Oracle® Solaris Cluster 4.3 Geographic Edition Installation and Configuration Guide

Part No: E56740
February 2017

ORACLE

Oracle Solaris Cluster 4.3 Geographic Edition Installation and Configuration Guide

Part No: E56740

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: E56740

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 11

1 Planning the Geographic Edition Installation 13
- Installation Process 13
- Planning Cluster Hardware 14
- Planning Required Software 15
  - Planning the Geographic Edition Software 15
  - Planning the Data Replication Software 15
  - Planning Volume Management 16
- Planning Resource and Resource Group Names 17
- Planning Required IP Addresses and Hostnames 17
  - IP Address Requirements 17
  - Hostname Requirements 17
- Planning Security 18
  - Setting Up and Using RBAC 18
  - RBAC Rights Profiles 19
  - Configuring Firewalls 19
  - Securing Intercluster Communication 20
- Planning the Geographic Edition Environment 22
  - Licensing 22
  - Logical Hostnames 22
  - Zone Clusters 23
  - Partnerships 24
  - Protection Groups 24
  - Sites 25
  - Multigroups 26

2 Installing and Configuring the Geographic Edition Software 27

Installation Overview 27
Prerequisite Configuration Tasks 28
Installation and Configuration Tasks 28
Installing the Geographic Edition Software 29
▼ How to Install the Geographic Edition Software 30
Securing Geographic Edition Software 33
▼ How to Configure IPsec for Secure Cluster Communication 34
Preparing a Zone Cluster for Partner Membership 35
▼ How to Prepare a Zone Cluster for Partner Membership 36
Enabling the Geographic Edition Framework 38
▼ How to Enable the Geographic Edition Framework 39
Configuring a Partnership 41
Configuring Trust Between Partner Clusters 42
Creating a Partnership 43
Joining an Existing Partnership 46
Configuring Protection Groups 49
Creating a Protection Group That Uses Data Replication 50
Creating a Protection Group That Does Not Require Data Replication 50
Validating a Protection Group 55
Activating a Protection Group 56
Configuring Sites and Multigroups 59
▼ How to Create a Site 59
▼ How to Create a Multigroup 62

3 Upgrading or Updating Geographic Edition Software 65
Upgrading a Geographic Edition Configuration 65
Upgrade and Update Requirements and Software Support Guidelines 66
▼ How to Prepare the Cluster for an Upgrade or Software Update 67
▼ How to Upgrade or Update Geographic Edition Software 69
▼ How to Verify Upgrade or Update of Geographic Edition Software 71

4 Uninstalling the Geographic Edition 4.3 Software 73
Uninstalling the Geographic Edition Software 73
▼ How to Uninstall the Geographic Edition Software 73

Index 77

Tables

TABLE 1 Geographic Edition RBAC Rights Profiles 19

TABLE 2 Ports and Protocols Used by Geographic Edition Partnerships - Required Services 20

TABLE 3 Ports and Protocols Used by Geographic Edition Partnerships - Optional Services 20

TABLE 4 Prerequisite Configuration Tasks 28

TABLE 5 Geographic Edition Installation and Configuration Tasks 28

Examples

EXAMPLE 1 Enabling the Geographic Edition Framework on a Cluster 40

EXAMPLE 2 Creating a Partnership 46

EXAMPLE 3 Creating a Partnership That Uses a Custom Heartbeat and a Custom Heartbeat Plug-In 46

EXAMPLE 4 Joining a Partnership 48

EXAMPLE 5 Creating and Joining a Partnership With a Remote Cluster in a Different Domain 48

EXAMPLE 6 Creating and Configuring a Protection Group That Is Configured Not to Use Data Replication 53

EXAMPLE 7 Globally Activating a Protection Group 58

EXAMPLE 8 Locally Activating a Protection Group 59

EXAMPLE 9 Creating a New Site 61

Using This Documentation

- **Overview** – Describes how to administer an Oracle Solaris Cluster Geographic Edition configuration
- **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

Planning the Geographic Edition Installation

This chapter provides planning information and guidelines for installing an Oracle Solaris Cluster Geographic Edition (Geographic Edition) configuration. This chapter also describes how to plan the data replication between two clusters.

This chapter contains the following sections:

- "Installation Process" on page 13
- "Planning Cluster Hardware" on page 14
- "Planning Required Software" on page 15
- "Planning Resource and Resource Group Names" on page 17
- "Planning Required IP Addresses and Hostnames" on page 17
- "Planning Security" on page 18
- "Planning the Geographic Edition Environment" on page 22

Installation Process

To successfully install Geographic Edition software, you must complete the following installation phases:

1. Planning your installation.
2. Connecting your hardware.
3. Installing Oracle Solaris Cluster software.
4. Installing data replication products.
5. Installing and configuring the required software.
6. Installing Geographic Edition software.
7. Configuring the Geographic Edition framework.

This installation process progresses from the initial planning phase to the eventual startup of the Geographic Edition framework. This guide provides information about phases 1, 6, and 7.

Note - You can also install Geographic Edition software at the same time that you install Oracle Solaris Cluster software.

For information about installing Oracle Solaris Cluster software, see the *Oracle Solaris Cluster 4.3 Software Installation Guide*.

For information about configuring a cluster after startup, see the *Oracle Solaris Cluster 4.3 Geographic Edition System Administration Guide*.

Planning Cluster Hardware

The information in this section helps you to plan your hardware for the primary cluster, the secondary cluster, and the intercluster communication.

The Geographic Edition hardware configuration consists of the following elements:

- At least two separate clusters that are running Oracle Solaris Cluster software with attached data storage. One of these clusters must be designated the primary cluster.

  Note - While you can use a single-node cluster at both the primary and backup sites, a single-node cluster offers no internal redundancy. To ensure no single point of failure, you must have a minimum of two nodes in a cluster at the primary site. You can use a single-node cluster at the secondary site as a cost-effective backup solution if the secondary site is used only for backup purposes and is not for running mission-critical applications.

- Internet connections for intercluster management communication between the clusters and for default intercluster heartbeats.
- Connections for either host-based or storage-based data replication.
- Connections for custom heartbeats, if any.

The Geographic Edition framework supports the same hardware configurations that the Oracle Solaris Cluster product supports. The cluster hardware configurations that use the Geographic Edition framework with storage-based data replication mechanisms must support the related storage hardware. Also, partner clusters must be compatibly configured to support data replication between the clusters.

Internet access is required between partner clusters. The communication between partner clusters for intercluster management operations is through a logical-hostname IP address. The default intercluster heartbeat module also communicates through a logical-hostname IP address.

A cluster in a Geographic Edition partnership conforms to the standard configuration rules of a cluster that is running Oracle Solaris Cluster software.

Planning Required Software

The information in this section helps you to adapt the configuration of your Oracle Solaris Cluster software for the installation of Geographic Edition software. This section also helps you to plan the installation of your data replication software.

This section provides the following information:

- "Planning the Geographic Edition Software" on page 15
- "Planning the Data Replication Software" on page 15
- "Planning Volume Management" on page 16

Planning the Geographic Edition Software

Geographic Edition software must be installed on a cluster that is running the Oracle Solaris operating system and the Oracle Solaris Cluster software. You can install Geographic Edition software at the same time that you install Oracle Solaris Cluster software or at any time afterwards. The Geographic Edition software configuration is identical to the Oracle Solaris Cluster software configuration.

The clusters in a Geographic Edition configuration can run different versions of Geographic Edition software, as long as they are no more than one consecutive version different. For example, the same Geographic Edition configuration could have clusters running either version 4.3 or 4.2. But a cluster running version 4.3 cannot run in the same Geographic Edition configuration as a cluster running version 4.0.

Planning the Data Replication Software

A cluster that is using Geographic Edition software with a data replication product is subject to the standard configuration rules of a cluster that is running the data replication product with Oracle Solaris Cluster software. Partner clusters must have compatible software configurations to support data replication between the clusters.

The Geographic Edition product supports the following data replication products:

- The Availability Suite feature of the Oracle Solaris OS
- EMC Symmetrix Remote Data Facility software
- Hitachi TrueCopy and Universal Replicator software
- MySQL software
- Oracle Data Guard software, in configurations that use Oracle Database software
- Oracle GoldenGate software
- Oracle Solaris ZFS snapshots feature
- Oracle ZFS Storage Appliance software
- Geographic Edition script-based plug-ins

These products provide the following types of replication:

- **Host-based replication** – The ZFS snapshots and Availability Suite features of Oracle Solaris software are host-based replication methods. This method consists of software installed on a host that controls replication from one server to a secondary server.
- **Storage-based replication** – Oracle ZFS Storage Appliance, Hitachi TrueCopy and Universal Replicator, and EMC Symmetrix Remote Data Facility replication use a storage-based method. This method uses replication that is built into the storage hardware. If you use Oracle ZFS Storage Appliance software, Hitachi TrueCopy and Universal Replicator RAID Manager software, or EMC Symmetrix Remote Data Facility software, you must install the software on each node of the cluster.
- **Replication for databases** – Oracle Data Guard functionality is part of the Oracle Database software and so does not require you to install additional software onto your system. The Geographic Edition module for Oracle Data Guard can only be used with Oracle databases.

  Oracle GoldenGate is a data replication software for databases. It takes changes from a source database and replicates them to a target database.
- **Built-in replication** – MySQL database software offers a built-in replication protocol. Configuring the Geographic Edition MySQL replication module enables you to control replication between MySQL instances on each site.
- **Custom replication** – The Geographic Edition script-based plug-in enables the user to develop replication modules to integrate additional replication protocols into Geographic Edition. The plug-in provides the interface to register custom replication control scripts with Geographic Edition.

Planning Volume Management

See the Oracle Solaris Cluster 4 Compatibility Guide (`http://www.oracle.com/technetwork/server-storage/solaris-cluster/overview/solariscluster4-compatibilityguide-`

1429037.pdf) for information about volume management support for your data replication product.

Planning Resource and Resource Group Names

A partnership requires two clusters to be combined into one environment. Because one cluster might be a running production system, advance planning of resources and resource groups is essential for a successful installation.

The Geographic Edition framework requires that resource-group names be identical on each partner cluster to ensure that a resource or resource group can be managed as a single entity across both clusters in the partnership.

Planning Required IP Addresses and Hostnames

You must have all the required IP addresses and hostnames before you begin the installation process. This section provides information about these requirements.

IP Address Requirements

You must set up a number of IP addresses for various Geographic Edition components, depending on your cluster configuration. Observe the following guidelines:

- You must have an IP address for the cluster name and for each cluster node.
- Some components require IP addresses. See "Public-Network IP Addresses" in *Oracle Solaris Cluster 4.3 Software Installation Guide* for a list. Add these IP addresses to any naming services that are used. Also add these IP addresses to the local `/etc/inet/hosts` file on each cluster node after you install Oracle Solaris software.
- You might also need additional IP addresses for data replication products. For more information about requirements for configuring data replication, see the Geographic Edition manual for your data replication product.

Hostname Requirements

Note the following requirements for hostnames:

- **Logical hostname** – Because the Geographic Edition framework creates the logical hostname by using the cluster name, a cluster name must be suitable as a hostname, and must be in the naming system.
- **Unique cluster name** – Cluster names must be unique. For example, if you have a cluster wholly within the domain `.france`, you can use hostnames like `paris` and `grenoble`. However, if you have a cross-domain cluster, you must specify the hostnames with enough qualification to identify the host on the network. For example:
  - You can link `paris` and `munich` with hostnames `paris.france` and `munich.germany`, and the cluster names remain `paris` and `munich`.
  - You cannot create a partnership between clusters `paris.france` and `paris.texas` because of a collision on the cluster name `paris`.

Planning Security

This section contains the following information about securing the Geographic Edition framework:

- "Setting Up and Using RBAC" on page 18
- "RBAC Rights Profiles" on page 19
- "Configuring Firewalls" on page 19
- "Securing Intercluster Communication" on page 20

Setting Up and Using RBAC

The Geographic Edition framework bases its RBAC profiles on the RBAC rights profiles that are used in the Oracle Solaris Cluster software. For general information about setting up and using RBAC with Oracle Solaris Cluster software, refer to Chapter 2, "Oracle Solaris Cluster and User Rights" in *Oracle Solaris Cluster 4.3 System Administration Guide*.

The Geographic Edition framework adds the following RBAC entities to the appropriate file in the `/etc/security` directory:

- RBAC authentication names to `auth_attr`
- RBAC execution profiles to `prof_attr`
- RBAC execution attributes to `exec_attr`

Note - The default search order for the `auth_attr` and `prof_attr` databases is `files nis`, which is defined in the `/etc/nsswitch.conf` file. If you have customized the search order in your environment, confirm that `files` is in the search list, so your system can find the RBAC entries that Geographic Edition defined.

RBAC Rights Profiles

The Geographic Edition command-line interface (CLI) and the Oracle Solaris Cluster Manager browser interface use RBAC rights to control end-user access to operations. The following table provides the general conventions for these rights.

TABLE 1 Geographic Edition RBAC Rights Profiles

Rights Profile	Included Authorizations	Role Identity Permission
Geo Management	`solaris.cluster.geo.read`	Read information about the Geographic Edition entities
	`solaris.cluster.geo.admin`	Perform administrative tasks with the Geographic Edition framework
	`solaris.cluster.geo.modify`	Modify the configuration of the Geographic Edition framework
Basic Solaris User	Oracle Solaris authorizations	Perform the same operations that the Basic Solaris User role identity can perform
	`solaris.cluster.geo.read`	Read information about the Geographic Edition entities

Configuring Firewalls

Geographic Edition partner clusters communicate using transport services and ICMP echo requests and replies (pings). Their packets must therefore pass data center firewalls, including any firewalls configured on cluster nodes in partner clusters. Table 2, “Ports and Protocols Used by Geographic Edition Partnerships - Required Services,” on page 20 and Table 3, “Ports and Protocols Used by Geographic Edition Partnerships - Optional Services,” on page 20 contain lists of required and optional services and protocols used by Geographic Edition partnerships, and the associated ports that you must open in your firewalls for these services to function. The ports listed are defaults. If you customize the port numbers that serve the specified transfer protocols, the customized ports must be opened instead.

Ports other than those listed in the following tables might be required by storage replication services such as the Availability Suite feature of Oracle Solaris software. See the related product documentation for details.

TABLE 2 Ports and Protocols Used by Geographic Edition Partnerships - Required Services

Port Number	Protocols	Use in Geographic Edition partnership
22	UDP and TCP	Secure shell (`ssh`). Used during the initial certificate transfer that establishes trust between partner clusters.
2084	UDP (default), TCP	Intercluster heartbeat
11162	TCP	The Java Management Extensions (JMX) port (`jmxmp-connector-port`). A messaging protocol used for the exchange of configuration and status information between the two sites in a partnership.
-	ICMP Echo Request/ Reply	Backup heartbeat between partner clusters

TABLE 3 Ports and Protocols Used by Geographic Edition Partnerships - Optional Services

Port Number	Protocols	Use in Geographic Edition partnership
161	TCP and UDP	Simple Network Management Protocol (SNMP) communications
162	TCP and UDP	SNMP traps

Securing Intercluster Communication

You can use either security certificates or IP Security Architecture (IPsec) to secure communication between partner clusters.

Security Certificates

You must configure the Geographic Edition framework for secure communication between partner clusters. The configuration must be reciprocal, so cluster `cluster-paris` must be configured to trust its partner cluster `cluster-newyork`, and cluster `cluster-newyork` must be configured to trust its partner cluster `cluster-paris`.

For information and procedures to set up security certificates for partner clusters, see “Configuring Trust Between Partner Clusters” on page 42.

IP Security (IPsec)

You can use IP Security Architecture (IPsec) to configure secure communication between partner clusters. IPsec enables you to set policies that permit or require either secure datagram authentication, or actual data encryption, or both, between machines communicating by using IP.

Consider using IPsec for the following intercluster communications:

- Secure communication through Availability Suite from Oracle if you use the Availability Suite software for data replication
- Secure TCP/UDP heartbeat communications

IPsec uses two configuration files:

- **IPsec policy file**, `/etc/inet/ipsecinit.conf` – Contains directional rules to support an authenticated, encrypted heartbeat. The contents of this file are different on the two clusters of a partnership.
- **IPsec keys file**, `/etc/init/secret/ipseckeys` – Contains keys files for specific authentication and encryption algorithms. The contents of this file are identical on both clusters of a partnership.

Observe the following guidelines when using IPsec for secure intercluster communication:

- Oracle Solaris Cluster software and Geographic Edition software support IPsec by using only manual keys. Keys must be stored manually on the cluster nodes for each combination of server and client IP address. The keys must also be stored manually on each client.
- In the Geographic Edition framework, the hostname of a logical host is identical to the cluster name. The logical hostname is a special HA resource. You must set up a number of IP addresses for various Geographic Edition components, depending on your cluster configuration.
- On each partner cluster, you must configure encryption and authorization for exchanging inbound and outbound packets from a physical node to the logical-hostname addresses. The values for the Oracle Solaris IP Security Architecture (IPsec) configuration parameters on these addresses must be consistent between partner clusters.
- Oracle Solaris Cluster software does not support the use of IPsec for the cluster interconnect.

Refer to *Securing the Network in Oracle Solaris 11.3* for more information about IPsec.

Planning the Geographic Edition Environment

This section provides guidelines for planning and preparing the following components for Geographic Edition software installation:

- "Licensing" on page 22
- "Logical Hostnames" on page 22
- "Zone Clusters" on page 23
- "Partnerships" on page 24
- "Protection Groups" on page 24
- "Sites" on page 25
- "Multigroups" on page 26

Licensing

Ensure that you have available all necessary license certificates before you begin software installation. Geographic Edition software does not require a license certificate. However, each node that is installed with Geographic Edition software must be covered under your Geographic Edition software license agreement.

For licensing requirements for data replication software and application software, see the installation documentation for those products.

Logical Hostnames

The Geographic Edition framework uses the logical hostname of a cluster for intercluster management communication and heartbeat communication. The IP address for a cluster name must be available for the Geographic Edition framework to wrap a logical hostname around the IP address when the framework is started by using the `geoadm start` command.

To find the name of the cluster when you need to verify that the cluster name is suitable for use as a hostname, run the following command:

```
# cluster list
```

For more information, see the `cluster`(1CL) man page.

Zone Clusters

In some Geographic Edition configurations, a zone cluster can be configured as a cluster partner. Observe the following guidelines for the use of zone clusters in a cluster partnership:

- **Public-network IP addresses** - A zone cluster that is configured in a Geographic Edition configuration must meet the following public-network requirements:
  - Each zone-cluster node must have a public-network IP address that corresponds to the zone-cluster node's hostname.
  - The zone-cluster node's public-network IP address must be accessible by all nodes in the Geographic Edition configuration's partner cluster.
  - Each zone-cluster node must have a failover IP address that maps to the hostname that corresponds to the zone-cluster name.
- **Data replication requirements** – Zone clusters can be cluster partners in a Geographic Edition configuration that meets either of the following conditions:
  - Application-based data replication is used. Geographic Edition supports Oracle Data Guard, Oracle GoldenGate, MySQL, and Geographic Edition script-based plug-ins application-based data replication.
  - EMC Symmetrix Remote Data Facility storage-based replication is used.
  - No data replication is used.
- **Mixed cluster types** – The partnership can use other zone clusters or a combination of zone clusters and global clusters.
- **Framework package** – The Geographic Edition framework package is required in the global zones in all cases, even if Geographic Edition is going to be enabled only in the zone clusters. The Geographic Edition framework package is `ha-cluster/geo/geo-framework`.
- **Storage-based replication** – If storage-based replication is used, with the exception of Oracle ZFS Storage Appliance replication, all members of a cluster partnership must be global clusters. Zone clusters can exist in a global-cluster partnership that uses storage-based replication, but the zone clusters themselves cannot be members of a partnership that uses storage-based replication.

  If Oracle ZFS Storage Appliance replication is used, members of a cluster partnership can be global clusters, zone clusters, or a combination of the two.
- **Starting the framework** – You can start the Geographic Edition framework from within a zone cluster node, but not from within any other type of non-global zone.
- **Oracle Solaris Cluster Manager** – You cannot use the Oracle Solaris Cluster Manager browser interface to manage Geographic Edition components of a zone cluster that is a partnership member.

Partnerships

You can create partnerships between clusters to provide mutual protection against disasters. The clusters in a partnership monitor each other by sending heartbeat messages to each other in the same way that nodes of a single cluster do. Unlike local clusters, the clusters in a partnership use the public network for these messages but support additional plug-in mechanisms as well.

You create a partnership between two specific clusters by using the `geops`(1M) command. After you have created a partnership, you can use this command to modify the properties of the partnership.

Observe the following guidelines:

- **Unique cluster names** – When creating partnerships, ensure that the name of all the clusters in the partnership are unique. For example, if you have a cluster wholly within the domain `.france`, you can use hostnames like `paris` and `grenoble`. However, if you have a cross-domain cluster, you must specify the hostnames with enough qualification to identify the host on the network. For example:
  - You can link `paris` and `munich` with hostnames `paris.france` and `munich.germany`, and the cluster names remain `paris` and `munich`.
  - You cannot create a partnership between clusters `paris.france` and `paris.texas` because of a collision on the cluster name `paris`.
- **Application resource group names** – The names of the application resource groups that are managed by the Geographic Edition framework must be the same on both partner clusters. You can configure the names of these resource groups manually.
- **Single partnership between cluster pairs** – You can define only one partnership between two specific clusters. A single cluster can participate in other partnerships with different clusters.
- **Device groups** – You cannot add device groups to a protection group that does not use data replication.

Protection Groups

Protection groups enable a set of clusters to tolerate and recover from disaster by managing the resource groups for services. A protection group contains application resource groups and properties for managing data replication for those application resource groups.

Observe the following general guidelines when you configure a protection group:

- **Partnerships** –You must create a partnership before you can create a protection group for that partnership. Protection groups can exist only in a partnership.
- **Duplicate application resource group configuration** – You can duplicate the application resource group configuration on partner clusters. The configuration for a protection group is identical on partner clusters, so partner clusters must have the application resource groups of the protection group defined in their configuration. The Geographic Edition framework propagates protection group configurations between partners.
- **Data replication** – You can specify a data replication type in the protection group to indicate the mechanism to use for data replication between partner clusters. When a service is protected from disaster by data replication, the protection group also contains replication resource groups. Protection groups link an application in a resource group with the application data that should be replicated. This linkage and replication enable the application to fail over seamlessly from one cluster to another cluster.
- **Replicating the Oracle Solaris boot environment** – Do not replicate an Oracle Solaris boot environment between two systems. Doing so is not appropriate for disaster recovery environments, as it might introduce instability in the target boot environment.

Each data replication product has its own additional requirements when configuring a protection group. For more information, see the appropriate Geographic Edition manual for the data replication software that you will use:

- *Oracle Solaris Cluster Geographic Edition Data Replication Guide for EMC Symmetrix Remote Data Facility*
- *Oracle Solaris Cluster Geographic Edition Data Replication Guide for Hitachi TrueCopy and Universal Replicator*
- *Oracle Solaris Cluster Geographic Edition Data Replication Guide for Oracle GoldenGate*
- *Oracle Solaris Cluster Geographic Edition Data Replication Guide for MySQL*
- *Oracle Solaris Cluster Geographic Edition Data Replication Guide for Oracle Data Guard*
- *Oracle Solaris Cluster Geographic Edition Data Replication Guide for Oracle Solaris Availability Suite*
- *Oracle Solaris Cluster Geographic Edition Data Replication Guide for ZFS Snapshots*
- *Oracle Solaris Cluster Geographic Edition Remote Replication Guide for Oracle ZFS Storage Appliance*

Sites

A site is a group of clusters for which you want to manage sets of protection groups, or multigroup, in a single operation. When you perform a switchover or takeover of a multigroup, a site is specified as the target.

Observe the following general guidelines when you configure a site:

- **First site controller** – The cluster from which you create a new site is automatically configured as a site controller.
- **Multiple controllers** – To avoid a single point of failure, configure at least two controller clusters in a site.
- **Zone clusters** – A zone cluster can be a site member.
- **Remote management of an Oracle Data Guard database** – A cluster can be configured with a protection group to manage a remote Oracle Data Guard Database instance that is not running on an Oracle Solaris Cluster configuration.

Multigroups

A multigroup is a set of protection groups that you can manage in a single operation.

Observe the following general guidelines when you configure a multigroup:

- **Single site** – All protection groups in a multigroup must be configured on clusters that are part of the same site.
- **Unique name** – Multigroup names must be unique throughout the site. In addition, if multiple sites share a common cluster, those sites cannot contain multigroups of the same name.
- **Site-to-cluster configurations** – A multigroup can consist of protection groups where one of the partner clusters is not configured in a site. In such a configuration, multigroup operations can be performed only from a cluster that is in a site. To manage protection groups from the partner cluster that is not in a site, you must manage the protection groups individually by using the `geopg` command.
- **Protection group dependencies** – You can configure one or more protection groups to have a strong dependency on a third protection group in the multigroup. When the protection groups in a multigroup are taken offline for a switchover or takeover, the depended-on protection group is taken offline after the protection groups that depend on it are taken offline. When a multigroup is brought online, the depended-on protection group is brought online before the protection groups with a dependency on it are brought online.
- **Nested protection group dependencies** – A protection group that other protection groups depend on can itself have a dependency on another protection group.
- **Single dependency** – A protection group cannot have a direct dependency on more than one protection group.

♦ ♦ ♦ CHAPTER 2

Installing and Configuring the Geographic Edition Software

This chapter describes the steps for installing Geographic Edition software and then enabling and configuring the Geographic Edition framework. This chapter contains the following sections:

- "Installation Overview" on page 27
- "Installing the Geographic Edition Software" on page 29
- "Securing Geographic Edition Software" on page 33
- "Preparing a Zone Cluster for Partner Membership" on page 35
- "Enabling the Geographic Edition Framework" on page 38
- "Configuring a Partnership" on page 41
- "Configuring Protection Groups" on page 49
- "Configuring Sites and Multigroups" on page 59

Installation Overview

You can install Geographic Edition software on a running cluster without disruption. Because the Geographic Edition software installation process does not require you to restart Oracle Solaris Cluster software, the cluster remains in production with services running.

Note - Ensure that you have installed all the required software updates for your cluster configuration on each node of every cluster before you start installing the Geographic Edition software. See Chapter 11, "Updating Your Software" in *Oracle Solaris Cluster 4.3 System Administration Guide* for installation instructions.

For zone clusters that are already created, when you install the Geographic Edition software, the software is propagated to the zone-cluster nodes by default. If you create a zone cluster after Geographic Edition software is installed in the global cluster, you must install the Geographic Edition software in the new zone-cluster nodes.

This section contains lists of the tasks you need to perform to create a Geographic Edition configuration.

Prerequisite Configuration Tasks

Before you begin administering the Geographic Edition framework, you must identify the Oracle Solaris Cluster installations you want to host protection groups. Then, you need to adjust the Oracle Solaris Cluster configuration and environment to support the formation of partnerships and protection groups with the Geographic Edition framework. The following table describes these prerequisite tasks.

TABLE 4 Prerequisite Configuration Tasks

Task	Description
1. Set the cluster name to the name you want to use with the Geographic Edition framework.	Use the `cluster` command. For more information about this requirement, see "How to Enable the Geographic Edition Framework" on page 39.
2. Set up the IP address and host maps for the cluster that is enabled to run Geographic Edition framework.	See Chapter 2, "Installing Software on Global-Cluster Nodes" in *Oracle Solaris Cluster 4.3 Software Installation Guide*.
3. Install and configure your data replication product. **Note -** This step is required before you can create protection groups with the `geopg create` command.	See the Geographic Edition data replication guide for the product you are using. A list of available manuals is provided in "Protection Groups" on page 24.
4. Port and configure application configuration and corresponding resource groups on clusters that are candidates for partnership.	See the guidelines and prerequisites in "Creating a Partnership" on page 43.

Installation and Configuration Tasks

After you have completed the prerequisite configuration tasks, you can install and configure the Geographic Edition software as described in the following table.

TABLE 5 Geographic Edition Installation and Configuration Tasks

Task	Description and Documentation
1. Install Geographic Edition software.	See "Installing the Geographic Edition Software" on page 29.
2. Set up security between the candidate partner clusters.	■ Exchange certificates, as described in "Security Certificates" on page 20. ■ (Optional) Configure a secure logical hostname that uses IP Security Architecture (IPsec), as described in "IP Security (IPsec)" on page 21.

Task	Description and Documentation
3. If using a zone cluster as a partner, prepare the zone cluster for membership.	See “Preparing a Zone Cluster for Partner Membership” on page 35.
4. Enable the Geographic Edition framework.	Issue the `geoadm start` command. For more information, see “Enabling the Geographic Edition Framework” on page 38.
5. Create partnerships.	See “Configuring a Partnership” on page 41.
6. Configure data replication.	See the Geographic Edition data replication manual for the product you use. A list of available manuals is provided in “Protection Groups” on page 24.
7. Create and validate protection groups.	See the Geographic Edition manual for the data replication product you use. To create a protection group that does not require data replication, see “Creating a Protection Group That Does Not Require Data Replication” on page 50.
8. Add data replication device groups and application resource groups to the protection group.	See the Geographic Edition manual for the data replication product you use.
9. Bring online (activate) the protection groups.	See “How to Activate a Protection Group” on page 56.
10 (Optional) Create sites and multigroups.	Set up sets of clusters and protection groups on which to perform switchover or takeover in a single operation. For more information, see “Configuring Sites and Multigroups” on page 59.
11. Test the configured partnership and protection groups to validate the setup.	Perform a trial switchover or takeover and test some simple failure scenarios. See Chapter 10, “Migrating Services” in *Oracle Solaris Cluster 4.3 Geographic Edition System Administration Guide* and procedures to migrate services in the Geographic Edition manual for your data replication product. **Note -** You cannot perform personality swaps if you are running EMC Symmetrix Remote Data Facility/Asynchronous data replication.

Installing the Geographic Edition Software

You must install the Geographic Edition software on every node of each cluster in your geographically separated cluster by using the `pkg add` command.

How to Install the Geographic Edition Software

This procedure explains how to install the Geographic Edition software. Perform the procedure in the global zone for each node of a global cluster or zone cluster that you are configuring in a partnership.

Before You Begin

The following manuals contain information that can help you plan your configuration and prepare your installation strategy:

- *Oracle Solaris Cluster 4.3 Release Notes* – Restrictions, bug workarounds, and other late-breaking information.
- *Oracle Solaris Cluster 4.3 Geographic Edition Overview*.
- Documentation for related third-party software products.

Before you begin to install software, make the following preparations:

- Ensure that the Oracle Solaris OS is installed to support the Geographic Edition software.

  If Oracle Solaris software is already installed on the node, you must ensure that the Oracle Solaris installation meets the requirements for Geographic Edition software and any other software that you intend to install on the cluster.

  Note - If you want to use the Oracle Solaris Cluster Manager browser interface to administer Geographic Edition components, ensure that all cluster nodes have the same root password.

- Read Chapter 1, "Planning the Geographic Edition Installation".

1. **Become the `root` role in the global zone of the node where you intend to run the Geographic Edition software.**

   Note - Geographic Edition software must be installed in the global zone for all nodes of each cluster in the partnership, regardless of whether the partner cluster is a global cluster or a zone cluster. For a zone cluster that will be configured in a partnership, Geographic Edition software must be installed in both the zone cluster nodes and on the underlying global cluster nodes.

2. **Set up the repository for the Oracle Solaris Cluster software packages.**

   The repository setup process depends on whether the nodes have access to the Internet or whether you are using an ISO image of the software.

   - **If the cluster nodes have direct access or web proxy access to the Internet:**

a. **Go to https://pkg-register.oracle.com.**

b. **Choose Oracle Solaris Cluster Software.**

c. **Accept the license.**

d. **Request a new certificate by choosing Oracle Solaris Cluster Software and submitting a request.**

The certification page is displayed with download buttons for the key and the certificate.

e. **Download the key and certificate files and install them as described in the returned certification page.**

f. **Configure the ha-cluster publisher with the downloaded SSL keys and set the location of the Oracle Solaris Cluster 4.3 repository.**

In the following example, the repository name is https://pkg.oracle.com/solaris/cluster/.

```
# pkg set-publisher \
-k /var/pkg/ssl/Oracle_Solaris_Cluster_4.1.key.pem \
-c /var/pkg/ssl/Oracle_Solaris_Cluster_4.1.certificate.pem \
-O https://pkg.oracle.com/solaris/cluster/ ha-cluster
```

`-k /var/pkg/ssl/Oracle_Solaris_Cluster_4.1.key.pem`

Specifies the full path to the downloaded SSL key file.

`-c /var/pkg/ssl/Oracle_Solaris_Cluster_4.1.certificate.pem`

Specifies the full path to the downloaded certificate file.

`-O https://pkg.oracle.com/solaris/cluster/`

Specifies the URL to the Oracle Solaris Cluster 4.1 package repository.

For more information, see the pkg(1) man page.

- **If you are using an ISO image of the software:**

a. **Download the Oracle Solaris Cluster 4.3 ISO image from Oracle Software Delivery Cloud at https://edelivery.oracle.com/.**

Note - A valid Oracle license is required to access Oracle Software Delivery Cloud.

Oracle Solaris Cluster software, which includes Geographic Edition software, is part of the Oracle Solaris Product Pack. Follow online instructions to complete selection of the media pack and download the software.

b. Make the Oracle Solaris Cluster 4.3 ISO image available.

```
# lofiadm -a path-to-ISO-image
/dev/lofi/N
# mount -F hsfs /dev/lofi/N /mnt
```

-a *path-to-ISO-image*

Specifies the full path and file name of the ISO image.

c. Set the location of the Oracle Solaris Cluster 4.3 package repository.

```
# pkg set-publisher -g file:///mnt/repo ha-cluster
```

3. Ensure that the `solaris` and `ha-cluster` publishers are valid.

```
# pkg publisher
PUBLISHER                             TYPE     STATUS   P  LOCATION
solaris                               origin   online   F  solaris-repository
ha-cluster                            origin   online   F  ha-cluster-repository
```

For information about setting the `solaris` publisher, see "Adding, Modifying, or Removing Package Publishers" in *Adding and Updating Software in Oracle Solaris 11.3*.

Tip - Use the `-nv` options whenever you install or update to see what changes will be made, such as which versions of which packages will be installed or updated and whether a new BE will be created. The `-v` option also shows any release notes that apply to this particular install or update operation.

If you do not get any error messages when you use the `-nv` options, run the command again without the `-n` option to actually perform the installation or update. If you do get error messages, run the command again with more `-v` options (for example, `-nvv`) or more of the package FMRI to get more information to help you diagnose and fix the problem. For troubleshooting information, see Appendix A, "Troubleshooting Package Installation and Update," in *Adding and Updating Software in Oracle Solaris 11.3*.

4. Install the Geographic Edition 4.3 software.

```
# /usr/bin/pkg install ha-cluster-geo-full
```

5. **Verify that the package installed successfully.**

   Output is similar to the following example, which checks the installation state of the `ha-cluster-geo-full` group package.

```
% pkg info ha-cluster/group-package/ha-cluster-geo-full
Name: ha-cluster/group-package/ha-cluster-geo-full
Summary: Oracle Solaris Cluster Geographic Edition full group package
Description: Oracle Solaris Cluster Geographic Edition full group package
Category: Meta Packages/Group Packages
State: Installed
Publisher: ha-cluster
Version: 4.1.0
Build Release: 5.11
Branch: 0.22
Packaging Date: Sat Oct 22 07:28:36 2011
Size: 77.00 B
FMRI: pkg://ha-cluster/ha-cluster/group-package/ha-cluster-geo-full@version:dateTtimeZ
```

6. **If you installed from a DVD-ROM, unload the installation DVD-ROM from the DVD-ROM drive.**

7. **Repeat this procedure on each node of each partner cluster.**

Next Steps If you need to install any required software updates, see Chapter 3, “Upgrading or Updating Geographic Edition Software”.

Securing Geographic Edition Software

This section provides procedures to configure IP Security Architecture (IPsec) to secure communication between partner clusters.

For additional information about configuring secure communication between partner clusters, see “Planning Security” on page 18.

How to Configure IPsec for Secure Cluster Communication

The following example procedure configures a cluster, `cluster-paris`, for IPsec secure communication with another cluster, `cluster-newyork`. The procedure assumes that the local logical hostname on `cluster-paris` is `lh-paris-1` and that the remote logical hostname is `lh-newyork-1`. Inbound messages are sent to `lh-paris-1` and outbound messages are sent to `lh-newyork-1`.

Perform the following procedure on each node of `cluster-paris`.

1. **Log in to the first node of the primary cluster, `phys-paris-1`, as the `root` role.**

   For a reminder of which node is `phys-paris-1`, see "Example Geographic Edition Cluster Configuration" in *Oracle Solaris Cluster 4.3 Geographic Edition System Administration Guide*.

2. **Set up an entry for the local address and remote address in the IPsec policy file.**

   The policy file is located at `/etc/inet/ipsecinit.conf`. Permissions on this file should be `644`. For more information about this file, see the `ipsecconf(1M)` man page.

   For information about the names and values that are supported by Geographic Edition software, see "Legal Names and Values of Geographic Edition Entities" in *Oracle Solaris Cluster 4.3 Geographic Edition System Administration Guide*.

   a. **Configure the communication policy.**

      The default port for the `tcp_udp` plug-in is 2084. You can specify this value in the `etc/cacao/instances/default/modules/com.sun.cluster.geocontrol.xml` file.

      The following entry in the `/etc/inet/ipsecinit.conf` file configures a policy with no preference for authorization or encryption algorithms.

      ```
      # {raddr lh-newyork-1 rport 2084} ipsec {auth_algs any encr_algs any \
      sa shared} {laddr lh-paris-1 lport 2084} ipsec {auth_algs any encr_algs \
      any sa shared}
      ```

      When you configure the communication policy on the secondary cluster, `cluster-newyork`, you must reverse the policies.

      ```
      # {laddr lh-newyork-1 lport 2084} ipsec {auth_algs any encr_algs \
      any sa shared} {raddr lh-paris-1 rport 2084} ipsec {auth_algs any encr_algs \
      any sa shared}
      ```

   b. **Add the policy by rebooting the node or by running the following command.**

```
# ipsecconf -a /etc/inet/ipsecinit.conf
```

3. **Set up encryption and authentication keys for inbound and outbound communication.**

   The communication file is located at `/etc/init/secret/ipseckeys`. Permissions on the file should be `600`.

   Add keys:

   ```
   # ipseckey -f /etc/init/secret/ipseckeys
   ```

   Key entries have the following general format:

   ```
   # inbound to cluster-paris
   add esp spi paris-encr-spi dst lh-paris-1 encr_alg paris-encr-algorithm \
   encrkey paris-encrkey-value
   add ah spi newyork-auth-spi dst lh-paris-1 auth_alg paris-auth-algorithm \
   authkey paris-authkey-value

   # outbound to cluster-newyork
   add esp spi newyork-encr-spi dst lh-newyork-1 encr_alg newyork-encr-algorithm \
   encrkey newyork-encrkey-value
   add ah spi newyork-auth-spi dst lh-newyork-1 auth_alg newyork-auth-algorithm \
   authkey newyork-authkey-value
   ```

   For more information about the communication files, see the `ipsecconf`(1M) man page.

Next Steps If you are configuring a zone cluster as a member of a partnership, go to “Preparing a Zone Cluster for Partner Membership” on page 35.

Otherwise, go to “Enabling the Geographic Edition Framework” on page 38.

Preparing a Zone Cluster for Partner Membership

To enable a zone cluster to function as a member of a Geographic Edition partnership, the common agent container must be manually configured within the zone cluster.

How to Prepare a Zone Cluster for Partner Membership

This procedure configures common agent container security in a zone cluster to prepare the zone cluster for use in a cluster partnership.

Before You Begin Ensure that the following conditions are met:

- The zone cluster is created. See "Creating and Configuring a Zone Cluster" in *Oracle Solaris Cluster 4.3 Software Installation Guide*.
- You have read the requirements for using a zone cluster in a cluster partnership. See "Zone Clusters" on page 23.
- Geographic Edition software is installed in the global cluster that supports the zone cluster you are configuring.

1. **Assume the `root` role on a node of the global cluster that supports the zone cluster you are configuring.**

2. **Set up the network address for the zone cluster.**

```
phys-schost# clzonecluster configure zone-cluster-name
clzc:zone-cluster-name> add net
clzc:zone-cluster-name:net> set address=zone-cluster-name
clzc:zone-cluster-name:net> end

clzc:zone-cluster-name> verify
clzc:zone-cluster-name> commit
clzc:zone-cluster-name> exit
```

3. **Copy the security files for the common agent container to all zone cluster nodes.**

   This step ensures that security files for the common agent container are identical on all cluster nodes and that the copied files retain the correct file permissions.

   Perform all steps in the zone cluster.

   a. **Log in to each node of the zone cluster.**

```
phys-schost# zlogin zone-cluster-name
zcname#
```

   b. **On each node, stop the common agent container.**

```
zcname# /usr/sbin/cacaoadm stop
```

c. On one node, create the security keys.

```
zcname# cacaoadm create-keys --force
```

d. Create a tar file of the `/etc/cacao/instances/default/security` directory.

```
zcname# cd /etc/cacao/instances/default
zcname# tar cf /tmp/SECURITY.tar ./security
```

e. Copy the `/tmp/SECURITY.tar` file to each of the other cluster nodes.

f. On each node to which you copied the `/tmp/SECURITY.tar` file, extract the security files.

Any security files that already exist in the `/etc/cacao/instances/default/security` directory are overwritten.

```
zcname# cd /etc/cacao/instances/default
zcname# tar xf /tmp/SECURITY.tar
```

g. Delete the `/tmp/SECURITY.tar` file from each node in the cluster.

You must delete each copy of the tar file to avoid security risks.

```
zcname# rm /tmp/SECURITY.tar
```

h. On each node, set the common agent container network-bin address.

```
zcname# cacaoadm set-param network-bind-address=0.0.0.0
```

i. On each node, enable and start the common agent container.

```
zcname# /usr/sbin/cacaoadm enable
zcname# /usr/sbin/cacaoadm start
```

4. Verify that the Geographic Edition modules are loaded on the zone cluster node.

```
phys-schost# cacaoadm status com.sun.cluster.geocontrol
phys-schost# cacaoadm status com.sun.cluster.geoutilities
phys-schost# cacaoadm status com.sun.cluster.notifier
```

- If a module is loaded, command output would be similar to the following example. You can safely ignore the message `Module is not in good health`.

```
Operational State:ENABLED
Administrative State:LOCKED
```

```
Availability Status:[]
Module is not in good health.
```

- If a module is not loaded, command output would be similar to the following example.

```
Module com.sun.cluster.geocontrol has not been loaded.
Cause of the problem:[DEPENDENCY]
```

For information about common errors, see the Troubleshooting section at the end of this procedure.

5. **Exit the zone cluster node.**

```
zcname# exit
phys-schost#
```

Troubleshooting If a Geographic Edition module is not loaded, check that the zone cluster configuration is correct.

After you have verified that the configuration is complete and correct and you have fixed any errors, do one of the following:

- On each zone cluster node, restart the common agent container.

```
zcnode# /usr/sbin/cacaoadm restart
```

- From a global-cluster node, reboot the zone cluster.

```
phys-schost# clzonecluster reboot zone-cluster-name
```

After processing is complete on all zone cluster nodes, check that the Geographic Edition modules are now loaded. If any modules are still not loaded, contact your Oracle service representative for assistance.

Next Steps Go to "Enabling the Geographic Edition Framework" on page 38.

Enabling the Geographic Edition Framework

When the Geographic Edition framework is enabled, the cluster is ready to enter a partnership with another enabled cluster.

For more information about setting up and installing Geographic Edition, see Chapter 3, "Administering the Geographic Edition Framework" in *Oracle Solaris Cluster 4.3 Geographic Edition System Administration Guide*.

▼ How to Enable the Geographic Edition Framework

This procedure enables the Geographic Edition framework on the local cluster only. Repeat this procedure on all the clusters of your geographically separated cluster.

Before You Begin Ensure that the following conditions are met:

- The cluster is running the Oracle Solaris operating system and Oracle Solaris Cluster software.
- If you want to use the Oracle Solaris Cluster Manager browser interface to administer Geographic Edition components, ensure that all cluster nodes have the same root password.
- The Oracle Solaris Cluster management-agent container for Oracle Solaris Cluster Manager is running.
- Geographic Edition software is installed.
- The cluster has been configured for secure cluster communication by using security certificates, that is, nodes within the same cluster must share the same security certificates. This is configured during Oracle Solaris Cluster installation.

1. **Assume the `root` role on a cluster node.**

2. **Ensure that the logical hostname, which is the same as the cluster name, is available and defined.**

   ```
   # cluster list
   ```

   For global clusters, if the cluster name is not the name that you want to use, change the cluster name with the following command:

   `# cluster rename -c` *new-cluster-name cluster-name*

   `-c` *new-cluster-name*

   Specifies the new cluster name.

   cluster-name

   The cluster whose name you are changing.

   For more information, see the `cluster`(1CL) man page.

   Note - After you have enabled the Geographic Edition framework, you must not change the cluster name while the framework is enabled.

3. **Confirm that the naming service and the local `hosts` files contain a host entry that matches the cluster name.**

The local hosts file, `hosts`, is located in the `/etc/inet` directory.

4. **On a node of the cluster, start the Geographic Edition framework.**

```
# geoadm start
```

The `geoadm start` command enables the Geographic Edition framework on the local cluster only. For more information, see the `geoadm`(1M) man page.

5. **Verify that you have enabled the framework and that the Geographic Edition resource groups are online.**

```
# geoadm show
# clresourcegroup status geo-clusterstate geo-infrastructure
# clresource status -g geo-clusterstate,geo-infrastructure
```

The output for the `geoadm show` command indicates that the Geographic Edition framework is active from a particular node in the cluster.

The output for the `clresourcegroup status` and `clresource status` commands display that the `geo-failovercontrol`, `geo-hbmonitor`, and `geo-clustername` resources and the `geo-infrastructure` resource group are online on one node of the cluster. The `geo-clusterstate` resource group is online on both nodes.

For more information, see the `clresourcegroup`(1CL) and `clresource`(1CL) man pages.

Example 1 Enabling the Geographic Edition Framework on a Cluster

This example enables the Geographic Edition framework on the `cluster-paris` cluster.

1. Start the Geographic Edition framework on `cluster-paris`.

```
phys-paris-1# geoadm start
```

2. Ensure that the Geographic Edition framework was successfully enabled.

```
phys-paris-1# geoadm show

--- CLUSTER LEVEL INFORMATION ---
Oracle Solaris Cluster Geographic Edition is active on cluster-paris from node phys-
paris-1
Command execution successful
phys-paris-1#
```

3. Verify the status of the Geographic Edition resource groups and resources.

```
phys-paris-1# clresourcegroup status geo-clusterstate geo-infrastructure
```

```
=== Cluster Resource Groups ===

Group Name                     Node Name             Suspended           Status
----------                     ---------             ---------           ------
geo-clusterstate               phys-paris-1          No                  Online
                               phys-paris-2          No                  Online

geo-infrastructure             phys-paris-1          No                  Online
                               phys-paris-2          No                  Offline

phys-paris-1# clresource status -g geo-clusterstate,geo-infrastructure

=== Cluster Resources ===

Resource Name           Node Name       State         Status Message
-------------           ---------       -----         --------------
geo-clustername         phys-paris-1    Online        Online - LogicalHostname
 online.
                        phys-paris-2    Offline       Offline

geo-hbmonitor           phys-paris-1    Online        Online - Daemon OK
                        phys-paris-2    Offline       Offline

geo-failovercontrol     phys-paris-1    Online        Online - Service is online.
                        phys-paris-2    Offline       Offline
```

Next Steps Configure trust between partner clusters. Go to "How to Configure Trust Between Two Clusters" on page 42.

Configuring a Partnership

This section provides the following Information:

- "Configuring Trust Between Partner Clusters" on page 42
- "Creating a Partnership" on page 43
- "Joining an Existing Partnership" on page 46

Configuring Trust Between Partner Clusters

Before you create a partnership between two clusters, you must configure the Geographic Edition framework for secure communication between the two clusters. The configuration must be reciprocal. For example, you must configure the cluster `cluster-paris` to trust the cluster `cluster-newyork`, and you must also configure the cluster `cluster-newyork` to trust the cluster `cluster-paris`.

▼ How to Configure Trust Between Two Clusters

Note - You can also perform this task by using the Oracle Solaris Cluster Manager browser interface. Click Partnerships, then click Add Partner Trust. For Oracle Solaris Cluster Manager log-in instructions, see "How to Access Oracle Solaris Cluster Manager" in *Oracle Solaris Cluster 4.3 System Administration Guide*.

Before You Begin Ensure that the following conditions are met:

- The cluster on which you want to create the partnership is running.
- The `geoadm start` command has already been run on this cluster and the partner cluster. For more information about using the `geoadm start` command, see "Enabling the Geographic Edition Framework" on page 38.
- The cluster name of the partner cluster is known.
- The host information of the partner cluster is defined in the local hosts file. The local cluster needs to be able to reach the partner cluster by name.

1. **Assume the `root` role on a cluster node.**

2. **Import the public keys from the remote cluster to the local cluster.**

   Run the following command on one node of the local cluster to import the keys from the remote cluster to one node of the cluster.

   local-cluster# **`geops add-trust -c`** *remote-cluster*

   `-c` *remote-cluster*

   Specifies the logical hostname of the cluster with which to form a partnership. The logical hostname is used by the Geographic Edition framework and maps to the name of the remote partner cluster. For example, a remote partner cluster name might resemble `cluster-paris`.

When you use this option with the `add-trust` or `remove-trust` subcommand, the option specifies the alias where the public keys on the remote cluster are stored. An alias for certificates on the remote cluster has the following pattern:

remote-cluster`.certificate[0-9]*`

Only keys that belong to the remote cluster should have an alias that matches this pattern.

For more information about the `geops` command, refer to the `geops(1M)` man page.

3. **Repeat the preceding steps on a node of the remote partner cluster.**

4. **Verify trust from one node of each cluster.**

Note - You can also accomplish this step by using the Oracle Solaris Cluster Manager browser interface. Click Partnerships, then click Verify Partner Trust. For Oracle Solaris Cluster Manager log-in instructions, see "How to Access Oracle Solaris Cluster Manager" in *Oracle Solaris Cluster 4.3 System Administration Guide*.

```
# geops verify-trust -c remote-cluster
```

Next Steps Configure the partnership. Go to "Creating a Partnership" on page 43.

See Also To find out how to remove trust, see "Removing Trust Between Partner Clusters" in *Oracle Solaris Cluster 4.3 Geographic Edition System Administration Guide*.

Creating a Partnership

This section provides procedures to create a Geographic Edition partnership between two clusters.

▼ How to Create a Partnership

Note - You can also accomplish this procedure by using the Oracle Solaris Cluster Manager browser interface. Click Partnerships, and then click Create. For Oracle Solaris Cluster Manager log-in instructions, see "How to Access Oracle Solaris Cluster Manager" in *Oracle Solaris Cluster 4.3 System Administration Guide*.

Before You Begin Ensure that the following conditions are met:

- The cluster on which you want to create the partnership is up and running.

- If a partner cluster is a zone cluster, either application-based replication such as, Oracle Data Guard, or EMC Symmetrix Remote Data Facility storage-based replication is configured or no data replication is used.
- The `geoadm start` command must have already been run on the this cluster and the partner cluster. For more information about using the `geoadm start` command, see "Enabling the Geographic Edition Framework" on page 38.
- The cluster name of the partner cluster is known.
- The host information of the partner cluster must defined in the local host file. The local cluster needs to be able to reach the partner cluster by name.
- Security has been configured on the two clusters by installing the appropriate certificates. See "Configuring Trust Between Partner Clusters" on page 42 for more information.

1. Log in to a cluster node.

You must be assigned the Geo Management RBAC rights profile to complete this procedure. For more information about RBAC, see "Securing Geographic Edition Software" on page 33.

2. Create the partnership.

local-partner-cluster`#` **`geops create -c`** *remote-partner-cluster*`[`**`.`***domain-name*`]` `[`**`-h`** *heartbeat*`]` `\`
`[`**`-p`** *property-setting* `[`**`-p…`**`]]` *partnership*

`-c` *remote-partner-cluster*[.*domain-name*]

Specifies the name of the remote cluster that will participate in the partnership. If clusters in the partnership are in different domains, you must also specify the domain name of the remote cluster.

This name matches the logical hostname used by the Geographic Edition framework on the remote cluster.

`-h` *heartbeat*

Specifies a custom heartbeat to use in the partnership to monitor the availability of the partner cluster.

If you omit this option, the default Geographic Edition heartbeat is used.

Custom heartbeats are provided for special circumstances and require careful configuration. Consult your Oracle specialist for assistance if your system requires the use of custom heartbeats. For more information about configuring custom heartbeats and custom heartbeat plug-ins, see Chapter 5, "Administering Heartbeats and Heartbeat Plug-Ins" in *Oracle Solaris Cluster 4.3 Geographic Edition System Administration Guide*.

If you create a custom heartbeat, you must add at least one plug-in to prevent the partnership from remaining in degraded mode.

You must configure the custom heartbeat that you provide in this option before you run the `geops` command.

Note - A custom heartbeat prevents the default heartbeat from being used during partnership creation. If you want to use the default heartbeat for your partnership, you must delete the custom heartbeat before you run the `geops create` command.

`-p` *property-setting*

Specifies the value of partnership properties with a string of *property*=*value* pair statements.

Specify a description of the partnership with the `Description` property.

You can configure heartbeat-loss notification with the `Notification_emailaddrs` and `Notification_actioncmd` properties. For more information about configuring heartbeat-loss notification, see "Configuring Heartbeat-Loss Notification" in *Oracle Solaris Cluster 4.3 Geographic Edition System Administration Guide*.

For more information about the properties you can set, see Appendix A, "Standard Geographic Edition Properties," in *Oracle Solaris Cluster 4.3 Geographic Edition System Administration Guide*.

partnership

Specifies the name of the partnership.

For information about the names and values that are supported by the Geographic Edition framework, see "Legal Names and Values of Geographic Edition Entities" in *Oracle Solaris Cluster 4.3 Geographic Edition System Administration Guide*.

For more information about the `geops` command, refer to the `geops`(1M) man page.

3. **Verify that the partnership was created and the status of the partnership.**

Note - You can also accomplish this step by using the Oracle Solaris Cluster Manager browser interface. Click Partnerships to view partnership information. For additional details, click the partnership name. For Oracle Solaris Cluster Manager log-in instructions, see "How to Access Oracle Solaris Cluster Manager" in *Oracle Solaris Cluster 4.3 System Administration Guide*.

The partnership states will be Degraded and the heartbeat state will be Offline. These states will change after the partnership is joined from the partner cluster.

local-partner-cluster# **`geoadm status`**

Example 2 Creating a Partnership

This example creates the `paris-newyork-ps` partnership on the `cluster-paris.usa` cluster.

```
cluster-paris.usa1# geops create -c cluster-newyork.usa \
-p Description=Transatlantic \
-p Notification_emailaddrs=sysadmin@example.com \
paris-newyork-ps
```

Example 3 Creating a Partnership That Uses a Custom Heartbeat and a Custom Heartbeat Plug-In

This example creates the heartbeat `paris-to-newyork`, creates the custom heartbeat plug-in `command1` and adds it to the custom heartbeat, creates a the partnership `paris-newyork-ps` to use the custom heartbeat, and verifies the partnership status.

```
# geohb create -r cluster-newyork paris-to-newyork
# geohb add-plugin command1 paris-to-newyork -p Query_cmd=/usr/bin/hb/
# geops create -c cluster-newyork -h paris-to-newyork paris-newyork-ps
# geoadm status
```

Next Steps To finalize the new partnership, the remote partner cluster must join the partnership. Go to "Joining an Existing Partnership" on page 46.

See Also To remove a partnership between two clusters, see "How to Remove Trust Between Two Clusters" in *Oracle Solaris Cluster 4.3 Geographic Edition System Administration Guide*.

Joining an Existing Partnership

When you define and configure a partnership, the partnership specifies a second cluster to be a member of that partnership. Then, you must configure this second cluster to join the partnership.

▼ How to Join a Partnership

Note - You can also accomplish this procedure by using the Oracle Solaris Cluster Manager browser interface. Click Partnerships, then click Join Partnership. For Oracle Solaris Cluster Manager log-in instructions, see "How to Access Oracle Solaris Cluster Manager" in *Oracle Solaris Cluster 4.3 System Administration Guide*.

Before You Begin Ensure that the following conditions are met:

- The local cluster is enabled to run the Geographic Edition software.
- The partnership you want the cluster to join is defined and configured on another cluster (`cluster-paris`) and the local cluster (`cluster-newyork`) is specified as a member of this partnership. See "Creating a Partnership" on page 43.
- If a partner cluster is a zone cluster, either application-based replication, such as Oracle Data Guard, or EMC Symmetrix Remote Data Facility storage-based replication is configured, or no data replication is used.
- Security has been configured on the clusters by installing the appropriate certificates.

  See "Security Certificates" in *Oracle Solaris Cluster 4.3 Geographic Edition Installation and Configuration Guide* for more information.

1. **Log in to a node of the cluster that is joining the partnership.**

   You must be assigned the Geo Management RBAC rights profile to complete this procedure. For more information about RBAC, see "Planning Security" on page 18.

2. **Confirm that the remote cluster that originally created the partnership, `cluster-paris`, can be reached at its logical hostname.**

   local-partner-cluster`# ping lh-paris-1`

   For information about the logical hostname of the cluster, see "How to Enable the Geographic Edition Framework" on page 39.

3. **Join the partnership.**

   local-partner-cluster`# geops join-partnership [-h` *heartbeat*`]` *remote-partner-cluster partnership*

   -h *heartbeat*

   Specifies a custom heartbeat to use in the partnership to monitor the availability of the partner cluster.

   If you omit this option, the default Geographic Edition heartbeat is used.

   Custom heartbeats are provided for special circumstances and require careful configuration. Consult your Oracle specialist for assistance if your system requires the use of custom heartbeats. For more information about configuring custom heartbeats, see Chapter 5, "Administering Heartbeats and Heartbeat Plug-Ins" in *Oracle Solaris Cluster 4.3 Geographic Edition System Administration Guide*.

   If you create a custom heartbeat, you must add at least one plug-in to prevent the partnership from remaining in degraded mode.

   You must configure the custom heartbeat that you provide in this option before you run the `geops` command.

remote-partner-cluster

Specifies the name of a cluster that is currently a member of the partnership that is being joined. This cluster is used to retrieve the partnership configuration information.

partnership

Specifies the name of the partnership.

For information about the names and values that are supported by Geographic Edition software, see "Legal Names and Values of Geographic Edition Entities" in *Oracle Solaris Cluster 4.3 Geographic Edition System Administration Guide*.

For more information about the `geops` command, refer to the `geops(1M)` man page.

4. **Verify that the cluster was added to the partnership and that the partnership properties were defined correctly.**

```
local-partner-cluster# geops list
local-partner-cluster# geoadm status
```

Example 4 Joining a Partnership

This example joins the `cluster-newyork` cluster to the `paris-newyork-ps`partnership.

```
phys-newyork-1# geops join-partnership cluster-paris paris-newyork-ps
phys-newyork-1# geops list
phys-newyork-1# geoadm status
```

Example 5 Creating and Joining a Partnership With a Remote Cluster in a Different Domain

This example creates and configures the `paris-newyork-ps` partnership between clusters `cluster-paris.france.example.com` and `cluster-newyork.usa.example.com`.

1. On one node of `cluster-paris.france.example.com`, configure trust for the partnership.

```
phys-paris-1# geops add-trust -c cluster-newyork.usa.example.com
```

2. On one node of `cluster-newyork.usa`, configure trust for the partnership.

```
phys-newyork-1# geops add-trust -c cluster-paris.france.example.com
```

3. On each node of both clusters, verify that trust has been set up properly, both between the local cluster and partner cluster and among nodes of the local cluster.

```
phys-newyork-1# geops verify-trust -c cluster-paris.france.example.com
phys-newyork-2# geops verify-trust -c cluster-paris.france.example.com
```

```
phys-newyork-1# geops verify-trust
phys-newyork-2# geops verify-trust

phys-paris-1# geops verify-trust -c cluster-newyork.usa.example.com
phys-paris-2# geops verify-trust -c cluster-newyork.usa.example.com
phys-paris-1# geops verify-trust
phys-paris-2# geops verify-trust
```

4. On `cluster-paris.france.example.com`, create the partnership `paris-newyork-ps`.

```
cluster-paris# geops create -c cluster-newyork.usa.example.com \
-p Description=Transatlantic \
-p Notification_emailaddrs=sysadmin@example.com
paris-newyork-ps
```

5. On `cluster-newyork.usa`, join the partnership `paris-newyork-ps`.

```
cluster-newyork# geops join-partnership cluster-paris.france.example.com
paris-newyork-ps
```

6. Verify that the partnership has been created successfully.

```
# geops list
# geoadm status
```

Next Steps Configure protection groups. See "Configuring Protection Groups" on page 49 and the Geographic Edition manual for the data replication product you will use.

Configuring Protection Groups

This section contains the following information:

- "Creating a Protection Group That Uses Data Replication" on page 50
- "Creating a Protection Group That Does Not Require Data Replication" on page 50
- "Validating a Protection Group" on page 55
- "Activating a Protection Group" on page 56

For information about how to create a protection group for your data replication product, see the appropriate Geographic Edition data replication manual.

Creating a Protection Group That Uses Data Replication

Note - If you do not need to use data replication, see "Creating a Protection Group That Does Not Require Data Replication" on page 50.

The procedures to configure a protection group that uses data replication vary depending on the data replication product you use. See the appropriate Geographic Edition manual for your data replication product for guidelines and procedures to configure a protection group:

- *Oracle Solaris Cluster Geographic Edition Data Replication Guide for EMC Symmetrix Remote Data Facility*
- *Oracle Solaris Cluster Geographic Edition Data Replication Guide for Hitachi TrueCopy and Universal Replicator*
- *Oracle Solaris Cluster Geographic Edition Data Replication Guide for Oracle GoldenGate*
- *Oracle Solaris Cluster Geographic Edition Data Replication Guide for MySQL*
- *Oracle Solaris Cluster Geographic Edition Data Replication Guide for Oracle Data Guard*
- *Oracle Solaris Cluster Geographic Edition Data Replication Guide for Oracle Solaris Availability Suite*
- *Oracle Solaris Cluster Geographic Edition Data Replication Guide for ZFS Snapshots*
- *Oracle Solaris Cluster Geographic Edition Remote Replication Guide for Oracle ZFS Storage Appliance*

After you create the protection group and add application resource groups and data-replicated components, validate the protection group. Go to "Validating a Protection Group" on page 55.

Creating a Protection Group That Does Not Require Data Replication

Some protection groups do not require data replication. If you are using the Geographic Edition framework to manage only resource groups, you can create protection groups that do not replicate data.

Note - To find out how to create a protection group that uses data replication, see "Creating a Protection Group That Uses Data Replication" on page 50.

This section provides the following procedures:

- "How to Create a Protection Group That Is Configured Not to Use Data Replication" on page 52
- "How to Add an Application Resource Group to a Protection Group That Does Not Use Data Replication" on page 53

Note - You cannot add device groups to a protection group that does not use data replication.

You can configure the following properties for a protection group that does not use data replication:

`Description`

Describes the protection group.

`External_Dependency_Allowed`

Specifies whether to allow any dependencies between resource groups and resources that belong to this protection group and resource groups and resources that do not belong to this protection group.

`RoleChange_ActionArgs`

Specifies a string that follows system-defined arguments at the end of the command line when the role-change callback command runs.

`RoleChange_ActionCmd`

Specifies the path to an executable command. This path should be valid on all nodes of all partner clusters that can host the protection group. The script is invoked during a switchover or takeover on the new primary cluster when the protection group is started on the new primary cluster. The script is invoked on the new primary cluster after the data replication role changes from secondary to primary and before the application resource groups are brought online. If the data replication role change does not succeed, then the script is not called.

`Timeout`

Specifies the timeout period for the protection group in seconds. You can change the timeout period from the default value depending on the complexity of your data replication configuration.

For more information about the properties you can set, see Appendix A, "Standard Geographic Edition Properties," in *Oracle Solaris Cluster 4.3 Geographic Edition System Administration Guide*.

▼ How to Create a Protection Group That Is Configured Not to Use Data Replication

---

Note - You can also accomplish this procedure by using the Oracle Solaris Cluster Manager browser interface. Click Partnerships, click the partnership name to go to its page, and click Create in the Protection Groups section. For Oracle Solaris Cluster Manager log-in instructions, see "How to Access Oracle Solaris Cluster Manager" in *Oracle Solaris Cluster 4.3 System Administration Guide*.

Before You Begin Before you create a protection group without data replication, ensure that the following conditions are met:

- The local cluster is a member of a partnership.
- The protection group that you are creating does not already exist.
- You are assigned the Geo Management RBAC rights profile. For more information about RBAC, see "Securing Geographic Edition Software" on page 33.

Note - Protection group names are unique in the global Geographic Edition namespace. You cannot use the same protection group name in more than one partnership on the same system.

---

1. **Log in to a cluster node.**

2. **Create a new protection group by using the `geopg create` command.**

   This command creates a protection group on the local cluster.

   ```
   # geopg create -s partnership -o local-role \
   [-p property [-p …]] protection-group
   ```

   -s *partnership*

   Specifies the name of the partnership.

   -o *local-role*

   Specifies the role of this protection group on the local cluster as either `Primary` or `Secondary`.

   -p *property-setting*

   Specifies the properties of the protection group.

   You can specify the following properties:

protection-group

Specifies the name of the protection group.

For information about the names and values that are supported by Geographic Edition software, see "Legal Names and Values of Geographic Edition Entities" in *Oracle Solaris Cluster 4.3 Geographic Edition System Administration Guide*.

For more information about the `geopg` command, refer to the `geopg(1M)` man page.

Example 6 Creating and Configuring a Protection Group That Is Configured Not to Use Data Replication

This example creates a protection group that is configured not to use data replication.

```
# geopg create -s paris-newyork-ps -o primary example-pg
```

Next Steps Go to "How to Add an Application Resource Group to a Protection Group That Does Not Use Data Replication" on page 53.

See Also To delete a protection group, see "Deleting Protection Groups and Data Replication Components" in *Oracle Solaris Cluster 4.3 Geographic Edition System Administration Guide*.

▼ How to Add an Application Resource Group to a Protection Group That Does Not Use Data Replication

1. **Log in to a cluster node.**

   You must be assigned the Geo Management RBAC rights profile to complete this procedure. For more information about RBAC, see "Securing Geographic Edition Software" on page 33.

2. **Ensure that the `Auto_start_on_new_cluster` property of the resource group is set to `False`.**

   ```
   # clresourcegroup show -p Auto_start_on_new_cluster resource-group
   ```

   If necessary, change the property value to `False`.

   ```
   # clresourcegroup set -p Auto_start_on_new_cluster=False resource-group
   ```

3. **If the application resource group must have dependencies on resource groups and resources that are not managed by this protection group, ensure that the `External_Dependency_Allowed` property of the protection group is set to `TRUE`.**

```
# geopg show protection-group | grep -i external_dependency_allowed
```

If necessary, change the property value to `TRUE`.

```
# geopg set-prop -p External_Dependency_Allowed=TRUE protection-group
```

4. **Start the protection group or change the state of the application resource group to a state that is required for the addition to be allowed.**

   - The Geographic Edition framework requires that the application resource group be in the `UNMANAGED` state on the secondary cluster.
   - If the protection group is stopped on the primary cluster, the application resource group must also be unmanaged on the primary cluster.
   - If the protection group is active on the primary cluster, the application resource group must be in the `UNMANAGED` or `ONLINE` state on the primary cluster.

   For instructions, see "How to Disable a Resource and Move Its Resource Group Into the UNMANAGED State" in *Oracle Solaris Cluster 4.3 Data Services Planning and Administration Guide* or "How to Bring Resource Groups Online" in *Oracle Solaris Cluster 4.3 Data Services Planning and Administration Guide*.

5. **Add an application resource group to the protection group.**

   ```
   # geopg add-resource-group application-resource-group protection-group
   ```

application-resource-group	Specifies the name of an application resource group. You can specify more than one resource group in a comma-separated list.
protection-group	Specifies the name of the protection group. The command adds an application resource group to a protection group on the local cluster. Then, if the partner cluster contains a protection group of the same name, the command propagates the new configuration information to the partner cluster.

   For information about the names and values that are supported by Geographic Edition software, see "Legal Names and Values of Geographic Edition Entities" in *Oracle Solaris Cluster 4.3 Geographic Edition System Administration Guide*.

   After the application resource group is added to the protection group, the application resource group is managed as an entity of the protection group. The application resource group is now affected by protection group operations such as `start`, `stop`, `switchover`, and `takeover`.

Validating a Protection Group

If the configuration status of a protection group is displayed as `Error` in the `geoadm status` output, you can validate the configuration by using the `geopg validate` command. This command checks the current state of the protection group and its entities.

▼ How to Validate a Protection Group

Note - You can also accomplish this procedure by using the Oracle Solaris Cluster Manager browser interface. Click Partnerships, click the partnership name to go to its page, highlight the protection group name, and click Validate. For Oracle Solaris Cluster Manager log-in instructions, see "How to Access Oracle Solaris Cluster Manager" in *Oracle Solaris Cluster 4.3 System Administration Guide*.

Before You Begin Ensure that the following conditions are met:

- The protection group you want to validate exists locally.
- The common agent container is online on all nodes of both clusters in the partnership.
- You are assigned the Geo Management RBAC rights profile. For more information about RBAC, see "Securing Geographic Edition Software" on page 33.

1. **Log in to one of the cluster nodes.**

2. **Validate the configuration of the protection group.**

   This command validates the configuration of the protection group on the local cluster only. To validate the protection group configuration on the partner cluster, run the command again on the partner cluster.

   ```
   # geopg validate protection-group
   ```

   protection-group

   Specifies a unique name that identifies a single protection group

   - If the protection group and its entities are valid, the configuration status of the protection groups is set to `OK`.
   - If the `geopg validate` command finds an error in the configuration files, the command displays an error message and the configuration remains in the `Error` state. Fix the error in the configuration, then rerun the `geopg validate` command.

Next Steps Go to "Activating a Protection Group" on page 56.

Activating a Protection Group

When configuration of a protection group is complete, activate the protection group to put its configuration into service.

▼ How to Activate a Protection Group

This procedure activates the protection group on the primary and secondary clusters, depending on the scope of the command. When you activate a protection group on the primary cluster, its application resource groups are also brought online.

Before You Begin If you use a role with Geo Management RBAC rights, ensure that the `/var/cluster/geo` access control lists (ACLs) are correct on each node of both partner clusters. If necessary, assume the `root` role on the cluster node and set the correct ACLs.

```
# chmod A+user:username:rwx:allow /var/cluster/geo
```

The `/var/cluster/geo` directory must have the ACLs applied for compatibility between the Geo Management RBAC rights profile and data replication software.

For more information about RBAC, see "Securing Geographic Edition Software" on page 33.

1. **Assume the `root` role or assume a role that is assigned the Geo Management RBAC rights profile.**

2. **Activate the protection group.**
When you activate a protection group on the primary cluster, its application resource groups are also brought online.

```
phys-node-n# geopg start -e scope [-n] protection-group
```

-e *scope*

Specifies the scope of the command.

If the scope is `local`, then the command operates on the local cluster only. If the scope is `global`, the command operates on both clusters that deploy the protection group.

Note - The property values `global` and `local` are *not* case sensitive.

-n

Prevents the start of replication at protection group startup.

If you omit this option, the replication subsystem starts at the same time as the protection group. In addition, the following data replication products have additional behaviors when the `-n` option is omitted:

- **Availability Suite** – The data replication subsystem starts at the same time as the protection group and the `geopg start` command performs the following operations on each device group in the protection group:
  - Verifies that the role configured for the replication resource is the same as the role of the protection group on the local cluster.
  - Verifies that the role of the volume sets associated with the device group is the same as the role of the protection group on the local cluster.
  - If the role of the protection group on the local cluster is `secondary`, unmounts the local volumes defined in all volume sets associated with the device group.
  - If the role of the protection group on the local cluster is `primary`, enables the autosynchronization feature of the Availability Suite remote mirror feature. Also, resynchronizes the volume sets associated with the device group.
- **MySQL** – The `geopg start` command performs the following actions if the role of the protection group is secondary on the local cluster:
  - Starts the MySQL slave threads
  - Prevents modification by non-`root` roles if this option is configured
  - Prepares the `my.cnf` file to start the database with modifications prevented for non-`root` roles if this option is configured
- **Oracle Data Guard** – The `geopg start` command performs the following operations on each Oracle Data Guard broker configuration in the protection group:
  - Verifies that the resource group that is named in the `local_oracle_svr_rg_name` property contains a resource of type `SUNW.scalable_rac_server_proxy` for a scalable resource group or a resource of type `SUNW.oracle_server` for a failover resource group.
  - Verifies that the Oracle Data Guard `dgmgrl` command can connect using the values that are given for `sysdba_username`, `sysdba_password`, and `local_db_service_name`. Or if the `sysdba_username` and `sysdba_password` properties are null, verifies that the `dgmgrl` command can connect using the Oracle wallet connection format, `dgmgrl /@`*local-db-service-name*.
  - Verifies that the role configured for the replication resource is the same as the role of the protection group on the local cluster.
  - Verifies that the Oracle Data Guard broker configuration details match those that are held by Geographic Edition. The details to check include which cluster is primary, the configuration name, the database mode (for both the primary

and standby clusters), the replication mode, the standby type, that `FAST_START FAILOVER` is disabled, and that `BystandersFollowRoleChange` equals `NONE`.

protection-group

Specifies the name of the protection group.

The `geopg start` command uses the `clresourcegroup online -eM` *resource-group-list* command to bring resource groups and resources online. See the `clresourcegroup`(1CL) man page for more information.

If the role of the protection group is primary on the local cluster, the `geopg start` command performs the following operations:

- Runs a script that is defined by the `RoleChange_ActionCmd` property.
- Brings the application resource groups in the protection group online on the local cluster. For Oracle Data Guard, these groups include the shadow Oracle database server resource groups.

The `geopg start` command also performs additional operations for the following data replication products:

- **Availability Suite**
  - If the application resource group is a failover type resource group that shares affinities with a device group in the same protection group, the command adds strong, positive affinities and failover delegation between the application resource group and the lightweight resource group.

    The application resource group must not have strong, positive affinities with failover delegation. Otherwise, the attempt to add strong, positive affinities with failover delegation with the lightweight resource group will fail.
  - The command creates strong dependencies between the HAStoragePlus resource in the application resource group and the HAStoragePlus resource in the lightweight resource group for this device group.
- **MySQL**
  - Prepares the `my.cnf` file to start the database without the slave threads
  - Brings online the application resource groups in the protection group on the local cluster

Example 7 Globally Activating a Protection Group

This example globally activates a protection group.

```
phys-paris-1# geopg start -e global sales-pg
```

Example 8 Locally Activating a Protection Group

This example activates a protection group on a local cluster only. This local cluster might be a primary cluster or a standby cluster, depending on the role of the cluster.

```
phys-paris-1 geopg start -e local sales-pg
```

Troubleshooting

If the `geopg start` command fails, the `Configuration` status might be set to `Error` depending on the cause of the failure. The protection group remains deactivated, but data replication might be started and some resource groups might be brought online. Run the `geoadm status` command to obtain the status of your system.

If the `Configuration` status is set to `Error`, revalidate the protection group by using the procedures that are described in "Validating a Protection Group" on page 55.

Next Steps

If you want to administer a set of protection groups as a single entity, go to "Configuring Sites and Multigroups" on page 59.

See Also

To find out how to deactivate a protection group, see "Activating and Deactivating a Protection Group" in *Oracle Solaris Cluster 4.3 Geographic Edition System Administration Guide*.

Configuring Sites and Multigroups

This section describes how to create and validate sites and multigroups.

▼ How to Create a Site

Note - You can also use the Oracle Solaris Cluster Manager browser interface to perform this task. Click Sites, then click Create. For Oracle Solaris Cluster Manager log-in instructions, see "How to Access Oracle Solaris Cluster Manager" in *Oracle Solaris Cluster 4.3 System Administration Guide*.

Before You Begin

- Determine which clusters the site will contain and whether each cluster will be a site controller or a site member. The cluster from which you create the new site is automatically configured as a site controller. To avoid a possible single point of failure, configure at least two clusters as site controllers.
- If you use a role with Geo Management RBAC rights, ensure that the `/var/cluster/geo` ACLs are correct on each node of both partner clusters. If necessary, assume the `root` role on the cluster node and set the correct ACLs.

```
# chmod A+user:username:rwx:allow /var/cluster/geo
```

The `/var/cluster/geo` directory must have the correct access control lists (ACL) applied for compatibility between the Geo Management RBAC rights profile and data replication software.

For more information about RBAC, see "Securing Geographic Edition Software" on page 33.

1. **From a node of a cluster that you want to be a controller of the new site, assume the `root` role or assume a role that is assigned the Geo Management RBAC rights profile.**

2. **Ensure that all nodes in the cluster are online.**

```
phys-schost-1# cluster status -t node
=== Cluster Nodes ===

--- Node Status ---

Node Name                                       Status
---------                                       ------
phys-schost-2                                   Online
phys-schost-1 Online
```

If any node is offline, wait until the node is back online before you create the new site. The creation of a new site, or the acceptance by invited members to join the site, will fail if any node in the issuing cluster is not online.

3. **Configure the new site.**

The issuing cluster is automatically configured as a site controller, so you do not have to specify that cluster name to the `geosite create` command. You can specify the `-c` option and the `-m` option in the same `geosite create` command.

first-site-controller-cluster-node`# geosite create [-c` *cluster*`[,…]] [-m` *cluster*`[,…]]` *site*

`-c` *cluster*

The name of a cluster to configure as a site controller. You can specify multiple cluster names separated by commas (,).

`-m` *cluster*

The name of a cluster to configure as a site member. You can specify multiple cluster names separated by commas (,).

site

The name for the site that you are creating.

The command issues an invitation to each cluster that is specified to the `geosite create` command. No site-based operations are accepted from a cluster until the cluster accepts the invitation to join the site.

4. **For each cluster that was invited, accept the invitation to join the new site.**

   a. **Ensure that the common agent container is enabled on all nodes of this cluster and all nodes of the cluster that this cluster is joining.**

      ```
      # /usr/lib/cacao/bin/cacaoadm status
      ```

   b. **If the common agent container is not running on any of the cluster nodes, start it.**

      ```
      # /usr/lib/cacao/bin/cacaoadm start
      ```

   c. **From one node, join the site.**

      invited-cluster-node`# geosite join` *first-site-controller-cluster site*

      first-site-controller-cluster

      The name of the cluster that issued the invitation to join the site.

5. **Verify the site configuration.**

   `# geosite status` *site*

Example 9 Creating a New Site

The following example creates a new site named `europe`. The issuing cluster, `london`, is automatically configured as a site controller. The cluster `madrid` is configured as a second site controller, and the clusters `berlin` and `paris` are configured as site members. The invited clusters accept the invitation from the `london` cluster to join the `europe` site.

```
phys-london-1# geosite create -c madrid -m berlin,paris europe

phys-madrid-1# geosite join london europe
phys-berlin-1# geosite join london europe
phys-paris-1# geosite join london europe
```

Next Steps Go to "How to Create a Multigroup" on page 62.

See Also To find out how to delete a site, see "Deleting a Site" in *Oracle Solaris Cluster 4.3 Geographic Edition System Administration Guide*.

How to Create a Multigroup

Perform this procedure to configure a multigroup to manage designated sets of protection groups.

Note - You can also use the Oracle Solaris Cluster Manager browser interface to perform this task. Click Sites, click the site name to go to its page, and click Add. For Oracle Solaris Cluster Manager log-in instructions, see "How to Access Oracle Solaris Cluster Manager" in *Oracle Solaris Cluster 4.3 System Administration Guide*.

Before You Begin

- Ensure that the protection groups you want to contain in the multigroup are configured and working properly. See the Geographic Edition manual for your data replication product for procedures to configure a protection group.
- Ensure that a partner cluster for each protection group to configure in the multigroup is configured in the same site. See "How to Create a Site" on page 59.
- If you use a role with Geo Management RBAC rights, ensure that the `/var/cluster/geo` access control lists (ACLs) are correct on each node of both partner clusters. If necessary, assume the `root` role on the cluster node and set the correct ACLs.

  ```
  # chmod A+user:username:rwx:allow /var/cluster/geo
  ```

  The `/var/cluster/geo` directory must have the ACLs applied for compatibility between the Geo Management RBAC rights profile and data replication software.

  For more information about RBAC, see "Securing Geographic Edition Software" on page 33.

1. **From a node of a site controller cluster, assume the `root` role or assume a role that is assigned the Geo Management RBAC rights profile.**

2. **Create the multigroup.**

   site-controller-cluster-node# **`geomg create -s`** *site multigroup*

   `-s` *site*

   The name of the site.

multigroup

The name to assign the new multigroup. The name must be unique throughout the specified site. If the name is not unique, the command fails with an error.

3. From a node of a site controller cluster, add protection groups to the multigroup.

site-controller-cluster-node# **geomg add-protection-group** *protection-group-list multigroup*

The following describes the syntax choices for *protection-group-list*:

cluster:*protection-group*

Specifies a single protection group. The colon (:) separates the cluster name *cluster* from the name of the protection group that is configured in that cluster.

cluster1:*protection-group1*/*cluster2*:*protection-group2*

Specifies a protection group that has a dependency on another protection group. The protection group that is specified in the dependency chain before the slash (/) depends on the protection group that is specified after the slash.

cluster1:*protection-group1*,*cluster1*:*protection-group2*,*cluster2*:*protection-group1*/*cluster3*:*protection-group1*

The comma (,) separates multiple protection group names in the same command.

(*cluster1*:*protection-group2*,*cluster2*:*protection-group1*)/*cluster3*:*protection-group1*

Specifies that the protection groups *cluster1*:*protection-group2* and *cluster2*:*protection-group1* have a dependency on the *cluster3*:*protection-group1* protection group. Use parentheses to only enclose multiple protection groups with a dependency on another, single protection group. Only one protection group can be specified as the depended-on protection group.

4. Verify the multigroup configuration.

 # geomg status *multigroup*

See Also To delete a multigroup, see "Deleting a Multigroup" in *Oracle Solaris Cluster 4.3 Geographic Edition System Administration Guide*.

To find out how to administer a multigroup, see Chapter 8, "Administering Multigroups" in *Oracle Solaris Cluster 4.3 Geographic Edition System Administration Guide*.

♦ ♦ ♦ CHAPTER 3

Upgrading or Updating Geographic Edition Software

This chapter describes how to upgrade or install Software Repository Updates (SRU) of Geographic Edition software in the global cluster or in a zone cluster.

You can upgrade or update Geographic Edition software on a running cluster without disruption. Because the Geographic Edition software installation process does not require you to restart the Geographic Edition framework, the cluster remains in production with services running. Geographic Edition software configuration data is retained across the upgrade or update process. Highly available applications do not have downtime during a Geographic Edition software upgrade or update.

Note - If you upgrade Geographic Edition software to a version that is more than one consecutive version different than the Geographic Edition version running on the nodes of its partner cluster, you must also upgrade the partner cluster nodes to a supported Geographic Edition version. Do not start the Geographic Edition framework on nodes of an upgraded cluster unless the version of Geographic Edition software on each node of the partner cluster is no more than one consecutive version different.

If you are upgrading or updating the Oracle Solaris Cluster software, the Geographic Edition software is automatically upgraded at the same time but only in the global cluster. You do not then need to perform this procedure to upgrade the Geographic Edition software in the global cluster. However, for zone clusters you must always upgrade or update Geographic Edition software manually.

Upgrading a Geographic Edition Configuration

This section provides the following information to upgrade or update a cluster to a new Geographic Edition software version:

- "Upgrade and Update Requirements and Software Support Guidelines" on page 66

- "How to Prepare the Cluster for an Upgrade or Software Update" on page 67
- "How to Upgrade or Update Geographic Edition Software" on page 69
- "How to Verify Upgrade or Update of Geographic Edition Software" on page 71

Upgrade and Update Requirements and Software Support Guidelines

This section provides requirements and software-support guidelines for all clusters that have a partnership with the global cluster or zone cluster that you are either upgrading to Geographic Edition 4.3 software or updating.

- "Geographic Edition Upgrade Requirements" on page 66
- "Geographic Edition Update Requirements" on page 67

Geographic Edition Upgrade Requirements

When you upgrade your cluster to the Geographic Edition 4.3 version, observe the following requirements:

- **Supported hardware** – The cluster hardware must be a supported configuration for Geographic Edition 4.3 software. Contact your Oracle representative for information about Geographic Edition configurations that are currently supported.
- **Minimum Oracle Solaris OS version** – The cluster must run on at least Oracle Solaris 11.1 software, including the most current required software updates.
- **Minimum Oracle Solaris Cluster version** – The cluster must run on or be upgraded to either Oracle Solaris Cluster 4.2 or Oracle Solaris Cluster 4.3 software.

Note - All clusters in a partnership must run either Oracle Solaris Cluster 4.2 or Oracle Solaris Cluster 4.3 software. If a cluster is already running on Oracle Solaris Cluster 4.2 software, you are not required to upgrade it to Oracle Solaris Cluster 4.3 software to upgrade that cluster to the Geographic Edition 4.3 software.

- **Supported Geographic Edition versions in cluster partnerships** – All clusters that are in a partnership with the cluster that you are upgrading to the Geographic Edition 4.3 software version must run either the Geographic Edition 4.2 or 4.3 version. If any node on the partner cluster does not already run one of these versions of Geographic Edition software, you must also upgrade that node to a supported version before you restart the Geographic Edition framework on the upgraded cluster.

Geographic Edition Update Requirements

Observe the following requirements if you are installing a software update of your Geographic Edition 4.3 configuration.

- You must run the same software updates for Oracle Solaris Cluster software and the common agent container software on all nodes of the same cluster.
- Within a cluster, the software updates for each node on which you have installed Geographic Edition software must meet the Oracle Solaris Cluster software update requirements.
- All nodes in the same cluster must have the same version of Geographic Edition software and the same software updates. However, primary and secondary clusters can run different versions of Geographic Edition software provided that each version of Geographic Edition is correctly updated and the versions are no more than one release different.
- To ensure that the updates have been installed properly, install the software updates on your secondary cluster before you install the software updates on the primary cluster.

▼ How to Prepare the Cluster for an Upgrade or Software Update

On the cluster you are upgrading or updating, remove the Geographic Edition layer from production. Perform all steps from the global zone only.

Before You Begin Perform the following tasks:

- Ensure that the configuration meets the requirements for the upgrade. See "Upgrade and Update Requirements and Software Support Guidelines" on page 66.
- Have available the installation media or the IPS publisher configured, documentation, and software updates for all software products that you are upgrading, including Oracle Solaris OS, Oracle Solaris Cluster software, and Geographic Edition 4.3 software.
- Ensure that you have installed all the required software updates for your cluster configuration on each node of the cluster before you start upgrading the software.
- If you are installing a software update, ensure that you have read the `README` file for each software update you will install.

1. Ensure that the cluster is functioning properly.

a. From any node, view the current status of the cluster.

```
% cluster status
```

See the cluster(1CL) man page for more information.

b. Search the `/var/adm/messages` log on the same node for unresolved error messages or warning messages.

2. Assume the `root` role on a node of the cluster.

3. Remove all application resource groups from protection groups.

Highly available applications do not have downtime during the Geographic Edition software upgrade or update. This step ensures that resource groups are not stopped when you later stop the protection groups.

```
# geopg remove-resource-group resource-group protection-group
```

See the geopg(1M) man page for more information.

4. Stop all protection groups that are active on the cluster.

```
# geopg stop -e local protection-group
```

See the geopg(1M) man page for more information.

5. Stop the Geographic Edition framework.

Stopping the Geographic Edition framework ensures that a software upgrade or update on one cluster does not affect the other cluster in the partnership.

```
# geoadm stop
```

See the geoadm(1M) man page for more information.

6. On each node, stop the common agent container.

```
# /usr/sbin/cacaoadm stop
```

Next Steps Upgrade or update the Geographic Edition software on the cluster. Go to "How to Upgrade or Update Geographic Edition Software" on page 69.

How to Upgrade or Update Geographic Edition Software

Perform this procedure on each cluster node where you want Geographic Edition software to run. To permit testing, upgrade or update the secondary cluster before you upgrade the primary cluster. You can perform this procedure on more than one node at the same time.

Caution - The cluster in a partnership with the cluster you are upgrading or updating must also have the Geographic Edition 4.2 or 4.3 software version installed before you can restart the Geographic Edition 4.3 framework on the upgraded or updated cluster.

Before You Begin Ensure that the cluster is prepared for upgrade or software update. See "How to Prepare the Cluster for an Upgrade or Software Update" on page 67.

1. **Assume the `root` role on a node where you intend to upgrade or update Geographic Edition software.**
   If you are upgrading or updating a zone cluster, log in to a node of the zone cluster.

2. **Subscribe to the `ha-cluster` publisher that contains the software you want to upgrade or update to.**

   ```
   # pkg set-publisher -G '*' -g URL_for_ha-cluster_publisher ha-cluster
   ```

3. **Ensure that the `solaris` publisher is valid.**

   ```
   # pkg publisher
   PUBLISHER                             TYPE     STATUS   P  LOCATION
   solaris                               origin   online   F  solaris-repository
   ```

   For information about setting the `solaris` publisher, see "Adding, Modifying, or Removing Package Publishers" in *Adding and Updating Software in Oracle Solaris 11.3*.

4. **Ensure that the cluster is functioning properly and that all nodes are online and part of the cluster.**

   a. **From any node, view the current status of the cluster.**

      ```
      % cluster status
      ```

      See the `cluster`(1CL) man page for more information.

   b. **Search the `/var/adm/messages` log on the same node for unresolved error messages or warning messages.**

5. **Upgrade or update the Geographic Edition software to the new release or software update.**

   ```
   # pkg update ha-cluster-geo-incorporation
   ```

   Ensure that Geographic Edition software upgrade is completed on all cluster nodes before you continue to the next step.

6. **Verify that all partner clusters are installed with Geographic Edition version 4.3 or 4.2 software.**

   a. **On each node of each partner cluster, display the installed version of Geographic Edition software.**

      ```
      # geoadm -V
      ```

   b. **Determine your next step.**

      - **If the partner cluster is installed with Geographic Edition software version 4.3 or 4.2, proceed to Step 8.**
      - **If the partner cluster is not installed with Geographic Edition software version 4.3 or 4.2, upgrade it to a supported version.**

        Do not start the Geographic Edition framework until all cluster nodes in the partnership are installed with a supported version of Geographic Edition software. Then proceed to Step 8 of this procedure.

7. **After you have installed all required software updates on all nodes of the cluster, start the common agent container.**

   ```
   # /usr/sbin/cacaoadm start
   ```

   Perform this step on each node of the global cluster or zone cluster that you are configuring with Geographic Edition software.

8. **On one node of each partner cluster that you upgraded or updated, enable the Geographic Edition framework.**

   ```
   # geoadm start
   ```

9. **Repeat the preceding steps on each remaining node of the cluster.**

10. **From one node in one of the partner clusters, add back to the protection group all application resource groups that you removed while you were preparing the cluster for upgrade or update.**

```
# geopg add-resource-group resource-group protection-group
```

See the geopg(1M) man page for more information.

11. **Start all the protection groups that you added back.**

```
# geopg start protection-group -e local [-n]
```

See the geopg(1M) man page for more information.

Next Steps Go to "How to Verify Upgrade or Update of Geographic Edition Software" on page 71.

▼ How to Verify Upgrade or Update of Geographic Edition Software

Perform this procedure to verify that the cluster is successfully upgraded to or updated the Geographic Edition 4.3 software. Perform all steps from the global zone only.

Before You Begin Ensure that all upgrade or update procedures are completed for all cluster nodes that you are upgrading or updating.

1. **Assume the `root` role.**

   If you upgraded or updated a zone cluster, log in to a zone cluster node.

2. **View the installed levels of the Geographic Edition software.**

```
# geoadm -V
```

   The last line of output states which version of the Geographic Edition software the node is running. This version should match the version to which you just upgraded or updated.

Note - The version number that the `geoadm -v` command returns does not always coincide with the marketing release version numbers. The version number for the Geographic Edition 4.3 software is 4.3.

---

3. **Repeat the preceding steps for each cluster node you upgraded or updated.**

4. **Ensure that the cluster is running properly.**

```
# geoadm status
```

5. **(Optional) Perform a switchover to ensure that the Geographic Edition software is installed properly.**

   # geopg switchover *remote-cluster protection-group*

   You must test your geographically separated cluster properly, so that no problems prevent a switchover. Upgrading or updating only the secondary cluster first and switching over to it enables you to verify that a switchover operation still works. If the switchover fails, the primary site is untouched and you can switch back. If the switchover works on the secondary site, then after a certain time to confirm that the secondary cluster performs correctly, you can upgrade or update the primary site as well.

   Note - A switchover might interrupt the services that are running on the cluster. You should carefully plan the required tasks and resources before you perform a switchover.

   If you have added your application resource groups back into the protection groups, performing a switchover shuts down the applications on the original primary cluster and migrates the applications to the secondary cluster.

♦ ♦ ♦ CHAPTER 4

Uninstalling the Geographic Edition 4.3 Software

This chapter describes how to uninstall the Geographic Edition software.

When you uninstall the Geographic Edition 4.3 software, the node or cluster is no longer a part of the geographically separated cluster.

Note - You must uninstall the Geographic Edition software before you uninstall Oracle Solaris Cluster software.

Uninstalling the Geographic Edition Software

▼ How to Uninstall the Geographic Edition Software

Use this procedure to uninstall the Geographic Edition software that was installed with the `pkg add` command. Remove the Geographic Edition software from all nodes in the cluster unless you are removing the software from node that you are also removing from the cluster. You can continue to run applications during the uninstallation of the Geographic Edition software.

1. **Assume the `root` role on the node where you intend to uninstall the Geographic Edition software.**

2. **Unmanage data replication resource groups or remove the protection groups on the local cluster.**

   Use one of the following methods, depending on whether you might want to reinstall the Geographic Edition software at a future time.

- **If you want to remove the Geographic Edition software from the cluster but retain the protection group configuration for possible future use, unmanage data replication resource groups for each protection group on the local cluster.**

  Unmanaging these resource groups prevents them from attempting to interact with the Geographic Edition software after the software is uninstalled.

  ```
  # clresourcegroup offline data-replication-resource-group
  # clresource disable -g data-replication-resource-group +
  # clresourcegroup unmanage data-replication-resource-group
  ```

  `-g` Specifies the data replication resource group to disable.

  `+` Performs the operation on all resources.

- **If you do not intend to reinstall the Geographic Edition software on the cluster in the future, deactivate and remove each protection group from the local cluster.**

  ```
  # geopg stop -e local protection-group
  # geopg delete protection-group
  ```

  `-e local` Performs the operation only on the local cluster.

3. **Stop the Geographic Edition framework on the local cluster.**

   ```
   # geoadm stop
   ```

   For more information about disabling the Geographic Edition framework on a cluster, see "Enabling and Disabling the Geographic Edition Framework" in *Oracle Solaris Cluster 4.3 Geographic Edition System Administration Guide*.

4. **Remove the `ha-cluster-full` group package from each node in the local cluster.**

   You must remove the core Oracle Solaris Cluster group package before you can remove the Geographic Edition software. However, this process does not remove the installed Oracle Solaris Cluster software.

   ```
   # pkg uninstall ha-cluster-full
   ```

5. **Uninstall all Geographic Edition software packages from each node in the local cluster.**

   For a list of the Geographic Edition 4.3 packages, see "How to Install the Geographic Edition Software" on page 30.

```
# pkg uninstall ha-cluster/geo* ha-cluster/group-package/ha-cluster-geo*
```

6. **Verify that all Geographic Edition packages are removed.**

```
# pkg info | grep geo
```

Index

A

activating
  protection groups, 56
adding, 43, 43
  See also configuring
  See also creating
  application resource groups, 53
  resource groups to protection groups, 70
administration tasks
  prerequisite, 28
application resource groups
  adding to a protection group with no data replication, 53
Availability Suite
  IPsec, 21
  planning, 15

B

built-in replication
  description, 16

C

certificates
  configuring, 20
changing the cluster name, 39
`clresource` command
  verifying resources, 40
`clresourcegroup` command
  verifying resource groups, 40
`cluster` command
  listing cluster information, 39
  renaming the cluster, 39
  verifying cluster status, 67, 69
clusters
  naming requirements, 18
  renaming, 39
common agent container
  starting, 70
  stopping, 68
Compatibility Guide, 16
configuring, 43, 43
  See also adding
  See also creating
  IPsec, 21
  multigroups, 62
  partnerships, 41
  protection groups, 49
    replicated, 50
    unreplicated, 52
  RBAC, 18
  security certificates, 20
  sites, 59
  trust, 42
creating, 43, 43
  See also adding
  See also configuring
  partnerships, 43, 43
  protection groups
    replicated, 50
    unreplicated, 52
custom replication
  description, 16

D

data replication software
  planning types of, 15

E

`/etc/inet/hosts` file
  planning, 17
`/etc/inet/ipsecinit.conf`, 34
`/etc/init/secret/ipseckeys`, 34
EMC Symmetrix Remote Data Facility
  planning, 15
enabling
  Geographic Edition framework, 39
    after upgrade, 70
examples
  activating a protection group
    globally, 58
    locally, 59
  creating a partnership, 46
  creating a partnership with a custom heartbeat and a custom heartbeat plug-in, 46
  creating a protection group that does not use data replication, 53
  creating a site, 61
  creating and joining a partnership with multiple-domain clusters, 48
  enabling Geographic Edition framework, 40
  joining a partnership, 48
  starting Geographic Edition framework, 40

F

firewall configuration
  port numbers, 19
framework *See* Geographic Edition framework

G

`geoadm` command
  enabling Geographic Edition framework, 70
  enabling Oracle Solaris Cluster Geographic Edition software, 40
  stopping Geographic Edition framework, 68, 74
  verifying
    cluster status, 71
    Geographic Edition framework, 40
    Geographic Edition version, 71
Geographic Edition framework, 38
  See also Geographic Edition software
  enabling, 39, 70
  package requirement, 23
  stopping, 68, 74
  verifying, 40
Geographic Edition script-based plug-ins
  planning, 15
Geographic Edition software, 38
  See also Geographic Edition framework
  framework package requirement, 23
  installing, 29
  planning, 15
  uninstalling, 73
  updating, 65
  upgrading, 65
  verifying the version, 71
`geopg` command
  adding resource groups to protection groups, 70
  removing resource groups from protection groups, 68
  starting protection groups, 71
  stopping protection groups, 68
  switchover between partner clusters, 72
`geops` command
  importing public keys, 42

H

`ha-cluster-full` group package
  removing before upgrade, 74
hardware
  planning, 14
heartbeats
  IPsec security with, 21
Hitachi TrueCopy

planning, 15
Hitachi Universal Replicator
planning, 15
host-based replication
description, 16
hostnames
planning, 17
hosts file
planning, 17

I

importing public keys, 42
infrastructure *See* Geographic Edition framework
installing
from an ISO image, 31
from the Internet, 30
Geographic Edition software, 29
in zone clusters, 27
overview, 27
package repository, 30
planning for, 13
publisher, 31
verifying, 33
Internet
downloading packages, 30
IP addresses
planning, 17
IPsec, 21
keys file, 34
policy file, 34
ISO image
repository setup, 31

J

joining
partnerships, 46

L

licensing, 22
logical hostnames
inter-cluster communication, 14
naming requirements, 22

M

multigroups
configuring, 62
planning, 26
MySQL
planning, 15

N

naming requirements
clusters, 18
logical hostnames, 22
resource groups, 17
resources, 17

O

Oracle Data Guard
planning, 15
Oracle GoldenGate
planning, 15
Oracle Solaris Cluster Geographic Edition software *See*
Geographic Edition software
Oracle Solaris Cluster Manager
tasks you can perform
configuring trust, 42
creating a partnership, 43
creating an unreplicated protection group, 52
joining a partnership, 46
validating a protection group, 55
verifying a partnership, 45
verifying trust, 43
Oracle Solaris Cluster software
publisher, 32
Oracle Solaris software
publisher, 32, 69
Oracle Solaris ZFS snapshots

planning, 15
Oracle wallet
dgmgrl and, 57
Oracle ZFS Storage Appliance
planning, 15

P

package repository, 30
partnerships
configuring, 41
configuring trust, 42
creating, 43, 43
joining, 46
planning, 24
preparing a zone cluster, 35
removing, 46
removing a partnership, 46
switchover between partner clusters, 72
planning
data replication software, 15
Geographic Edition software, 15
hardware, 14
hostnames, 17
installation, 13
multigroups, 26
partnerships, 24
protection groups, 24
public network IP addresses, 17
resource groups, 17
resources, 17
security, 18
sites, 25
software, 15
volume management, 16
port numbers
firewall configuration, 19
protection groups
activating, 56
adding an application resource group, 53
adding resource groups, 70
configuring, 49
planning, 24
removing resource groups, 68
replicated
creating, 50
starting, 71
stopping, 68
unreplicated
creating, 52
validating, 55
public keys
importing, 42
verifying, 43
public network IP addresses
planning, 17
publisher, 31
Oracle Solaris Cluster software, 32
Oracle Solaris software, 32, 69

R

RBAC, 33
rights profiles, 19
setting up and using, 18
removing
resource groups from protection groups, 68
renaming the cluster, 39
replication *See* data replication software
replication for databases
description, 16
requirements
Geographic Edition framework package, 23
updating Geographic Edition software, 67
upgrading Geographic Edition software, 66
resource groups
adding to protection groups, 70
naming requirements, 17
planning, 17
removing from protection groups, 68
verifying, 40
resources
naming requirements, 17
planning, 17
verifying, 40
role-based access control *See* RBAC

S

security
  configuring certificates, 20
  IPsec, 21
  planning, 18
security files
  distributing upgraded files, 36
sites
  configuring, 59
  planning, 25
`solaris.cluster.geo.admin`, 19
`solaris.cluster.geo.modify`, 19
`solaris.cluster.geo.read`, 19
starting
  common agent container, 70
  Geographic Edition framework, 39
  protection groups, 71
status
  verifying cluster operation
    after upgrade, 71
    before upgrade, 67, 69
stopping
  common agent container, 68
  Geographic Edition framework, 68, 74
  protection groups, 68
storage-based replication
  description, 16
switchover between partner clusters, 72

T

troubleshooting
  Geographic Edition module not loading, 38
  `geopg start` command fails, 59
trust
  configuring, 42
  verifying, 43

U

uninstalling
  Geographic Edition software, 73
updating
  Geographic Edition software, 69
  preparing the cluster, 67
  requirements, 67
  verifying, 71
upgrade
  removing `ha-cluster-full` group package, 74
upgrading
  Geographic Edition software, 69
  preparing the cluster, 67
  requirements, 66
  verifying, 71

V

validating
  protection groups, 55
verifying
  cluster status, 67, 69, 71
  Geographic Edition framework, 40
  Geographic Edition software version, 71
  trust, 43
volume management
  planning, 16

Z

zone clusters, 23
  installing Geographic Edition software, 27
  preparing for partnership, 35