Sun Cluster Data Service for SWIFTAlliance Access Guide for Solaris OS

SPARC Platform Edition

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Part No: 820–2576–10
February 2008, Revision A

080328@19860

Contents

Preface

Sun Cluster Data Service for SWIFTAlliance Access Guide for Solaris OS explains how to install and configure Sun™ Cluster HA for SWIFTAlliance Access.

This document is intended for system administrators with extensive knowledge of Sun software and hardware. Do not use this document as a planning or presales guide. Before reading this document, you should have already determined your system requirements and purchased the appropriate equipment and software.

The instructions in this book assume knowledge of the Solaris™ Operating System (Solaris OS) and expertise with the volume-manager software that is used with Sun Cluster software.

Using UNIX Commands

This document contains information about commands that are specific to installing and configuring Sun Cluster data services. The document does *not* contain comprehensive information about basic UNIX® commands and procedures, such as shutting down the system, booting the system, and configuring devices. Information about basic UNIX commands and procedures is available from the following sources:

- Online documentation for the Solaris Operating System
- Solaris Operating System man pages
- Other software documentation that you received with your system

Typographic Conventions

The following table describes the typographic conventions that are used in this book.

TABLE P–1 Typographic Conventions

Typeface	Meaning	Example
`AaBbCc123`	The names of commands, files, and directories, and onscreen computer output	Edit your `.login` file. Use `ls -a` to list all files. `machine_name% you have mail.`
`AaBbCc123`	What you type, contrasted with onscreen computer output	`machine_name%` **`su`** `Password:`
aabbcc123	Placeholder: replace with a real name or value	The command to remove a file is `rm` *filename*.
AaBbCc123	Book titles, new terms, and terms to be emphasized	Read Chapter 6 in the *User's Guide*. A *cache* is a copy that is stored locally. Do *not* save the file. **Note:** Some emphasized items appear bold online.

Shell Prompts in Command Examples

The following table shows the default UNIX system prompt and superuser prompt for the C shell, Bourne shell, and Korn shell.

TABLE P–2 Shell Prompts

Shell	Prompt
C shell	`machine_name%`
C shell for superuser	`machine_name#`
Bourne shell and Korn shell	`$`
Bourne shell and Korn shell for superuser	`#`

Related Documentation

Information about related Sun Cluster topics is available in the documentation that is listed in the following table. All Sun Cluster documentation is available at `http://docs.sun.com`.

Topic	Documentation
Data service administration	*Sun Cluster Data Services Planning and Administration Guide for Solaris OS*
	Individual data service guides
Concepts	*Sun Cluster Concepts Guide for Solaris OS*
Overview	*Sun Cluster Overview for Solaris OS*
Software installation	*Sun Cluster Software Installation Guide for Solaris OS*
System administration	*Sun Cluster System Administration Guide for Solaris OS*
Hardware administration	*Sun Cluster 3.1 - 3.2 Hardware Administration Manual for Solaris OS*
	Individual hardware administration guides
Data service development	*Sun Cluster Data Services Developer's Guide for Solaris OS*
Error messages	*Sun Cluster Error Messages Guide for Solaris OS*
Command and function reference	*Sun Cluster Reference Manual for Solaris OS*

For a complete list of Sun Cluster documentation, see the release notes for your release of Sun Cluster at `http://docs.sun.com`.

Related Third-Party Web Site References

Third-party URLs that are referenced in this document provide additional related information.

Note – Sun is not responsible for the availability of third-party web sites mentioned in this document. Sun does not endorse and is not responsible or liable for any content, advertising, products, or other materials that are available on or through such sites or resources. Sun will not be responsible or liable for any actual or alleged damage or loss caused or alleged to be caused by or in connection with use of or reliance on any such content, goods, or services that are available on or through such sites or resources.

Documentation, Support, and Training

The Sun web site provides information about the following additional resources:

- Documentation (`http://www.sun.com/documentation/`)
- Support (`http://www.sun.com/support/`)
- Training (`http://www.sun.com/training/`)

Getting Help

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

- Your name and email address (if available)
- Your company name, address, and phone number
- The model number and serial number of your systems
- The release number of the Solaris Operating System (for example, Solaris 10)
- The release number of Sun Cluster (for example, Sun Cluster 3.2)

Use the following commands to gather information about each node on your system for your service provider.

Command	Function
`prtconf -v`	Displays the size of the system memory and reports information about peripheral devices
`psrinfo -v`	Displays information about processors
`showrev –p`	Reports which patches are installed
`prtdiag -v`	Displays system diagnostic information
`/usr/cluster/bin/clnode show-rev`	Displays Sun Cluster release and package version information

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

Installing and Configuring Sun Cluster HA for SWIFTAlliance Access

This Chapter explains how to install and configure Sun Cluster HA for SWIFTAlliance Access.

This Chapter contains the following sections.

Overview of Installing and Configuring Sun Cluster HA for SWIFTAlliance Access

Table 1 Lists the tasks for installing and configuring Sun Cluster HA for SWIFTAlliance Access. Perform these tasks in the order that they are listed.

TABLE 1 Task Map: Installing and Configuring Sun Cluster HA for SWIFTAlliance Access

Task	For Instructions, Go To
1. Plan the installation.	"Planning the Sun Cluster HA for SWIFTAlliance Access Installation and Configuration" on page 11
2. Install Sun Cluster HA for SWIFTAlliance Access Packages.	"How to Install and Configure SWIFTAlliance Access" on page 13
3. Verify installation and configuration.	"Verifying the Installation and Configuration of SWIFTAlliance Access" on page 17
4. Register and Configure Sun Cluster HA for SWIFTAlliance Access.	"Registering and Configuring Sun Cluster HA for SWIFTAlliance Access" on page 20
5. Verify Sun Cluster HA for SWIFTAlliance Access Installation and Configuration.	"Verifying the Sun Cluster HA for SWIFTAlliance Access Installation and Configuration" on page 21
6. Understand Sun Cluster HA for SWIFTAlliance Access fault monitor.	"Understanding the Sun Cluster HA for SWIFTAlliance Access Fault Monitor" on page 22
7. Debug Sun Cluster HA for SWIFTAlliance Access.	"Debugging Sun Cluster HA for SWIFTAlliance Access" on page 23

Sun Cluster HA for SWIFTAlliance Access Overview

The HA agent is written to work with SWIFTAlliance Access versions 5.5, 5.9, and 6.0. IBM DCE version 3.2 is not used anymore by SWIFTAlliance Access 5.9 and later, and must only be installed for SWIFTAlliance Access 5.5. SWIFTAlliance Access™is a trademark of SWIFT.

The Sun Cluster HA for SWIFTAlliance Access data service provides a mechanism for orderly startup, shutdown, fault monitoring, and automatic failover of the Sun Cluster service. The Sun Cluster components protected by the Sun Cluster HA for SWIFTAlliance Access data service are the following.

TABLE 2 Protection of Components

Component	Protected by
DCE daemon	Sun Cluster HA for SWIFTAlliance Access (version 5.5 only)
SWIFT Alliance Access	Sun Cluster HA for SWIFTAlliance Access

Note – By default the HA agent provides a fault monitor for the DCE component only when using the SWIFTAlliance Access 5.5. The fault monitoring for SWIFTAlliance Access is switched off by default. If the SWIFTAlliance Access application fails, the agent will not restart the SWIFTAlliance Access application automatically. This behavior was explicitly requested by SWIFT. It will enable you to operate the application in a way that the probe does not interfere with the normal behavior of some SWIFTAlliance Access features like:

- operator manually triggering the SWIFTAlliance Access restart function , for example, to run SWIFTAlliance Access in housekeeping mode.
- automatic or scheduled SWIFTAlliance Access restart, for example, to run database backup and other maintenance or end-of-day processes.
- any graceful SWIFTAlliance Access restart or recovery, in case of a SWIFTAlliance Access transient local error.

The HA agent provides the start, stop, takeover, and switchover functionality. This means that when a node fails, the other node will automatically start the SWIFTAlliance Access application. The HA agent also provides an option to turn on fault monitoring for SWIFTAlliance Access at registration time. However, this option is not recommended by SWIFT.

Planning the Sun Cluster HA for SWIFTAlliance Access Installation and Configuration

This section contains the information you need to plan your Sun Cluster HA for SWIFTAlliance Access installation and configuration.

Configuration Restrictions

This section provides a list of software and hardware configuration restrictions that apply to Sun Cluster HA for SWIFTAlliance Access only.

Caution – Your data service configuration might not be supported if you do not observe these restrictions.

- You can configure the Sun Cluster HA for SWIFTAlliance Access *only as a HA agent and not as a scalable agent.*
- You can install the SWIFTAlliance Access software on a global file system. Best practice is to use a failover file system. For SWIFTAlliance Access 5.5, you must install the IBM DCE software on local storage.

- Only one SWIFTAlliance Access instance is supported by this agent.

For restrictions that apply to all data services, see the *Sun Cluster Release Notes*.

Configuration Requirements

These requirements apply to Sun Cluster HA for SWIFTAlliance Access only. You must meet these requirements before you proceed with your Sun Cluster HA for SWIFTAlliance Access installation and configuration. Follow the SWIFTAlliance Access installation guide for the installation of the mandatory patch levels and the installation of the software.

Caution – Your data service configuration might not be supported if you do not adhere to these requirements.

Sun Cluster components and their dependencies

Configure the Sun Cluster HA for SWIFTAlliance Access data service to protect a Sun Cluster instance and its respective components. These components, and their dependencies, are briefly described next.

Component	Description
DCE daemon	→ *SUNW.LogicalHost* resource
SWIFTAlliance Access	→ *SUNW.LogicalHost*resource → *SUNW.HAStoragePlus* resource The SUNW.HAStoragePlus resource manages the SWIFTAlliance Access System Mount points and ensures that Sun Cluster is not started until these are mounted. → *DCE daemon (version 5.5 only)*

The Sun Cluster component has two configuration and registration files in the `/opt/SUNWscsaa/util` directory. These files enable you to register the Sun Cluster component with Sun Cluster.

Within these files, the appropriate dependencies have already been defined. You must update the `saa_config` file before you run the `saa_register` script.

Installing and Configuring SWIFTAlliance Access

This section contains the procedures you need to install and configure SWIFTAlliance Access.

Throughout the following sections, references will be made to some user-accessible directories for SWIFTAlliance Access.

Note – Sun Cluster HA for SWIFTAlliance Access can be configured to run in a whole root or a sparse root non-global zone for SWIFTAlliance Access version 6.0, if required.

▼ How to Install and Configure SWIFTAlliance Access

Use this procedure to install and configure SWIFTAlliance Access.

Note – IBM DCE client software is a prerequisite for SWIFTAlliance Access version 5.5. The client software must be installed and configured before the SWIFTAlliance Access application.

---

1 Create the resources for SWIFTAlliance Access.

- **Create a resource group for SWIFTAlliance Access.**

  ```
  # clresourcegroup create [-n node-zone-list] swift-rg
  ```

  `-n node-zone-list`
  Specifies a comma-separated, ordered list of zones that can master the resource group. The format of each entry in the list is node. In this format, node specifies the node name and zone specifies the name of a non-global Solaris zone. To specify the global zone, or to specify a node without non-global zones, specify only node. This list is optional. If you omit this list, the global zone of each cluster node can master the resource group.

- **Create a logical host**.

  Add the hostname and IP address in the `/etc/inet/hosts` file on all cluster nodes or zones that can master the resource group. Register the logical host and add it to the resource group.

  ```
  # clreslogicalhostname create -g swift-rg -l swift-lh swift-saa-lh-rs
  ```

- **Create the device group and file system**.

  See *Sun Cluster Data Services Installation and Configuration Guide* for instructions on how to create global file systems.

- **Create an HAstoragePlus resource**.

  Although you can use global file system, it is recommended to create a HAStoragePlus failover resource to contain the SWIFTAlliance Access application and configuration data.

In the example, we use `/global/saadg/alliance` as the path, but you can choose the location.

```
# clresource create -g swift-rg \
-t SUNW.HAStoragePlus \
-x FilesystemMountPoints=/global/saadg/alliance  swift-ds
```

- **Bring the resource group online**.

```
# clresouregroup online -M swift-rg
```

- **Create configuration directory —**This directory contains SWIFTAlliance Access information and creates a link from the `/usr`.

```
# cd /global/saadg/alliance

# mkdir swa

# ln -s /global/saadg/alliance/swa /usr/swa
```

Note – For Solaris 10 only: if you install SWIFTAlliance Access in a sparse root zone, that is the `/usr` directory is inherited in read-only mode through a loopback mount, the link needs to be created within the global zone.

---

2 Install IBM DCE client software on all cluster nodes or zones that can master the resource group.

Caution – This step is valid only for SWIFTAlliance Access versions prior to 5.9 and should only be installed when needed.

Skip this step if you are using SWIFTAlliance Access version 5.9 or 6.0.

- **Install IBM DCE client software on all cluster nodes or zones that can master the resource group** Use local disks to install this application. The software comes in Sun package format (`IDCEclnt`). Because the installed files will reside at various locations on your system, it is not practical to have this installed on global file systems. Install this application on both cluster nodes.

```
# pkgadd -d ./IDCEclnt.pkg
```

- **Configure DCE client RPC.**

```
# /opt/dcelocal/tcl/config.dce –cell_name swift –dce_hostname swift-lh RPC
```

- **Test DCE.**

  Run the tests on all cluster nodes or zones that can master the resource group.

```
# /opt/dcelocal/tcl/start.dce
```

Verify that the dced daemon is running.

```
# /opt/dcelocal/tcl/stop.dce
```

3 Install SWIFTAlliance Access software.

Perform the following steps on all cluster nodes or zones that can master the resource group.

- Create the users `all_adm`, `all_usr` and the group `alliance` on all cluster nodes or zones that can master the resource group with the same user ID and group ID.

  ```
  # groupadd -g groupid alliance

  # useradd -m -g alliance -d /export/home/all_adm -s /usr/bin/ksh all_adm

  # useradd -m -g alliance -d /export/home/all_usr -s /usr/bin/ksh all_usr
  ```

- On Solaris 10: Create a project called `swift` and assign the users `all_adm` and `all_usr` to it.

  ```
  # projadd -U all_adm,all_usr swift
  ```

- On Solaris 10: Set the values of the resource controls for the project `swift`:

  ```
  # projmod -s -K "project.max-sem-ids=(privileged,128,deny)" swift

  # projmod -s -K "project.max-sem-nsems=(privileged,512,deny)" swift

  # projmod -s -K "project.max-sem-ops=(privileged,512,deny)" swift

  # projmod -s -K "project.max-shm-memory=(privileged,4294967295,deny)" swift

  # projmod -s -K "project.max-shm-ids=(privileged,128,deny)" swift

  # projmod -s -K "project.max-msg-qbytes=(privileged,4194304,deny)" swift

  # projmod -s -K "project.max-msg-ids=(privileged,500,deny)" swift

  # projmod -s -K "project.max-sem-messages=(privileged,8192,deny)" swift
  ```

  The previous values are examples only. For more accurate values refer to the latest SWIFT documentation release notes.

- On Solaris 10: Assign the project `swift` as the default project for `all_adm` and `all_usr` by editing the file `/etc/user_attr` and adding the following two lines at the end of the file:

  ```
  all_adm::::project=swift

  all_usr::::project=swift
  ```

- For versions prior to Solaris 10, refer the latest SWIFT documentation and release notes to determine the necessary setup for `/etc/system`.

  Use the shared storage configured in Step 1 for the installation of this application. The installation procedure will modify system files and might also reboot the system. After the reboot, you must continue with the installation on the same node or zone. Ensure that the resource group is online on this node or zone. Repeat the installation of the software on the other node or zone that can master the resource group, but you must end the installation before the SWIFTAlliance Access software licensing step.

4 Continue configuring SWIFTAlliance Access.

To enable clients to connect to the failover IP address, create a file named `.alliance_ip_name` (`interfaces.rpc` in versions 5.9 and 6.0) on the data subdirectory of the SWIFTAlliance Access software.

When you are using the same file system as shown in the examples, this directory will be `/global/saadg/alliance/data`. This file must contain the IP address of the logical host as configured within the SWIFTAlliance Access resource group.

```
# cd /global/saadg/alliance/data

# chown all_adm:alliance interfaces.rpc
```

If MESSENGER is licensed, create a file called `interfaces.mas` and add the cluster logical IP address used to communicate with SAM.

```
# cd /global/saadg/alliance/data

# chown all_adm:alliance interfaces.mas
```

5 Add a symbolic link and entries.

- Add the symbolic link `/usr/swa` on all cluster nodes or zones that can master the resource group, see Step 1 last bullet.
- Entries in `/etc/services` has to be added on all cluster nodes or zones that can master the resource group. This can be done as root by running the `/usr/swa/apply_alliance_ports` script.
- The `rc.alliance` and `rc.swa_boot` scripts (`swa_rpcd` in SWIFTAlliance Access versions prior to 5.9) in `/etc/init.d` must remain in place. Any references to these files in `/etc/rc?.d` need to be removed, the access rights must be as follows:

  ```
  # cd /etc/init.d

  # chmod 750 rc.alliance rc.swa_boot

  # chown root:sys rc.alliance rc.swa_boot
  ```

If the SWIFTAlliance Access Installer displays “Start this SWIFTAlliance at Boottime”, choose **No**.

You must copy the `rc.alliance` and `rc.swa_boot` scripts to all other cluster nodes or zones that can master the resource group:

```
# scp rc.alliance rc.swa_boot node2:/etc/init.d
```

6 **Install SWIFTAlliance Access Remote API (RA)**

- Install RA after SWIFTAlliance Access on shared storage using the following options:

  Instance `RA1` (default), user `all_adm`
- Copy all files in the home directory of the `all_adm` and `all_usr` user to all cluster nodes or zones that can master the resource group.

Verifying the Installation and Configuration of SWIFTAlliance Access

This section contains the procedure you need to verify the installation and configuration.

▼ How to Verify the Installation and Configuration of SWIFTAlliance Access

This procedure does not verify that your application is highly available because you have not yet installed your data service.

1 **Start the SWIFTAlliance Access application.**

For SWIFTAlliance Access versions other than SWIFTAlliance Access version 5.5, type:

```
# su - all_adm
```

For SWIFTAlliance Access version 5.5, choose Alliance —> Start SWIFTAlliance Servers.

Note – If DCE does not start, choose GUI: OS Configuration —> DCE RPC.

---

2 **Test the application.**

a. **Start the SWIFTAlliance Access application.**

b. **Choose Alliance —> Start User Interface.**

3 **Stop the SWIFTAlliance Access application.**

Start the GUI:

```
# su - all_adm
```

Choose the menu: Alliance —> Stop SWIFTAlliance Servers.

Installing the Sun Cluster HA for SWIFTAlliance Access Packages

If you did not install the Sun Cluster HA for SWIFTAlliance Access packages during your initial Sun Cluster installation, perform this procedure to install the packages. To install the packages, use the Sun Java™ Enterprise System Installation Wizard.

▼ How to Install the Sun Cluster HA for SWIFTAlliance Access Packages

Perform this procedure on each cluster node where you are installing the Sun Cluster HA for SWIFTAlliance Access packages.

You can run the Sun Java Enterprise System Installation Wizard with a command-line interface (CLI) or with a graphical user interface (GUI). The content and sequence of instructions in the CLI and the GUI are similar.

Note – Even if you plan to configure this data service to run in non-global zones, install the packages for this data service in the global zone. The packages are propagated to any existing non-global zones and to any non-global zones that are created after you install the packages.

Before You Begin Ensure that you have the Sun Java Availability Suite DVD-ROM.

If you intend to run the Sun Java Enterprise System Installation Wizard with a GUI, ensure that your `DISPLAY` environment variable is set.

1 **On the cluster node where you are installing the data service packages, become superuser.**

2 **Load the Sun Java Availability Suite DVD-ROM into the DVD-ROM drive.**

If the Volume Management daemon `vold`(1M) is running and configured to manage DVD-ROM devices, the daemon automatically mounts the DVD-ROM on the `/cdrom` directory.

3 **Change to the Sun Java Enterprise System Installation Wizard directory of the DVD-ROM.**

- **If you are installing the data service packages on the SPARC® platform, type the following command:**

```
# cd /cdrom/cdrom0/Solaris_sparc
```

4 **Start the Sun Java Enterprise System Installation Wizard.**

```
# ./installer
```

5 **When you are prompted, accept the license agreement.**

If any Sun Java Enterprise System components are installed, you are prompted to select whether to upgrade the components or install new software.

6 **From the list of Sun Cluster agents in Availability Services, select the data service for SWIFTAlliance Access.**

7 **If you require support for languages other than English, select the option to install multilingual packages.**

English language support is always installed.

8 **When prompted whether to configure the data service now or later, choose Configure Later.**

Choose Configure Later to perform the configuration after the installation.

9 **Follow the instructions on the screen to install the data service packages on the node.**

The Sun Java Enterprise System Installation Wizard displays the status of the installation. When the installation is complete, the wizard displays an installation summary and the installation logs.

10 **(GUI only) If you do not want to register the product and receive product updates, deselect the Product Registration option.**

The Product Registration option is not available with the CLI. If you are running the Sun Java Enterprise System Installation Wizard with the CLI, omit this step.

11 **Exit the Sun Java Enterprise System Installation Wizard.**

12 **Unload the Sun Java Availability Suite DVD-ROM from the DVD-ROM drive.**

a. **To ensure that the DVD-ROM is not being used, change to a directory that does *not* reside on the DVD-ROM.**

b. **Eject the DVD-ROM.**

```
# eject cdrom
```

Next Steps Go to "Registering and Configuring Sun Cluster HA for SWIFTAlliance Access" on page 20

Registering and Configuring Sun Cluster HA for SWIFTAlliance Access

This section contains the procedures you need to configure Sun Cluster HA for SWIFTAlliance Access.

▼ How to Register and Configure Sun Cluster HA for SWIFTAlliance Access as a Failover Service

This procedure assumes that you installed the data service packages during your initial Sun Cluster installation.

Steps 1 to 6 will normally already be done in order to prepare for the installation of the IBM DCE and SWIFTAlliance Access software. See "How to Install and Configure SWIFTAlliance Access" on page 13. Typically, you should go directly to step 7.

1 Become superuser on one of the nodes in the cluster that will host Sun Cluster.

2 Register the SUNW.gds resource type.

```
# clresourcetype register SUNW.gds
```

3 Register the SUNW.HAStoragePlus resource type.

```
# clresourcetype register SUNW.HAStoragePlus
```

4 Create a failover resource group .

```
# clresourcegroup create [-n node-zone-list] swift-rg
```

`-n node-zone-list` Specifies a comma-separated, ordered list of zones that can master the resource group. The format of each entry in the list is node. In this format, node specifies the node name and zone specifies the name of a non-global Solaris zone. To specify the global zone, or to specify a node without non-global zones, specify only node. This list is optional. If you omit this list, the global zone of each cluster node can master the resource group.

5 Create a resource for the Sun Cluster Disk Storage.

```
# clresource create -g swift-rg  \
-t SUNW.HAStoragePlus  \
-x FilesystemMountPoints=/global/saadg/alliance  swift-ds
```

6 **Create a resource for the Sun Cluster Logical Hostname.**

```
# clreslogicalhostname create  -g swift-rg\
  -h swift-lh  swift-lh-rs
```

7 **Enable the failover resource group that now includes the Sun Cluster Disk Storage and Logical Hostname resources.**

```
# clresourcegroup online -M swift-rg
```

8 **Create a resource for SWIFTAlliance Access.**

a. **Before running this script, check that the names of the resources match what is configured in** `/opt/SUNWscsaa/util/saa_config`**.**

```
# /opt/SUNWscsaa/util/saa_register
```

b. **Run the registration script provided as part of the SWIFTAlliance Access HA agent.**

9 **Start the SWIFTAlliance Access instance manually.**

```
su - all_adm
The GUI will open up. From within the GUI, select the menu
Alliance - Start Alliance Servers
```

10 **Stop the SWIFTAlliance Access manually.**

```
su - all_adm
 The GUI will come up. Stop the application from within the GUI.
```

11 **Enable each Sun Cluster resource.**

```
# clresourcegroup status -g swift-rg
# clresource enable swift-saa-rs
```

Verifying the Sun Cluster HA for SWIFTAlliance Access Installation and Configuration

This section contains the procedure you need to verify that you installed and configured your data service correctly.

▼ How to Verify the Sun Cluster HA for SWIFTAlliance Access Installation and Configuration

1. **Become superuser on one of the nodes in the cluster that will host Sun Cluster.**

2. **Ensure all the Sun Cluster resources are online with `cluster status`.**

   ```
   # cluster status
   ```

   For each Sun Cluster resource that is not online, use the `clresource` command as follows.

   ```
   # clresource enable resource-name
   ```

3. **Run the `clresourcegroup` command to switch the Sun Cluster resource group to another cluster node, such as *node2*.**

   ```
   # clresourcegroup switch swift-rg -h node2
   ```

4. **Check that SWIFTAlliance Access is stopped on the first node and that the application is restarted on the second node.**

   When using a failover file system, this should disappear on the first node and will be mounted on the second node.

Understanding the Sun Cluster HA for SWIFTAlliance Access Fault Monitor

This section describes the Sun Cluster HA for SWIFTAlliance Access fault monitor's probing algorithm or functionality, and states the conditions, messages, and recovery actions associated with unsuccessful probing.

For conceptual information on fault monitors, see the *Sun Cluster Concepts Guide*.

Resource Properties

The Sun Cluster HA for SWIFTAlliance Access fault monitor uses the same resource properties as resource type `SUNW.gds`, refer to the `SUNW.gds(5)` man page for a complete list of resource properties used.

Probing Algorithm and Functionality

By default, the HA agent provides a fault monitor for the DCE component only when using SWIFTAlliance Access 5.5. The fault monitoring for SWIFTAlliance Access is switched off by default. If the SWIFTAlliance Access application fails, the agent will not restart the SWIFTAlliance Access application automatically. This behavior was explicitly requested by SWIFT. It will enable you to operate the application in a way that the probe does not interfere with the normal behavior of some SWIFTAlliance Access features like:

- operator manually triggering the SWIFTAlliance Access restart function , for example, to run SWIFTAlliance Access in housekeeping mode.
- automatic or scheduled SWIFTAlliance Access restart, for example, to run database backup and other maintenance or end-of-day processes.
- any graceful SWIFTAlliance Access restart or recovery, in case of a SWIFTAlliance Access transient local error.

The HA agent will update the resource status message to output `Degraded - SAA Instance offline`.

If an automatic failover occurs with default setting, it is most likely that there was a DCE problem. The SWIFTAlliance Access application will cause a failover only when it does not start on the current node.

The HA agent provides an option to turn on fault monitoring for SWIFTAlliance Access at registration time. However, this option is not recommended by SWIFT. The optional probing checks for the existence of the SWIFTAlliance Access instance by calling the `alliance` command that is part of the application and by evaluating its return code. If the SWIFTAlliance Access instance is not running, return code 100 is sent to `SUNW.gds`, which in turn will perform an automatic restart depending on the configuration of the resource properties.

Debugging Sun Cluster HA for SWIFTAlliance Access

▼ How to turn on debugging for Sun Cluster HA for SWIFTAlliance Access

Each Sun Cluster component has a `DEBUG` file in `/opt/SUNWscsaa/etc` directory, where `saa` is a three-character abbreviation for the respective Sun Cluster component.

These files enable you to turn on debugging for all Sun Cluster instances or for a specific Sun Cluster instance on a particular node with Sun Cluster. If you require debugging to be turned

on for Sun Cluster HA for SWIFTAlliance Access across the entire Sun Cluster installation, repeat this step on all nodes or zones that can master the resource group.

1 **Edit** `/etc/syslog.conf`

Change `daemon.notice` to `daemon.debug`

```
# grep daemon /etc/syslog.conf
*.err;kern.debug;daemon.notice;mail.crit        /var/adm/messages
*.alert;kern.err;daemon.err                     operator
#
```

Change the `daemon.notice` to `daemon.debug` and restart `syslogd`. The following output, from the command `grep daemon /etc/syslog.conf`, shows that `daemon.debug` has been set.

```
# grep daemon /etc/syslog.conf
*.err;kern.debug;daemon.debug;mail.crit        /var/adm/messages
*.alert;kern.err;daemon.err                    operator
#
# pkill -1 syslogd
#
```

2 **Edit** `/opt/SUNWscsaa/etc/config`

Change `DEBUG=` to `DEBUG=ALL` or `DEBUG=`*resource*

```
# cat /opt/SUNWscsaa/etc/config
#
# Copyright 2003 Sun Microsystems, Inc.  All rights reserved.
# Use is subject to license terms.
#
# Usage:
#       DEBUG=<RESOURCE_NAME> or ALL
#
DEBUG=ALL
#
```

Note – To turn off debugging, reverse the previous steps.

Index