Oracle® Solaris Cluster 3.3 5/11 Security Guide

Part No: E23166
May 2011, Revision A

ORACLE

130129@25097

Contents

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	*Oracle Solaris Cluster Concepts Guide*
Hardware installation and administration	*Oracle Solaris Cluster 3.3 Hardware Administration Manual* and individual hardware administration guides
Software installation	*Oracle Solaris Cluster Software Installation Guide*
Data service installation and administration	*Oracle Solaris Cluster Data Services Planning and Administration Guide* and individual data service guides
Data service development	*Oracle Solaris Cluster Data Services Developer's Guide*
System administration	*Oracle Solaris Cluster System Administration Guide*
	Oracle Solaris Cluster Quick Reference
Software upgrade	*Oracle Solaris Cluster Upgrade Guide*
Error messages	*Oracle Solaris Cluster Error Messages Guide*

Topic	Documentation
Command and function references	*Oracle Solaris Cluster Reference Manual* *Oracle Solaris Cluster Data Services Reference Manual*

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`)
- Support (`http://www.oracle.com/us/support/systems/index.html`)
- Training (`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`).
- Get hands-on step-by-step tutorials with Oracle By Example (`http://www.oracle.com/technetwork/tutorials/index.html`).
- Download Sample Code (`http://www.oracle.com/technology/sample_code/index.html`).

◆ ◆ ◆ CHAPTER 1

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

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`).

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