Oracle® Solaris Cluster Security Guide

Part No: E23622
March 2012, E23622-02

ORACLE

120416@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
Hardware installation and administration	*Oracle Solaris Cluster 4.0 Hardware Administration Manual* Individual hardware administration guides
Concepts	*Oracle Solaris Cluster Concepts Guide*
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
	Oracle Solaris Cluster Geographic Edition Reference Manual
	Oracle Solaris Cluster Quorum Server Reference Manual

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` or visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` if you are hearing impaired.

Getting Help

If you have problems installing or using Oracle Solaris Cluster software, contact your service provider and provide the following information:

- Your name and email address (if available)
- Your company name, address, and phone number
- The model and serial numbers of your systems
- The release number of the operating system (for example, Oracle Solaris 11)
- The release number of the Oracle Solaris Cluster software (for example, 4.0)
- The contents of the `/var/cacao/instances/default/logs/cacao.0/1/2` file

Also have available the contents of the `/var/adm/messages` file.

◆ ◆ ◆ 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 Oracle Solaris Cluster software with the Oracle Solaris 11 Automated Installer (AI) . For more information, see "Installing the Software" in *Oracle Solaris Cluster Software Installation Guide*.
- Secure cluster packages – Oracle Solaris Cluster packages now use Oracle Solaris Image Packaging System (IPS) package names. To see a list of the Oracle Solaris Cluster Geographic Edition 4.0 packages, see *Oracle Solaris Cluster Geographic Edition 4.0 Security Guide*. The following tables lists the core packages and data services packages that were included with Oracle Solaris Cluster 4.0.

Previous Core Cluster Package Name	New IPS Package Name	Description
SUNWscdsbuilder	ha-cluster/developer/agent-builder	Oracle Solaris Cluster Agent Builder
SUNWscdev	ha-cluster/developer/api	Oracle Solaris Cluster developer software
SUNWsccacao	ha-cluster/library/cacao	Oracle Solaris Cluster Common Cacao Support

Previous Core Cluster Package Name	New IPS Package Name	Description
SUNWscucm	ha-cluster/library/ucmm	Oracle Solaris Cluster UCMM reconfiguration interface
SUNWcsc, SUNWesc, SUNWfsc, SUNWjsc	ha-cluster/locale	Localization for Oracle Solaris Cluster messages
SUNWscnmr, SUNWscnmu	ha-cluster/release/name	Oracle Solaris Cluster name
SUNWscmasar, SUNWscmasazu, SUNWscmautil, SUNWscmautilr	ha-cluster/service/management	Oracle Solaris Cluster Manageability and Serviceability Agent
SUNWscmasasen	ha-cluster/service/management/slm	Oracle Solaris Cluster Manageability Agent for Service Level Management
SUNWscqsr, SUNWscqsu	ha-cluster/service/quorum-server	Oracle Solaris Cluster Quorum Server
SUNWscqsman	ha-cluster/service/quorum-server/manual	Oracle Solaris Cluster Quorum Server Manual Pages
SUNWcscqsu, SUNWjscqsu	ha-cluster/service/quorum-server/locale	Localization for Oracle Solaris Cluster Quorum Server
SUNWjscqsman	ha-cluster/service/quorum-server/manual/locale	Localization for Oracle Solaris Cluster Quorum Server Manual Pages
SUNWscmasa, SUNWscmasau	ha-cluster/system/dsconfig-wizard	Oracle Solaris Cluster Data Service Configuration Wizard
SUNWscr, SUNWscu, SUNWsczr, SUNWsczu, SUNWsccomu, SUNWsccomzu	ha-cluster/system/core	Oracle Solaris Cluster software
SUNWscsckr, SUNWscscku	ha-cluster/system/cfgchk	Oracle Solaris Cluster configuration checks
SUNWscman	ha-cluster/system/manual	Oracle Solaris Cluster Manual Pages
SUNWjscman	ha-cluster/system/manual/locale	Localization for Oracle Solaris Cluster Manual Pages
SUNWmdmr, SUNWmdmu	ha-cluster/storage/svm-mediator	Solaris Volume Manager (Mediator)
SUNWscrtlh	ha-cluster/ha-service/ logical-hostname	Oracle Solaris Cluster Resource Type for Logical Hostname

Previous Core Cluster Package Name	New IPS Package Name	Description
SUNWscgds	ha-cluster/ha-service/gds	Oracle Solaris Cluster Generic data Service
SUNWscderby	ha-cluster/ha-service/derby	Derby Oracle Solaris Cluster Agent
SUNWscsmf	ha-cluster/ha-service/smf-proxy	Oracle Solaris Cluster SMF proxy methods
SUNWsctelemetry	ha-cluster/ha-service/telemetry	Oracle Solaris Cluster telemetry agent
ha-cluster-framework-full	ha-cluster/group-package/ha-cluster-framework-full	Oracle Solaris Cluster Framework full group package
ha-cluster-framework-l10n	ha-cluster/group-package/ha-cluster-framework-l10n	Oracle Solaris Cluster Framework Localization group package
ha-cluster-framework-minimal	ha-cluster/group-package/ha-cluster-framework-minimal	Oracle Solaris Cluster Framework minimal group package
ha-cluster-framework-scm	ha-cluster/group-package/ha-cluster-framework-scm	Oracle Solaris Cluster Framework Oracle Solaris Cluster Manager components group package
ha-cluster-framework-slm	ha-cluster/group-package/ha-cluster-framework-slm	Oracle Solaris Cluster Framework Service Level Management (SLM) components group package
ha-cluster-full	ha-cluster/group-package/ha-cluster-full	Oracle Solaris Cluster full installation group package
ha-cluster-incorporation	ha-cluster/group-package/ha-cluster-incorporation	Oracle Solaris Cluster incorporation package
ha-cluster-minimal	ha-cluster/group-package/ha-cluster-minimal	Oracle Solaris Cluster minimal installation group package
ha-cluster-quorum-server-full	ha-cluster/group-package/ha-cluster-quorum-server-full	Oracle Solaris Cluster Quorum Server full group package
ha-cluster-quorum-server-l10n	ha-cluster/group-package/ha-cluster-quorum-server-l10n	Oracle Solaris Cluster Quorum Server Localization group package

Additional data service agents will be supported after the Oracle Solaris Cluster 4.0 release. Check the *Oracle Solaris Cluster 4.0 Release Notes* for those agents. The following table lists the supported data services packages for Oracle Solaris Cluster 4.0.

Previous Data Service Package Name	New IPS Package Name	Description
SUNWscapc	ha-cluster/data-service/apache	Oracle Solaris Cluster Apache Web Server Component
SUNWscdhc	ha-cluster/data-service/dhcp	Oracle Solaris Cluster HA for DHCP
SUNWscdns	ha-cluster/data-service/dns	Oracle Solaris Cluster Domain Name Server Component
SUNWscxvm	ha-cluster/data-service/ha-ldom	Oracle Solaris Cluster HA for xVM x86-64/SPARC Guest Domains
SUNWsczone	ha-cluster/data-service/ha-zones	Oracle Solaris Cluster HA for Solaris Containers
SUNWscnfs	ha-cluster/data-service/nfs	Oracle Solaris Cluster NFS Server Component
SUNWscor	ha-cluster/data-service/oracle-database	Oracle Solaris Cluster HA Oracle data service
SUNWsctomcat	ha-cluster/data-service/tomcat	Oracle Solaris Cluster HA for Apache Tomcat
SUNWscwls	ha-cluster/data-service/weblogic	Oracle Solaris Cluster HA for Oracle WebLogic Server
SUNWscdsman	ha-cluster/system/manual/data-services	Oracle Solaris Cluster Data Services online manual pages
ha-cluster-data-services-full	ha-cluster/group-package/ha-cluster-data-services-full	Oracle Solaris Cluster Data Services full group package

- 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*.

- 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*.
- 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 `solaris` brand that are set with the `cluster` attribute. No other brand type is permitted in a zone cluster. You can run supported services on the zone cluster similar to a global cluster, with the isolation that is provided by Oracle Solaris zones. 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 on the `pconsole` utility, 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.
- 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