144F0DBF8AF19000052E820D60003
  id: 0
  bootpri: 0
```

管理内核区域网络设备和配置

通过添加 `net` 或 `anet` 资源，内核区域可提供对内核区域的网络访问。有关这两种资源类型的详细信息，请参见《[Oracle Solaris Zones 介绍](#)》中的“[区域网络接口](#)”。

专用 IP 区域必须用于内核区域。有关专用 IP 区域的更多信息，请参见《[创建和使用 Oracle Solaris 区域](#)》中的“[专用 IP 区域网络地址](#)”。

您可以提供其他 MAC 地址，以支持嵌套区域或内核区域托管非全局 `solaris` 和 `solaris10` 标记区域的区域。有关嵌套区域的更多信息，请参见“[管理嵌套区域](#)” [37]。

您可以选择指定网络设备 ID 来在区域内部标识 VNIC 地址和确定网络接口在内核区域中的显示顺序。此过程类似于将 NIC 从一个物理插槽移到另一个物理插槽。

有关如何设置网络区域资源的一般信息，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](#)”。

例 1-7 将其他网络资源添加到内核区域

本示例说明如何将网络资源添加到内核区域 kzone1。将 ID 设置为 3 以确定 anet 接口在内核区域中的显示顺序。

```
global# zonecfg -z kzone1
zonecfg:kzone1> add anet
zonecfg:kzone1:anet> set id=3
global# zonecfg:kzone1:anet> end
zonecfg:kzone1> exit
```

例 1-8 从内核区域中移除网络设备

本示例说明如何从内核区域 kzone1 中移除网络设备。列出有关现有 anet 资源的信息并删除值为 1 的 anet 设备。

```
global# zonecfg -z kzone1 info anet
anet:
  lower-link: auto
  allowed-address not specified
  allowed-dhcp-cids not specified
  link-protection: mac-nospoof
  mac-address: random
  mac-prefix not specified
  mac-slot not specified
  vlan-id not specified
  priority not specified
  rxrings not specified
  txrings not specified
  mtu not specified
  maxbw not specified
  rxfanout not specified
  vsi-typeid not specified
  vsi-vers not specified
  vsi-mgrid not specified
  etsbw-lcl not specified
  cos not specified
  id: 0
anet:
  lower-link: auto
  allowed-address not specified
  allowed-dhcp-cids not specified
  link-protection: mac-nospoof
  mac-address: default
  mac-prefix not specified
```

```
mac-slot not specified
vlan-id not specified
priority not specified
rxrings not specified
txrings not specified
mtu not specified
maxbw not specified
rxfanout not specified
vsi-typeid not specified
vsi-vers not specified
vsi-mgrid not specified
etsbw-lcl not specified
cos not specified
id: 1
global# zoncfg -z kzone1 remove anet id=1
```


安装、关闭、克隆和迁移 Oracle Solaris 内核区域

本章介绍安装内核区域的不同方法并介绍如何停止、关闭、重新启动和克隆内核区域。本章包含以下主题：

- “安装内核区域” [19]
- “卸载内核区域” [25]
- “关闭、重新引导和停止内核区域” [26]
- “克隆内核区域” [26]
- “挂起和恢复内核区域” [28]
- “使用挂起和恢复迁移内核区域” [28]

有关区域安装和区域克隆概念的一般信息，请参见《[Oracle Solaris Zones 介绍](#)》。

安装内核区域

可使用 `zoneadm install` 命令安装内核区域。在安装之前，必须配置所有区域。有关更多信息，请参见《[Oracle Solaris Zones 介绍](#)》中的第 2 章“非全局区域配置概述”。

可以通过以下方法之一安装内核区域：

- 内核区域直接安装。请参见“[直接安装内核区域](#)” [19]。
- 自动化安装 (Automated Installation, AI) 清单或 Oracle Solaris 系统配置 (`sysconfig`) 配置文件。请参见“[在内核区域安装中使用 AI 清单和 `sysconfig` 配置文件](#)” [22]
- Oracle Solaris 介质。请参见“[从安装介质安装内核区域](#)” [24]

直接安装内核区域

直接安装是缺省的内核区域安装方法。在直接安装中，安装程序将在全局区域中运行。缺省情况下，安装程序将创建和格式化内核区域引导磁盘，并使用全局区域的 `pkg` 发布者在该磁盘上安装 Oracle Solaris 软件包。

注 - 在内核区域直接安装中，安装程序只能识别和安装在全局区域中运行的 Oracle Solaris 版本。要安装 Oracle Solaris 版本不同于全局区域的内核区域，则必须使用 AI 介质安装或交互式文本安装。请参见“[从安装介质安装内核区域](#)” [24]。

如果在 `zoneadm install` 操作期间未指定 `-b` 选项，则会进行内核区域直接安装。

▼ 如何直接安装内核区域

1. 成为管理员。

有关更多信息，请参见《[在 Oracle Solaris 11.2 中确保用户和进程的安全](#)》中的“[使用所指定的管理权限](#)”。

2. 安装内核区域。

```
# zoneadm -z zonename install
```

例如，在主机 `global` 上安装内核区域 `kzone1`：

```
global# zoneadm -z kzone1 install
```

注 - 如果在区域验证后直接安装失败，请确认全局区域中的发布者是否具有所有必需的软件包组件。有关更多信息，请参见《[在 Oracle Solaris 11.2 中复制和创建软件包系统信息库](#)》。

3. 引导内核区域。

```
# zoneadm -z zonename boot
```

例如，引导主机 `kzone1` 上的内核区域 `global`：

```
global# zoneadm -z kzone1 boot
```

4. 登录到内核区域控制台以完成区域配置过程。

```
# zlogin -C zonename
```

例如，登录到内核区域 `kzone1` 中的控制台：

```
global# zlogin -C kzone1
```

例 2-1 直接安装内核区域

本示例显示成功对内核区域 `kzone1` 执行了直接安装。

```
global# zoneadm -z kzone1 install
Progress being logged to /var/log/zones/zoneadm.20146T195713Z.kzone1.install
pkg cache: Using /var/pkg/publisher.
Install Log: /system/volatile/install.778521/install_log
```

```

AI Manifest: /tmp/zoneadm777933.spq5FV/devel-ai-manifest.xml
SC Profile: /usr/share/auto_install/sc_profiles/enable_sci.xml
Installation: Starting ...

    Creating IPS image
    Startup: Retrieving catalog 'nightly' ... Done
    Startup: Caching catalogs ... Done
    Startup: Refreshing catalog 'nightly' ... Done
    Startup: Refreshing catalog 'solaris' ... Done
    Startup: Refreshing catalog 'extra' ... Done
    Startup: Caching catalogs ... Done
    Installing packages from:
        solaris
        origin: http://ipkg.us.oracle.com/solaris11/dev/
    Startup: Linked image publisher check ... Startup: Refreshing catalog 'nightly' ...
Done
    Startup: Refreshing catalog 'solaris' ... Done
    Startup: Refreshing catalog 'extra' ... Done
    Planning: Solver setup ... Done
    Planning: Running solver ... Done
    Planning: Finding local manifests ... Done
    Planning: Fetching manifests: 0/477 0% complete
    Planning: Fetching manifests: 477/477 100% complete
    Planning: Package planning ... Done
    Planning: Merging actions ... Done
    Planning: Checking for conflicting actions ... Done
    Planning: Consolidating action changes ... Done
    Planning: Evaluating mediators ... Done
    Planning: Planning completed in 29.49 seconds
    The following licenses have been accepted and not displayed.
    Please review the licenses for the following packages post-install:
        consolidation/osnet/osnet-incorporation
    Package licenses may be viewed using the command:
        pkg info --license <pkg_fmri>

    Download: 0/52325 items 0.0/535.0MB 0% complete
    Download: 1024/52325 items 30.8/535.0MB 5% complete
    Download: 2233/52325 items 42.7/535.0MB 7% complete
    ...
    Download: 46744/52325 items 518.8/535.0MB 96% complete (6.4M/s)
    Download: Completed 534.98 MB in 79.80 seconds (5.0M/s)
    Actions: 1/74042 actions (Installing new actions)
    Actions: 17036/74042 actions (Installing new actions)
    ...
    Actions: 72796/74042 actions (Installing new actions)
    Actions: Completed 74042 actions in 97.96 seconds.
    Done
Installation: Succeeded
    Done: Installation completed in 359.901 seconds.

```

在内核区域安装中使用 AI 清单和 `sysconfig` 配置文件

需要安装具有特定资源和软件包配置（配置不同于全局区域）的多个内核区域时，可使用 AI 清单或 `sysconfig` 配置文件。

使用 `zoneadm install` 命令和 `-m` 选项指定备用 AI 清单：

```
# zoneadm -z zonename install -m manifest
```

使用 `-c` 选项指定 `sysconfig` 配置文件：

```
# zoneadm -z zonename install -c sysconfig-profile
```

例如，使用 AI 清单 `/data/archives/kzone-manifest.xml` 安装内核区域 `kzone1`：

```
global# zoneadm -z kzone1 install -m /data/archives/kzone-manifest.xml
```

安装备用 AI 清单或 `sysconfig` 配置文件到内核区域时，请注意以下准则：

- 为了成功安装，AI 清单和 `sysconfig` 文件必须包含完整路径和 `.xml` 后缀。
- 不能将 AI 清单中的定制 `disk` 引用应用于内核区域安装。由于内核区域根磁盘对全局区域不可用，因此内核区域安装脚本将在配置期间自动指定带标签的回送文件或 `lofi` 设备以便创建根磁盘。有关如何配置 `lofi` 设备的信息，请参见《[Oracle Solaris Zones 介绍](#)》中的“非全局区域中的可删除 `lofi` 设备”。
有关开发和定制 AI 清单的其他信息，请参见《[安装 Oracle Solaris 11.2 系统](#)》中的第 9 章“定制安装”。有关创建区域根磁盘的详细信息，请参见《[创建和使用 Oracle Solaris 区域](#)》中的“区域安装和管理概念”。

例 2-2 使用单独的自动化安装程序 (Automated Installer, AI) 清单安装内核区域

本示例说明如何使用非缺省自动化安装程序 (Automated Installer, AI) 清单 `/var/tmp/kz_manifest.xml` 安装内核区域 `kzone1`。

```
global# zoneadm -z kzone1 install -m /var/tmp/manifest/kz_manifest.xml
Progress being logged to /var/log/zones/zoneadm.20146T195713Z.kzone1.install
pkg cache: Using /var/pkg/publisher.
Install Log: /system/volatile/install.10708/install_log
AI Manifest: /tmp/zoneadm10343.5la4Vu/devel-ai-manifest.xml
SC Profile: /usr/share/auto_install/sc_profiles/enable_sci.xml
Installation: Starting ...

Creating IPS image
Startup: Retrieving catalog 'solaris' ... Done
Startup: Caching catalogs ... Done
Startup: Refreshing catalog 'solaris' ... Done
Installing packages from:
solaris
origin: http://pkg.oracle.com/solaris/release/
```

```

Startup: Linked image publisher check ... Startup: Refreshing catalog 'solaris' ...
Done
Planning: Solver setup ... Done
Planning: Running solver ... Done
Planning: Finding local manifests ... Done
Planning: Fetching manifests: 0/501 0% complete
Planning: Fetching manifests: 501/501 100% complete
Planning: Package planning ... Done
Planning: Merging actions ... Done
Planning: Checking for conflicting actions ... Done
Planning: Consolidating action changes ... Done
Planning: Evaluating mediators ... Done
Planning: Planning completed in 32.07 seconds
The following licenses have been accepted and not displayed.
Please review the licenses for the following packages post-install:
consolidation/osnet/osnet-incorporation
Package licenses may be viewed using the command:
pkg info --license <pkg_fmri>

Download: 0/64687 items 0.0/569.3MB 0% complete
Download: 931/64687 items 5.8/569.3MB 1% complete (1.2M/s)
...
Download: 64589/64687 items 569.2/569.3MB 99% complete (825k/s)
Download: Completed 569.25 MB in 358.54 seconds (1.6M/s)
Actions: 1/88614 actions (Installing new actions)
Actions: 19471/88614 actions (Installing new actions)
...
Actions: 86994/88614 actions (Installing new actions)
Actions: 87128/88614 actions (Installing new actions)
Actions: Completed 88614 actions in 73.71 seconds.
Installation: Succeeded
Done: Installation completed in 342.508 seconds.

Log saved in non-global zone as /zones/kzone1/root/var/log/zones/
zoneadm.20146T195713Z.kzone1.install
global#

```

例 2-3 使用备用 sysconfig 配置文件安装内核区域

本示例介绍如何使用 sysconfig 配置文件 /var/tmp/kzone1.sysconfig.xml 安装内核区域 kzone1。

```

global# zoneadm -z kzone1 install -c /var/tmp/kzone1-sysconfig.xml
The following ZFS file system(s) have been created:
rpool/zones/kzone1
Progress being logged to /var/log/zones/zoneadm.20146T195713Z.kzone1.install
pkg cache: Using /var/pkg/publisher.
AI Manifest: /tmp/zoneadm124827.zQWo0h/devel-ai-manifest.xml
SC Profile: /var/tmp/kzone1-sysconfig.xml
Installation: Starting ...

```

```

Creating IPS image

```

```
Startup: Retrieving catalog 'nightly' ... Done
Startup: Caching catalogs ... Done
Startup: Refreshing catalog 'nightly' ... Done
Startup: Refreshing catalog 'solaris' ... Done
Startup: Refreshing catalog 'extra' ... Done
Startup: Caching catalogs ... Done
Installing packages from:
  nightly
    origin: file:///server/nightly
  solaris
    origin: file:///server/solaris
  extra
    origin: http://server/extra
Startup: Refreshing catalog 'nightly' ... Done
Startup: Refreshing catalog 'solaris' ... Done
Startup: Refreshing catalog 'extra' ... Done
Planning: Solver setup ... Done
Planning: Running solver ... Done
Planning: Finding local manifests ... Done
...
Planning: Fetching manifests: 552/552 100% complete
Planning: Package planning ... Done
Planning: Merging actions ... Done
Planning: Checking for conflicting actions ... Done
Planning: Consolidating action changes ... Done
Planning: Evaluating mediators ... Done
Planning: Planning completed in 56.62 seconds
...
Download: 9746/65597 items 143.6/661.7MB 21% complete
Download: 35018/65597 items 370.8/661.7MB 56% complete
Download: 62181/65597 items 654.5/661.7MB 98% complete
Download: Completed 661.67 MB in 40.57 seconds (0B/s)
...
Actions: 87940/89672 actions (Installing new actions)
Actions: 88107/89672 actions (Installing new actions)
Actions: 88745/89672 actions (Installing new actions)
Actions: Completed 89672 actions in 108.50 seconds.
Done
Installation: Succeeded
      Done: Installation completed in 342.508 seconds.

Log saved in non-global zone as /zones/kzone1/root/var/log/zones/
zoneadm.20146T195713Z.kzone1.install
global#
```

从安装介质安装内核区域

您可以通过 Oracle Solaris 安装介质安装内核区域。

请注意以下注意事项：

- 支持从介质进行交互式介质文本安装和自动化安装。内核区域不支持 Live Media 安装。有关这些安装方法的其他信息，请参见《[安装 Oracle Solaris 11.2 系统](#)》中的第 II 部分，“使用安装介质安装”。
- 安装介质必须支持内核区域。请参见“[检验内核区域主机上的硬件和软件支持](#)” [9]。
- 在安装过程中，必须包含安装介质映像的完整路径。否则，Oracle Solaris 介质安装将失败。

在 Oracle Solaris 介质安装过程中，引导内核区域并连接到区域控制台。有关如何使用区域控制台的信息，请参见《[创建和使用 Oracle Solaris 区域](#)》中的“[区域控制台登录](#)”。



注意 - 如果在 Oracle Solaris 介质安装完成前退出内核区域控制台或与之断开连接，安装将失败。

▼ 如何对内核区域执行 Oracle Solaris 介质安装

1. 成为管理员。
有关更多信息，请参见《[在 Oracle Solaris 11.2 中确保用户和进程的安全](#)》中的“[使用所指定的管理权限](#)”。
2. 使用 Oracle Solaris 安装介质安装内核区域。

```
global# zoneadm -z zonename install -b media-file
```

例如，要将位于 `/var/tmp/solaris-media.iso` 中的内核区域介质安装到内核区域 `kzone1`：

```
global# zoneadm -z kzone2 install -b /var/tmp/solaris-media.iso
```

卸载内核区域

可使用 `zoneadm uninstall` 命令卸载内核区域。例如，在安装新的区域配置或更新区域配置之前卸载内核区域。请注意，在执行此操作时，区域不能处于运行状态。有关区域卸载过程的信息，请参见《[创建和使用 Oracle Solaris 区域](#)》中的“[关闭、停止、重新引导和卸载区域](#)”。

您必须是全局管理员或在全局区域中具有相应授权的用户才能卸载区域。

关闭、重新引导和停止内核区域

使用 `zoneadm shutdown`、`zoneadm reboot` 和 `zoneadm halt` 命令关闭、重新引导和停止内核区域。有关使用这些命令的信息，请参见《[创建和使用 Oracle Solaris 区域](#)》中的“[关于关闭、停止、重新引导和卸载区域](#)”。

如果希望区域在主机系统重新引导时自动引导，请设置 `autoboot zonecfg` 资源。有关如何设置此资源的其他信息，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](#)”。

您必须是全局管理员或在全局区域中具有相应授权的用户才能关闭、重新引导或停止区域。

克隆内核区域

通过克隆可以将系统上现有的已配置和已安装区域复制到同一系统上的新区域。克隆区域包括现有区域的所有定制设置。例如，源区域上添加的软件包、修改的区域资源和所做的文件修改均将显示在每个克隆的区域中。克隆区域是添加具有类似定制区域配置的其他区域的有效方法。

可以通过以下方法克隆内核区域：

- 如果需要克隆少量的区域，可使用 `zoneadm clone` 命令。请参见例 2-4 “[使用 zoneadm clone 命令克隆内核区域](#)”。
- 如果需要在大型部署中克隆多个区域（如在数据中心环境中），可使用统一归档文件。请参见例 2-5 “[使用统一归档文件克隆和部署内核区域](#)”。

注 - 统一归档文件只能包括处于运行状态的内核区域。在创建统一归档文件期间，您可以排除未运行的所有内核区域。有关更多信息，请参见《[在 Oracle Solaris 11.2 中使用统一归档文件进行系统恢复和克隆](#)》中的第 2 章“[使用统一归档文件](#)”。

克隆完内核区域后，即可引导和登录到新区域。

例 2-4 使用 `zoneadm clone` 命令克隆内核区域。

本示例说明如何将内核区域 `kzone1` 克隆到主机 `global` 上的内核区域 `kzone2`。有关逐步过程，请参见《[创建和使用 Oracle Solaris 区域](#)》中的“[在同一系统中克隆非全局区域](#)”。

```
global# zoneadm -z kzone1 halt
```

```

global# zonecfg -z kzzone2 create -t kzzone1
global# zoneadm -z kzzone2 clone kzzone1
Progress being logged to /var/log/zones/zoneadm.20140327T223951Z.kzzone2.clone
Install Log: /system/volatile/install.100847/install_log
  AI Manifest: /system/shared/ai.xml
Installation: Starting ...

    Creating direct clone image...
    Registering dynamic archive transfer
    Pre-validating manifest targets before actual target selection
    Pre-validation of manifest targets completed
    Validating combined manifest and archive origin targets
    Commencing transfer of stream: ...
    Completed transfer of direct stream: ...
    Archive transfer completed
Installation: Succeeded

```

例 2-5 使用统一归档文件克隆和部署内核区域

以下示例说明如何使用 `archiveadm` 命令克隆和部署内核区域 `kzzone1`。为内核区域 `kzzone1` 创建统一归档文件。验证归档信息，并将 `kzzone1` 中修改过的区域配置克隆到内核区域 `kzzone2`。有关逐步过程，请参见《[在 Oracle Solaris 11.2 中使用统一归档文件进行系统恢复和克隆](#)》。

```

global# archiveadm create -z kzzone1 /var/tmp/kzzone1.uar
Unified Archive initialized: /var/tmp/kzzone1.uar.
    \
Logging to: /system/volatile/archive_log.26248
Dataset discovery completed...
    /
Media creation complete for zone(s)...
    -
Archive stream creation completed...
    -
Archive creation completed...
global# zoneadm list -cv
  ID NAME          STATUS    PATH          BRAND    IP
  0 global          running  /             solaris  shared
  2 kzzone1         running  -             solaris-kz  excl
global# archiveadm info /var/tmp/kzzone1.uar
Archive Information
  Creation Time: 2014-04-10T17:12:12Z
  Source Host: global
  Architecture: i386
  Operating System: Oracle Solaris 11.2 X86
  Deployable Systems: kzzone1
global# zonecfg -z kzzone2 create -a /var/tmp/kzzone1.uar
global# zoneadm -z kzzone2 install -a /var/tmp/kzzone1.uar
global# zoneadm list -cv
  ID NAME          STATUS    PATH          BRAND    IP
  0 global          running  /             solaris  shared
  2 kzzone1         running  -             solaris-kz  excl

```

```
- kzone2          configured -          solaris-kz excl
```

挂起和恢复内核区域

可以使用 `zoneadm suspend` 命令将内核区域挂起到磁盘，此命令是内核区域特有的。

`zoneadm suspend` 命令会使内核区域进入 `suspended`（挂起）状态。创建挂起映像，然后使用高级加密标准 AES-128-CCM 进行压缩和加密。`/dev/random` 会自动生成加密密钥。压缩和加密后，区域的运行状态将写入到内核区域的区域路径。

压缩和加密后的挂起映像的大小通常将小于区域的 RAM 大小。写入区域的运行状态将占用区域所使用的 RAM 总量。因此，`zoneadm suspend` 操作可能会占用大量系统资源。

可以通过调用 `zoneadm boot` 命令恢复挂起的区域（使所有区域操作重新处于活动状态）。

仅当内核区域的配置中有 `suspend` 资源属性时，内核区域才支持挂起和恢复。缺省情况下，内核区域模板 `SYSsolaris-kz` 会提供 `suspend` 资源属性。例如，内核区域 `kzone1` 的 `suspend` 信息如下：

```
global# zonecfg -z kzone1 info suspend
suspend:
    path: /system/zones/kzone1/suspend
    storage not specified
```

`suspend` 资源必须指定完整文件路径或存储位置。有关 `suspend` 资源属性要求的更多信息，请参见 [solaris-kz\(5\)](#) 手册页。

如果 `suspend` 映像和其余区域存储可供共享存储上的多台主机访问，则可以使用 `suspend` 映像支持区域迁移。请参见“[使用挂起和恢复迁移内核区域](#)” [28]。

使用挂起和恢复迁移内核区域

可以使用 `zoneadm suspend` 命令将内核区域迁移到另一台主机。对于区域迁移，区域配置必须在多台计算机之间具有可移植性。例如，不能在源主机上使用 `zvol`。

区域源和目标必须位于相同平台才能进行区域迁移。在 x86 系统上，供应商和 CPU 版本必须相同。在 SPARC 上，硬件平台必须相同。例如，不能将内核区域从 T4 主机迁移到 T3 主机。

注 - 要防止在内核区域迁移过程中丢失加密密钥，请在源系统上使用 `zonecfg export` 命令生成一个可在目标系统上使用的命令文件。例如，生成用于将区域从 `global1` 迁移到 `global2` 的命令文件：

```
global1# zonecfg -z kzone1 export -f /net/.../kzone1.cfg
global2# zonecfg -z kzone1 -f /net/.../kzone1.cfg
```

有关其他信息，请参见“[内核区域主机数据和主机 ID](#)” [38]。

▼ 如何迁移内核区域

1. 成为管理员。
有关更多信息，请参见《[在 Oracle Solaris 11.2 中确保用户和进程的安全](#)》中的“[使用所指定的管理权限](#)”。
2. 在全局区域上，挂起要迁移的内核区域上的文件系统。

```
#zoneadm -z zonename suspend
```


例如，要挂起全局区域 `global` 上的内核区域 `kzone1`：

```
global# zoneadm -z kzone1 suspend
```
3. 分离全局区域上的内核区域文件系统。

```
#zoneadm -z zonename detach
```


例如，要分离全局区域 `global` 上的内核区域 `kzone1`：

```
global#zoneadm -z kzone1 detach
```
4. 导出区域配置并将文件传输到新主机。

```
# zonecfg -z zonename export | ssh root@newhost zonecfg -z zonename -f -
```


例如：

```
global# zonecfg -z kzone1 export | ssh root@global2 zonecfg -z kzone1 -f -
```
5. 在新主机上附加区域。

```
# zoneadm -z zonename attach
```


例如：

```
global2# zoneadm -z kzone1 attach
```
6. 引导新主机上的内核区域以恢复迁移的区域。

```
#zoneadm -z zonename boot
```

例如：

```
global2# zoneadm -z kone1 boot
```

另请参见 [有关共享存储上的区域和区域迁移的其他信息](#)，请参见《[创建和使用 Oracle Solaris 区域](#)》中的“[将非全局区域迁移到其他计算机](#)”。

◆◆◆ 第 3 章

管理 Oracle Solaris 内核区域

本章包含以下 Oracle Solaris 内核区域管理主题：

- “在内核区域环境中工作” [31]
- “使用内核区域和不可编辑的区域” [32]
- “管理内核区域中的可移除设备” [33]
- “使用内核区域辅助状态” [36]
- “管理嵌套区域” [37]
- “内核区域主机数据和主机 ID” [38]
- “使用内核区域引导装载程序” [39]

有关 solaris 和 solaris10 标记区域的管理主题的信息，请参见《[创建和使用 Oracle Solaris 区域](#)》中的第 10 章“[关于 Oracle Solaris 区域管理](#)”。

在内核区域环境中工作

在内核区域环境中工作与在全局区域中工作非常相似。本节介绍内核区域管理环境与使用全局区域的主要差异。

区域中的进程 ID 可见性

内核区域进程对于内核区域主机并非直接可见。您必须使用 `zlogin` 命令后跟进程管理命令以查看有关内核区域的任何进程信息。例如，要从内核区域主机 `global` 查看内核区域 `kzone1` 中有关 `syslogd` 的进程信息：

```
global# zlogin kzone1 ps -ef |grep syslogd
root 1520      1  0 20:23:08 ?          0:00 /usr/sbin/syslogd
```

内核区域中的重复进程 ID

全局区域和每个内核区域管理自己的进程 ID 空间。相同的数值进程 ID 可能识别全局区域以及一个或多个内核区域中的不同系统进程。例如，在相同的物理主机中，数值进程 5678 可在全局区域中运行 `syslogd`，在内核区域中运行 `sendmail`。

要在 `kzone1` 中使用 `ps` 命令中止进程 5678，请使用 `zlogin` 命令后跟 `kill` 命令。

```
global# zlogin kzone1 kill 5678
```

内核区域的区域路径

按照设计，无法设置内核区域的区域路径。它不包含任何持久数据或可维护性数据。

内核区域中的资源管理功能

配置内核区域时，`max-processes` 等资源控制不可用。因为内核区域具有独立于全局区域的内核，在内核区域内运行的进程不会占用全局区域中的进程表槽。

使用内核区域和不可编辑的区域

不可编辑的区域提供只读（即不可编辑）的文件系统配置文件。`solaris` 标记区域（在非全局区域中）和内核区域都支持不可编辑的区域。有关不可编辑的区域的详细信息，请参见《[创建和使用 Oracle Solaris 区域](#)》中的“[只读区域概述](#)”。

配置不可编辑的区域

要将内核区域配置为不可编辑的区域，请在内核区域中设置 `file-mac-profile` 属性。有关 `file-mac-profile` 属性的其他信息，请参见《[创建和使用 Oracle Solaris 区域](#)》中的“[配置只读区域](#)”。

▼ 如何将内核区域配置为不可编辑的（只读）区域

1. 成为管理员。
有关更多信息，请参见《[在 Oracle Solaris 11.2 中确保用户和进程的安全](#)》中的“[使用所指定的管理权限](#)”。

2. 引导内核区域。

```
# zoneadm kernel-zone-name boot
```

3. 登录到内核区域。

```
# zlogin kernel-zone-name
```

4. 在内核区域中设置不可编辑的区域。

```
kernel-zone-name# zonecfg -z global set file-mac-profile=value
```

例如：

```
kzone1# zonecfg -z global set file-mac-profile=flexible-configuration
updating /platform/i86pc/amd64/boot_archive
```

5. 重新引导内核区域。

```
kernel-zone-name# reboot
```

维护和管理只读内核区域

在 `zlogin` 命令中使用可信路径模式对只读内核区域执行维护和管理操作。可信路径模式具有以下选项：

- T 允许管理员进入已设置可信路径属性 `PRIV_PROC_TPD` 的不可编辑区域。此会话可以修改通常不可编辑的文件。但不能读取不受保护的的文件。
- U 执行的进程与 `-T` 选项执行的进程相同，但处于非安全模式。 `file-mac-profile` 属性设置为 `flexible-configuration` 的区域需要此选项。

注 - 这些选项不能与控制台登录会话一起使用。对于可编辑的区域，会忽略 `zlogin` 命令的 `-T` 和 `-U` 选项。

有关更多信息，请参见 [zlogin\(1\)](#) 手册页。

管理内核区域中的可移除设备

您可以配置可移除回送文件 `lofi` 设备，该设备可作为 CD-ROM 设备在内核区域中使用。有关如何配置 `lofi` 设备的更多信息，请参见《[Oracle Solaris Zones 介绍](#)》中的“非全局区域中的可删除 `lofi` 设备”。

▼ 如何将虚拟 CD-ROM 设备添加到内核区域

1. 成为管理员。
有关更多信息，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全》中的“使用所指定的管理权限”。

2. 创建一个空的可移除只读 `lofi` 设备。

```
# lofiadm -r
```

以下示例显示了示例输出。

```
global# lofiadm -r  
/dev/lofi/1
```

3. 将 `lofi` 设备添加到内核区域中。

```
# zonecfg -z zonename
```

以下示例说明如何将位于 `/dev/rlofi/1` 中的 `lofi` 设备添加到内核区域 `kzone1` 中：

```
global# zonecfg -z kzone1  
zonecfg:kzone1> add device  
zonecfg:kzone1:device> set match=/dev/rlofi/1  
zonecfg:kzone1:device> end  
zonecfg:kzone1> exit
```

4. 重新引导内核区域以使配置更改生效。

```
# zoneadm -z zonename reboot
```

5. 在内核区域中，更新设备文件系统 (`devfs`) 和硬件抽象层 (`hal`)，以便 `hal` 看到新的 `cdrom` 设备。

```
# devfsadm -i zvblk
```

例如：

```
global# devfsadm -i zvblk  
global# svcadm restart hal  
global# rmformat -l
```

```
...
```

```
2. Logical Node: /dev/rdisk/cldp0  
   Physical Node: /zvnex/zvblk@1  
   Connected Device: kz          vCDROM          0  
   Device Type: CD Reader  
   Bus: <Unknown>  
   Size: 0.0 MB  
   Label: <Unknown>  
   Access permissions: Medium is write protected.
```

6. 在内核区域中重新启动 `hal` 服务。

```
# svcadm restart hal
```

7. 列出区域中的可移除设备。

```
# rmformat -l
```

例如，以下示例列出了内核区域 kzone1 中的可移除设备：

```
kzone1# rmformat -l
Looking for devices...
  1. Logical Node: /dev/rdisk/c1d0p0
     Physical Node: /zvnex/zvblk@0
     Connected Device: kz          vDisk          0
     Device Type: Removable
     Bus: <Unknown>
     Size: 16.4 GB
     Label: <Unknown>
     Access permissions: <Unknown>
  2. Logical Node: /dev/rdisk/c1d1p0
     Physical Node: /zvnex/zvblk@1
     Connected Device: kz          vCDROM      0
     Device Type: CD Reader
     Bus: <Unknown>
     Size: 0.0 MB
     Label: <Unknown>
     Access permissions: <Unknown>
```

8. 在内核区域中，将 CD-ROM 插入 CD-ROM 驱动器。

```
# lofiadm -r device-name device-path
```

以下示例说明如何在内核区域 kzone1 中将 CD-ROM 映像 /root/sol-11_3-repo.full.iso 插入 lofi 设备 /dev/lofi/1：

```
kzone1# lofiadm -r /root/sol-11_2-repo-full.iso /dev/lofi/1
kzone1# lofiadm
Block Device          File                                Options
/dev/lofi/1           /root/sol-11_2-repo-full.iso      Removable,ReadOnly
```

9. 挂载 CD-ROM。

```
# mount -F hsfs device-location /mnt
```

以下示例挂载了位于 /dev/dsk/c1d1p0 的 CD-ROM 设备

```
kzone1# mount -F hsfs /dev/dsk/c1d1p0 /mnt
```

10. 取消挂载 CD-ROM 设备。

```
# umount /mnt
```

11. 弹出 CD-ROM。

```
# eject cdrom
```

12. 确认内核区域主机中不再存在 CD-ROM 设备。

```
# lofiadm
```

例如：

```
global# lofiadm
Block Device      File      Options
/dev/lofi/1      -         Removable,ReadOnly
```

使用内核区域辅助状态

内核区域使用辅助状态将补充状态信息传递给全局区域。缺省情况下，内核区域不会设置辅助状态。仅当启动调试和内核维护操作时，才会设置辅助状态。

要查看全局区域当前状态和内核区域辅助状态，请使用 `zoneadm list -s` 命令。

```
global# zoneadm list -s
NAME      STATUS      AUXILIARY STATE
global    running
kzone1    running
kzone2    running
kzone3    running    debugging
```

可用的内核区域辅助状态如下：

suspended	此区域已挂起，下一次引导时将恢复。请注意，必须连接此区域才能看到此状态。当正在进行迁移时，内核区域处于 <code>suspended</code> 辅助状态。请参见 “使用挂起和恢复迁移内核区域” [28] 。
debugging	内核区域位于内核调试器 <code>kldb</code> 中。尽管此区域处于 <code>running</code> 状态，但区域无法为任何网络请求提供服务。您必须连接到区域控制台以与 <code>kldb</code> 交互。有关如何连接到区域控制台的信，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”。
panicked	此区域处于 <code>running</code> 状态，但遇到紧急情况。不过主机不受影响。您必须访问区域控制台以登录到处于紧急辅助状态的内核区域。

有关区域状态的信息，请参见[《Oracle Solaris Zones 介绍》](#) 中的第 1 章“Oracle Solaris Zones 介绍”。有关内核区域辅助状态的其他信息，请参见 `solaris-kz(5)` 手册页。有关内核调试器的信息，请参见 `kldb(1)` 手册页。

管理嵌套区域

嵌套区域是指从内核区域安装和引导的非全局区域。在嵌套区域中，内核区域用作全局区域。嵌套区域可以是新的 solaris 标记区域或迁移的 solaris 或 solaris10 标记区域。不支持将内核区域作为嵌套区域。

嵌套区域具有以下要求：

操作系统	<p>所有嵌套区域都必须支持 Oracle Solaris 11.2 或更高版本。</p> <ul style="list-style-type: none"> ▪ 必须将运行 Oracle Solaris 11 或 Oracle Solaris 11.1 的 solaris 标记区域更新到 Oracle Solaris 11.2。有关更新系统软件包的信息，请参见《在 Oracle Solaris 11.2 中添加和更新软件》中的第 3 章“安装和更新软件包”。 ▪ 可以将 solaris10 标记区域迁移到至少运行 Oracle Solaris 11.2 的非全局区域。有关如何将 solaris10 区域迁移到 Oracle Solaris 11.2 主机的过程，请参见《创建和使用 Oracle Solaris 10 区域》中的“将 solaris10 标记区域迁移至另一台主机”。
网络配置	<p>作为嵌套区域运行的 solaris 或 solaris10 标记区域可以使用专用 IP 或共享 IP。如果需要专用 IP 配置，则需要配置内核区域允许其他 MAC 地址。</p>
系统资源	<p>嵌套区域只能使用可供内核区域使用的系统资源。这些资源包括虚拟磁盘和 iSCSI 磁盘。</p>
克隆	<p>如果克隆包含嵌套配置的内核区域，则将仅克隆外部内核区域。在区域克隆过程中，不会克隆内核区域内的任何区域。请参见“克隆内核区域” [26]。</p>

▼ 如何将多个 MAC 地址添加到内核区域

1. 成为管理员。
有关更多信息，请参见《[在 Oracle Solaris 11.2 中确保用户和进程的安全](#)》中的“使用所指定的管理权限”。
2. 添加新的 MAC 地址。

```
global# zonecfg:kz-1> select anet id=0
zonecfg:kz-1:anet> add mac
zonecfg:kz-1:anet:mac> set mac-address=0:16:3e:86:19:70
zonecfg:kz-1:anet:mac> end
zonecfg:kz-1:anet> info
anet:
```

```
lower-link: net0
...
mac-address: 0:16:3e:86:11:70
...
id: 0
mac:
  mac-address: 0:16:3e:86:19:70
  mac-prefix not specified
  id: 0
```

嵌套区域和新的非全局区域配置

您可以使用 `zonecfg` 和 `zoneadm` 命令在内核区域中配置、安装和引导新的 `solaris` 标记区域。例如：

```
kzone1# zonecfg -z zone1
Use 'create' to begin configuring a new zone.
zonecfg:zone1> create -t SYSsolaris
zonecfg:zone1> commit
zonecfg:zone1> exit
```

有关规划、配置和安装非全局区域的其他信息，请参见《[创建和使用 Oracle Solaris 区域](#)》。

内核区域主机数据和主机 ID

内核区域的每个可引导设备都包含称为主机数据的状态信息。内核区域的主机数据用于监视内核区域状态信息，其中包括：

- 区域使用情况
- 区域挂起，如“[挂起和恢复内核区域](#)” [28]中所述
- 内核区域时钟与全局区域时钟之间的时间偏移
- OpenBoot 变量（仅适用于 SPARC）

内核区域主机数据使用高级加密标准 AES-128-CCM 进行加密和验证，将相同的加密密钥用于内核区域 suspend 映像。

在配置或引导某个内核区域时，会读取主机数据以确定是否有其他系统在使用该内核区域的引导存储。如果其他系统在使用引导存储，则该内核区域将进入 `unavailable`（不可用）状态，且将显示一条错误消息以指出正在使用引导存储的系统。例如：

```
global# zoneadm -z kzone1 attach
zone 'kzone1': error: ERROR: zone kzone1 is in use by host with hostid 848611d4
zone 'kzone1': error:      last known state: installed
```

```

zone 'kzone1': error:                hostname: global2
zone 'kzone1': error: boot environment name: solaris-1
zone 'kzone1': error: boot environment uuid: 69ed2e6a-e25a-6d36-e022-ed7261ed8899
zone 'kzone1': error: last update time: Sun Apr 13 20:08:13 2014
zone 'kzone1': error: To fix, detach the zone from the other host then attach it to this host
zone 'kzone1': error: If the zone is not active on another host, attach it with
zone 'kzone1': error: zoneadm -z kzone1 attach -x force-takeover

```

如果没有其他系统在使用引导存储，则可以使用 `zoneadm attach -x force-takeover` 命令修复该内核区域。



注意 - 强制接管或重新初始化主机数据将导致无法检查是否有其他系统在使用该区域。对引用同一个存储的某个区域运行多个实例将对该区域的文件系统带来不可修复的损坏。

如果区域的加密密钥不可访问，则将无法读取主机数据和任何挂起映像。在这种情况下，任何读取或引导区域的尝试都将导致区域进入 `unavailable`（不可用）状态。如果无法恢复区域的加密密钥，则可以使用 `zoneadm attach -x initialize-hostdata` 命令来生成新的加密密钥和主机数据。

要防止在内核区域迁移过程中丢失加密密钥，请在源系统上使用 `zonecfg export` 命令生成一个可在目标系统上使用的命令文件。例如：

```

global# zonecfg -z kzone1 export -f /net/.../kzone1.cfg
global# zonecfg -z kzone1 -f /net/.../kzone1.cfg

```

使用内核区域引导装载程序

内核区域引导装载程序可管理内核区域中的引导操作。要调用引导装载程序，则内核区域必须处于就绪或已安装状态。您可以使用内核区域引导装载程序执行以下操作：

- 列出可用的引导环境
- 将区域引导至备用引导环境

使用 `zoneadm boot` 命令调用内核区域引导装载程序。在调用内核区域引导装载程序时，您还必须调用区域控制台。引导装载程序输出将显示在区域控制台中。

注 - 从区域控制台中退出的命令序列为 `~.`。有关其他信息，请参见《[创建和使用 Oracle Solaris 区域](#)》中的“[如何登录到区域控制台](#)”。

有关在操作系统级别创建和管理引导环境的信息，请参见《[创建和管理 Oracle Solaris 11.2 引导环境](#)》中的第 1 章“[管理引导环境简介](#)”。《[创建和管理 Oracle Solaris 11.2 引导环境](#)》中的第 2 章“[beadm 区域支持](#)”中提供了有关管理区域和引导环境的其他信息。

▼ 如何指定内核区域中的备用引导环境

1. 成为管理员。

有关更多信息，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全》中的“使用所指定的管理权限”。

2. 登录到区域控制台。

```
# zlogin -C zonename
```

例如，要登录到 kzone1 中的控制台：

```
global# zlogin -C kzone1
```

3. 在单独的终端窗口中，列出可用的内核区域引导环境。

```
# zoneadm -z zonename boot -- -L
```

以下示例显示了示例输出。

```
global# zoneadm -z kzone2 boot -- -L
[Connected to zone 'kzone2' console]
1 kz-130118 (rpool/ROOT/kz-130118)
2 kz-1 (rpool/ROOT/kz-1)
3 solaris-5 (rpool/ROOT/solaris-5)
4 solaris-7 (rpool/ROOT/solaris-7)
Select environment to boot: [ 1 - 4 ]:
```

4. 引导至所选引导环境。

```
# zoneadm -z zonename boot -- -Z boot-environment
```

例如：

```
global# zoneadm -z kzone1 boot -- -Z rpool/ROOT/solaris-backup-1
```

例 3-1 在 SPARC 主机上选择和引导备用引导环境

以下示例显示了内核区域 kzone1 中备用引导环境的区域控制台输出。内核区域主机硬件为 SPARC 系统。

```
[Connected to zone 'kzone1' console]
NOTICE: Entering OpenBoot.
NOTICE: Fetching Guest MD from HV.
NOTICE: Starting additional cpus.
NOTICE: Initializing LDC services.
NOTICE: Probing PCI devices.
NOTICE: Finished PCI probing.
```

```
SPARC T4-2, No Keyboard
Copyright (c) 1998, 2014, Oracle and/or its affiliates. All rights reserved.
OpenBoot 4.36.0.build_05, 2.0000 GB memory available, Serial #1845652596.
Ethernet address 0:0:0:0:0:0, Host ID: 6e026c74.
```

```
Boot device: disk0 File and args: -L
1 Oracle Solaris 11.2 SPARC
2 bootenv123
3 bootenv456
Select environment to boot: [ 1 - 3 ]: 2
```

```
To boot the selected entry, invoke:
boot [<root-device>] -Z rpool/ROOT/bootenv123
```

```
Program terminated
ok boot -Z rpool/ROOT/bootenv123
```

```
[NOTICE: Zone rebooting]
NOTICE: Entering OpenBoot.
NOTICE: Fetching Guest MD from HV.
NOTICE: Starting additional cpus.
NOTICE: Initializing LDC services.
NOTICE: Probing PCI devices.
NOTICE: Finished PCI probing.
```

```
SPARC T4-2, No Keyboard
Copyright (c) 1998, 2014, Oracle and/or its affiliates. All rights reserved.
OpenBoot 4.36.0.build_05, 2.0000 GB memory available, Serial #1845652596.
Ethernet address 0:0:0:0:0:0, Host ID: 6e026c74.
```

```
...
Hostname: kzone1
kzone1 console login:
```

例 3-2 在 x86 主机上选择和引导备用引导环境

以下示例显示了内核区域 kzone1 中备用引导环境的区域控制台输出。内核区域主机硬件为 x86 系统。

```
[Connected to zone 'kzone1' console]
1 boot-2 (rpool/ROOT/boot-2)
2 Oracle Solaris 11.2 x86 (rpool/ROOT/solaris)
3 boot-1 (rpool/ROOT/boot-1)
Select environment to boot: [ 1 - 3 ]:2
Boot device: disk0 File and args:
reading module /platform/i86pc/amd64/boot_archive...done.
reading kernel file /platform/i86pc/kernel/amd64/unix...done.
SunOS global 5.11 11.2 i86pc i386 i86pc
Copyright (c) 1983, 2014, Oracle and/or its affiliates. All rights reserved.
Hostname: kzone1
```

```
...  
kzone1 console login:
```

索引

A

安装介质
 用于内核区域安装，24
add-device 资源属性，14
anet 资源，15
archiveadm 命令，26

B

标记，7
标记区域，7
不可编辑的区域，32
bootpri 资源属性，14
BrandZ，7

C

capped-memory 资源属性，13
重复进程 ID
 内核区域和，32
CPU
 管理，12

D

dedicated-cpu 资源属性，12

F

分层区域
 要求，37
 配置，37
辅助状态，36

G

挂起内核区域，28
关闭内核区域，26

H

恢复内核区域，28

J

检验主机上的支持，9
进程 ID
 在内核区域中的可见性，31

K

可移除设备配置，33
克隆内核区域，26

L

lofi 设备，33

N

内存
 管理，13
内核区域安装
 sysconfig 配置文件，22
 安装介质，24
 直接安装，19
 自动化安装 (Automated Installation, AI) 清单，22
内核区域根磁盘，13
内核区域配置，10

内核区域迁移, 28
内核区域引导装载程序, 39
net 资源, 15

O

Oracle Solaris 内核区域, 8
 参见 内核区域、solaris-kz 标记区域、操作系统要求
 定义, 7
 相关概念, 8

P

配置不可编辑的内核区域, 32
配置内核区域, 10
配置内核区域资源, 12
配置只读内核区域, 32

Q

迁移内核区域, 28
嵌套区域, 37
区域
 标记 见 solaris-kz 标记区域
区域路径, 32
缺省内核区域安装方法, 19

R

热迁移, 28
软件要求, 8

S

solaris-kz 标记区域, 7
SPARC 固件要求, 8
sysconfig 配置文件
 内核区域安装, 22

T

添加存储设备, 14
添加内存, 13
添加网络设备, 15

V

virtinfo 命令, 9
virtual-cpu 资源属性, 12

W

网络设备
 添加, 15
 移除, 15
网络设备 ID, 15

X

卸载内核区域, 25
x86 BIOS 要求, 8

Y

一般的区域概念, 8
引导环境, 指定, 40
引导装载程序, 39
硬件要求, 8

Z

直接安装, 19
只读内核区域, 32
主机 ID, 38
主机数据, 38
主机要求, 8
自动化安装 (Automated Installation, AI) 清单
 用于内核区域安装, 22
ZFS ARC 高速缓存要求, 8
 调优, 10
zoneadm boot 命令, 39
zoneadm clone 命令, 26
zoneadm halt 命令, 26
zoneadm install 命令, 19
zoneadm list -s 命令, 36
zoneadm reboot 命令, 26
zoneadm resume 命令, 28
zoneadm shutdown 命令, 26
zoneadm suspend 命令, 28
zoneadm uninstall 命令, 25