Oracle® Solaris Cluster Security Guide

Part No: E39649
July 2014, E39649-01

Contents

Using This Documentation

- **Overview** – Provides an overview of security in Oracle Solaris Cluster, information on secure installations and configuration, security features, and security considerations for developers.
- **Audience** – Technicians, system administrators, and authorized service providers
- **Required knowledge** – Advanced experience troubleshooting and replacing hardware

Product Documentation Library

Late-breaking information and known issues for this product are included in the documentation library at http://www.oracle.com/pls/topic/lookup?ctx=E39579.

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.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program web site at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Feedback

Provide feedback about this documentation at http://www.oracle.com/goto/docfeedback.

♦ ♦ ♦ 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 4.2 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:

For more information about Oracle Solaris Operating System (OS) security, see "Oracle Solaris 11 Security Guidelines ".

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 ".
- Cluster packages – Oracle Solaris Cluster packages use Oracle Solaris Image Packaging System (IPS) package names.

  When cluster packages are installed on an Oracle Solaris host, some configuration must be performed first so that the host can become a cluster member. If you do not plan to create a cluster immediately, you should stop the `scrcmd` service by becoming superuser and running the following command on each node where the packages are installed: `/usr/sbin/svcadm disable svc:/network/rpc/scrcmd:default`.

  When you are ready to create the cluster, restart the service with the following command: `/usr/sbin/svcadm enable svc:/network/rpc/scrcmd:default`.

  To see a list of the Oracle Solaris Cluster Geographic Edition 4.2 packages, see "Oracle Solaris Cluster Geographic Edition Security Guide ". The following table lists the core packages that are included with Oracle Solaris Cluster 4.2.

IPS Package Name	Description
ha-cluster/developer/agent-builder	Oracle Solaris Cluster Agent Builder

IPS Package Name	Description
ha-cluster/developer/api	Oracle Solaris Cluster developer software
ha-cluster/group-package/ha-cluster-framework-full	Oracle Solaris Cluster Framework full group package
ha-cluster/group-package/ha-cluster-framework-l10n	Oracle Solaris Cluster Framework Localization group package
ha-cluster/group-package/ha-cluster-framework- minimal	Oracle Solaris Cluster Framework minimal group package
ha-cluster/group-package/ha-cluster-framework-scm	Oracle Solaris Cluster Framework Oracle Solaris Cluster Manager components group package
ha-cluster/group-package/ha-cluster-framework-slm	Oracle Solaris Cluster Framework Service Level Management (SLM) components group package
ha-cluster/group-package/ha-cluster-full	Oracle Solaris Cluster full installation group package
ha-cluster/group-package/ha-cluster-incorporation	Oracle Solaris Cluster incorporation package
ha-cluster/group-package/ha-cluster-minimal	Oracle Solaris Cluster minimal installation group package
ha-cluster/group-package/ha-cluster-quorum- server-full	Oracle Solaris Cluster Quorum Server full group package
ha-cluster/group-package/ha-cluster-quorum- server-l10n	Oracle Solaris Cluster Quorum Server Localization group package
ha-cluster/ha-service/derby	Derby Oracle Solaris Cluster agent
ha-cluster/ha-service/gds	Oracle Solaris Cluster Generic Data Service
ha-cluster/ha-service/gds2	Oracle Solaris Cluster Generic Data Service Version 2
ha-cluster/ha-service/logical-hostname	Oracle Solaris Cluster Resource Type for Logical Hostname
ha-cluster/ha-service/smf-proxy	Oracle Solaris Cluster SMF proxy methods
ha-cluster/ha-service/telemetry	Oracle Solaris Cluster Telemetry agent
ha-cluster/library/cacao	Oracle Solaris Cluster Common Cacao Support
ha-cluster/library/ucmm	Oracle Solaris Cluster UCMM reconfiguration interface
ha-cluster/locale	Localization for Oracle Solaris Cluster messages
ha-cluster/release/name	Oracle Solaris Cluster name
ha-cluster/service/management	Oracle Solaris Cluster Manageability and Serviceability Agent
ha-cluster/service/management/slm	Oracle Solaris Cluster Manageability Agent for Service Level Management
ha-cluster/service/quorum-server	Oracle Solaris Cluster Quorum Server
ha-cluster/service/quorum-server/locale	Localization for Oracle Solaris Cluster Quorum Server
ha-cluster/service/quorum-server/manual	Oracle Solaris Cluster Quorum Server Manual Pages
ha-cluster/service/quorum-server/manual /locale	Localization for Oracle Solaris Cluster Quorum Server Manual Pages
ha-cluster/storage/svm-mediator	Solaris Volume Manager (Mediator)

IPS Package Name	Description
ha-cluster/system/cfgchk	Oracle Solaris Cluster configuration checks
ha-cluster/system/core	Oracle Solaris Cluster software
ha-cluster/system/dsconfig-wizard	Oracle Solaris Cluster Data Service Configuration Wizard
ha-cluster/system/install	Oracle Solaris Cluster installation
ha-cluster/system/manager	Oracle Solaris Cluster Manager
ha-cluster/system/manager-glassfish3	Oracle Solaris Cluster Manager GlassFish Instance
ha-cluster/system/manual	Oracle Solaris Cluster Manual Pages
ha-cluster/system/manual/locale	Localization for Oracle Solaris Cluster Manual Pages

Additional data service agents might be supported after the Oracle Solaris Cluster 4.2 release. Check the "Oracle Solaris Cluster 4.2 Release Notes " for those agents. The following table lists the supported data services packages for Oracle Solaris Cluster 4.2.

IPS Package Name	Description
ha-cluster/data-service/apache	Oracle Solaris Cluster Apache Web Server Component
ha-cluster/data-service/dhcp	Oracle Solaris Cluster HA for DHCP
ha-cluster/data-service/dns	Oracle Solaris Cluster Domain Name Server Component
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 for xVM x86-64/SPARC Guest Domains
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 Server Component
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 data service
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

IPS Package Name	Description
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
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 Data Services full group package
ha-cluster/system/manual/data-services	Oracle Solaris Cluster Data Services online manual pages

- 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) – Use the RBAC authorizations of `solaris.cluster.modify`, `solaris.cluster.admin`, and `solaris.cluster.read` to access the cluster. You must become an administrator who is assigned the User Security rights profile to change most of the security attributes of a role. For more information, see “Managing the Use of Rights” in “Securing Users and Processes in Oracle Solaris 11.2 ” and “Oracle Solaris Cluster RBAC Rights Profiles” in “Oracle Solaris Cluster System Administration Guide ”.

- New Nodes – Use the `claccess` command or `clsetup` utility with privileges to add a node to a cluster. For more information, see Chapter 8, “Administering Cluster Nodes,” in “Oracle Solaris Cluster System Administration Guide ”.

  The default setting for access status is `claccess deny-all`. You should change this only when you want to perform a privileged operation, such as adding a new node. You should restore the `deny-all` status when you are finished. If you expect to make frequent changes to cluster configurations, you can ensure maximum trust for new systems by selecting a more secure authentication protocol using the `/usr/cluster/bin/claccess -p protocol=authentication-protocol` command. For more information, see the `claccess`(1CL) man page and Chapter 10, “Configuring Network Services Authentication,” in “Managing Kerberos and Other Authentication Services in Oracle Solaris 11.2 ”.
- 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 Install and Configure Trusted Extensions” in “Oracle Solaris Cluster Software Installation Guide ”.
- Zone Clusters – A zone cluster is composed of one or more non-global zones of the `solaris`, `solaris10`, or `labeled` brand that are set with the `cluster` attribute. A `labeled` brand zone cluster is only for use with the Trusted Extensions feature of Oracle Solaris software. You create a zone cluster by using the `clzonecluster` command or the `clsetup` utility. 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 “Creating and 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 management stacks on each cluster node. For more information, see “Troubleshooting” 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 “Administering the Cluster” in “Oracle Solaris Cluster System Administration Guide ”.
- Auditing – Oracle Solaris Cluster is enabled by default, as it is in the Oracle Solaris OS. Auditing 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 OS Hardening – Oracle Solaris Cluster uses security hardening techniques to reconfigure the Oracle Solaris OS into a hardened state. Additionally, it can activate the Oracle Solaris system audit.

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. 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:

- Oracle Solaris Cluster supports a wide range of application agents, which are implemented as a set of callback methods to control starting, stopping, probing, and validation of the application. The callback methods such as `Start`, `Stop`, or `Validate` always execute as root. If one of these executable method files is writable by a non-root user, this creates a vulnerability in which such a non-root user can achieve an unauthorized elevation of privilege by inserting code into the callback method. Oracle Solaris Cluster checks the ownership and permissions of such callback method executables. The checking is controlled by the `resource_security` cluster property setting. If `resource_security` is set to `SECURE` and the method code is found to be writable by non-root, the method execution fails.

  Agent methods in turn often run external programs, such as application-specific administrative commands. Agent methods should run all such external programs using a wrapper to ensure that the external program is executed with the least possible privilege. Oracle Solaris Cluster provides the `application_user` and `resource_security` properties and the `scha_check_app_user` API to enable data services to ensure that the application is executed securely. The `scha_check_app_user` command can be called in scripts to verify the username against the configured `Application_user` and `Resource_security` settings. See the `scha_check_app_user`(1HA) man page, `r_properties`(5) man page, and `cluster`(1CL) man page for information.
- 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. Oracle Solaris Cluster provides the `clpstring` command to enable you to create private strings that can be used to store encoded passwords securely in the cluster and retrieved when passwords must be used to perform management tasks. See the `clpstring`(1CL) man page for information about this command.

See the “Oracle Solaris Cluster Data Services Developer’s Guide ” for more information about how to use these security features when developing data services.

Index