

Oracle® Solaris Cluster 3.3 5/11 Security Guide

Copyright © 2000, 2011, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related software documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. UNIX is a registered trademark licensed through X/Open Company, Ltd.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Ce logiciel et la documentation qui l'accompagne sont protégés par les lois sur la propriété intellectuelle. Ils sont concédés sous licence et soumis à des restrictions d'utilisation et de divulgation. Sauf disposition de votre contrat de licence ou de la loi, vous ne pouvez pas copier, reproduire, traduire, diffuser, modifier, breveter, transmettre, distribuer, exposer, exécuter, publier ou afficher le logiciel, même partiellement, sous quelque forme et par quelque procédé que ce soit. Par ailleurs, il est interdit de procéder à toute ingénierie inverse du logiciel, de le désassembler ou de le décompiler, excepté à des fins d'interopérabilité avec des logiciels tiers ou tel que prescrit par la loi.

Les informations fournies dans ce document sont susceptibles de modification sans préavis. Par ailleurs, Oracle Corporation ne garantit pas qu'elles soient exemptes d'erreurs et vous invite, le cas échéant, à lui en faire part par écrit.

Si ce logiciel, ou la documentation qui l'accompagne, est concédé sous licence au Gouvernement des Etats-Unis, ou à toute entité qui délivre la licence de ce logiciel ou l'utilise pour le compte du Gouvernement des Etats-Unis, la notice suivante s'applique :

U.S. GOVERNMENT RIGHTS. Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

Ce logiciel ou matériel a été développé pour un usage général dans le cadre d'applications de gestion des informations. Ce logiciel ou matériel n'est destiné à être utilisé dans des applications à risque, notamment dans des applications pouvant causer des dommages corporels. Si vous utilisez ce logiciel ou matériel dans le cadre d'applications dangereuses, il est de votre responsabilité de prendre toutes les mesures de secours, de sauvegarde, de redondance et autres mesures nécessaires à son utilisation dans des conditions optimales de sécurité. Oracle Corporation et ses affiliés déclinent toute responsabilité quant aux dommages causés par l'utilisation de ce logiciel ou matériel pour ce type d'applications.

Oracle et Java sont des marques déposées d'Oracle Corporation et/ou de ses affiliés. Tout autre nom mentionné peut correspondre à des marques appartenant à d'autres propriétaires qu'Oracle.

AMD, Opteron, le logo AMD et le logo AMD Opteron sont des marques ou des marques déposées d'Advanced Micro Devices. Intel et Intel Xeon sont des marques ou des marques déposées d'Intel Corporation. Toutes les marques SPARC sont utilisées sous licence et sont des marques ou des marques déposées de SPARC International, Inc. UNIX est une marque déposée concédée sous licence par X/Open Company, Ltd.

Contents

- Preface5**
- 1 Introduction to Oracle Solaris Cluster Security 7**
 - Overview of Oracle Solaris Cluster and Security7
 - General Security Principles8
 - Secure Installation and Configuration8
 - Security Features8
 - Security Considerations for Developers 10
- Index11**

Preface

The *Oracle Solaris Cluster Security Guide* contains conceptual information about the Oracle Solaris Cluster software product.

How This Book Is Organized

The *Oracle Solaris Cluster Security Guide* contains the following chapter:

- [Chapter 1, “Introduction to Oracle Solaris Cluster Security,”](#) provides an overview of the overall concepts that you need to know about Oracle Solaris Cluster security.

Related Documentation

Information about related Oracle Solaris Cluster topics is available in the documentation that is listed in the following table. All Oracle Solaris Cluster documentation is available at <http://www.oracle.com/technetwork/indexes/documentation/index.html>.

Topic	Documentation
Concepts	<i>Oracle Solaris Cluster Concepts Guide</i>
Hardware installation and administration	<i>Oracle Solaris Cluster 3.3 Hardware Administration Manual</i> and individual hardware administration guides
Software installation	<i>Oracle Solaris Cluster Software Installation Guide</i>
Data service installation and administration	<i>Oracle Solaris Cluster Data Services Planning and Administration Guide</i> and individual data service guides
Data service development	<i>Oracle Solaris Cluster Data Services Developer’s Guide</i>
System administration	<i>Oracle Solaris Cluster System Administration Guide</i> <i>Oracle Solaris Cluster Quick Reference</i>
Software upgrade	<i>Oracle Solaris Cluster Upgrade Guide</i>
Error messages	<i>Oracle Solaris Cluster Error Messages Guide</i>

Topic	Documentation
Command and function references	<i>Oracle Solaris Cluster Reference Manual</i>
	<i>Oracle Solaris Cluster Data Services Reference Manual</i>

For a complete list of Oracle Solaris Cluster documentation, see the release notes for your version of Oracle Solaris Cluster software.

Documentation, Support, and Training

See the following web sites for additional resources:

- [Documentation](http://www.oracle.com/technetwork/indexes/documentation/index.html) (<http://www.oracle.com/technetwork/indexes/documentation/index.html>)
- [Support](http://www.oracle.com/us/support/systems/index.html) (<http://www.oracle.com/us/support/systems/index.html>)
- [Training](http://education.oracle.com) (<http://education.oracle.com>) – Click the Sun link in the left navigation bar.

Oracle Welcomes Your Comments

Oracle welcomes your comments and suggestions on the quality and usefulness of its documentation. If you find any errors or have any other suggestions for improvement, go to <http://www.oracle.com/technetwork/indexes/documentation/index.html> and click Feedback. Indicate the title and part number of the documentation along with the chapter, section, and page number, if available. Please let us know if you want a reply.

Oracle Technology Network (<http://www.oracle.com/technetwork/index.html>) offers a range of resources related to Oracle software:

- Discuss technical problems and solutions on the [Discussion Forums](http://forums.oracle.com) (<http://forums.oracle.com>).
- Get hands-on step-by-step tutorials with [Oracle By Example](http://www.oracle.com/technetwork/tutorials/index.html) (<http://www.oracle.com/technetwork/tutorials/index.html>).
- Download [Sample Code](http://www.oracle.com/technology/sample_code/index.html) (http://www.oracle.com/technology/sample_code/index.html).

Introduction to Oracle Solaris Cluster Security

The Oracle Solaris Cluster product is an integrated hardware and software solution that you use to create highly available and scalable services. The *Oracle Solaris Cluster Security Guide* provides an overview of security in Oracle Solaris Cluster, information on secure installations and configuration, security features, and security considerations for developers. Use this book with the entire Oracle Solaris Cluster documentation set to provide a complete view of the Oracle Solaris Cluster software.

This chapter contains the following sections:

- [“Overview of Oracle Solaris Cluster and Security” on page 7](#)
- [“Secure Installation and Configuration” on page 8](#)
- [“Security Features” on page 8](#)
- [“Security Considerations for Developers” on page 10](#)

Overview of Oracle Solaris Cluster and Security

The Oracle Solaris Cluster environment extends the Oracle Solaris Operating System into a cluster operating system. A cluster is a collection of one or more nodes that belong exclusively to that collection.

The benefits of the Oracle Solaris Cluster software include the following:

- Reduce or eliminate system downtime because of software or hardware failure
- Ensure availability of data and applications to end users, regardless of the kind of failure that would normally take down a single-server system
- Increase application throughput by enabling services to scale to additional processors by adding nodes to the cluster and balancing load
- Provide enhanced availability of the system by enabling you to perform maintenance without shutting down the entire cluster

A cluster offers several advantages over traditional single-server systems. These advantages include support for failover and scalable services, capacity for modular growth, the ability to set load limits on nodes, and low entry price compared to traditional hardware fault-tolerant systems.

In a cluster that runs on the Oracle Solaris OS, a *global cluster* and a *zone cluster* are types of clusters. Clusters can be global clusters, zone clusters, or a combination of both. To learn more about the benefits of configuring a zone cluster, see [Oracle Solaris Cluster Concepts Guide](#).

General Security Principles

The following principles are fundamental to using the Oracle Solaris Cluster application securely.

- Keep software up to date
- Restrict network access to critical services
- Follow the principle of least privilege
- Monitor system activity
- Keep up to date on the latest Oracle security information

Secure Installation and Configuration

This section provides links for planning and executing a secure installation and configuration of Oracle Solaris Cluster.

- Installation – You can install the use the Oracle Solaris Cluster software by using the `scinstall` utility, XML, or JumpStart. For more information, see [“Installing the Software” in Oracle Solaris Cluster Software Installation Guide](#).
- Configuration – You can configure and administer a global cluster and a zone cluster. For more information, see [Chapter 1, “Introduction to Administering Oracle Solaris Cluster,” in Oracle Solaris Cluster System Administration Guide](#).

Security Features

This section contains information about specific security mechanisms offered by Oracle Solaris Cluster.

A secure installation uses the following critical security features:

- Role-Based Access Control (RBAC) – If you are not a superuser, use the RBAC roles of `solaris.cluster.modify`, `solaris.cluster.admin`, and `solaris.cluster.read` to access the cluster. For more information, see [“Oracle Solaris Cluster RBAC Rights Profiles” in Oracle Solaris Cluster System Administration Guide](#).

- IP Security Architecture (IPsec) – Configure IPsec for the `clprivnet` interface to provide secure TCP/IP communication on the cluster interconnect. For more information, see [“How to Configure IP Security Architecture \(IPsec\) on the Cluster Private Interconnect”](#) in *Oracle Solaris Cluster Software Installation Guide*.
- New Nodes – Use the `claccess` command or `clsetup` utility with superuser privileges to add a node to a cluster. For more information, see [Chapter 8, “Adding and Removing a Node,”](#) in *Oracle Solaris Cluster System Administration Guide*.
- Trusted Extensions – The Oracle Solaris Trusted Extensions feature can be enabled for use in a zone cluster. For more information, see [“Guidelines for Trusted Extensions in a Zone Cluster”](#) in *Oracle Solaris Cluster Software Installation Guide* and [“How to Prepare for Trusted Extensions Use With Zone Clusters”](#) in *Oracle Solaris Cluster Software Installation Guide*.
- Zone Clusters – A zone cluster is a cluster of non-global Oracle Solaris Container zones. All nodes of a zone cluster are configured as non-global zones of the cluster brand. For more information, see [“Configuring a Zone Cluster”](#) in *Oracle Solaris Cluster Software Installation Guide* and [“Working With a Zone Cluster”](#) in *Oracle Solaris Cluster System Administration Guide*.
- Secure Connections to Cluster Consoles – You must establish secure shell connections to the consoles of the cluster nodes. For more information, see [“How to Connect Securely to Cluster Consoles”](#) in *Oracle Solaris Cluster System Administration Guide*.
- Common Agent Container – Oracle Solaris Cluster Manager uses strong encryption techniques to ensure secure communication between the Oracle Solaris Cluster Manager web server and each cluster node. For more information, see [“How to Regenerate Common Agent Container Security Keys”](#) in *Oracle Solaris Cluster System Administration Guide* and [“How to Use the Common Agent Container to Change the Port Numbers for Services or Management Agents”](#) in *Oracle Solaris Cluster System Administration Guide*.
- Logging – Oracle Solaris Cluster uses the `syslogd(1M)` command to record error and status messages. Ensure that you set up the `/etc/syslog.conf` file to control where the messages are stored. You should also securely protect the log files, such as the `/var/adm/messages` file. For more information, see [“Beginning to Administer the Cluster”](#) in *Oracle Solaris Cluster System Administration Guide*.
- Auditing – Oracle Solaris Cluster stores all executed commands in the `/var/cluster/logs/commandlog` file, and you should set the protections on the file as appropriate. For more information, see [“How to View the Contents of Oracle Solaris Cluster Command Logs”](#) in *Oracle Solaris Cluster System Administration Guide*.
- Oracle Solaris Operating System (OS) Hardening – Oracle Solaris Cluster uses security hardening techniques to reconfigure the Solaris OS into a hardened state. Additionally, it can activate the Oracle Solaris system audit. Oracle's Solaris Security Toolkit, formerly known as the JumpStart Architecture and Security Scripts (JASS) Toolkit, can be used to secure SPARC-based and x86/x64-based systems. For more information, see the [Solaris Security Toolkit \(http://www.oracle.com/technetwork/systems/tools/products/index-jsp-142740.html\)](http://www.oracle.com/technetwork/systems/tools/products/index-jsp-142740.html).

Security Considerations for Developers

This section provides information useful to developers producing applications that use Oracle Solaris Cluster. Developers use the Oracle Solaris Cluster API and Oracle's Sun Developer's Toolkit (SDK). For more information, see [Chapter 3, “Key Concepts for System Administrators and Application Developers,”](#) in *Oracle Solaris Cluster Concepts Guide*.

The agent applications that developers create should work within the security framework of the product and consider the following security features:

- **Superuser and Root User Access**— Oracle Solaris Cluster uses superuser privileges to control starting, stopping, and probing of Data Service agents. All programs and scripts that are directly executed by an agent must be owned by the root user. If a program or script executable file is owned by a non-root user, that user could create a “back door” to access the system.

If it is necessary to run an application under Oracle Solaris Cluster control as a non-root user, the agent software should verify security and run the application as the required user. The Apache web server agent is an example of this type of application.

- **Secure Access to an Application** – Some cases will require secure access to an application when you issue management or configuration commands. This secure access should be done with a credential-based method, such as the Oracle Wallet Manager. If you must supply a password, the password should be securely used and stored in an obfuscated form. For example, it should not be passed on the command line where it is visible to a user through the `ps(1)` command.

Index

A

adding nodes, 9

C

claccess command, 9

clsetup utility, 9

cluster

- configuration, 8

- installation, 8

- security features, 8–9

common agent container, 9

configuration, 8

D

developers, security considerations for, 10

G

global cluster, 8

I

installation, 8

IPsec, 9

O

Oracle Solaris Cluster

- overview, 7–8

- security, 7–8

overview, Oracle Solaris Cluster, 7–8

R

RBAC, 8

root access, 10

S

secure access to an application, 10

secure connections to cluster consoles, 9

security

- considerations for developers, 10

- general principles, 7–8

superuser access, 10

T

Trusted Extensions, 9

Z

zone cluster, 8, 9

