

Oracle® Solaris Cluster 4.3 安全指南

ORACLE®

文件号码 E62326
2015 年 10 月

文件号码 E62326

版权所有 © 2000, 2015, 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，则适用以下注意事项：

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，并按许可协议的规定使用。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。除非您与 Oracle 签订的相应协议另行规定，否则对于第三方内容、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保证，亦不对其承担任何责任。除非您和 Oracle 签订的相应协议另行规定，否则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。

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=dacc>。

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
Geographic Edition 和安全性概述	10
一般安全原则	10
安全安装和配置 Oracle Solaris Cluster	11
保证 Geographic Edition 安装和配置安全	11
Oracle Solaris Cluster 安全功能	12
Geographic Edition 安全功能	13
开发者需要注意的安全事项	14
索引	15

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

有关该产品及相关产品的文档和资源，可从以下网址获得：<http://www.oracle.com/pls/topic/lookup?ctx=E62283>。

反馈

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

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。本指南概述了 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需要注意的安全事项。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。

Geographic Edition 软件是 Oracle Solaris Cluster 软件的一个分层扩展。Geographic Edition 框架使用多个地理上远距离分开的群集来防止应用程序发生意外中断。这些群集包含 Geographic Edition 基础结构的副本，可管理群集间复制的数据。

本章包括以下各节：

- [“Oracle Solaris Cluster 和安全性概述” \[9\]](#)
- [“Geographic Edition 和安全性概述” \[10\]](#)
- [“一般安全原则” \[10\]](#)
- [“安全安装和配置 Oracle Solaris Cluster” \[11\]](#)
- [“保证 Geographic Edition 安装和配置安全” \[11\]](#)
- [“Oracle Solaris Cluster 安全功能” \[12\]](#)
- [“Geographic Edition 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 [《Oracle Solaris 11 安全和强化准则》](#) 和 [《在 Oracle Solaris 11.3 中确保系统和连接设备的安全》](#)。

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《[Oracle Solaris Cluster 4.3 Concepts Guide](#)》。

Geographic Edition 和安全性概述

Geographic Edition 软件是 Oracle Solaris Cluster 软件的一个分层扩展。利用数据复制软件，在 Geographic Edition 群集上运行的应用程序可以通过将服务迁移到地理上分开的辅助群集来承受灾难。诸如地震、火灾或风暴之类的灾难可能会让主站点的群集失能。

灾难发生时，Geographic Edition 群集可以通过使用以下各级别的冗余继续提供服务：

- 辅助群集
- 辅助群集上的复制应用程序配置
- 辅助群集上的复制数据

Geographic Edition 软件提供了一套工具，可通过在站点间迁移服务来管理和配置地理上分开的群集。群集可以是全局群集、区域群集或者两者的组合。Geographic Edition 软件可以通过稳健的安全性、应用程序服务迁移以及数据复制来管理多个物理位置的可用性，从而可在整个企业系统承受灾难。

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 Oracle Solaris Cluster

本节提供了用于规划和执行 Oracle Solaris Cluster 安全安装和配置的连接。

- **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《[Oracle Solaris Cluster 4.3 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。
要查看 Oracle Solaris Cluster 核心、数据服务和 Geographic Edition 软件包的列表，请参见《[Oracle Solaris Cluster 4.3 Package Group Lists](#)》。
- **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《[Oracle Solaris Cluster 4.3 软件安装指南](#)》中的第 3 章“建立全局群集”、《[Oracle Solaris Cluster 4.3 软件安装指南](#)》中的第 6 章“创建区域群集”和《[Oracle Solaris Cluster 4.3 系统管理指南](#)》中的第 1 章“Oracle Solaris Cluster 管理介绍”。
对于建立全局群集节点的所有方法，需要先对一个指定的发起节点进行授权，仅允许该指定的系统访问其将配置的节点。如果需要，可以使用 DES 加密以实现更安全的配置。有关更多信息，请参见 [clauth\(1CL\)](#) 手册页。
- **Common Agent Container 漏洞** – 组合使用 Common Agent Container 和一些早期 Java 版本会在 Oracle Solaris Cluster 软件中产生安全漏洞。有关确定系统是否具有此漏洞以及如何更正该漏洞的信息，请参见 My Oracle Support 参考文档《[CVE-2014-3566 Instructions to Mitigate the SSL v3.0 Vulnerability \(aka "Poodle Attack"\) in Oracle Solaris Cluster \(Doc ID 1999997.1\)](#)》 (<https://support.oracle.com/epmos/faces/DocumentDisplay?id=1999997.1&displayIndex=1>) (《[CVE-2014-3566 在 Oracle Solaris 中减轻 SSL v3.0 漏洞 \(也称为“Poodle 攻击”\) 的说明 \(文档 ID 1999997.1\)](#)》)。需要登录 My Oracle Support 才能访问此文档。
- **使用 Kerberos V5 保护 HA for NFS** – 如果需要保护对由 HA for NFS 数据服务管理的 NFS 服务的访问，可以配置 Kerberos V5 客户机来保护 HA for NFS 数据服务。这包括在所有群集节点上的逻辑主机名上添加 NFS 的 Kerberos 主体。有关更多信息，请参见《[Oracle Solaris Cluster Data Service for NFS Guide](#)》中的“Securing HA for NFS With Kerberos V5”。

保证 Geographic Edition 安装和配置安全

本部分提供了有关规划和执行 Geographic Edition 软件的安全安装和配置的连接。

- **安装** – Geographic Edition 软件必须安装在运行 Oracle Solaris 操作系统和 Oracle Solaris Cluster 软件的群集上。使用 Oracle Solaris 自动化安装程序 (Automated Installer, AI) 在安装 Oracle Solaris Cluster 软件的同时安装 Geographic Edition 软件，也可以在以后的任何时间安装该软件。Geographic Edition 框架配置与 Oracle Solaris Cluster 软件配置完全相同。请参见《[Oracle Solaris Cluster 4.3 Geographic Edition Installation and Configuration Guide](#)》中的第 2 章“Installing and Configuring the Geographic Edition Software”。

- **Geographic Edition 软件包** – Geographic Edition 软件包使用 Oracle Solaris 映像包管理系统 (Image Packaging System, IPS) 软件包名称。要查看软件包列表，请参见《[Oracle Solaris Cluster 4.3 Package Group Lists](#)》。
- **配置** – 可以在运行 Geographic Edition 框架的群集上执行所有管理任务，不会导致任何节点或群集发生故障。可以在可运转的群集上安装、配置、启动、使用、停止和卸载 Geographic Edition 软件。请参见《[Oracle Solaris Cluster 4.3 Geographic Edition System Administration Guide](#)》中的第 4 章“Administering RBAC”。

Oracle Solaris Cluster 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。您必须是具有 User Security (用户安全) 权限配置文件的系统管理员，才能够更改角色的大多数安全属性。有关更多信息，请参见《[在 Oracle Solaris 11.3 中确保用户和进程的安全](#)》中的“管理权限的使用”和《[Oracle Solaris Cluster 4.3 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《[Oracle Solaris Cluster 4.3 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 `claccess(1CL)` 手册页和《[在 Oracle Solaris 11.3 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《[Oracle Solaris Cluster 4.3 软件安装指南](#)》中的“[区域群集中使用 Trusted Extensions 的准则](#)”和《[Oracle Solaris Cluster 4.3 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` 标记、`solaris10` 标记或 `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《[Oracle Solaris Cluster 4.3 软件安装指南](#)》中的“[创建和配置区域群集](#)”和《[Oracle Solaris Cluster 4.3 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《Oracle Solaris Cluster 4.3 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 GUI 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《Oracle Solaris Cluster 4.3 系统管理指南》中的“排除 Oracle Solaris Cluster Manager 的故障”。
- 日志记录 – Oracle Solaris Cluster 软件使用 syslogd 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《Oracle Solaris Cluster 4.3 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《Oracle Solaris Cluster 4.3 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。

Geographic Edition 安全功能

本部分包含有关 Geographic Edition 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) – Geographic Edition 软件将其 RBAC 配置文件基于在 Oracle Solaris Cluster 软件中使用的 RBAC 权限配置文件。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。承担 root 角色以及使用 RBAC 角色 solaris.cluster.geo.modify、solaris.cluster.geo.admin 和 solaris.cluster.geo.read 访问群集。有关更多信息，请参见《在 Oracle Solaris 11.3 中确保用户和进程的安全》和《Oracle Solaris Cluster 4.3 Geographic Edition System Administration Guide》中的“Modifying a User's RBAC Properties”。
- 安全证书 – 在安装过程中，通过使用安全证书为群集配置安全群集通信（同一个群集中的节点必须共享同一个安全证书）。Geographic Edition 合作伙伴关系中群集间的通信安全通过 Java Management Extensions (JMX) 端口以及使用安全证书的安全套接字层 (Secure Sockets Layer, SSL) 实现。有关更多信息，请参见《Oracle Solaris Cluster 4.3 Geographic Edition Installation and Configuration Guide》中的“Configuring Trust Between Partner Clusters”。
- Common Agent Container – 要使区域群集具有 Oracle Solaris Cluster 伙伴关系成员的功能，必须在区域群集中手动配置 Common Agent Container。有关更多信息，请参见《Oracle Solaris Cluster 4.3 Geographic Edition Installation and Configuration Guide》中的“Preparing a Zone Cluster for Partner Membership”。

- IP 安全体系结构 (IP Security Architecture, IPsec) – 使用 IPsec 配置伙伴群集间的安全 TCP/UDP 心跳通信。有关更多信息，请参见《[Oracle Solaris Cluster 4.3 Geographic Edition Installation and Configuration Guide](#)》中的“Securing Inter-Cluster Communication”。

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《[Oracle Solaris Cluster 4.3 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：

- 代理回调方法 – 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 [scha_check_app_user\(1HA\)](#)、[r_properties\(5\)](#) 和 [cluster\(1CL\)](#) 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 ps 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 [clpstring\(1CL\)](#) 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《[Oracle Solaris Cluster Data Services Developer's Guide](#)》。

索引

A

安全

- 安装 Geographic Edition , 11
- 证书, 13

- 安全功能, 13

安全性

- 一般原则, 9

- 开发者需要注意的安全事项, 14

- 安装, 11

C

- claccess 命令, 12

- clauth 命令, 11

- clsetup 实用程序, 12

- Common Agent Container , 13

D

- 带标签的标记区域群集, 12

- 对应用程序的安全访问, 14

G

概述

- Oracle Solaris Cluster , 9

- Oracle Solaris Cluster Geographic Edition , 10

I

- IPsec , 14

K

- 开发者

- 安全注意事项, 14

O

- Oracle Solaris Cluster

 - 安全性, 9

 - 概述, 9

- Oracle Solaris Cluster Geographic Edition

 - 优势, 10

 - 安装, 11

 - 概述, 10

 - 配置, 11

- OS 强化, 13

P

- 配置, 11, 12

- pconsole 实用程序, 13

Q

- 区域群集, 10

 - Geographic Edition , 10

 - Trusted Extensions , 12

 - 带标签的标记, 12

- 全局群集, 10, 10

群集

 - 安全功能, 12

 - 安装, 11

 - 配置, 11

R

- 日志记录, 13

- 软件包

Oracle Solaris Cluster , 11
Oracle Solaris Cluster Geographic Edition , 12
RBAC , 12 , 13

S

审计 , 13
数据复制 , 10

T

添加节点 , 12
Trusted Extensions , 12

Y

与群集控制台的安全连接 , 13

Z

灾难恢复 , 10
自动化安装程序 , 11 , 11