



Sun Cluster Data Service for Apache Guide for Solaris OS

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

Part No: 817-6998-10
August 2005, Revision A

Copyright 2005 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 U.S.A. All rights reserved.

This product or document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this product or document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any. Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, docs.sun.com, AnswerBook, AnswerBook2, SunPlex, Java, and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

U.S. Government Rights – Commercial software. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Copyright 2005 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 U.S.A. Tous droits réservés.

Ce produit ou document est protégé par un copyright et distribué avec des licences qui en restreignent l'utilisation, la copie, la distribution, et la décompilation. Aucune partie de ce produit ou document ne peut être reproduite sous aucune forme, par quelque moyen que ce soit, sans l'autorisation préalable et écrite de Sun et de ses bailleurs de licence, s'il y en a. Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun.

Des parties de ce produit pourront être dérivées du système Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, docs.sun.com, AnswerBook, AnswerBook2, SunPlex, Java, et Solaris sont des marques de fabrique ou des marques déposées, de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays. Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

L'interface d'utilisation graphique OPEN LOOK et Sun™ a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développement du concept des interfaces d'utilisation visuelle ou graphique pour l'industrie de l'informatique. Sun détient une licence non exclusive de Xerox sur l'interface d'utilisation graphique Xerox, cette licence couvrant également les licenciés de Sun qui mettent en place l'interface d'utilisation graphique OPEN LOOK et qui en outre se conforment aux licences écrites de Sun.

CETTE PUBLICATION EST FOURNIE "EN L'ETAT" ET AUCUNE GARANTIE, EXPRESSE OU IMPLICITE, N'EST ACCORDEE, Y COMPRIS DES GARANTIES CONCERNANT LA VALEUR MARCHANDE, L'APTITUDE DE LA PUBLICATION A REpondre A UNE UTILISATION PARTICULIERE, OU LE FAIT QU'ELLE NE SOIT PAS CONTREFAISANTE DE PRODUIT DE TIERS. CE DENI DE GARANTIE NE S'APPLIQUERAIT PAS, DANS LA MESURE OU IL SERAIT TENU JURIDIQUEMENT NUL ET NON AVENU.



050503@11223



Contents

Preface 5

Installing and Configuring Sun Cluster HA for Apache 11

Planning the Installation and Configuration 11

Overview of the Installation and Configuration Process for Sun Cluster HA for Apache 16

Installing and Configuring Apache 16

Installing a Non-Secure Apache Webserver 17

▼ How to Install and Configure the Apache Software from the Solaris CD-ROM 17

▼ How to Install and Configure the Apache Software from the Apache Web Site 18

Installing a Secure Apache Webserver 20

▼ How to Install and Configure the Apache Software Using mod_ssl 20

▼ How to Install and Configure the Apache Software Using apache-ssl 22

Installing Sun Cluster HA for Apache Packages 24

▼ How to Install Sun Cluster HA for Apache Packages by Using the Web Start Program 24

▼ How to Install Sun Cluster HA for Apache Packages by Using the `scinstall` Utility 25

Registering and Configuring Sun Cluster HA for Apache 26

Setting Sun Cluster HA for Apache Extension Properties 27

Monitoring Arbitrary URIs 27

▼ How to Register and Configure Sun Cluster HA for Apache 28

How to Configure `SUNW.HAStoragePlus` Resource Type 34

How to Verify Data Service Installation and Configuration 35

Tuning the Sun Cluster HA for Apache Fault Monitor 35

Operations by the Sun Cluster HA for Apache Fault Monitor	35
Actions in Response to Faults	37
Upgrading the SUNW.apache Resource Type	37
Information for Registering the New Resource Type Version	38
Information for Migrating Existing Instances of the Resource Type	38

A Sun Cluster HA for Apache Extension Properties 41

Index	43
--------------	-----------

Preface

Sun Cluster Data Service for Apache Guide for Solaris OS explains how to install and configure Sun™ Cluster HA for Apache on both SPARC® and x86 based systems.

Note – In this document, the term “x86” refers to the Intel 32-bit family of microprocessor chips and compatible microprocessor chips made by AMD.

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 document assume knowledge of the Solaris™ Operating System and expertise with the volume manager software that is used with Sun Cluster.

Note – Sun Cluster software runs on two platforms, SPARC and x86. The information in this document pertains to both platforms unless otherwise specified in a special chapter, section, note, bulleted item, figure, table, or example.

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 changes that are used in this book.

TABLE P-1 Typographic Conventions

Typeface or Symbol	Meaning	Example
AaBbCc123	The names of commands, files, and directories, and onscreen computer output	Edit your <code>.login</code> file. Use <code>ls -a</code> to list all files. <code>machine_name%</code> you have mail.
AaBbCc123	What you type, contrasted with onscreen computer output	<code>machine_name%</code> su Password:
<i>AaBbCc123</i>	Command-line placeholder: replace with a real name or value	The command to remove a file is <code>rm filename</code> .
<i>AaBbCc123</i>	Book titles, new terms, and terms to be emphasized	Read Chapter 6 in the <i>User's Guide</i> . Perform a <i>patch analysis</i> . Do <i>not</i> save the file. [Note that some emphasized items appear bold online.]

Shell Prompts in Command Examples

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

TABLE P-2 Shell Prompts

Shell	Prompt
C shell prompt	machine_name%
C shell superuser prompt	machine_name#
Bourne shell and Korn shell prompt	\$
Bourne shell and Korn shell superuser prompt	#

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	<i>Sun Cluster Data Services Planning and Administration Guide for Solaris OS</i> Individual data service guides
Concepts	<i>Sun Cluster Concepts Guide for Solaris OS</i>
Overview	<i>Sun Cluster Overview for Solaris OS</i>
Software installation	<i>Sun Cluster Software Installation Guide for Solaris OS</i>
System administration	<i>Sun Cluster System Administration Guide for Solaris OS</i>
Hardware administration	<i>Sun Cluster 3.0-3.1 Hardware Administration Manual for Solaris OS</i> Individual hardware administration guides
Data service development	<i>Sun Cluster Data Services Developer's Guide for Solaris OS</i>
Error messages	<i>Sun Cluster Error Messages Guide for Solaris OS</i>
Command and function reference	<i>Sun Cluster Reference Manual for Solaris OS</i>

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.

Accessing Sun Documentation Online

The docs.sun.comSM Web site enables you to access Sun technical documentation online. You can browse the docs.sun.com archive or search for a specific book title or subject. The URL is <http://docs.sun.com>.

Ordering Sun Documentation

Sun Microsystems offers select product documentation in print. For a list of documents and how to order them, see “Buy printed documentation” at <http://docs.sun.com>.

Product Training

Sun Microsystems offers training in many Sun technologies through a variety of instructor-led courses and self-paced courses. For information about the training courses that Sun offers and to enroll in a class, visit Sun Microsystems Training at <http://training.sun.com/>.

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 and serial numbers of your systems
- The release number of the Solaris Operating System (for example, Solaris 8)
- The release number of Sun Cluster (for example, Sun Cluster 3.0)

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

Command	Function
<code>prtconf -v</code>	Displays the size of the system memory and reports information about peripheral devices
<code>psrinfo -v</code>	Displays information about processors
<code>showrev -p</code>	Reports which patches are installed
SPARC: <code>prtdiag -v</code>	Displays system diagnostic information
<code>scinstall -pv</code>	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 Apache

This chapter describes the steps to install and configure Sun Cluster HA for Apache on your Sun Cluster servers.

This chapter contains the following sections.

- “Planning the Installation and Configuration” on page 11
- “Overview of the Installation and Configuration Process for Sun Cluster HA for Apache” on page 16
- “Installing and Configuring Apache” on page 16
- “Installing Sun Cluster HA for Apache Packages” on page 24
- “Registering and Configuring Sun Cluster HA for Apache” on page 26
- “Tuning the Sun Cluster HA for Apache Fault Monitor” on page 35
- “Upgrading the SUNW . apache Resource Type” on page 37

You can configure Sun Cluster HA for Apache as a failover or a scalable data service. See Chapter 1, “Planning for Sun Cluster Data Services,” in *Sun Cluster Data Services Planning and Administration Guide for Solaris OS* and the *Sun Cluster Concepts Guide for Solaris OS* document for an overview of failover and scalable data services.

Note – You can use SunPlex™ Manager to install and configure this data service. See the SunPlex Manager online help for details.

Planning the Installation and Configuration

Before you install Sun Cluster HA for Apache, update the following information in the Apache configuration file `httpd.conf`.

Note – The location of the `httpd.conf` file varies according to installation. System administrators typically install the `httpd.conf` file on the cluster file system. The default installation places the `httpd.conf` file in the `/usr/local/apache/conf` directory. When installing Apache packages bundled with Solaris, the file is located in the `/etc/apache` directory.

- **The `ServerName` directive that contains the hostname** – For Sun Cluster HA for Apache to be highly available, you must set this directive to the name of the network address (logical hostname or shared address) that is used to access the server. You should have set up the logical hostname or shared address when you installed the cluster. See the *Sun Cluster Concepts Guide for Solaris OS* document for details on network resources.
- **The `BindAddress` directive, which you must set to the logical host or shared address** – You can configure Apache to bind to `INADDR_ANY`. However, each resource must bind to a unique combination of network resource and port number. For example, if you run multiple resources, you can use `INADDR_ANY` provided that the port number for each resource is different.
- **The `ServerType` directive** – This directive must be set to `standalone`, the default.
- **Multiple instances of Apache** – If you have multiple instances of Apache, you must manage each instance with a separate resource. Furthermore, each separate resource must have a unique `Bin_dir` setting. Under the specified `Bin_dir` property that starts the particular instance of Apache, an `apachectl` script must exist.

Note – Different Apache resources can share the same `httpd` binary, that is, the `apachectl` scripts for different resources can specify the path to the same `httpd` binary. However, you must modify each `apachectl` script to use a different configuration file for specific Apache resources. To do so, use the `-f` option of the `httpd` command to specify a specific `httpd.conf` file.

- **The `DocumentRoot` directive that specifies the location of the documentation root directory** – This directive is a pointer to a location on the cluster file system, where the HTML documents are installed.
- **The `ScriptAlias` directive that contains the location on a cluster file system of the `cgi-bin` directory** – This directive is a pointer to a location on the cluster file system, where the `cgi-bin` files are installed.

Note – You must follow certain conventions when you configure URL mappings for the Web server. For example, when setting the CGI directory, locate the CGI directory on the cluster file system to preserve availability. For example, you might map your CGI directory to `/global/diskgroup/ServerRoot/cgi-bin`, where *diskgroup* is the disk device group that contains the Apache software. In situations where the CGI programs access “back-end” servers, such as an RDBMS, ensure that the Sun Cluster software controls the “back-end” server. If the server is an RDBMS that the Sun Cluster software supports, use one of the highly available RDBMS packages. Alternatively, you can use the APIs that the *Sun Cluster Data Services Developer’s Guide for Solaris OS* documents to put the server under Sun Cluster control.

- **The lock file** – If you use a lock file, set the value of the `LockFile` directive in your `httpd.conf` file to a local file.
- **The `PidFile` directive** – Point this directive to a local file, as in the following example.

```
PidFile /usr/local/apache/log/httpd.pid
```

- **The `Port` directive setting that the server port or ports access** – The defaults are set in each node’s `httpd.conf` file. The `Port_list` resource property must include all of the ports that the `httpd.conf` files specify.

The `Port_list` property assumes that the Web server serves all combinations of ports and IP addresses from the network resources as defined in the `Network_resources_used` property.

```
Port_list="80/tcp,443/tcp,8080/tcp"
```

The preceding `Port_list` configuration, for example, probes the following IP-port combinations.

Host	Port	Protocol
<i>node1</i>	80	tcp
<i>node1</i>	443	tcp
<i>node1</i>	8080	tcp
<i>node2</i>	80	tcp
<i>node2</i>	443	tcp
<i>node2</i>	8080	tcp

However, if *node1* serves ports 80 and 443 only and *node2* serves ports 80 and 8080 only, you can configure the `Port_list` property for Apache as follows.

```
Port_list=node1/80/tcp,node1/443/tcp,node2/80/tcp,node2/8080/tcp
```

Consider the following rules.

- You must specify hostnames or IP addresses (not network resource names) for *node1* and *node2*.
- If Apache serves *nodeN/port* for every *nodeN* in the `Network_resources_used` property, you can use a short form to replace the combination of *node1/port1*, *node2/port2*, and so on. See the following examples.

Example One

```
Port_list="80/tcp,node1/443/tcp,node2/8080/tcp"
Network_resources_used=node1,node2
```

This example probes the following IP-port combinations.

Host	Port	Protocol
<i>node1</i>	80	tcp
<i>node1</i>	443	tcp
<i>node2</i>	80	tcp
<i>node2</i>	8080	tcp

Example Two

```
Port_list="node1/80/tcp,node2/80/tcp"
Network_resources_used=net-1,net-2
#net-1 contains node1.
#net-2 contains node2 and node3.
```

This example probes the following IP-port combinations.

Host	Port	Protocol
<i>node1</i>	80	tcp
<i>node2</i>	80	tcp

- All of the hostnames (IP addresses) that the `Port_list` property specifies must not belong to a network resource that is specified in any other scalable resource's `Network_resources_used` property. Otherwise, as soon as a scalable service detects that another scalable resource already uses an IP address, creation of the Apache resource fails.

Note – If you run Sun Cluster HA for Apache and another HTTP server, configure the HTTP servers to listen on different ports. Otherwise, a port conflict can occur between the two servers.

To register and configure Sun Cluster HA for Apache, you must consider or provide information on the following points.

- Decide whether to run Sun Cluster HA for Apache as a failover or scalable data service.
- Decide whether to install a secure or non-secure version of the apache webserver.
- Decide which fault monitoring resource properties to set. In most cases, the default values suffice. See *Sun Cluster Data Services Planning and Administration Guide for Solaris OS* for information about the standard properties and [Appendix A](#) for information about the extension properties.
- Provide the name of the resource type for Sun Cluster HA for Apache. This name is `SUNW.apache`.
- Provide the names of the cluster nodes that will master the data service.
- Provide the logical hostname (failover services) or shared address (scalable services) that clients use to access the data service. You typically set up this IP address when you install the cluster. See the *Sun Cluster Concepts Guide for Solaris OS* document for details on network resources.
- Provide the path to the application binaries. You can install the binaries on the local disks or on the cluster file system. See “Configuration Guidelines for Sun Cluster Data Services” in *Sun Cluster Data Services Planning and Administration Guide for Solaris OS* for a discussion of the advantages and disadvantages of each location.
- Modify each copy of `apachectl` to use the appropriate `httpd.conf` configuration file.
- Exercise caution when you change the `Load_balancing_weights` property for an online scalable service that has the `Load_balancing_policy` property set to `LB_STICKY` or `LB_STICKY_WILD`. Changing these properties while the service is online can cause existing client affinities to be reset, hence a different node might service a subsequent client request even if another cluster member previously serviced the client.

Similarly, when a new instance of the service is started on a cluster, existing client affinities might be reset.

- Determine the entry for the `Port_list` property. The `Port_list` property can have multiple entries. See “[How to Register and Configure Sun Cluster HA for Apache](#)” on page 28 for details.
- Determine whether to utilize the `Monitor Uri List` extension property. This extension property enables you to monitor an arbitrary list of URIs. Arbitrary monitoring of URIs is beneficial if you require the Sun Cluster HA for Apache agent probe to monitor any applications (URIs) deployed on the Sun Cluster HA for

Apache server. Use of the `Monitor Uri List` extension property is not supported with secure instances of Sun Cluster HA for Apache. You must install release 3.1 10/03 of Sun Cluster HA for Apache to use this property. If you are upgrading Sun Cluster HA for Apache from a previous version, you must perform a resource type upgrade procedure to use the new property. For instructions, see “Upgrading a Resource Type” in *Sun Cluster Data Services Planning and Administration Guide for Solaris OS*. See “Monitoring Arbitrary URIs” on page 27 for detailed information about using the `Monitor Uri List` extension property.

Overview of the Installation and Configuration Process for Sun Cluster HA for Apache

The table below lists the sections that describe the installation and configuration tasks.

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

Task	For Instructions, Go To
Install the Apache software	“Installing and Configuring Apache” on page 16
Install the Sun Cluster HA for Apache packages	“How to Install Sun Cluster HA for Apache Packages by Using the Web Start Program” on page 24 “How to Install Sun Cluster HA for Apache Packages by Using the <code>scinstall</code> Utility” on page 25
Configure and start Sun Cluster HA for Apache	“How to Register and Configure Sun Cluster HA for Apache” on page 28
Tune the Sun Cluster HA for Apache fault monitor	“Tuning the Sun Cluster HA for Apache Fault Monitor” on page 35

Installing and Configuring Apache

The Apache webserver can be installed and set up as either a non-secure or a secure webserver. This section provides procedures for both types of installations. To install a non-secure version of the webserver, see one of the following procedures.

- “How to Install and Configure the Apache Software from the Solaris CD-ROM” on page 17

- [“How to Install and Configure the Apache Software from the Apache Web Site”](#) on page 18

To install a secure version of the webserver, see one of the following procedures.

- [“How to Install and Configure the Apache Software Using mod_ssl”](#) on page 20
- [“How to Install and Configure the Apache Software Using apache-ssl”](#) on page 22

Sun Cluster HA for Apache works with the Apache software configured as either a Web server or a proxy server.

See Apache documentation at <http://www.apache.org> for standard installation instructions. Contact your Sun sales representative for a complete list of Apache versions that are supported with the Sun Cluster software.

Installing a Non-Secure Apache Webserver

This section provides procedures for installing a non-secure Apache webserver. For procedures for installing a secure Apache webserver, see [“Installing a Secure Apache Webserver”](#) on page 20.

▼ How to Install and Configure the Apache Software from the Solaris CD-ROM

This procedure installs a non-secure version of the Apache webserver. For procedures for installing a secure Apache webserver, see [“Installing a Secure Apache Webserver”](#) on page 20.

The Apache binaries are included in three packages—`SUNWapchr`, `SUNWapchu`, and `SUNWapchd`—that form the `SUNWCapache` package metacluster. You must install the `SUNWapchr` package before you install the `SUNWapchu` package.

Place the Web server binaries on the local file system on each of your cluster nodes or on a cluster file system.

- Steps**
1. **Run the `pkginfo(1)` command to determine if the Apache packages `SUNWapchr`, `SUNWapchu`, and `SUNWapchd` have been installed.**

If these packages have not been installed, install them as follows.

- With Solaris 8 and Solaris 9, run the following command.

```
# pkgadd -d Solaris-product-directory SUNWapchr SUNWapchu SUNWapchd
```

- With Solaris 10, run the following command.

```
# pkgadd -G -d Solaris-product-directory SUNWapchr SUNWapchu SUNWapchd
```

The output from the command is as follows.

```
...  
Installing Apache Web Server (root) as SUNWapchr
```

```

...
[ verifying class initd ]
/etc/rc0.d/K16apache linked-pathname
/etc/rc1.d/K16apache linked-pathname
/etc/rc2.d/K16apache linked-pathname
/etc/rc3.d/S50apache linked-pathname
/etc/rcS.d/K16apache linked-pathname
...

```

2. Disable the START and STOP run control scripts that were just installed as part of the SUNWapchr package.

This step is necessary because Sun Cluster HA for Apache starts and stops the Apache application after you have configured the data service. Perform the following steps.

- a. List the Apache run control scripts.
- b. Rename the Apache run control scripts.
- c. Verify that all of the Apache-related scripts have been renamed.

The following example changes the first letter in the name of the run control script from uppercase to lowercase. However, you can rename the scripts to be consistent with your normal administration practices.

```

# ls -l /etc/rc?.d/*apache
/etc/rc0.d/K16apache
/etc/rc1.d/K16apache
/etc/rc2.d/K16apache
/etc/rc3.d/S50apache
/etc/rcS.d/K16apache

# mv /etc/rc0.d/K16apache /etc/rc0.d/k16apache
# mv /etc/rc1.d/K16apache /etc/rc1.d/k16apache
# mv /etc/rc2.d/K16apache /etc/rc2.d/k16apache
# mv /etc/rc3.d/S50apache /etc/rc3.d/s50apache
# mv /etc/rcS.d/K16apache /etc/rcS.d/k16apache

# ls -l /etc/rc?.d/*apache
/etc/rc0.d/k16apache
/etc/rc1.d/k16apache
/etc/rc2.d/k16apache
/etc/rc3.d/s50apache
/etc/rcS.d/k16apache

```

▼ How to Install and Configure the Apache Software from the Apache Web Site

This procedure installs a non-secure version of the Apache webserver. For procedures for installing a secure Apache webserver, see [“Installing a Secure Apache Webserver”](#) on page 20.

Place the Web server binaries on the local file system on each of your cluster nodes or on a cluster file system.

Steps 1. Become superuser on a cluster member.

2. Install the Apache software using the installation procedures found in the Apache installation documentation.

Install the Apache software using the Apache installation documentation you received with your Apache software or see the installation instructions at <http://www.apache.org>.

3. Update the `httpd.conf` configuration file.

- Set the `ServerName` directive. (In Version 2.0 of Apache, the `ServerName` directive specifies the hostname and the port.)
- Set the `BindAddress` directive (optional). (The `BindAddress` directive only exists in versions prior to Apache 2.0. For Apache 2.0, see the following bullet for the `Listen` directive.)
- Set the `Listen` directive. The `Listen` directive must use the address of the logical host or shared address. (The `Listen` directive only exists in Apache 2.0 and beyond. For Apache versions prior to Apache 2.0, see the previous bullet for the `BindAddress` directive.)
- Set the `ServerType`, `ServerRoot`, `DocumentRoot`, `ScriptAlias`, and `LockFile` directives.

Note – The `ServerType` directive does not exist in Apache 2.0.

- Set the `Port` directive to the same number as the `Port_list` standard resource property. See [Step 4](#) for more information.
- Make changes to run as a proxy server if you choose to run the Apache software as a proxy server. See the Apache documentation for more information. If you will run the Apache software as a proxy server, the `CacheRoot` setting must point to a location on the cluster file system.

4. Verify that the port number or numbers in the `httpd.conf` file match those of the `Port_list` standard resource property.

You can edit the `httpd.conf` configuration file to change its port number or numbers to match the standard Sun Cluster resource property default (port 80). Alternatively, while you configure Sun Cluster HA for Apache, you can set the `Port_list` standard property to match the setting in the `httpd.conf` file.

5. Update the paths in the Apache start/stop script file (`Bin_dir/apachectl`).

You must change the paths from the Apache defaults to match your Apache directory structure. For example, change the line in the `BIN_dir/apachectl`

script beginning with `HTTPD=/usr/local/apache/bin/httpd` to the following.

```
HTTPD=' /usr/local/apache/bin/httpd -f /global/foo/apache/conf/httpd.conf'
```

6. **Perform the following tasks to verify your configuration changes.**
 - a. **Run `apachectl configtest` to check the Apache `httpd.conf` file for correct syntax.**
 - b. **Ensure that any logical hostnames or shared addresses that Apache uses are configured and online.**
 - c. **Issue `apachectl start` to start up your Apache server by hand.**
If Apache does not start up correctly, correct the problem.
 - d. **After Apache has started, stop it before moving to the next procedure.**

Installing a Secure Apache Webserver

This section provides procedures for installing a secure Apache webserver. For procedures for installing a non-secure Apache webserver, see [“Installing a Non-Secure Apache Webserver” on page 17](#).

▼ How to Install and Configure the Apache Software Using `mod_ssl`

This procedure installs a secure version of the Apache webserver. For procedures for installing a non-secure Apache webserver, see [“Installing a Non-Secure Apache Webserver” on page 17](#).

- Steps**
1. **Become superuser on a cluster member.**
 2. **Install the Apache software, including `mod_ssl`.**
To install `mod_ssl`, see the Apache installation documentation or the installation instructions at <http://www.modssl.org>.
 3. **Update the `httpd.conf` configuration file.**
 - Set the `ServerName` directive.
 - Set the `BindAddress` directive (optional).
 - Set the `ServerType`, `ServerRoot`, `DocumentRoot`, `ScriptAlias`, and `LockFile` directives.
 - Set the `Port` directive to the same number as the `Port_list` standard resource property. See [Step 4](#) for more information.
 - Make changes to run as a proxy server if you choose to run the Apache software as a proxy server. See the Apache documentation for more information. If you will run the Apache software as a proxy server, the `CacheRoot` setting must

point to a location on the cluster file system.

4. Verify that the port number or numbers in the `httpd.conf` file match those of the `Port_list` standard resource property.

You can edit the `httpd.conf` configuration file to change its port number or numbers to match the standard Sun Cluster resource property default (port 80). Alternatively, while you configure Sun Cluster HA for Apache, you can set the `Port_list` standard property to match the setting in the `httpd.conf` file.

5. Install all certificates and keys.

6. In `Bin_dir` directory, create a file called `keypass`. Make sure that no one other than the owner has any permissions for this file.

```
# cd Bin_dir
# touch keypass
# chmod 700 keypass
```

7. If you are using encrypted private key(s), perform the following Step a and Step b.

a. In the `httpd.conf` file, look for `SSLPassPhraseDialog` directive and modify it as follows.

```
# SSLPassPhraseDialog exec:/Bin_dir/keypass
```

See the `mod_ssl` documentation for details about the `SSLPassPhraseDialog` directive.

b. Edit the `keypass` file so that it prints the pass phrase for the encrypted key corresponding to a host and a port.

This file will be called with `server:port` algorithm as arguments. Make sure that the file can print the pass phrase for each of your encrypted keys when called with the correct parameters.

Later, when you attempt to start the webserver manually, it must not prompt you for a pass phrase. For example, for a secure webserver listening on ports 8080 and 8888, with private keys for both encrypted using RSA, the `keypass` file could be the following.

```
# !/bin/ksh
host=`echo $1 | cut -d: -f1`
port=`echo $1 | cut -d: -f2`
algorithm=$2

if [ "$host" = "button-1.eng.sun.com" -a "$algorithm" = "RSA" ]; then
  case "$port" in
    8080) echo passphrase-for-8080;;
    8888) echo passphrase-for-8888;;
  esac
fi
```

Note – The `keypass` file must not be readable, writable, or executable by anyone other than the owner.

8. In the `httpd.conf` file, set the `SSLLogLevel` to `warn` to avoid logging a message every time the webserver is probed by Sun Cluster HA for Apache.

```
SSLLogLevel warn
```

9. Update the paths in the Apache start/stop script file (`Bin_dir/apachectl`).

You must change the paths from the Apache defaults to match your Apache directory structure.

10. Perform the following tasks to verify your configuration changes.

- a. Run `apachectl configtest` to check the Apache `httpd.conf` file for correct syntax.
- b. Ensure that any logical hostnames or shared addresses that Apache uses are configured and online.
- c. Issue `apachectl start` to start up your Apache server by hand.
Make sure that the webserver does not ask you for a passphrase.
If Apache does not start up correctly, correct the problem.
- d. After Apache has started, stop it before moving to the next procedure.

▼ How to Install and Configure the Apache Software Using `apache-ssl`

This procedure installs a secure version of the Apache webserver. For procedures for installing a non-secure Apache webserver, see [“Installing a Non-Secure Apache Webserver”](#) on page 17.

- Steps**
1. Become superuser on a cluster member.
 2. Install the Apache software, including `apache-ssl`, using the installation procedures found in the Apache installation documentation.
To install `apache-ssl`, see the Apache installation documentation or the installation instructions at <http://www.apache-ssl.org>.
 3. Update the `httpd.conf` configuration file.
 - Set the `ServerName` directive.
 - Set the `BindAddress` directive (optional).

- Set the `ServerType`, `ServerRoot`, `DocumentRoot`, `ScriptAlias`, and `LockFile` directives.
 - Set the `Port` directive to the same number as the `Port_list` standard resource property. See [Step 4](#) for more information.
 - Make changes to run as a proxy server if you choose to run the Apache software as a proxy server. See the Apache documentation for more information. If you will run the Apache software as a proxy server, the `CacheRoot` setting must point to a location on the cluster file system.
4. **Verify that the port number or numbers in the `httpd.conf` file match those of the `Port_list` standard resource property.**

You can edit the `httpd.conf` configuration file to change its port number or numbers to match the standard Sun Cluster resource property default (port 80). Alternatively, while you configure Sun Cluster HA for Apache, you can set the `Port_list` standard property to match the setting in the `httpd.conf` file.
 5. **Install all certificates and keys.**
 6. **Make sure that all your private keys are stored unencrypted.**

Later, when you attempt to start the webserver manually, it must not prompt you for a pass phrase.
 7. **Update the paths in the Apache start/stop script file (`Bin_dir/httpsdctl`).**

You must change the paths from the Apache defaults to match your Apache directory structure.
 8. **Perform the following tasks to verify your configuration changes.**
 - a. **Run `httpsdctl configtest` to check the Apache `httpd.conf` file for correct syntax.**
 - b. **Ensure that any logical hostnames or shared addresses that Apache uses are configured and online.**
 - c. **Issue `httpsdctl start` to start up your Apache server by hand.**

If Apache does not start up correctly, correct the problem.
 - d. **After Apache has started, stop it before moving to the next procedure.**

Next Steps If you did not install the Sun Cluster HA for Apache during your initial Sun Cluster installation, go to [“Installing Sun Cluster HA for Apache Packages”](#) on page 24. Otherwise, go to [“Registering and Configuring Sun Cluster HA for Apache”](#) on page 26.

Installing Sun Cluster HA for Apache Packages

If you did not install the Sun Cluster HA for Apache packages during your initial Sun Cluster installation, perform this procedure to install the packages. Perform this procedure on each cluster node where you are installing the Sun Cluster HA for Apache packages. To complete this procedure, you need the Sun Cluster Agents CD.

If you are installing more than one data service simultaneously, perform the procedure in “Installing the Software” in *Sun Cluster Software Installation Guide for Solaris OS*.

Install the Sun Cluster HA for Apache packages by using one of the following installation tools:

- The Web Start program
- The `scinstall` utility

Note – If you are using Solaris 10, install these packages *only* in the global zone. To ensure that these packages are not propagated to any local zones that are created after you install the packages, use the `scinstall` utility to install these packages. Do *not* use the Web Start program.

▼ How to Install Sun Cluster HA for Apache Packages by Using the Web Start Program

You can run the Web Start program 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. For more information about the Web Start program, see the `installer(1M)` man page.

- Steps**
1. **On the cluster node where you are installing the Sun Cluster HA for Apache packages, become superuser.**
 2. **(Optional) If you intend to run the Web Start program with a GUI, ensure that your `DISPLAY` environment variable is set.**
 3. **Insert the Sun Cluster Agents CD into the CD-ROM drive.**
If the Volume Management daemon `vold(1M)` is running and configured to manage CD-ROM devices, it automatically mounts the CD-ROM on the `/cdrom/cdrom0` directory.
 4. **Change to the Sun Cluster HA for Apache component directory of the CD-ROM.**

The Web Start program for the Sun Cluster HA for Apache data service resides in this directory.

```
# cd /cdrom/cdrom0/components/SunCluster_HA_Apache_3.1
```

5. Start the Web Start program.

```
# ./installer
```

6. When you are prompted, select the type of installation.

- To install only the C locale, select Typical.
- To install other locales, select Custom.

7. Follow the instructions on the screen to install the Sun Cluster HA for Apache packages on the node.

After the installation is finished, the Web Start program provides an installation summary. This summary enables you to view logs that the Web Start program created during the installation. These logs are located in the `/var/sadm/install/logs` directory.

8. Exit the Web Start program.

9. Remove the Sun Cluster Agents CD from the CD-ROM drive.

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

```
# eject cdrom
```

Next Steps Go to [“Registering and Configuring Sun Cluster HA for Apache”](#) on page 26.

▼ How to Install Sun Cluster HA for Apache Packages by Using the `scinstall` Utility

Perform this procedure on all of the cluster members that can master Sun Cluster HA for Apache.

Before You Begin Ensure that you have the Sun Cluster Agents CD.

- Steps**
- 1. Load the Sun Cluster Agents CD into the CD-ROM drive.**
 - 2. Run the `scinstall` utility with no options.**
This step starts the `scinstall` utility in interactive mode.

3. Select the menu option, Add Support for New Data Service to This Cluster Node.

The `scinstall` utility prompts you for additional information.

4. Provide the path to the Sun Cluster Agents CD.

The utility refers to the CD as the “data services cd.”

5. Specify the data service to install.

The `scinstall` utility lists the data service that you selected and asks you to confirm your choice.

6. Exit the `scinstall` utility.

7. Unload the CD from the drive.

Next Steps Go to “[Registering and Configuring Sun Cluster HA for Apache](#)” on page 26.

Registering and Configuring Sun Cluster HA for Apache

This procedure describes how to use the `scrgadm(1M)` command to register and configure Sun Cluster HA for Apache.

You can configure Apache as a failover service or as a scalable service, as follows.

- When you configure Apache as a failover service, you place the Apache application resources and the network resources in a single resource group.
- When you configure Apache as a scalable service, you create a scalable resource group for the Apache application resources and a failover resource group for the network resources.

The scalable resource group depends on the failover resource group. Additional steps are required to configure Apache as a scalable service. The leading text “For scalable services only” in the following procedure identifies these steps. If you are not configuring Apache as a scalable service, skip the steps marked “For scalable services only.”

Setting Sun Cluster HA for Apache Extension Properties

The sections that follow contain instructions for registering and configuring Sun Cluster HA for Apache resources. For information about the extension properties, see [Appendix A](#). The Tunable entry indicates when you can update a property.

See Appendix A, “Standard Properties,” in *Sun Cluster Data Services Planning and Administration Guide for Solaris OS* for details on all of the Sun Cluster properties.

To set an extension property of a resource, include the following option in the `scrgadm (1M)` command that creates or modifies the resource:

`-x property=value`

`-x property`

Identifies the extension property that you are setting

`value`

Specifies the value to which you are setting the extension property

You can also use the procedures in Chapter 2, “Administering Data Service Resources,” in *Sun Cluster Data Services Planning and Administration Guide for Solaris OS* to configure resources after the resources are created.

Monitoring Arbitrary URIs

Set the `Monitor Uri List` extension property if you want the web server fault monitor to probe an arbitrary list of applications (URIs) served by the web server. This extension property provides extended probing functionality and is useful if you are layering services in addition to your web server. The `Monitor Uri List` extension property is not supported with a secure Sun Cluster HA for Apache instance. If you do not set the `Monitor Uri List` extension property, the fault monitor will perform the basic probing. See “[Tuning the Sun Cluster HA for Apache Fault Monitor](#)” on page 35 for details. The following examples show how to set the `Monitor Uri List` extension property when you add the Sun Cluster HA for Apache instance to your configuration.

Example— Setting `Monitor Uri List` for Scalable Sun Cluster HA for Apache Instance

(Add an insecure Apache instance with default load balancing.)

```
# scrgadm -a -j apache-insecure-1 -g resource-group-1 \  
-t SUNW.apache -y Network_resources_used=schost-1, ... \  
-y Scalable=True -y Port_list=8000/tcp -x Bin_dir=/opt/apache/bin \  

```

```
-x Monitor Uri_list=http://schost-1:8000/servlet/monitor
```

Example— Setting Monitor Uri List for Failover Sun Cluster HA for ApacheInstance

(Add an insecure Apache application resource instance.)

```
# scrgadm -a -j apache-insecure-1 -g resource-group-1 \  
-t SUNW.apache -y Network_resources_used=schost-1 \  
-y Scalable=False -y Port_list=80/tcp \  
-x Bin_dir=/opt/apache/bin \  
-x Monitor Uri_list=http://schost-1:80/servlet/monitor
```

▼ How to Register and Configure Sun Cluster HA for Apache

Note – Run this procedure on any cluster member.

Steps 1. Become superuser on a cluster member.

2. Register the resource type for the data service.

```
# scrgadm -a -t SUNW.apache
```

-a

Adds the data service resource type.

```
-t SUNW.apache
```

Specifies the predefined resource type name for your data service.

3. Create a failover resource group to hold the network and application resources.

This resource group is required for both failover and scalable services. For failover services, the resource group contains both network and failover application resources. For scalable services, the resource group contains network resources only. A dependency is created between this group and the resource group that contains the application resources.

Optionally, you can select the set of nodes on which the data service can run with the `-h` option.

```
# scrgadm -a -g resource-group [-h nodelist]
```

-a

Adds a new configuration.

```
-g resource-group
```

Specifies the name of the failover resource group to add. This name can be your choice but must be unique for the resource groups within the cluster.

`[-h nodelist]`

An optional comma-separated list of physical node names or IDs that identify potential masters. The order specified here determines the order in which the nodes are considered as primary during failover.

Note – Use `-h` to specify the order of the node list. If all of the nodes that are in the cluster are potential masters, you do not need to use the `-h` option.

4. Verify that all of the network addresses that you use have been added to your name service database.

You should have performed this verification during your initial Sun Cluster installation. See the planning chapter in the *Sun Cluster Software Installation Guide for Solaris OS* for details.

Note – To avoid failures because of name service lookup, verify that all of the network addresses are present in the `/etc/inet/hosts` file on all of the cluster nodes. Configure name service mapping in the `/etc/nsswitch.conf` file on the servers to first check the local files prior to accessing NIS, NIS+, or DNS.

5. Add a network resource (logical hostname or shared address) to the failover resource group that you created in Step 3.

```
# scrgadm -a {-S | -L} -g resource-group \  
-l hostname, ... [-j resource] \  
[-x auxnodelist] [-n netiflist]
```

`-S | -L`

The `-S` option specifies shared address resources. The `-L` option specifies logical hostname resources.

`-l hostname, ...`

Specifies a comma-separated list of network resources to add. You can use the `-j` option to specify a name for the resources. If you do not do so, the network resources have the name of the first entry on the list.

`-g resource-group`

Specifies the name of the failover resource group that you created in [Step 3](#).

`-j resource`

Specifies a resource name. If you do not supply your choice for a resource name, the name of the network resource defaults to the first name that is specified after the `-l` option.

`-x auxnodelist`

Specifies a comma-separated list of physical node names or node IDs that identify cluster nodes that can host the shared address but never serve as

primary in the case of failover. These nodes are mutually exclusive with the nodes identified in *nodelist* for the resource group, if specified.

-n *netiflist*

Specifies an optional, comma-separated list that identifies the IP Networking Multipathing groups that are on each node. Each element in *netiflist* must be in the form of *netif@node*. *netif* can be given as an IP Networking Multipathing group name, such as *sc_ipmp0*. The node can be identified by the node name or node ID, such as *sc_ipmp0@1* or *sc_ipmp@phys-schost-1*.

Note – Sun Cluster does not currently support using the adapter name for *netif*.

6. For scalable services only – Create a scalable resource group to run on all of the desired cluster nodes.

If you run Sun Cluster HA for Apache as a failover data service, proceed to [Step 8](#). Create a resource group to hold a data service application resource. You must specify the maximum and desired number of primary nodes.

Note – If only a subset of nodes can be primaries for this resource group, you must use the *-h* option to specify the names of these potential primaries when you create the resource group.

You must also specify any dependency between this resource group and the failover resource group that you created in [Step 3](#). This dependency ensures that when failover occurs, if the two resource groups are being brought online on the same node, the Resource Group Manager (RGM) starts up the network resource before any data services that depend on the network resource.

```
# scrgadm -a -g resource-group \  
-y Maximum primaries=m -y Desired primaries=n \  
-y RG_dependencies=resource-group \  
[-h nodelist]
```

-g *resource-group*

Specifies the name of the scalable service resource group to add.

-y *Maximum primaries=m*

Specifies the maximum number of active primary nodes allowed for this resource group. If you do not assign a value to this property, the default is 1.

-y *Desired primaries=n*

Specifies the desired number of active primary nodes allowed for this resource group. If you do not assign a value to this property, the default is 1.

- y *RG_dependencies= resource-group*
Identifies the resource group that contains the shared address resource on which the resource group being created depends, that is, the name of the failover resource group that you created in [Step 3](#).
- h *nodelist*
An optional list of nodes that can be primaries for this resource group. You only need to specify this list if some nodes cannot act as primaries for this resource group.

7. For scalable services only – Create an application resource in the scalable resource group.

If you run Sun Cluster HA for Apache as a failover data service, proceed to [Step 8](#).

```
# scrgadm -a -j resource -g resource-group \  
-t resource-type -y Network_resources_used=network-resource, ... \  
-y Port_list=port-number/protocol[,...] -y Scalable=True \  
-x Bin_dir=bin-directory, ...
```

- j *resource*
Specifies your choice for the name of the resource to add.
- g *resource-group*
Specifies the name of the scalable resource group into which the resources are to be placed.
- t *resource-type*
Specifies the type of the resource to add.
- y *Network_resources_used= network-resource, ...*
Specifies a comma-separated list of network resource names that identify the shared addresses that the data service uses.
- y *Port_list=port-number/protocol, ...*
Specifies a comma-separated list of port numbers and protocol to be used, for example, 80/tcp, 81/tcp.
- y *Scalable=*
Specifies a required parameter for scalable services. This parameter must be set to True.
- x *Bin_dir=bin-directory*
Specifies the location where the Apache binaries—in particular, `apachectl`—are installed. Sun Cluster HA for Apache requires this extension property.

Note – Optionally, you can set additional extension properties that belong to the Apache data service to override their default values. See [Appendix A](#) for a list of extension properties.

8. For failover services only – Create an application resource in the failover resource group.

Perform this step only if you run Sun Cluster HA for Apache as a failover data service. If you run Sun Cluster HA for Apache as a scalable data service, you should have performed [Step 6](#) and [Step 7](#) and should now proceed to [Step 10](#).

```
# scrgadm -a -j resource -g resource-group \  
-t resource-type -y Network_resources_used=network-resource, ... \  
-y Port_list=port-number/protocol[,...] -y Scalable=False \  
-x Bin_dir=bin-directory
```

-j *resource*

Specifies your choice for the name of the resource to add.

-g *resource-group*

Specifies the name of the resource group into which the resources are to be placed, created in [Step 3](#).

-t *resource-type*

Specifies the type of the resource to add.

-y *Network_resources_used= network-resource, ...*

Specifies a comma-separated list of network resources that identify the shared addresses that the data service uses.

-y *Port_list=port-number/protocol, ...*

Specifies a comma-separated list of port numbers and protocol to be used, for example, *80/tcp, 81/tcp*.

-y *Scalable=*

This property is required for scalable services only. Here the value is set to *False* or can be omitted.

-x *Bin_dir=bin-directory*

Specifies the location where the Apache binaries—in particular, *apachectl*—are installed. Sun Cluster HA for Apache requires this extension property.

9. Bring the failover resource group online.

```
# scswitch -Z -g resource-group
```

-Z

Enables the shared address resource and fault monitoring, switches the resource group into a MANAGED state, and brings the resource group online.

-g *resource-group*

Specifies the name of the failover resource group.

10. For scalable services only – Bring the scalable resource group online.

```
# scswitch -Z -g resource-group
```


- Z
Enables the resource and monitor, moves the resource group to the MANAGED state, and brings the resource group online.
- g *resource-group*
Specifies the name of the scalable resource group.

Example 1 Registering Scalable Sun Cluster HA for Apache

For scalable services, you create the following resource groups.

- A failover resource group that contains the network resources
- A scalable resource group that contains the application resources

The following example shows how to register a scalable Apache service on a two-node cluster.

Cluster Information

Node names: *phys-schost-1, phys-schost-2*

Shared address: *schost-1*

Resource groups: *resource-group-1* (for shared addresses),
resource-group-2 (for scalable Apache application resources)

Resources: *schost-1* (shared address), *apache-1* (Apache application resource)

(Add a failover resource group to contain shared addresses.)

```
# scrgadm -a -g resource-group-1
```

(Add the shared address resource to the failover resource group.)

```
# scrgadm -a -S -g resource-group-1 -l schost-1
```

(Register the Apache resource type.)

```
# scrgadm -a -t SUNW.apache
```

(Add a scalable resource group.)

```
# scrgadm -a -g resource-group-2 -y Maximum primaries=2 \  
-y Desired primaries=2 -y RG_dependencies=resource-group-1
```

(Add Apache application resources to the scalable resource group.)

```
# scrgadm -a -j apache-1 -g resource-group-2 \  
-t SUNW.apache -y Network_resources_used=schost-1 \  
-y Scalable=True -y Port_list=80/tcp \  
-x Bin_dir=/opt/apache/bin
```

(Bring the failover resource group online.)

```
# scswitch -Z -g resource-group-1
```

(Bring the scalable resource group online on both nodes.)

```
# scswitch -Z -g resource-group-2
```

Example 2 Registering Failover Sun Cluster HA for Apache

The following example shows how to register a failover Apache service on a two-node cluster.

Cluster Information

Node names: *phys-schost-1, phys-schost-2*

Logical hostname: *schost-1*

Resource group: *resource-group-1* (for all of the resources)

Resources: *schost-1* (logical hostname),
apache-1 (Apache application resource)

(Add a failover resource group to contain all of the resources.)

```
# scrgadm -a -g resource-group-1
```

(Add the logical hostname resource to the failover resource group.)

```
# scrgadm -a -L -g resource-group-1 -l schost-1
```

(Register the Apache resource type.)

```
# scrgadm -a -t SUNW.apache
```

(Add Apache application resources to the failover resource group.)

```
# scrgadm -a -j apache-1 -g resource-group-1 \  
-t SUNW.apache -y Network_resources_used=schost-1 \  
-y Scalable=False -y Port_list=80/tcp \  
-x Bin_dir=/opt/apache/bin
```

(Bring the failover resource group online.)

```
# scswitch -Z -g resource-group-1
```

How to Configure SUNW.HAStoragePlus Resource Type

The SUNW.HAStoragePlus resource type was introduced in Sun Cluster 3.0 5/02. This new resource type performs the same functions as SUNW.HAStorage, and synchronizes actions between HA storage and the data service.

SUNW.HAStoragePlus also has an additional feature to make a local file system highly available.

See the SUNW.HAStoragePlus(5) man page and “Relationship Between Resource Groups and Disk Device Groups” in *Sun Cluster Data Services Planning and Administration Guide for Solaris OS* for background information. See “Synchronizing the Startups Between Resource Groups and Disk Device Groups” in *Sun Cluster Data Services Planning and Administration Guide for Solaris OS* for the procedure. (If you are using a Sun Cluster 3.0 version prior to 5/02, you must set up SUNW.HAStorage instead of SUNW.HAStoragePlus. See “Synchronizing the Startups Between Resource Groups and Disk Device Groups” in *Sun Cluster Data Services Planning and Administration Guide for Solaris OS* for the procedure.)

How to Verify Data Service Installation and Configuration

After you configure Sun Cluster HA for Apache, verify that you can open a web page with the network resources (logical hostnames or shared addresses) and port number from a web browser. Perform a switchover with the `scswitch(1M)` command to verify that the service continues to run on a secondary node and can be switched back to the original primary.

Tuning the Sun Cluster HA for Apache Fault Monitor

The Sun Cluster HA for Apache fault monitor is contained in a resource whose resource type is `SUNW.apache`.

System properties and extension properties of the resource control the behavior of the fault monitor. The default values of these properties determine the preset behavior of the fault monitor. The preset behavior should be suitable for most Sun Cluster installations. Therefore, you should tune the Sun Cluster HA for Apache fault monitor *only* if you need to modify this preset behavior.

Tuning the Sun Cluster HA for Apache fault monitor involves the following tasks:

- Setting the interval between fault monitor probes
- Setting the timeout for fault monitor probes
- Defining the criteria for persistent faults
- Specifying the failover behavior of a resource

Information about the Sun Cluster HA for Apache fault monitor that you need to perform these tasks is provided in the subsections that follow.

Tune the Sun Cluster HA for Apache fault monitor when you register and configure Sun Cluster HA for Apache. For more information, see [“Registering and Configuring Sun Cluster HA for Apache”](#) on page 26.

For detailed information, see *“Tuning Fault Monitors for Sun Cluster Data Services”* in *Sun Cluster Data Services Planning and Administration Guide for Solaris OS*.

Operations by the Sun Cluster HA for Apache Fault Monitor

The Sun Cluster HA for Apache probe sends a request to the server to query the health of the Apache server.

Operations by the Fault Monitor Before a Probe

Before querying the Apache server, the probe checks to confirm that network resources are configured for this Apache resource. If no network resources are configured, an error message (No network resources found for resource) is logged, and the probe exits with failure.

Operations for a Nonsecure Web Server

For a *nonsecure* web server, the probe connects to the Apache server and performs an HTTP 1.0 HEAD check by sending the HTTP request and receiving a response. In turn, the probe connects to the Apache server on each IP address/port combination.

The result of this query can be either a failure or a success. If the probe successfully receives a reply from the Apache server, the probe returns to its infinite loop and continues the next cycle of probing and sleeping.

The query can fail for various reasons, such as heavy network traffic, heavy system load, and misconfiguration. Misconfiguration can occur if you did not configure the Apache server to listen on all of the IP address/port combinations that are being probed. The Apache server should service every port for every IP address that is specified for this resource.

The following probe failures are considered as complete failures.

- Failure to connect to the server, as the following error message flags, with %s indicating the hostname and %d the port number.

```
Failed to connect to %s port %d %s
```
- Running out of time (exceeding the resource property timeout `Probe_timeout`) after trying to connect to the server.
- Failure to successfully send the probe string to the server, as the following error message flags, with the first %s indicating the hostname, %d the port number, and the second %s indicating further details about the error.

```
Failed to communicate with server %s port %d: %s
```

When the monitor accumulates two partial failures within the resource property interval `Retry_interval`, it counts them as one complete failure.

The following probe failures are considered as partial failures:

- Running out of time (exceeding the resource property timeout `Probe_timeout`) while trying to read the reply from the server to the probe's query.
- Failing to read data from the server for other reasons, as the following error message flags, with the first %s indicating the hostname and %d the port number. The second %s indicates further details about the error.

```
Failed to communicate with server %s port %d: %s
```

Operations for a Monitored URI List

If you have configured URIs in the `Monitor_Uri_List` extension property, then the probe connects to the Sun Cluster HA for Apache server and performs an HTTP 1.1 GET check by sending a HTTP request and receiving a response to each of the URIs in `Monitor_Uri_List`. If the HTTP server return code is 500 (Internal Server Error) or if the connect fails, the probe will take action.

The result of the HTTP requests is either failure or success. If all of the requests successfully receive a reply from the Sun Cluster HA for Apache server, the probe returns and continues the next cycle of probing and sleeping.

Heavy network traffic, heavy system load, and misconfiguration can cause the HTTP GET probe to fail. Misconfiguration of the `Monitor_Uri_List` property can cause a failure if a URI in the `Monitor_Uri_List` includes an incorrect port or hostname. For example, if the web server instance is listening on logical host `schost-1` and the URI was specified as `http://schost-2/servlet/monitor`, the probe will try to contact `schost-2` to request `/servlet/monitor`.

Operations for a Secure Web Server

For a *secure* web server, the probe connects to each IP address and port combination. If this connection attempt succeeds, the probe disconnects and returns with a success status. No further checks are performed.

Actions in Response to Faults

Based on the history of failures, a failure can cause either a local restart or a failover of the data service. For detailed information, see “Tuning Fault Monitors for Sun Cluster Data Services” in *Sun Cluster Data Services Planning and Administration Guide for Solaris OS*.

Upgrading the SUNW.apache Resource Type

Upgrade the `SUNW.apache` resource type if the following conditions apply:

- You are upgrading from an earlier version of the Sun Cluster HA for Apache data service.
- You need to use the new features of this data service.

For general instructions that explain how to upgrade a resource type, see “Upgrading a Resource Type” in *Sun Cluster Data Services Planning and Administration Guide for Solaris OS*. The information that you require to complete the upgrade of the `SUNW.apache` resource type is provided in the subsections that follow.

Information for Registering the New Resource Type Version

The relationship between a resource type version and the release of Sun Cluster data services is shown in the following table. The release of Sun Cluster data services indicates the release in which the version of the resource type was introduced.

Resource Type Version	Sun ClusterData Services Release
1	1.0
3.1	3.1 5/03
4	3.1 10/03

To determine the version of the resource type that is registered, use one command from the following list:

- `scrgadm -p`
- `scrgadm -pv`

The resource type registration (RTR) file for this resource type is `/opt/SUNWscapc/etc/SUNW.apache`.

Information for Migrating Existing Instances of the Resource Type

The information that you require to edit each instance of the `SUNW.apache` resource type is as follows:

- You can perform the migration at any time.
- If you need to use the new features of the Sun Cluster HA for Apache data service, the required value of the `Type_version` property is 4.
- If you need to monitor deployed applications, set the `Monitor Uri List` extension property to a single URI or a list of URIs to specify the locations of the applications that are to be probed.

The following example shows a command for modifying an instance of the `SUNW.apache` resource type.

EXAMPLE 3 Migrating Instances of the SUNW.apache Resource Type

```
# scrgadm -c -j apache-rs -y Type_version=4 \  
-x Monitor Uri List=http://schost-1/test.html
```

This command modifies the SUNW.apache resource named apache-rs as follows:

- The Type_version property of this resource is set to 4.
- The Fault Monitor probe will monitor the URI http://schost-1/test.html.

Sun Cluster HA for Apache Extension Properties

This section describes the extension properties for the resource type `SUNW.apache`. This resource type represents the Apache application in a Sun Cluster configuration.

For details about system-defined properties, see the `r_properties(5)` man page and the `rg_properties(5)` man page.

The extension properties of the `SUNW.apache` resource type are as follows:

`Bin_dir`

The path to the Apache binaries, in particular, `apachectl`. Sun Cluster HA for Apache requires this extension property.

Data type	String
Default	No default defined
Range	Not applicable
Tunable	At creation

`Monitor_retry_count`

The number of times that the process monitor facility (PMF) restarts the fault monitor during the time window that the `Monitor_retry_interval` property specifies. This property refers to restarts of the fault monitor itself rather than to the resource. The system-defined properties `Retry_interval` and `Retry_count` control restarting of the resource.

Data type	Integer
Default	4
Range	0 - 2,147,483,641
	-1 indicates an infinite number of retry attempts.
Tunable	At any time

Monitor_retry_interval

The time (in minutes) over which failures of the fault monitor are counted. If the number of times that the fault monitor fails exceeds the value that is specified in the extension property Monitor_retry_count within this period, the PMF does not restart the fault monitor.

Data type	Integer
Default	2
Range	0 – 2,147,483,641 -1 indicates an infinite retry interval.
Tunable	At any time

Monitor Uri List

A single URI or a list of URIs that can be used by the fault monitor to probe any deployed applications on the Sun Cluster HA for Apache Web Server. Probe deployed applications by setting the property to one or more URIs that are serviced by applications deployed on the Sun Cluster HA for Apache Web Server.

Introduced in release 3.1 10/03.

Data type	String
Default	Null
Range	Not applicable
Tunable	At any time

Probe_timeout

The timeout value (in seconds) that the fault monitor uses to probe an Apache instance.

Data type	Integer
Default	90
Range	0 – 2,147,483,641
Tunable	At any time

Index

A

Apache

See also Sun Cluster HA for Apache

installation

installing non-secure webserver, 17

installing secure webserver, 20

installing software, 16

C

C locale, 25

commands, node information, 9

configuring, Sun Cluster HA for Apache, 28-34

D

directories, /var/sadm/install/logs, 25

E

extension properties, SUNW.apache resource
type, 41-42

F

fault monitor, Sun Cluster HA for Apache, 35
files

installation logs, 25

RTR, 38

G

global zone, 24

H

httpd.conf file, configuring, 11

I

installing

Apache, 16

Sun Cluster HA for Apache

by using scinstall utility, 25-26

by using Web Start program, 24-25

log files created, 25

L

local zones, 24

locales, 25

log files, installation, 25

M

Monitor Uri List, 15, 38

N

non-secure webserver, installing Apache webserver, 17

P

properties

See also extension properties

Monitor Uri List, 38

Type_version, 38

prtcnf -v command, 9

prtdiag -v command, 9

psrinfo -v command, 9

R

registering, Sun Cluster HA for Apache, 28-34

resource type registration (RTR) file, 38

restrictions, zones, 24

RTR (resource type registration) file, 38

S

scinstall -pv command, 9

scinstall utility, 25-26

secure webserver, installing Apache

webserver, 20

showrev -p command, 9

Sun Cluster HA for Apache

See also Apache

BindAddress directive, 11

configuration

planning, 11

DocumentRoot directive, 11

fault monitor, 35

httpd.conf file, 11

installation

planning, 11

verifying, 35

installing

by using scinstall utility, 25-26

by using Web Start program, 24-25

lock file, 11

multiple instances, 11

Port directive, 11

Sun Cluster HA for Apache (Continued)

registering and configuring, 28-34

resource type versions, 38

ScriptAlias directive, 11

ServerName directive, 11

ServerType directive, 11

SUNW.HAStoragePlus resource type, 34

task map, 16

SUNW.apache resource type, extension

properties, 41-42

SUNW.HAStoragePlus resource type, Sun

Cluster HA for Apache, 34

system properties, effect on fault monitors, 35

T

task map, Sun Cluster HA for Apache, 16

training, 8

Type_version property, 38

V

/var/sadm/install/logs directory, 25

verifying, Sun Cluster HA for Apache

installation, 35

versions, resource types, 38

W

Web Start program, 24-25

Z

zones, 24