Oracle® Solaris Cluster Geographic Edition Installation and Configuration Guide

Part No: E39666
July 2014, E39666-01

Contents

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

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

Access to Oracle Support

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

Documentation Accessibility

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

Feedback

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

♦ ♦ ♦ CHAPTER 1

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 9
- "Planning Cluster Hardware" on page 10
- "Planning Required Software" on page 11
- "Planning Resource and Resource Group Names" on page 13
- "Planning Required IP Addresses and Hostnames" on page 13
- "Planning Security" on page 14
- "Planning the Geographic Edition Environment" on page 18

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 Geographic Edition software.

This installation process progresses from the initial planning phase to the eventual startup of Geographic Edition software. 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 Software Installation Guide ”.

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

Planning Cluster Hardware

This section helps you to plan your hardware for the primary cluster, the secondary cluster, and the inter-cluster 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 inter-cluster management communication between the clusters and for default inter-cluster heartbeats.
- Connections for either host-based or storage-based data replication.
- Connections for custom heartbeats, if any.

The hardware configurations that Geographic Edition software supports are identical to the hardware configurations that the Oracle Solaris Cluster product supports. For use of Geographic Edition software with storage-based data replication mechanisms, the cluster hardware configurations are those configurations that support the related storage hardware. 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 inter-cluster management operations is through a logical-hostname IP address. The default inter-cluster 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

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.

The following information is provided in this section:

- "Planning the Geographic Edition Software" on page 11
- "Planning the Data Replication Software" on page 11
- "Planning Volume Management" on page 13

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 4.2 or 4.1. But clusters running version 4.2 and 4.0 cannot run in the same Geographic Edition configuration.

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.
- MySQL software.
- Oracle Data Guard software, in configurations that use Oracle Database software.
- Oracle ZFS Storage Appliance software from Oracle.

- Geographic Edition script-based plug-ins.

The following sections describe the types of replication that the above products provide:

- "Host-Based Replication" on page 12
- "Storage-Based Replication" on page 12
- "Oracle Database Replication" on page 12
- "Built-In Replication" on page 12
- "Custom Replication" on page 12

Host-Based Replication

The Availability Suite feature of Oracle Solaris software is a host-based replication method. 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 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 or EMC Symmetrix Remote Data Facility software, you must install the software on each node of the cluster.

Oracle Database Replication

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.

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

The following table describes the volume managers that are supported in this release for each data replication software product.

Data Replication Software	Supported Volume Managers
The Availability Suite feature of Oracle Solaris	Solaris Volume Manager
EMC Symmetrix Remote Data Facility	Solaris Volume Manager
Oracle Data Guard [†]	Oracle Automatic Storage Management Oracle Solaris ZFS Volume Manager Solaris Volume Manager for Sun Cluster
Oracle ZFS Storage Appliance from Oracle	Solaris Volume Manager Oracle Solaris ZFS Volume Manager

[†] For information about additional supported storage management options, see "Storage Management Requirements" in "Oracle Solaris Cluster Data Service for Oracle Real Application Clusters Guide ".

Planning Resource and Resource Group Names

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

Geographic Edition software 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.
- See "Public-Network IP Addresses" in "Oracle Solaris Cluster Software Installation Guide " for a list of components that require IP addresses. 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

Observe the following guidelines:

- **Logical hostname** – A cluster name must be suitable as a hostname because Geographic Edition software creates the logical hostname by using the cluster name. Therefore, the cluster name 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 Geographic Edition software:

- "Setting Up and Using RBAC" on page 14
- "RBAC Rights Profiles" on page 15
- "Configuring Firewalls" on page 15
- "Securing Inter-Cluster Communication" on page 16

Setting Up and Using RBAC

Geographic Edition software 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 RBAC,” in “Oracle Solaris Cluster System Administration Guide ”.

Geographic Edition software 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. Including `files` in the search list enables your system to find the RBAC entries that Geographic Edition defined.

RBAC Rights Profiles

The Geographic Edition CLI *and GUI* use RBAC rights to control end-user access to operations. The general conventions for these rights are described in Table 1-1.

TABLE 1-1 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 software
	`solaris.cluster.geo.modify`	Modify the configuration of the Geographic Edition software
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. The table below contains a list 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, so if you customize the port numbers serving the specified transfer protocols, the customized ports must be opened instead.

Ports other than those listed in Table 1-2 and Table 1-3 might be required by storage replication services such as the Availability Suite feature of Oracle Solaris software. See product documentation for details.

TABLE 1-2 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 1-3 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 Inter-Cluster Communication

This section provides the information about the following methods to secure communication between partner clusters:

- "Security Certificates" on page 16
- "IP Security (IPsec)" on page 17

Security Certificates

You must configure the Geographic Edition software 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 37.

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 inter-cluster 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 guideline when using IPsec for secure inter-cluster 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 infrastructure, 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 11.2 " 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 18
- "Logical Hostnames" on page 18
- "Zone Clusters" on page 19
- "Partnerships" on page 19
- "Protection Groups" on page 20
- "Sites" on page 21
- "Multigroups" on page 21

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

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

You can use the `cluster` command to find the name of the cluster when you need to verify that the cluster name is suitable for use as a hostname. To find the name of the cluster, 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, MySQL, and Geographic Edition script-based plug-ins application-based data replication.
  - 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 packages** –nGeographic Edition framework packages are required in the global zones in all cases, even if Geographic Edition is only going to be enabled 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 infrastructure** – You can start the Geographic Edition infrastructure from within a zone cluster node, but not from within any other type of non-global zone.
- **GUI** – The Oracle Solaris Cluster Manager GUI cannot be used to manage Geographic Edition components of a zone cluster that is a partnership member.

Partnerships

The Geographic Edition software enables clusters to form 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 only one 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 this 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 software 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 software propagates protection group configurations between partners.

- **Data replication** – You can specify a data replication type in the protection group to indicate the mechanism that is used 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 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 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.

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 only be performed 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 using the `geopg` command.
- **Protection group dependencies –** One or more protection groups can be configured 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. And 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 enabling and configuring the Geographic Edition infrastructure. This chapter contains the following sections:

- "Installation Overview" on page 23
- "Installing Geographic Edition Software" on page 25
- "Securing Geographic Edition Software" on page 29
- "Preparing a Zone Cluster for Partner Membership" on page 31
- "Enabling the Geographic Edition Infrastructure" on page 34
- "Configuring a Partnership" on page 37
- "Configuring Protection Groups" on page 44
- "Configuring Sites and Multigroups" on page 52

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 software. See Chapter 11, "Updating Your Software," in "Oracle Solaris Cluster 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 the following lists of tasks to perform to create a Geographic Edition configuration:

- "Prerequisite Configuration Tasks" on page 24
- "Installation and Configuration Tasks" on page 24

Prerequisite Configuration Tasks

Before you begin administering the Geographic Edition software, you must identify the Oracle Solaris Cluster installations you need 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 software. The following table describes these prerequisite tasks.

TABLE 2-1 Geographic Edition Prerequisite Configuration Tasks

Task	Description
1. Set the cluster name to the name you want to use with the Geographic Edition software.	Use the `cluster` command. For more information about this requirement, see "How to Enable Geographic Edition Software" on page 34.
2. Set up the IP address and host maps for the cluster that is enabled to run Geographic Edition software.	See Chapter 2, "Installing Software on Global-Cluster Nodes," in "Oracle Solaris Cluster 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 20.
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 38.

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 2-2 Geographic Edition Installation and Configuration Tasks

Task	Description and Documentation
1. Install Geographic Edition software.	See "Installing Geographic Edition Software" on page 25.
2. Set up security between the candidate partner clusters.	■ Exchange certificates, as described in "Security Certificates" on page 16. ■ (Optional) Configure a secure logical hostname that uses IP Security Architecture (IPsec), as described in "IP Security (IPsec)" on page 17.
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 31.

Task	Description and Documentation
4. Enable the Geographic Edition software.	Issue the `geoadm start` command. For more information, see "Enabling the Geographic Edition Infrastructure" on page 34.
5. Create partnerships.	See "Configuring a Partnership" on page 37.
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 20.
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 45.
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 49.
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 52.
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 11, "Migrating Services," in "Oracle Solaris Cluster 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 Geographic Edition Software

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

▼ How to Install Geographic Edition Software

This procedure explains how to install 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 Before you begin to install software, make the following preparations:

- Ensure that the Oracle Solaris OS is installed to support 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 GUI to administer Geographic Edition components, ensure that all cluster nodes have the same root password.

- Read Chapter 1, "Planning the Geographic Edition Installation".
- Read the following manuals, which contain information that can help you plan your configuration and prepare your installation strategy:
  - "Oracle Solaris Cluster 4.2 Release Notes " – Restrictions, bug workarounds, and other late-breaking information.
  - "Oracle Solaris Cluster Geographic Edition Overview ".
  - Documentation for all third-party software products.

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, 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.**

   - **If the cluster nodes have direct access or web proxy access to the Internet, perform the following steps.**

     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 4.2 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, perform the following steps.**

a. **Download the Oracle Solaris Cluster 4.2 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 4.2 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 4.2 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 11.2 ".

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 11.2 ".

4. **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 11.2 ".

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 11.2 ".

5. **Install the Geographic Edition 4.2 software.**

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

6. **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
```

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

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

Next Steps Install any required software updates. Go to Chapter 3, "Upgrading or Updating Geographic Edition Software".

Configure Geographic Edition software on the clusters. Go to Chapter 2, "Installing and Configuring the Geographic Edition Software".

Securing Geographic Edition Software

This section provides procedures to configure IPsec to secure communication between partner clusters.

For additional information about configuring secure communication between partner clusters, see "Planning Security" on page 14.

▼ 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 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 Appendix B, "Legal Names and Values of Geographic Edition Entities," in "Oracle Solaris Cluster 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 31.

Otherwise, go to "Enabling the Geographic Edition Infrastructure" on page 34.

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 Software Installation Guide ".
- You have read the requirements for using a zone cluster in a cluster partnership. See "Zone Clusters" on page 19.
- 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 zoneclustername
   clzc:zoneclustername> add net
   clzc:zoneclustername:net> set address=zoneclustername
   clzc:zoneclustername:net> end

   clzc:zoneclustername> verify
   clzc:zoneclustername> commit
   clzc:zoneclustername> 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 zoneclustername
   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. 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.

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

  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 zoneclustername
  ```

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 Infrastructure" on page 34.

Enabling the Geographic Edition Infrastructure

When Geographic Edition software 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 Infrastructure," in "Oracle Solaris Cluster Geographic Edition System Administration Guide ".

▼ How to Enable Geographic Edition Software

This procedure enables the Geographic Edition infrastructure 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 GUI 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 newclustername clustername
```

`-c` *newclustername*

Specifies the new cluster name.

clustername

The cluster whose name you are changing.

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

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

   ```
   # geoadm start
   ```

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

5. **Verify that you have enabled the infrastructure 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 displays that the Geographic Edition infrastructure 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 is 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 2-1 Enabling the Geographic Edition Infrastructure on a Cluster

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

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

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

2. Ensure that the Geographic Edition infrastructure 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 37.

Configuring a Partnership

This section provides the following Information:

- "Configuring Trust Between Partner Clusters" on page 37
- "Creating a Partnership" on page 38
- "Joining an Existing Partnership" on page 41

Configuring Trust Between Partner Clusters

This section provides procedures to configure secure communication, or trust, between the two clusters you want to be in a partnership.

▼ How to Configure Trust Between Two Clusters

Before you create a partnership between two clusters, you must configure Geographic Edition software 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`.

Note - You can also accomplish this procedure by using the Oracle Solaris Cluster Manager GUI. Click Partnerships and then click `Add Partner Trust`. For more information about Oracle Solaris Cluster Manager, see Chapter 13, "Using the Oracle Solaris Cluster GUI," in "Oracle Solaris Cluster 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 Infrastructure" on page 34.
- 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 know how 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 *remotecluster*

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

```
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:

remotecluster`.certificate[0-9]*`

Keys and only keys that belong to the remote cluster should have their alias match 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 GUI. Click Partnerships and then click `Verify Partner Trust`. For more information about Oracle Solaris Cluster Manager, see Chapter 13, “Using the Oracle Solaris Cluster GUI,” in “Oracle Solaris Cluster System Administration Guide”.

```
# geops verify-trust -c remotecluster
```

Next Steps Configure the partnership. Go to “Creating a Partnership” on page 38.

See Also To remove trust, see Configuring Trust Between Partner Clusters.

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 GUI. Click Partnerships and then click `Create`. For more information about Oracle Solaris Cluster Manager, see Chapter 13, "Using the Oracle Solaris Cluster GUI," in "Oracle Solaris Cluster 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 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 Infrastructure" on page 34.
- 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 know how 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 37 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 29.

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 infrastructure 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, see Chapter 6, “Administering Heartbeats,” in “Oracle Solaris Cluster 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 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 Geographic Edition System Administration Guide ”.

partnership

Specifies the name of the partnership.

For information about the names and values that are supported by Geographic Edition software, see Appendix B, “Legal Names and Values of Geographic Edition Entities,” in “Oracle Solaris Cluster 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 GUI. Click Partnerships to view partnership information. For additional details, click the partnership name. For more information about Oracle Solaris Cluster Manager, see Chapter 13, “Using the Oracle Solaris Cluster GUI,” in “Oracle Solaris Cluster 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 2-2 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
```

Next Steps To finalize the new partnership, the remote partner cluster must join the partnership. Go to "Joining an Existing Partnership" on page 41.

See Also To remove a partnership between two clusters, see "How to Remove Trust Between Two Clusters" in "Oracle Solaris Cluster 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 GUI. Click Partnerships and then click `Join Partnership`. For more information about Oracle Solaris Cluster Manager, see Chapter 13, "Using the Oracle Solaris Cluster GUI," in "Oracle Solaris Cluster 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 38.
- If a partner cluster is a zone cluster, either application-based replication such as Oracle Data Guard is configured or no data replication is used.

- Security has been configured on the clusters by installing the appropriate certificates.

  See Security Certificates 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 14.

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 Geographic Edition Software" on page 34.

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 6, "Administering Heartbeats," in "Oracle Solaris Cluster 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 Appendix B, "Legal Names and Values of Geographic Edition Entities," in "Oracle Solaris Cluster 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 2-3 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 2-4 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 44 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 44
- "Creating a Protection Group That Does Not Require Data Replication" on page 45
- "Validating a Protection Group" on page 47
- "Activating a Protection Group" on page 48

Also see the appropriate Geographic Edition manual for procedures to create a protection group for your data replication product.

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 45.

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 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 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 47.

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 software to manage only resource groups, you can create protection groups that do not replicate data. The `geoadm status` command displays that these protection groups are in the `Degraded` state. This section describes how to configure your protection group not to use data replication.

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

To create a protection group that uses data replication, see the appropriate Geographic Edition manual for your data replication product:

- "Oracle Solaris Cluster Geographic Edition Data Replication Guide for EMC Symmetrix Remote Data Facility "
- "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 Remote Replication Guide for Oracle ZFS Storage Appliance "

▼ 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 GUI. Click Partnerships, then click the partnership name. In the Protection Groups section, click `Create`. For more information about Oracle Solaris Cluster Manager, see Chapter 13, "Using the Oracle Solaris Cluster GUI," in "Oracle Solaris Cluster 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.

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.**

   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 29.

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:

   `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 Geographic Edition System Administration Guide ".

protection-group

Specifies the name of the protection group.

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

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

Example 2-5 Creating and Configuring a Protection Group That Is Configured to Not Use Data Replication

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

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

See Also To delete a protection group, see "Deleting a Protection Group and Its Components" in "Oracle Solaris Cluster Geographic Edition System Administration Guide ".

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

This procedure 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.

Note - You can also accomplish this procedure by using the Oracle Solaris Cluster Manager GUI. Click Partnerships, then click the partnership name. In the Protection Groups section, highlight the protection group name and click `Validate`.

For more information about Oracle Solaris Cluster Manager, see Chapter 13, "Using the Oracle Solaris Cluster GUI," in "Oracle Solaris Cluster 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.

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

   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 29.

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 48.

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.

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

   For more information about RBAC, see "Securing Geographic Edition Software" on page 29.

Note - 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.

---

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` is equal to `NONE`.

protection-group

Specifies the name of the protection group.

The `geopg start` command uses the `clresourcegroup online -eM` *resourcegrouplist* 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, this includes 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 2-6 Globally Activating a Protection Group

This example globally activates a protection group.

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

Example 2-7 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 47.

Next Steps If you want to administer a set of protection groups as a single entity, go to "Configuring Sites and Multigroups" on page 52.

See Also To deactivate a protection group, see "Activating and Deactivating a Protection Group" in "Oracle Solaris Cluster Geographic Edition System Administration Guide ".

Configuring Sites and Multigroups

This section contains the following procedures:

- "How to Create a Site" on page 52
- "How to Create a Multigroup" on page 54

▼ How to Create a Site

Perform this procedure to configure a new site.

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.

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.**

   For more information about RBAC, see "Securing Geographic Edition Software" on page 29.

   Note - 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.

   ---

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 it is not necessary 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 to give 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 2-8 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 54.

See Also To delete a site, see "Deleting a Site" in "Oracle Solaris Cluster Geographic Edition System Administration Guide ".

▼ How to Create a Multigroup

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

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 52.

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.**

   For more information about RBAC, see "Securing Geographic Edition Software" on page 29.

Note - 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.

---

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 multiple protection groups, *cluster1*:*protection-group2* and *cluster2*:*protection-group1*, all have a dependency on the *cluster3*:*protection-group1* protection group. Parentheses can only be used to 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 Geographic Edition System Administration Guide ".

To administer a multigroup, see Chapter 9, " Administering Multigroups," in "Oracle Solaris Cluster 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 software, 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 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 Geographic Edition software 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 58
- “How to Prepare the Cluster for an Upgrade or Software Update” on page 59

- "How to Upgrade or Update Geographic Edition Software" on page 60
- "How to Verify Upgrade or Update of Geographic Edition Software" on page 63

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 4.2 software or updating.

- "Geographic Edition Upgrade Requirements" on page 58
- "Geographic Edition Update Requirements" on page 59

Geographic Edition Upgrade Requirements

Observe the following requirements if you are upgrading your cluster to the Geographic Edition 4.2 version.

- **Supported hardware** - The cluster hardware must be a supported configuration for Geographic Edition 4.2 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 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 4.1 or Oracle Solaris Cluster 4.2 software.

Note - All clusters in a partnership must run either Oracle Solaris Cluster 4.1 or Oracle Solaris Cluster 4.2 software. If a cluster is already running on Oracle Solaris Cluster 4.1 software, you are not required to upgrade it to Oracle Solaris Cluster 4.2 software to upgrade that cluster to Geographic Edition 4.2 software.

- **Supported Geographic Edition versions in cluster partnerships** - All clusters that are in a partnership with the cluster that you are upgrading to Geographic Edition 4.2 software must run either Geographic Edition 4.1 or 4.2 software. 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 infrastructure on the upgraded cluster.

Geographic Edition Update Requirements

Observe the following requirements if you are installing a software update of your Geographic Edition 4.2 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

Perform this procedure on the cluster you are upgrading or updating, to 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 58.
- 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 4.2 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 infrastructure.**

   Stopping the Geographic Edition infrastructure 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 60.

▼ How to Upgrade or Update Geographic Edition Software

Perform this procedure on each cluster node where you want Geographic Edition software to run. Upgrade or update the secondary cluster before you upgrade the primary cluster, to permit testing. 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 be installed with Geographic Edition 4.1 or 4.2 software before you can restart the Geographic Edition 4.2 infrastructure 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 59.

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 11.2 ".

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 4.2 or 4.1 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 4.2 or 4.1, proceed to Step 8.**
- **If the partner cluster is not installed with Geographic Edition software version 4.2 or 4.1, upgrade it to a supported version.**

  Do not start the Geographic Edition software 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**

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

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

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

   ```
   # 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.

Troubleshooting If, after upgrade, you experience problems with certificates between the cluster nodes, update the public keys on both partner clusters.

1. **On each node in the local cluster, remove the public keys.**

```
localnode# geops remove-trust -c remote-cluster
```

2. **On each node in the remote cluster, remove the public keys.**

```
remotenode# geops remove-trust -c local-cluster
```

3. **On one node of the local cluster, import the public keys from the remote cluster.**

```
localnode# geops add-trust -c remote-cluster
```

4. **On one node of the remote cluster, import the public keys from the local cluster.**

```
remotenode# geops add-trust -c local-cluster
```

5. **On each node of each cluster, verify trust.**

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

Next Steps Go to "How to Verify Upgrade or Update of Geographic Edition Software" on page 63.

▼ How to Verify Upgrade or Update of Geographic Edition Software

Perform this procedure to verify that the cluster is successfully upgraded to or updated Geographic Edition 4.2 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 Geographic Edition software.**

   ```
   # geoadm -V
   ```

   The last line of output states which version of 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 Geographic Edition 4.2 software is 4.2.

   ---

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 Geographic Edition software is installed properly.**

   ```
   # geopg switchover remotecluster protectiongroup
   ```

   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 switchover still works. If the switchover fails, the primary site is untouched and you can switch back. If switchover works on the secondary site, then after a certain 'soak time' 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.

♦ ♦ ♦ C H A P T E R 4

Uninstalling Geographic Edition 4.2 Software

This chapter describes how to uninstall the Geographic Edition software.

When you uninstall Geographic Edition 4.2 software, the node or cluster is no longer a part of the geographically separated cluster.

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

Uninstalling Geographic Edition Software

▼ How to Uninstall Geographic Edition Software

Use this procedure to uninstall Geographic Edition software that was installed with the `pkg add` command. Remove 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 Geographic Edition software.

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

   - **If you want to remove 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 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 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 infrastructure on the local cluster.**

```
# geoadm stop
```

For more information about disabling the Geographic Edition software on a cluster, see "Disabling the Geographic Edition Software" in "Oracle Solaris Cluster 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 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 4.2 packages, see "How to Install Geographic Edition Software" on page 25.

```
# 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