# Oracle® Solaris Cluster 安全指南

文件号码 E62237
2014 年 7 月

ORACLE

**文档可访问性**

有关 Oracle 对可访问性的承诺，请访问 Oracle Accessibility Program 网站 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc。

**获得 Oracle 支持**

购买了支持服务的 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。

# 目录

使用本文档 ..... 7

1 Oracle Solaris Cluster 安全性简介 ..... 9
Oracle Solaris Cluster 和安全性概述 ..... 9
一般安全原则 ..... 10
安全安装和配置 ..... 10
安全功能 ..... 13
开发者需要注意的安全事项 ..... 14

索引 ..... 17

# 使用本文档

- **概述** – 概述了 Oracle Solaris Cluster 中的安全性、有关安全安装和配置的信息、安全功能以及开发者需要注意的安全事项。
- **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** – 对故障排除和硬件更换具有丰富经验

## 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=E52214。

## 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。

## 文档可访问性

有关 Oracle 对可访问性的承诺，请访问 Oracle Accessibility Program 网站 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc。

## 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

# 1 Oracle Solaris Cluster 安全性简介

Oracle Solaris Cluster 产品是一个软硬件集成解决方案，可用于创建高度可用且可伸缩的服务。《*Oracle® Solaris Cluster 4.2* 安全指南》概述了 Oracle Solaris Cluster 中的安全性、有关安全安装和配置的信息、安全功能以及开发者安全注意事项。将本书与整个 Oracle Solaris Cluster 文档集配合使用，可以全面了解 Oracle Solaris Cluster 软件。

本章包括以下各节：


- “Oracle Solaris Cluster 和安全性概述” [9]
- “安全安装和配置” [10]
- “安全功能” [13]
- “开发者需要注意的安全事项” [14]


有关 Oracle Solaris 操作系统 (Operating System, OS) 安全性的更多信息，请参见Unresolved link to " Oracle Solaris 11 安全准则 "。

## Oracle Solaris Cluster 和安全性概述

Oracle Solaris Cluster 环境将 Oracle Solaris 操作系统扩展到群集操作系统中。群集是一个或多个节点的集合，这些节点仅属于该集合。

Oracle Solaris Cluster 软件的好处包括以下几点：

- 减少或消除了由软件或硬件故障引起的系统停机时间
- 确保了数据和应用程序对最终用户的可用性，无论将使单个服务器系统停机的故障类型为何
- 通过向群集添加节点并进行负载平衡使服务分布到更多的处理器，从而提高了应用程序吞吐量
- 使用户能够在不关闭整个群集的情况下执行维护，从而增强系统可用性

相比传统单服务器系统，群集提供多个优点。这些优点包括支持故障转移和可伸缩服务、模块扩展能力、在节点上设置负载限制的能力以及与传统硬件容错系统相比较低的入门价格。

在 Oracle Solaris OS 上运行的群集中，群集类型是全局群集和区域群集。群集可以是全局群集、区域群集或者两者的组合。要了解有关配置区域群集的好处的更多信息，请参见Unresolved link to " Oracle Solaris Cluster Concepts Guide "。

## 一般安全原则

以下原则是安全使用 Oracle Solaris Cluster 应用程序的基础。

- 保持软件为最新版本
- 限制对关键服务的网络访问
- 遵循最小特权原则
- 监视系统活动
- 及时了解最新的 Oracle 安全信息

# 安全安装和配置

本节提供用于规划和执行 Oracle Solaris Cluster 安装和配置的链接。

- 安装 – 可以使用 Oracle Solaris 11 自动化安装程序 (Automated Installer, AI) 安装 Oracle Solaris Cluster 软件。有关更多信息，请参见Unresolved link to " Oracle Solaris Cluster 软件安装指南 中的安装软件"。
- 群集软件包 – Oracle Solaris Cluster 软件包使用 Oracle Solaris 映像包管理系统 (Image Packaging System, IPS) 软件包名称。

  在 Oracle Solaris 主机上安装群集软件包时，必须首先执行一些配置，以使该主机变为群集成员。如果不计划立即创建群集，应该通过以下方法停止 `scrcmd` 服务：变为超级用户并在安装软件包的每个节点上运行以下命令：`/usr/sbin/svcadm disable svc:/network/rpc/scrcmd:default`。

  可以创建群集时，使用以下命令重新启动服务：`/usr/sbin/svcadm enable svc:/network/rpc/scrcmd:default`。

  要查看 Oracle Solaris Cluster Geographic Edition 4.2 软件包的列表，请参见Unresolved link to " Oracle Solaris Cluster Geographic Edition Security Guide "。下表列出了 Oracle Solaris Cluster 4.2 随附的核心软件包。

| IPS 软件包名称 | 描述 |
| --- | --- |
| ha-cluster/developer/agent-builder | Oracle Solaris Cluster Agent Builder |
| ha-cluster/developer/api | Oracle Solaris Cluster 开发者软件 |
| ha-cluster/group-package/ha-cluster-framework-full | Oracle Solaris Cluster 框架完整组软件包 |
| ha-cluster/group-package/ha-cluster-framework-l10n | Oracle Solaris Cluster 框架本地化组软件包 |
| ha-cluster/group-package/ha-cluster-framework-minimal | Oracle Solaris Cluster 框架最小组软件包 |

| IPS 软件包名称 | 描述 |
| --- | --- |
| ha-cluster/group-package/ha-cluster-framework-scm | Oracle Solaris Cluster 框架 Oracle Solaris Cluster Manager 组件组软件包 |
| ha-cluster/group-package/ha-cluster-framework-slm | Oracle Solaris Cluster 框架服务级别管理 (Service Level Management, SLM) 组件组软件包 |
| ha-cluster/group-package/ha-cluster-full | Oracle Solaris Cluster 完整安装组软件包 |
| ha-cluster/group-package/ha-cluster-incorporation | Oracle Solaris Cluster incorporation 软件包 |
| ha-cluster/group-package/ha-cluster-minimal | Oracle Solaris Cluster 最小安装组软件包 |
| ha-cluster/group-package/ha-cluster-quorum-server-full | Oracle Solaris Cluster 法定服务器完整组软件包 |
| ha-cluster/group-package/ha-cluster-quorum-server-l10n | Oracle Solaris Cluster 法定服务器本地化组软件包 |
| ha-cluster/ha-service/derby | Derby Oracle Solaris Cluster 代理 |
| ha-cluster/ha-service/gds | Oracle Solaris Cluster 通用数据服务 |
| ha-cluster/ha-service/gds2 | Oracle Solaris Cluster 通用数据服务版本 2 |
| ha-cluster/ha-service/logical-hostname | Oracle Solaris Cluster 资源类型（用于逻辑主机名） |
| ha-cluster/ha-service/smf-proxy | Oracle Solaris Cluster SMF 代理方法 |
| ha-cluster/ha-service/telemetry | Oracle Solaris Cluster 遥测代理 |
| ha-cluster/library/cacao | Oracle Solaris Cluster 通用 Cacao 支持 |
| ha-cluster/library/ucmm | Oracle Solaris Cluster UCMM 重新配置接口 |
| ha-cluster/locale | Oracle Solaris Cluster 本地化消息 |
| ha-cluster/release/name | Oracle Solaris Cluster 名称 |
| ha-cluster/service/management | Oracle Solaris Cluster 可管理性和可维护性代理 |
| ha-cluster/service/management/slm | Oracle Solaris Cluster 可管理性代理（用于服务级别管理） |
| ha-cluster/service/quorum-server | Oracle Solaris Cluster 法定服务器 |
| ha-cluster/service/quorum-server/locale | Oracle Solaris Cluster 法定服务器本地化 |
| ha-cluster/service/quorum-server/manual | Oracle Solaris Cluster 法定服务器手册页 |
| ha-cluster/service/quorum-server/manual /locale | Oracle Solaris Cluster 法定服务器本地化手册页 |
| ha-cluster/storage/svm-mediator | Solaris Volume Manager（中介） |
| ha-cluster/system/cfgchk | Oracle Solaris Cluster 配置检查 |
| ha-cluster/system/core | Oracle Solaris Cluster 软件 |
| ha-cluster/system/dsconfig-wizard | Oracle Solaris Cluster 数据服务配置向导 |
| ha-cluster/system/install | Oracle Solaris Cluster 安装 |
| ha-cluster/system/manager | Oracle Solaris Cluster Manager |
| ha-cluster/system/manager-glassfish3 | Oracle Solaris Cluster Manager GlassFish 实例 |
| ha-cluster/system/manual | Oracle Solaris Cluster 手册页 |
| ha-cluster/system/manual/locale | Oracle Solaris Cluster 本地化手册页 |

在 Oracle Solaris Cluster 4.2 发行版后可能会支持其他数据服务代理。有关这些代理，请查看Unresolved link to " Oracle Solaris Cluster 4.2 发行说明 "。下表列出了 Oracle Solaris Cluster 4.2 支持的数据服务软件包。

| IPS 软件包名称 | 描述 |
| --- | --- |
| ha-cluster/data-service/apache | Oracle Solaris Cluster Apache Web Server 组件 |
| ha-cluster/data-service/dhcp | Oracle Solaris Cluster HA for DHCP |
| ha-cluster/data-service/dns | Oracle Solaris Cluster 域名服务器组件 |
| ha-cluster/data-service/goldengate | Oracle Solaris Cluster HA for GoldenGate |
| ha-cluster/data-service/glassfish-message-queue | Oracle Solaris Cluster HA for Oracle GlassFish Server Message Queue |
| ha-cluster/data-service/ha-ldom | Oracle Solaris Cluster HA（针对 xVM x86-64/SPARC 来宾域） |
| ha-cluster/data-service/ha-zones | Oracle Solaris Cluster HA for Solaris Containers |
| ha-cluster/data-service/iplanet-web-server | Oracle Solaris Cluster HA for Oracle iPlanet Web Server |
| ha-cluster/data-service/jd-edwards-enterpriseone | Oracle Solaris Cluster HA for Oracle JD Edwards EnterpriseOne Enterprise Server |
| ha-cluster/data-service/mysql | Oracle Solaris Cluster HA for MySQL |
| ha-cluster/data-service/nfs | Oracle Solaris Cluster NFS 服务器组件 |
| ha-cluster/data-service/obiee | Oracle Solaris Cluster HA for Oracle Business Intelligence Enterprise Edition |
| ha-cluster/data-service/oracle-database | Oracle Solaris Cluster HA Oracle 数据服务 |
| ha-cluster/data-service/oracle-ebs | Oracle Solaris Cluster HA for Oracle E-Business Suite |
| ha-cluster/data-service/oracle-external-proxy | Oracle Solaris Cluster HA for Oracle External Proxy |
| ha-cluster/data-service/oracle-http-server | Oracle Solaris Cluster HA for Oracle HTTP Server |
| ha-cluster/data-service/oracle-pmn-server | Oracle Solaris Cluster HA for Oracle Process Management and Notification Server |
| ha-cluster/data-service/oracle-traffic-director | Oracle Solaris Cluster HA for Oracle Traffic Director |
| ha-cluster/data-service/peoplesoft | Oracle Solaris Cluster HA for PeopleSoft Enterprise |
| ha-cluster/data-service/postgresql | Oracle Solaris Cluster HA for PostgreSQL |
| ha-cluster/data-service/samba | Oracle Solaris Cluster HA for Samba |
| ha-cluster/data-service/sap-livecache | Oracle Solaris Cluster HA for SAP liveCache |
| ha-cluster/data-service/sapdb | Oracle Solaris Cluster HA for SAP MaxDB |
| ha-cluster/data-service/sapnetweaver | Oracle Solaris Cluster HA for SAP NetWeaver |

| IPS 软件包名称 | 描述 |
| --- | --- |
| ha-cluster/data-service/siebel | Oracle Solaris Cluster HA for Siebel Gateway and Siebel Server |
| ha-cluster/data-service/sybase | Oracle Solaris Cluster HA for Sybase ASE |
| ha-cluster/data-service/timesten | Oracle Solaris Cluster HA for Oracle TimesTen |
| ha-cluster/data-service/tomcat | Oracle Solaris Cluster HA for Apache Tomcat |
| ha-cluster/data-service/weblogic | Oracle Solaris Cluster HA for Oracle WebLogic Server |
| ha-cluster/group-package/ha-cluster-data- services-full | Oracle Solaris Cluster 数据服务完整组软件包 |
| ha-cluster/system/manual/data-services | Oracle Solaris Cluster 数据服务联机手册页 |

- 配置 – 可以配置和管理全局群集和区域群集。有关更多信息，请参见Unresolved link to " Oracle Solaris Cluster 系统管理指南 中的第 1 章 Oracle Solaris Cluster 管理介绍"。

# 安全功能

本节包含有关 Oracle Solaris Cluster 提供的特定安全机制的信息。

安全安装使用以下重要安全功能：

- 基于角色的访问控制 (Role-Based Access Control, RBAC) – 使用 `solaris.cluster.modify`、`solaris.cluster.admin` 和 `solaris.cluster.read` 的 RBAC 授权访问群集。您必须是指定有 User Security（用户安全）权限配置文件的管理员，才能够更改角色的大多数安全属性。有关更多信息，请参见Unresolved link to " 在 Oracle Solaris 11.2 中确保用户和进程的安全 中的管理权限的使用"和Unresolved link to " Oracle Solaris Cluster 系统管理指南 中的Oracle Solaris Cluster RBAC 权限配置文件"。
- 新节点 – 将 `claccess` 命令或 `clsetup` 实用程序与特权配合使用来向群集添加节点。有关更多信息，请参见Unresolved link to " Oracle Solaris Cluster 系统管理指南 中的第 8 章 管理群集节点"。

  访问状态的默认设置为 `claccess deny-all`。仅当要执行特权操作（例如添加新节点）时才应该更改此设置。您完成后应该恢复 `deny-all` 状态。如果期望频繁更改群集配置，可以通过使用 `/usr/cluster/bin/claccess -p protocol=authentication-protocol` 命令选择更安全的验证协议来确保最大程度地信任新系统。有关更多信息，请参见 Unresolved link to " claccess1CL" 手册页和Unresolved link to " 在 Oracle Solaris 11.2 中管理 Kerberos 和其他验证服务 中的第 10 章 配置网络服务验证"。
- Trusted Extensions – 可以启用 Oracle Solaris Trusted Extensions 功能以用于区域群集中。有关更多信息，请参见Unresolved link to " Oracle Solaris Cluster 软件安装指南 中的区域群集中使用 Trusted Extensions 的准则"和Unresolved link to " Oracle Solaris Cluster 软件安装指南 中的如何安装和配置 Trusted Extensions"。

- 区域群集 – 区域群集包含使用 `cluster` 属性设置的 `solaris`、`solaris10` 或 `labeled` 标记的一个或多个非全局区域。`labeled` 标记的区域群集仅供 Oracle Solaris 软件的 Trusted Extensions 功能使用。通过使用 `clzonecluster` 命令或 `clsetup` 实用程序可以创建区域群集。您可以使用 Oracle Solaris Zones 提供的隔离功能，在类似于全局群集的区域群集上运行受支持的服务。有关更多信息，请参见Unresolved link to " Oracle Solaris Cluster 软件安装指南 中的创建和配置区域群集"和Unresolved link to " Oracle Solaris Cluster 系统管理指南 中的使用区域群集"。
- 与群集控制台的安全连接 – 必须与群集节点的控制台建立安全 shell 连接。有关 `pconsole` 实用程序的更多信息，请参见Unresolved link to " Oracle Solaris Cluster 系统管理指南 中的如何安全地连接到群集控制台"。
- Common Agent Container – Oracle Solaris Cluster Manager 使用强大的加密技术确保每个群集节点上 Oracle Solaris Cluster 管理栈之间的安全通信。有关更多信息，请参见Unresolved link to " Oracle Solaris Cluster 系统管理指南 中的故障排除"。
- 日志记录 – Oracle Solaris Cluster 使用 Unresolved link to " syslogd1M" 命令记录错误和状态消息。确保设置 `/etc/syslog.conf` 文件以控制存储消息的位置。还可以安全地保护日志文件，例如 `/var/adm/messages` 文件。有关更多信息，请参见Unresolved link to " Oracle Solaris Cluster 系统管理指南 中的管理群集"。
- 审计 – 默认情况下启用 Oracle Solaris Cluster，因为它位于 Oracle Solaris OS 中。审计在 `/var/cluster/logs/commandlog` 文件中存储所有执行的命令，您应该根据需要对文件设置保护。有关更多信息，请参见Unresolved link to " Oracle Solaris Cluster 系统管理指南 中的如何查看 Oracle Solaris Cluster 命令日志的内容"。
- Oracle Solaris OS 强化 – Oracle Solaris Cluster 使用安全强化技术将 Oracle Solaris OS 重新配置为强化状态。此外，它还激活 Oracle Solaris 系统审计。

# 开发者需要注意的安全事项

本节提供对使用 Oracle Solaris Cluster 生成应用程序的开发者有用的信息。开发者使用 Oracle Solaris Cluster API。有关更多信息，请参见Unresolved link to " Oracle Solaris Cluster Concepts Guide 中的第 3 章 Key Concepts for System Administrators and Application Developers"。

开发者创建的代理应用程序应该在产品的安全框架内工作并考虑以下安全功能：

- Oracle Solaris Cluster 支持大量应用程序代理，这些代理作为一组回调方法来实现，以控制应用程序的开始、停止、探测和验证。`Start`、`Stop` 或 `Validate` 等回调方法始终以 root 用户身份运行。如果这些可执行方法文件中的一个可由非 root 用户写入，这会造成漏洞，其中此类非 root 用户可以通过向回调方法插入代码来获得未经授权的特权提升。Oracle Solaris Cluster 检查此类回调方法可执行文件的所有权和权限。该检查由 `resource_security` 群集属性设置来控制。如果 `resource_security` 设置为 `SECURE` 并且发现方法代码可由非 root 用户写入，则方法执行将失败。

  反过来，代理方法经常运行外部程序，例如应用程序特定的管理命令。代理方法应该使用包装器运行所有此类外部程序，以确保使用最小的可能权限执行外

部程序。Oracle Solaris Cluster 提供 `application_user` 和 `resource_security` 属性以及 `scha_check_app_user` API 来启用数据服务，以确保安全执行应用程序。可以在脚本中调用 `scha_check_app_user` 命令来针对配置的 `Application_user` 和 `Resource_security` 设置验证用户名。有关信息，请参见 Unresolved link to " scha_check_app_user1HA " 手册页、Unresolved link to " r_properties5" 手册页和 Unresolved link to " cluster1CL" 手册页。

- 对应用程序的安全访问 – 您发出管理或配置命令时，一些情况需要对应用程序的安全访问。此安全访问应通过基于凭证的方法（例如 Oracle Wallet Manager）进行。如果必须提供密码，该密码应安全使用并以混乱的形式存储。例如，不应该通过 Unresolved link to " ps1" 命令在对用户可见的命令行上传递该密码。Oracle Solaris Cluster 提供 `clpstring` 命令来允许您创建专用字符串，可以使用这些字符串在群集中安全存储编码的密码并在必须使用密码执行管理任务时检索这些字符串。有关此命令的信息，请参见 Unresolved link to " clpstring1CL" 手册页。

有关开发数据服务时如何使用这些安全功能的更多信息，请参见Unresolved link to " Oracle Solaris Cluster Data Services Developer’s Guide "。

# 索引


A
安全性
  一般原则，9
  开发者需要注意的安全事项，14
安装，10

C
claccess 命令，13
clsetup 实用程序，13

D
对应用程序的安全访问，15

G
概述
  Oracle Solaris Cluster，9

K
开发者
  安全注意事项，14

O
Oracle Solaris Cluster
  安全性，9
  概述，9
OS 强化，14

P
配置，13
pconsole
  实用程序，14

Q
区域群集，10，14
全局群集，10
群集
  安全功能，13
  安装，10
  配置，13

R
日志记录，14
软件包，10
RBAC，13

S
审计，14

T
添加节点，13
Trusted Extensions，13

Y
与群集控制台的安全连接，14

Z
支持的标记
  solaris, solaris10, 有标签，14
自动化安装程序，10