Oracle® Solaris Cluster 4.3 Security Guide

Part No: E56684
September 2015

ORACLE

Oracle Solaris Cluster 4.3 Security Guide

Part No: E56684

Access to Oracle Support

Oracle customers that have purchased support 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.

Référence: E56684

Accès aux services de support Oracle

Les clients Oracle qui ont souscrit un contrat de support ont accès au support électronique via My Oracle Support. Pour plus d'informations, visitez le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` ou le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` si vous êtes malentendant.

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

Documentation and resources for this product and related products are available at http://www.oracle.com/pls/topic/lookup?ctx=E56676-01.

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. This guide provides an overview of security in Oracle Solaris Cluster, plus information about 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.

Geographic Edition software is a layered extension of the Oracle Solaris Cluster software. The Geographic Edition framework protects applications from unexpected disruptions by using multiple clusters that are geographically separated by long distances. These clusters contain copies of the Geographic Edition infrastructure, which manage replicated data between the clusters.

This chapter contains the following sections:

For more information about Oracle Solaris operating system (OS) security, see *Oracle Solaris 11 Security and Hardening Guidelines* and *Securing Systems and Attached Devices in Oracle Solaris 11.3* .

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 4.3 Concepts Guide* .

Overview of Geographic Edition and Security

Geographic Edition software is a layered extension of the Oracle Solaris Cluster software. Data replication software enables applications that are running on a Geographic Edition cluster to tolerate disasters by migrating services to a geographically separated secondary cluster. A disaster such as an earthquake, fire, or storm might disable the cluster at the primary site.

If a disaster occurs, the Geographic Edition cluster can continue to provide services by using the following levels of redundancy:

- A secondary cluster
- Duplicated application configuration on the secondary cluster
- Replicated data on the secondary cluster

Geographic Edition software provides a suite of tools to manage and configure geographically separated clusters with a migration of services between sites. The clusters can be global

clusters, zone clusters, or a combination of both. The Geographic Edition software can manage availability across multiple physical locations through robust security, application service migration, and data replication to tolerate disaster across an enterprise system.

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 of Oracle Solaris Cluster

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 4.3 Software Installation Guide* .
- **Cluster packages** – Oracle Solaris Cluster packages use Oracle Solaris Image Packaging System (IPS) package names.

  To see a list of the Oracle Solaris Cluster core, data service, and Geographic Edition packages, see *Oracle Solaris Cluster 4.3 Package Group Lists* .
- **Configuration** – You can configure and administer a global cluster and a zone cluster. For more information, see Chapter 3, "Establishing the Global Cluster," in *Oracle Solaris Cluster 4.3 Software Installation Guide* , Chapter 6, "Creating Zone Clusters," in *Oracle Solaris Cluster 4.3 Software Installation Guide* , and Chapter 1, "Introduction to Administering Oracle Solaris Cluster," in *Oracle Solaris Cluster 4.3 System Administration Guide* .

  For all methods to establish a global cluster node, prior authorization of one designated sponsor node is required, permitting only that designated system to access the node it will configure. If desired, DES encryption can be used for a more secure configuration. For more information, see the `clauth`(1CL) man page.

- **Common agent container vulnerability** – The combination of common agent container and some older Java versions poses a security vulnerability in Oracle Solaris Cluster software. For information to identify whether your system has this vulnerability and how to correct it, see My Oracle Support reference document, *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`). This document requires My Oracle Support login.
- **HA for NFS secured with Kerberos V5** – If you need to secure access to NFS services that are managed by the HA for NFS data service, you can configure a Kerberos V5 client to secure the HA for NFS data service. This includes adding a Kerberos principal for NFS over the logical hostnames on all cluster nodes. For more information, see "Securing HA for NFS With Kerberos V5" in *Oracle Solaris Cluster Data Service for NFS Guide* .

Secure Installation and Configuration of Geographic Edition

This section provides links for planning and executing a secure installation and configuration of Geographic Edition software.

- **Installation** – Geographic Edition software must be installed on a cluster that is running the Oracle Solaris operating system and the Oracle Solaris Cluster software. Use the Oracle Solaris Automated Installer (AI) to install Geographic Edition software at the same time that you install Oracle Solaris Cluster software or at any time afterwards. The Geographic Edition framework configuration is identical to the Oracle Solaris Cluster software configuration. See Chapter 2, "Installing and Configuring the Geographic Edition Software," in *Oracle Solaris Cluster 4.3 Geographic Edition Installation and Configuration Guide* .
- **Geographic Edition packages** – Geographic Edition packages use Oracle Solaris Image Packaging System (IPS) package names. To see a list of packages, see *Oracle Solaris Cluster 4.3 Package Group Lists* .
- **Configuration** – You can perform all administration tasks on a cluster that is running the Geographic Edition framework without causing any nodes or the cluster to fail. You can install, configure, start, use, stop, and uninstall the Geographic Edition software on an operational cluster. See Chapter 4, "Administering RBAC," in *Oracle Solaris Cluster 4.3 Geographic Edition System Administration Guide* .

Oracle Solaris Cluster 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 11.3* and "Oracle Solaris Cluster RBAC Rights Profiles" in *Oracle Solaris Cluster 4.3 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 4.3 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 11.3* .
- **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 4.3 Software Installation Guide* and "How to Install and Configure Trusted Extensions" in *Oracle Solaris Cluster 4.3 Software Installation Guide* .
- **Zone Clusters** – A zone cluster is composed of one or more non-global zones of the `solaris` brand, the `solaris10` brand, or the `labeled` brand 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 4.3 Software Installation Guide* and "Working With a Zone Cluster" in *Oracle Solaris Cluster 4.3 System Administration Guide* .
- **Secure Connections to Cluster Consoles** – You must establish secure shell connections to the consoles of the cluster nodes. For more information about the `pconsole` utility, see "How to Connect Securely to Cluster Consoles" in *Oracle Solaris Cluster 4.3 System Administration Guide* .
- **Common Agent Container** – The Oracle Solaris Cluster Manager GUI uses strong encryption techniques to ensure secure communication between the Oracle Solaris Cluster management stacks on each cluster node. For more information, see "Troubleshooting Oracle Solaris Cluster Manager" in *Oracle Solaris Cluster 4.3 System Administration Guide* .

- **Logging** – Oracle Solaris Cluster software uses the `syslogd` 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 4.3 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 4.3 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.

Geographic Edition Security Features

This section contains information about specific security mechanisms offered by Geographic Edition.

A secure installation uses the following critical security features:

- **Role-Based Access Control (RBAC)** – Geographic Edition software bases its RBAC profiles on the RBAC rights profiles that are used in the Oracle Solaris Cluster software. You must become an administrator who is assigned the User Security rights profile to change most of the security attributes of a role. Assume the root role and use the RBAC roles of `solaris.cluster.geo.modify`, `solaris.cluster.geo.admin`, and `solaris.cluster.geo.read` to access the cluster. For more information, see *Securing Users and Processes in Oracle Solaris 11.3* and "Modifying a User's RBAC Properties" in *Oracle Solaris Cluster 4.3 Geographic Edition System Administration Guide* .
- **Security Certificates** – During installation, the cluster is configured for secure cluster communication by using security certificates (nodes within the same cluster must share the same security certificates). The communication between clusters in a Geographic Edition partnership is secured through the Java Management Extensions (JMX) port with Secure Sockets Layer (SSL) using the security certificates. For more information, see "Configuring Trust Between Partner Clusters" in *Oracle Solaris Cluster 4.3 Geographic Edition Installation and Configuration Guide* .
- **Common Agent Container** – To enable a zone cluster to function as a member of a Oracle Solaris Cluster partnership, the common agent container must be manually configured within the zone cluster. For more information, see "Preparing a Zone Cluster for

Partner Membership" in *Oracle Solaris Cluster 4.3 Geographic Edition Installation and Configuration Guide* .

- **IP Security Architecture (IPsec)** – Use IPsec to configure secure TCP/UDP heartbeat communications between partner clusters. For more information, see "Securing Inter-Cluster Communication" in *Oracle Solaris Cluster 4.3 Geographic Edition Installation and Configuration Guide* .

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 4.3 Concepts Guide* .

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

- **Agent Callback Methods** – 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), `r_properties`(5), and `cluster`(1CL) man pages 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` 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

S

T

Z