HP Domain ServiceControl Concepts and Operation Guide

Edition 3

J1592-90007
HP 9000 Networking
E1298

Printed in: U.S.A.

Legal Notices

The information in this document is subject to change without notice.

Hewlett-Packard makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Warranty. A copy of the specific warranty terms applicable to your Hewlett- Packard product and replacement parts can be obtained from your local Sales and Service Office.

Restricted Rights Legend. Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c) (1) and (c) (2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

HEWLETT-PACKARD COMPANY 3000 Hanover Street Palo Alto, California 94304 U.S.A.

Use of this manual and flexible disk(s) or tape cartridge(s) supplied for this pack is restricted to this product only. Additional copies of the programs may be made for security and back-up purposes only. Resale of the programs in their present form or with alterations, is expressly prohibited.

Printing History

The manual printing date and part number indicate its current edition. The printing date will change when a new edition is printed. Minor changes may be made at reprint without changing the printing date. The manual part number will change when extensive changes are made.

Manual updates may be issued between editions to correct errors or document product changes. To ensure that you receive the updated or new editions, you should subscribe to the appropriate product support service. See your HP sales representative for details.

First Edition: June 1998 (HP-UX Release 10.20 and 11.0)

Second Edition: August 1998 (HP-UX Release 10.20 and 11.0)

Third Edition: December 1998 (HP-UX Release 10.20 and 11.0)

Contents

Contents

Contents

Contents

1 HP Domain ServiceControl

HP Domain ServiceControl (HP DSC) is a web-based solution that provides the quality of service needed to operate and maintain your web applications.

HP DSC is made up of HP AdmissionControl (HP AC), HP Domain Enterprise Server Management System (HP DESMS), and HP LocalDirector Controller (HP LDC):

- HP AC - HP AdmissionControl helps to improve the quality of service provided by your web site. It controls the number and length of sessions admitted to the web server, to ensure that the system does not become overloaded. HP AC can be installed and configured for either Netscape or the Apache web server.
- HP DESMS - HP Domain Enterprise Server Management System configures, administers, operates, and monitors your system, including HP AC for Netscape and HP LDC.
- HP LDC - HP LocalDirector Controller automatically generates the information needed by Cisco's LocalDirector to distribute load and manage TCP/IP connections.

Installation Requirements

The following is the list of requirements to install all the components of HP Domain ServiceControl (HP DSC). If you are installing a subset of the components, go to the appropriate chapter(s) in this manual for more information. Information about HP Domain Enterprise Server Management System can be found in the *Getting Started with HP Domain Software* manual.

Hardware

- HP 9000 computer system
- 32 MB of memory
- CD-ROM drive to load the software

Software

- HP-UX 10.20 or 11.0
- HP DESMS
- Netscape Enterprise or FastTrack Server version 3.0 or later (HP AC for Netscape), or Apache Server 1.3.1 or later (HP AC for Apache)
- Cisco LocalDirector version 2.1 or later

Disk Space (Estimated)

- 80 MB

Installing HP Domain ServiceControl

To install the HP DSC software, run `swinstall` (as root) and install the bundle J1592AA.

Configuring HP Domain ServiceControl

Each component of HP DSC needs to be configured individually. Go to the following areas for more information about configuration:

- HP AC for Netscape - See “Configuring HP AdmissionControl for Netscape” on page 17.
- HP AC for Apache - See “Configuring HP AdmissionControl for Apache” on page 34.
- HP DESMS - See the manual *Getting Started with HP Domain Software*.
- HP LDC - See Chapter 3, “HP LocalDirector Controller,” on page 47.

Also refer to the *HP Domain ServiceControl Release Note* for other important information.

2 HP AdmissionControl

What is HP AdmissionControl?

HP Admission Control (HP AC) is a software plug-in (module), which runs inside an HTTP server. The HTTP servers currently supported are Netscape Enterprise, Netscape Fasttrack and Apache. HP AC can be configured to make certain decisions based on changing system conditions. For example, it can admit, reject, or defer new sessions based on system load, or to end active sessions based on the interval between requests and/or the length of a session. In addition, HP AC maintains several operation and performance statistics which can be viewed in a Web client window.

Viewing the Server Statistics

The HP AC maintains a series of statistics, which can be inspected on-line by pointing your web client (browser) to the following URL: `/hpac/about.hpac` (or just `/hpac/`). From the `about.hpac` page you can access either the `Statistics` table, or the `Isolate` table, by selecting the appropriate link. You can also view an explanation of what each statistic means, by selecting the field name.

What is a Session?

A session is an HTTP request or sequence of HTTP requests made to a web server by a single user. A simple session might consist of a request for a server's home page. If that page contains images, the session would also consist of requests for each image.

A more complicated and longer session might consist of a request for a server's home page, following a link to a catalog, browsing the catalog and adding items to a shopping cart, and finally supplying payment information to complete a purchase.

When Does a Web Server Become Overloaded?

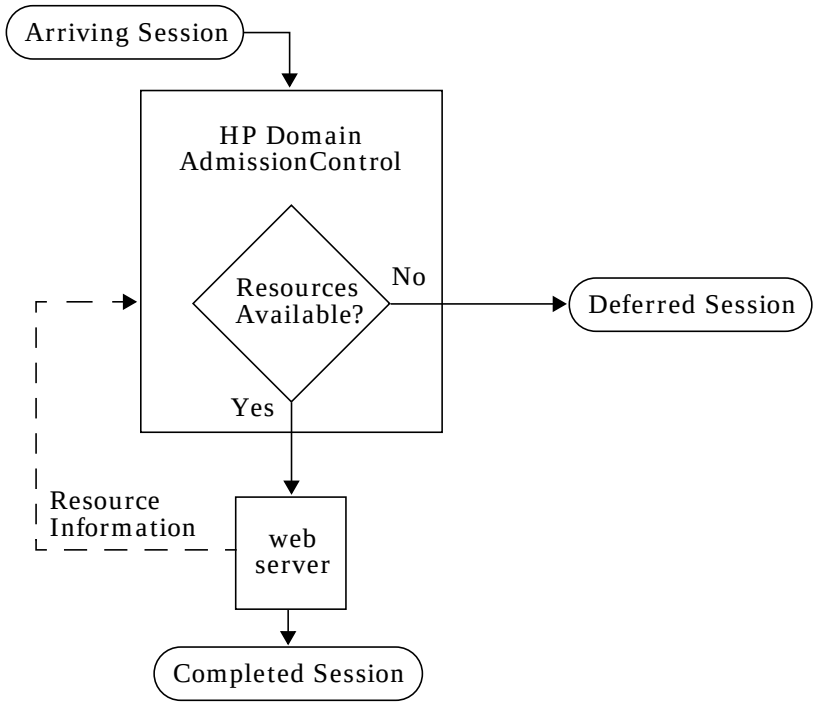
A web server becomes overloaded when there are too many requests for the server to fulfill; the server runs out of resources. Requests may be delayed or dropped. For example, a user involved in a long session may experience poor performance or may have to reload a page more than once for it to display.

How Does HP AdmissionControl Work?

HP AC monitors the resources and the number of arriving sessions on the web server. Based on available resources and how HP AC is configured, it will accept, defer, reject or redirect a session. HP AC makes sure the web server does not become overloaded by deferring, rejecting or redirecting any new sessions for which it does not have resources. It also allows an admitted session to be completed.

When the web server's resources are available, HP AC allows the session to begin and will fulfill all requests made during this session. HP AC monitors the time between requests as well as the length of the session. If one of these variables exceeds the thresholds configured in HP AC, the session is terminated. Otherwise, all requests are fulfilled until the session is completed.

When the web server's resources are not available, HP AC will defer, reject or redirect the session. The web administrator can choose to redirect the request to another URL, or serve a page with an error message or some helpful information.



HP AdmissionControl for Netscape

HP AdmissionControl (HP AC) for Netscape is part of the HP Domain ServiceControl (HP DSC) product. You do not need to load the entire HP DSC product if you only want to use HP AC for Netscape.

Installing HP AdmissionControl for Netscape

Installation Requirements

Verify that the following hardware, software, and disk space is available for the HPAdmissionControl for Netscape installation.

Hardware

- HP 9000 computer system
- 32 MB of memory
- CD-ROM drive to load the software

Software

- HP-UX 10.20 or 11.0
- Netscape FastTrack Server version 3.0 or later OR
  Netscape Enterprise Server version 3.0 or later

Disk Space (Estimated)

- 38 MB

Installing the Software

To install HP AC for Netscape, run `swinstall` (as root), double-click on the bundle J1592AA to view the software, and select the HP AC software.

Configuring HP AdmissionControl for Netscape

If Netscape Enterprise Server version 3.0 or later was already installed on your system in the `/opt/ns-enterprise3` directory before you installed HP Domain ServiceControl, HP AC for Netscape is automatically configured and enabled on your system.

If Netscape FastTrack Server version 3.0 or later was already installed on your system in the `/opt/ns-ftrack` directory before you installed HP Domain ServiceControl, HP AC is automatically configured and enabled on your system.

If both servers were already installed on your system before you installed HP Domain ServiceControl, HP AC is automatically configured and enabled for your Netscape Enterprise Server.

If neither server was installed before you installed HP Domain ServiceControl, you must first install the Netscape Enterprise Server version 3.0 or later or Netscape FastTrack Server version 3.0 or later and then run the setup script (see the next section for information about running the setup script).

If you installed either server after installing HP Domain ServiceControl, you must run the setup script (see the next section for information about running the setup script).

If you installed either server in another server root directory other than `/opt/ns-enterprise3` (for the Netscape Enterprise Server) or `/opt/ns-ftrack` (for the Netscape FastTrack Server), you must run the setup script (see the next section for information about running the setup script).

Running the Setup Script

You should only run the setup script if you installed the Netscape Enterprise Server or Netscape FastTrack Server after installing HP Domain ServiceControl or if the server root directory is something other than `/opt/ns-enterprise3` (for the Netscape Enterprise Server) or `/opt/ns-ftrack` (for the Netscape FastTrack Server).

To run the setup script, type:

`/opt/hpac/setup`

At the `Root pathname of Netscape server` prompt, enter the Netscape Server root directory.

The setup script will automatically configure and enable HP AC.

Default values set for all applicable configuration parameters are listed in "HP AdmissionControl Configurable Parameters for Netscape" on page 60.

Setting the HP AC Configurable Parameters for Netscape

You can edit the configuration parameters in three different ways:

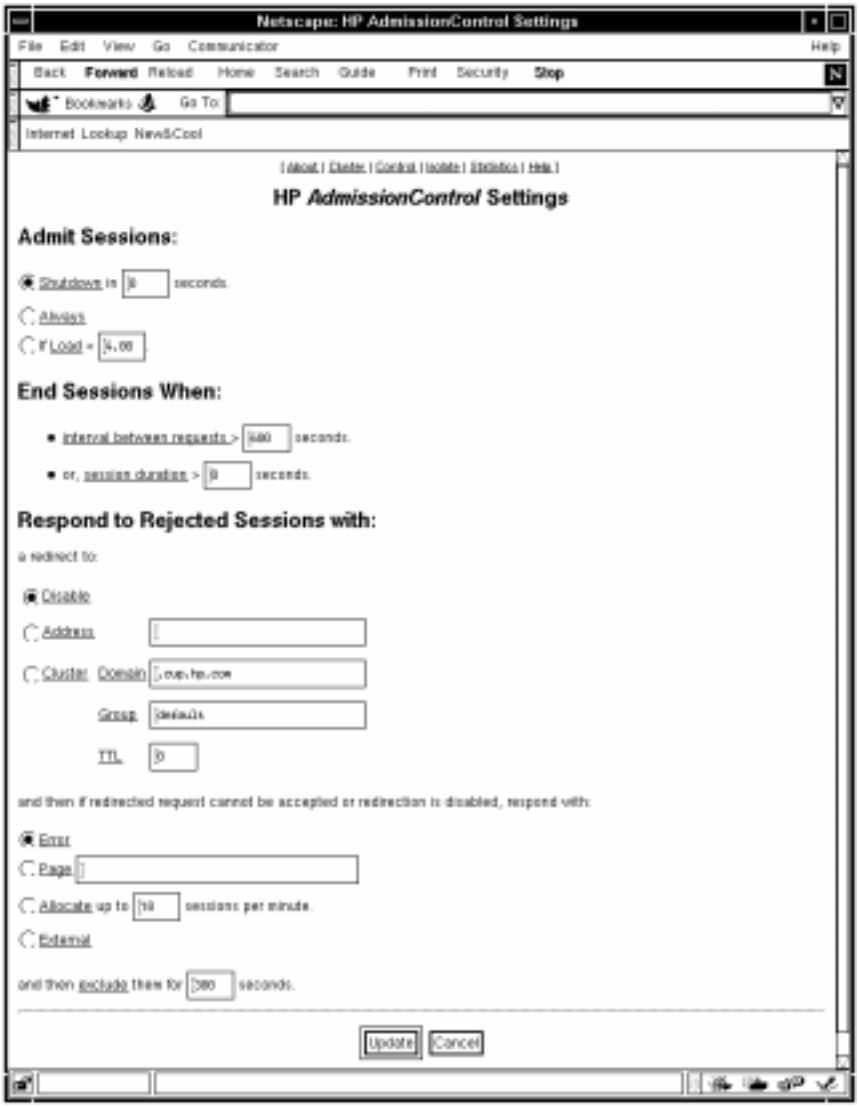
- You can access the `HP AdmissionControl Settings` administration web page at the URL `http://`*system_name*`/hpac`. Your Netscape Server must be running to access this page. Use the system's root user and password to access this page.
- You can edit the configuration file `/opt/ns-`*server_name*`/`*server_id*`/config/hpac/config.ac`

  Refer to "HP AdmissionControl Configurable Parameters for Netscape" on page 60 for a list of the available configurable parameters for the Netscape server.
- You can use the HP DESMS interface to access the `HP AdmissionControl Settings` administration web page (HP AC is located under Server Control). Your Netscape Server and HP administration server must be running.

  To start the HP administration server, type **`/opt/hpwebsuite/start-admin`** and go to the URL `http://`*system_name*`:8181/`. The default user ID is hpadmin; and the default password is hpadmin.

  To access HP AC for Netscape, you must enter the system's root user and password.

The following is an example of the “HP AdmissionControl Settings” page:



The following sections describe the parameters that can be set using the `HP AdmissionControl Settings` administration web page. See “HP AdmissionControl Configurable Parameters for Netscape” on page 60 for a list of the available configurable parameters for the Netscape server and a list of defaults already configured in `config.ac`.

Admit Sessions. For the default value, the load threshold is set to 2.

Table 2-1 HP AC for Netscape Configurable Parameters: Admit Sessions

Parameter	Description
Shutdown	After the specified number of seconds, do not admit any new sessions and reject all remaining sessions.
Always	Disable HP AC and admit all sessions to the web server. If you are permanently disabling HP AC, you should remove HP AC from you system (see “Removing HP AdmissionControl for Netscape” on page 25 for more information).
Load	If the load is less than this specified amount, admit the session. The load threshold works best when a web application is processor-intensive.

To calculate the load threshold, do the following:

1. Run the `top` command. Note the first listed “Load averages” and the percentage listed under “IDLE” of “Cpu states.”

Sample Output from the top Command

```
System: web_server           Wed Apr 22 10:41:59 1998
Load averages: 1.45, 1.46, 1.78
149 processes: 145 sleeping, 3 running, 1 stopped
Cpu states:
LOAD  USER  NICE  SYS  IDLE BLOCK  SWAIT   INTR  SSYS
1.45 100.0%  0.0% 0.0%  0.0%  0.0%  0.0%   0.0%  0.0%
```

2. If IDLE is greater than zero, then set the threshold to (100 - IDLE)/100.

   If IDLE equals zero, then set the threshold to the first listed load average.

Using the above sample output, you would set the load threshold to 1.45.

Run `top` when performance is poor and acceptable to determine an acceptable load level.

End Sessions. For the default, the interval between requests is set to 600 seconds (10 minutes) and the session duration is disabled.

Table 2-2 HP AC for Netscape Configurable Parameters: End Sessions

Parameter	Description
Interval between requests	The amount of time, in seconds, between requests within the session. If the time between requests exceeds the specified threshold, the session is ended.
Session duration	The amount of time of the session. If the session exceeds the specified threshold, the session is ended. Set this parameter to zero to disable this threshold.

Respond to Rejected Sessions. Rejected sessions can either be redirected or served a web page containing a standard error message or other information.

If redirection is disabled or the redirect request is not accepted, a web page containing a standard error message or other information is returned.

The default is to disable redirection and serve an error page to a rejected session.

Table 2-3 HP AC for Netscape Configurable Parameters: Redirect Rejected Sessions

Parameter	Description
Disable	Do not redirect the rejected session. Instead, return a web page with an error message or other information.
Address	Redirect the rejected session to a load balancing system (such as a cluster manager), to another web server, or to another system set up to specifically handle rejected sessions. Specify the full domain name or IP address.
Cluster	Redirect the rejected session to a randomly selected member of a cluster.
Domain	Redirect the rejected session to the domain to which the systems in the cluster belong. For example, if the cluster consists of the two systems `ww1.sales.acme.com` and `ww2.sales.acme.com`, specify the domain as `.sales.acme.com`. Note the leading dot. The domain specifies the scope over which the client-side cookies can be shared (HP AC uses client-side cookies to encode session information).
Group	The cluster group to which this system belongs.
TTL	Time to Live. The number of redirections allowed before rejecting the session. Add one to the TTL parameter to get the number of redirects. For example, setting the TTL to 0 allows one redirection. Setting the TTL to 1 allows two redirections. It is recommended that the TTL be set to a value no larger than 2.

When redirection is disabled, the following types of web pages can be served:

Table 2-4 HP AC for Netscape Configurable Parameters: Respond to Rejected Sessions

Parameter	Description
Error	The “Server Temporarily Unavailable” error message is served to rejected requests. This is the easiest but least informative way to respond to a rejected request. Extra load on the system may be generated by users trying to immediately re-establish a connection.
Page	The specified web page is served to rejected requests. You can provide information to the customer such as why the session was rejected and when would be a more opportune time to return to the site. A user is less likely to try immediately re-establishing a connection and more likely to return to the site.
Allocate sessions	A `countdown` web page is served to rejected requests. The user is asked to wait a certain amount of time before getting access to the site. This type of session is given priority over new sessions. Enter the number of sessions you wish to have admitted each minute. For example, if you allocate five sessions per minute, one session will be admitted every 12 seconds. If seven sessions are rejected, five will be admitted the next minute and two will be admitted the minute after. Make sure the allocation rate is less than the system’s capacity. You may want to compensate the allocation for no-shows. Monitoring the `% Priority Requests` statistic will show the system’s load due to priority sessions. Reduce the allocation rate if the number approaches or is over 50%. Also monitor the `Last Allocation Delay` statistic. It shows how long a deferred user waited before his/her session was admitted.

Parameter	Description
External	Use an external function or application. For example, the user could be offered a discount or other incentive to return to the site; or, the user could be offered to enroll in a service plan that guarantees access to the site. Currently, no supported functions or applications exist. If selected, the Error page is returned.
Exclude	After the initial rejection, the user is prevented from returning to the site after the specified amount of time (in seconds). This discourages a user from trying to immediately re-establish a connection. If a session is allocated, this is the minimum delay that can be scheduled.

Creating an Allocation Page for Rejected Sessions.

The following is the default allocation page served to the user:

Server Busy

```
We are sorry our server is busy, and in order to ensure adequate
levels of service to our current visitors, we cannot serve you at
this time. We have allocated you a position in line and will serve
you as soon as we can.

You will automatically enter the site in 1:23 (minutes:seconds).
```

To change the content of this page, you must edit the file `/opt/ns-`*`server_name/server_id`*`/config/hpac/config.ac`

To change the “Server Busy” title, edit the **deferral.title** parameter. To change the content of the message, edit the **deferral.message** parameter. To edit the countdown line, edit the **deferral.enterMsg** parameter. Note that each parameter is ended by a single period on its own line.

The default allocation page would include the following entries in the `config.ac` file:

```
deferral.title
Server Busy
.
deferral.message
We are sorry our server is busy, and in order to ensure
adequate levels of service to our current visitors, we
```

```
cannot serve you at this time. We have allocated you a
position in line and will serve you as soon as we can.
.
deferral.enterMsg
You will automatically enter the site in
.
```

Starting HP AdmissionControl for Netscape

HP AC is automatically enabled after you have installed HP ServiceControl (provided you have met certain conditions; see "Configuring HP AdmissionControl for Netscape" on page 17 for more information) or run the setup script (see "Running the Setup Script" on page 17 for more information).

If you have stopped HP AC, then you can start it again by configuring and specifying the load from the `HP AdmissionControl Settings` administration web page.

Stopping HP AdmissionControl for Netscape

To stop or disable HP AC, set the Admit Session to "Always" from the `HP AdmissionControl Settings` administration web page.

If you are permanently stopping HP AC, you should remove HP AC from your system (see "Removing HP AdmissionControl for Netscape" below for more information). Because HP AC does not cache HTML, performance may be slow for static pages.

Removing HP AdmissionControl for Netscape

To remove HP AC, do the following:

1. Type **`/opt/hpac/setup -r`**
2. At the `Enter root pathname of Netscape server` prompt, enter the Netscape Server root directory.

Logging HP AdmissionControl Information

Saving HP AdmissionControl Information

HP AC admission decisions can be saved to the server access log. To include them, do the following:

1. Start the Netscape Administration Server.
2. Select the server to configure.
3. Click on **`Server Status`**.
4. Select **`Log Preferences`**.
5. Enter the name of the new access logfile to create (Netscape will not let you change the format of a logfile that is in use).
6. Select **`Custom format`** near the bottom of the page.
7. Append **`%Req->vars.hpacSessionState%`** at the end of the Custom format field. Be sure to include a space at the beginning of this entry to separate it from the other entries.
8. Click **`OK`** to make the change.
9. Click on **`Save and Apply`** to save your changes.

One of the following values will be logged to the access logfile:

Table 2-5 Admission Decision Log Values

Value	Description
-	A management request was served from the cache.
2	The request was rejected.
3	The request was processed as part of a basic priority session.
4	The request was processed as part of a high priority session.
5	The request was deferred to a future time slot.
6	The request was redirected to another server.

Logging Statistics to a File

The statistics displayed on the `HP AdmissionControl Statistics` web page can be logged to a file. To log the statistics to a file add the following lines to `/opt/ns-`*`server_name`*`/`*`server_id`*`/config/hpac/config.ac`:

`log.file` *filename*
`log.interval` *seconds*

Where *filename* is the name of the file to which to save the statistics and *seconds* is how often the statistics are saved (in seconds). The `log.interval` default is 60 seconds.

Restart the web server for the changes to take effect.

The following is an example of a log entry:
`10/Mar/1998:20:39:00,15,0,0,0,0,0,0,0,181,0,0,0.5,0.00,92` where each field is delimited by a comma. The fields are:

Table 2-6 HP AC Log File Statistics

Statistic Name	Example Value
Time (GMT)	10/Mar/1998:20:39:00
Basic Sessions	15
Priority Sessions	0
Redirected Sessions	0
Sessions Rejected	0
Sessions Rejected Again	0
Sessions Timed Out	0
Sessions Too Long	0
Bad MD5 Requests	0
Basic Requests	181
Priority Requests	0
Management Requests	0
Load	0.5
Percentage Priority Requests	0.00
Last Allocation Delay	92

Other Configuration Considerations

This section covers tasks beyond basic configuration.

Tuning Your Web Server's Cache

To control session admissions, HP AC tracks the session state by including cookies in HTTP responses. For HP AC to operate effectively, the server cannot generate all of its responses from the cache. This may cause the performance of the web server to be slow.

However, you can tune the cache by configuring the `/opt/ns-`*`server_name/server_id`*`/config/hpac/config.ac` file to allow specified mime types to be cached or not cached.

For example, if you serve HTTP pages with embedded images, you can cache the images by adding the following lines to the configuration file:

```
mime.cache
mime.type image/gif
mime.type image/jpeg
```

Or, if your pages are generated by an application such as an NSAPI plug-in or CGI script, you can allow all mime types to be cached except for the mime types associated with the application. For example, to cache all mime types except those generated by CGI scripts, add the following lines to the configuration file:

```
mime.nocache
mime.type magnus-internal/cgi
```

You must restart the web server if you make changes to the configuration file.

If a page is not cachable, such as a dynamically created page or other pages marked by NSAPI as uncachable, you cannot cache it even if you specify it in the configuration file as cachable.

Allowing Equal Access to a System's Resources

If a web server hosts multiple virtual web sites, HP AC can be configured to balance traffic between each site, allowing each site to share the system's resources equally.

The description or pattern of the web servers' document roots for each virtual server must be configured in the `/opt/ns-`*`server_name/server_id`*`/config/hpac/config.ac` configuration file. HP AC uses the `isolate.pattern` parameter to monitor each site's traffic. You must restart the web server after editing the configuration file.

For example, a system is hosting two web sites for Company A and Company B. Company A's home page is located at `/web_pages/company_a/index.html` and Company B's home page is located at `/web_pages/company_b/index.html`. To monitor each site's traffic, add the following to the configuration file:

```
isolate.pattern /web_pages/%[^/]
```

Refer to documentation on the `sscanf` command for more information on constructing the pattern.

After editing the configuration file, restart the web server.

Detecting Failed Servers in a Cluster

When a web server is running, it periodically broadcasts a message that it is up. When a web server is shut down, it broadcasts a message that is unavailable. When a web server is not running, it does not broadcast a message.

Each web server in a cluster listens for these broadcast messages. Based on the messages received or not received, it will mark each system as up or down.

The web server marks a system as up when it receives the appropriate broadcast message from that system. The web server marks a system as down when it receives the appropriate message or it fails to receive a message after a specified number of broadcast intervals.

In the HP AC `/opt/ns-`*server_name*`/`*server_id*`/config/hpac/config.ac` configuration file, you can configure how often messages are sent (broadcast interval) and how many messages can be missed before the system is marked as down. The parameters are:

```
cluster.keepalive.interval 60
cluster.keepalive.misses 3
```

where the interval is measured in seconds. The values given are the default values.

If you configure these parameters, the web server must be restarted. Also, all systems in the cluster should use the same values for these parameters.

Decreasing the broadcast interval decreases the time it takes to detect a failure. However, it also increases broadcast traffic.

Sometimes, not all broadcast messages are received. Therefore, the number of misses should be set to a value greater than one. However, in a large cluster, removing a machine falsely does not severely impact the cluster's capacity and improves the responsiveness to failures.

The maximum time to detect a failure can be determined by multiplying the broadcast interval by the number of misses. For the default values, the maximum failure detection time is three minutes.

HP AdmissionControl for the Apache Web Server

Installing HP AdmissionControl for Apache

HP AdmissionControl (HP AC) for the Apache Web Server is part of the HP Domain ServiceControl (HP DSC) product. You do not need to load the entire HP DSC product if you only want to use HP AC for the Apache web server. Specifically, because HP AC for Apache is not integrated with HP DESMS, you do not need to install HP DESMS with this part of the product.

Installation Requirements

Hardware

- HP 9000 computer system
- 32 MB of memory
- CD-ROM drive to load the software

Software

- HP-UX 10.20 or 11.0
- Apache Server 1.3.3 or later

Disk Space (Estimated)

- 1 MB

Installing the Software

To install HP AC for the Apache web server, run `swinstall` (as root), double-click on the bundle J1592AA to view the software, and select the HP AC software. Unless instructed otherwise, `swinstall` copies the HP AC for Apache files from the distribution media to the directory `/opt/hpac-apache`.

Integrating HP AdmissionControl with the Apache Web Server

To integrate the HP AC module with the Apache server, follow the steps under the scenario that best describes your installation:

Scenario 1: The Apache server is already installed on the system.

1. Verify that your server has been built with Dynamic Shared Object (DSO) support.

   a. Run the command *apache_home*/sbin/httpd -l or *apache_home*/bin/httpd -l (depending on the layout). The output should list mod_so.c. This verifies that DSO support is present.

   b. If DSO support is not present, follow the instructions 2 to 4 in Scenario 2, then continue with step 3 below.

2. Find the file mod_hpac.so for your HP-UX release and Apache version in /opt/hpac-apache/lib , and copy it to *apache_home*/libexec

3. Edit the file *apache_home*/etc/httpd.conf (or *apache_home*/conf/httpd.conf, if you used the older layout).

   a. At the end of the section that contains entries of the form AddModule xxx_module libexec/mod_xxx.o or LoadModule xxx_module libexec/mod_xxx.so, add the following entry:
   LoadModule hpac_module libexec/mod_hpac.so

   b. At the end of the section that contains entries of the form AddModule mod_xxx.c, add the following entry:

   AddModule mod_hpac.c

   c. Add the following line:

   Alias /hpac/ /opt/hpac-apache/html/

NOTE If you prefer, you can add this line to the srm.conf file. The /hpac/ location should be protected by a password, to prevent unauthorized access to the server's statistics.

4. Restart the Apache server so that the changes will take effect. Before restarting the server it is recommended that you read "Configuring HP AdmissionControl for Apache" on page 34.

Scenario 2: The Apache server is not yet installed on the system.

1. Download and unpack the Apache distribution archive.
2. Create the directory `hpac` in *apache_dist*/src/modules, then find the file `mod_hpac.so` for your HP-UX release and Apache version in `/opt/hpac-apache/lib.` Copy this file to: *apache_dist*`/src/modules/hpac`.
3. Edit the file *apache_dist*`/src/Configuration.tmpl` and add the following line at the end of the file:

   `AddModule modules/hpac/mod_hpac.o`

4. Follow the instructions for building and installing the Apache server, as described in the Apache documentation (for example, run `config`, `make`, and `make install`). In particular, make sure that you enable the hpac module as a shared module. For example, run `config` with the options:

   `--enable-module=hpac`

   `--enable-shared=hpac`

5. Edit the configuration file *apache_home*`/etc/httpd.conf` or *apache_home*`/etc/srm.conf.` (These files are in *apache_home*`/conf/`, if you used the older installation layout.) Add the following line:

   `Alias /hpac/ /opt/hpac-apache/html/`

NOTE If you prefer, you can add this line to the `srm.conf` file. The `/hpac/` location should be protected by a password, to prevent unauthorized access to the server's statistics.

6. Restart the Apache server, so that the changes will take effect. Before restarting the server, it is recommended that you read the next section.

Configuring HP AdmissionControl for Apache

Once the HP Admission Control module is integrated with the Apache server, admission control becomes operational when the server is (re)started. However, the module's defaults are unlikely to satisfy the needs of all sites. This section describes the configurable parameters of the HP AC module and how to set these parameters.

Setting the Configurable Parameters

You can modify the behavior of the HP AC modules by placing the appropriate directives (commands) in your Apache configuration file(s): either `httpd.conf`, `srm.conf`, or `access.conf`. These configuration files can be found in *apache_home*`/etc/` (or in *apache_home*`/conf/`, if you used the older installation layout.) All HP AC directives start with the characters HPAC. See “HP AdmissionControl Configurable Parameters for the Apache Web Server” on page 65 for a list of the available configurable parameters for the Apache server.

Admitting Sessions. To turn the admission control on and off, use the `HPACAdmissionControl` directive. The default for this directive is “on”. For example, to turn admissions off, use the following directive in your configuration file:

```
HPACAdmissionControl off
```

If admission control is disabled (set to off), all sessions are admitted to the web server.

When the admission control is in effect, new sessions are admitted based on system load. You can set a load threshold using the `HPACAdmitLoadThreshold` directive. The default for this directive is “2.0”. For example, to set the load threshold at 1.5, use the following directive in your configuration file:

```
HPACAdmitLoadThreshold 1.5
```

To calculate the load threshold

1. Run the `top` command. Note the first number in the "Load averages" list and the percentage listed under "IDLE" of "Cpu states".

Sample Output from the top Command

```
System: web_server           Wed Apr 22 10:41:59 1998
Load averages: 1.45, 1.46, 1.78
149 processes: 145 sleeping, 3 running, 1 stopped
Cpu states:
LOAD  USER  NICE  SYS  IDLE BLOCK  SWAIT   INTR  SSYS
1.45 100.0%  0.0% 0.0%  0.0%  0.0%  0.0%   0.0%  0.0%
```

2. If IDLE is greater than zero, then set the threshold to (100 - IDLE)/100.

   If IDLE equals zero, then set the threshold to the first listed load average.

   Using the above sample output, you would set the load threshold to 1.45.

Run `top` when performance is poor, and when it is acceptable to determine an acceptable load threshold.

Ending Sessions. A session duration can be set with the `HPACSessionDuration` directive. The default for this directive is "0". For example to set a session to 3600 seconds, use the following directive in your configuration file:

```
HPACSessionDuration 3600
```

The duration of a session is specified in seconds. If the duration is set to 0, the session never expires. If a session exceeds the specified duration, it is ended.

A session can also be terminated if the time interval between two successive requests of a session exceeds a set number of seconds. You can set this time interval with the `HPACIdleSessionTimeout` directive. The default for this directive is "300" seconds. For example, to set the time interval to 120 seconds, use the following directive in your configuration file:

```
HPACIdleSessionTimeout 120
```

NOTE Termination of a session means that the next request coming from the same user agent will start a new session. All privileges that the old session might have enjoyed are lost.

Responding to Rejected Sessions. If conditions on the web server do not allow servicing new requests, sessions can be redirected or rejected.

You turn on redirection indirectly by setting the redirection URL with the `HPACRedirectURL` directive. For example, to redirect rejected sessions, use the following directive in your configuration file, filling in the appropriate URL:

`HPACRedirectURL [http://]`*host*`[:`*port*`]`

NOTE A request can be redirected only to a mirror site.

A redirected session can be bounced back to the original server. You can control how many times a session is redirected with the `HPACRedirectTTL` directive (TTL stands for time-to-live). The default for this directive is "0." For example, to set the number of times a session is redirected to 1, use the following directive in your configuration file:

```
HPACRedirectTTL 1
```

The number set by this directive is the number of redirections a session has been subjected to, beyond the first one. In other words, 0 means the session has been redirected once, 1 means the session has been redirected twice, etc. This number should not exceed 2, to avoid wasting the resources of the server(s) involved. (The default is probably appropriate for most sites.)

If a session has to be rejected, the action the admission controller takes depends on the rejection policy in effect. The rejection policy can be *reject*, *rejectpage*, or *defer*. It can be set using the directive `HPACRejectionPolicy`. The default for this directive is "reject." For example, to set the rejection policy to "defer," use the following directive in your configuration file:

```
HPACRejectionPolicy defer
```

When the *reject* rejection policy is in effect, the server sends the `HTTP_SERVICE_UNAVAILABLE` code and associated message to the client. This is the easiest but least informative way to respond to a rejected request. Users may try to reconnect right away, generating extra load on the system.

When the *rejectpage* rejection policy is in effect, the server returns the contents of a page containing a custom, more explanatory response to the client. For instance, the customer whose access has been rejected may be given a reason for the rejection and a suggestion of a more opportune time to return to the site. The extra information is more likely to dissuade users from retrying immediately, without discouraging them from returning to the site in the future.

The location of the file holding this custom response is specified with the directive `HPACRejectPagePath`. For example,

```
HPACRejectPagePath <file_path>
```

If the policy is set to *rejectpage*, but the rejectpage path has not been set (or cannot be accessed), the server response is the same as the *reject* policy server response.

The *defer* policy is a special case of rejection. The admission of a session rejected under this policy is merely postponed to a future time slot, when the session will automatically gain access to the server. Once a deferred session is admitted, it is handled as a priority session.

A `countdown` web page is returned to the user agent in response to deferred requests which shows how long the user has to wait in line.

You can set the rate (per minute) at which deferred sessions are admitted to the server with the `HPACDeferredAdmitRate` directive. The default for this directive is “10” sessions per minute. For example, to set the rate at which the deferred sessions are admitted to the server to 5 sessions per minute, use the following directive in your configuration file:

```
HPACDeferredAdmitRate 5
```

In the example above, one session will be admitted every 12 seconds. (At this rate, for example, if there are only 5 sessions waiting for admission, they will all gain access during the next minute. If there are 20 sessions waiting for admission, the last 5 sessions will be admitted 4 minutes later than the first 5.)

When setting the admission (allocation) rate of deferred sessions, make sure that the system has adequate capacity to handle it. Take into account that some of the deferred sessions may not come back (because the user gave up), and compensate accordingly.

Monitoring the `% Priority Requests` and `Last Allocation Delay` statistics can help in setting a realistic allocation rate. The first statistic will show the system's load due to priority sessions. Reduce the allocation rate if this number approaches, or is over, 50%. The second statistic shows how long the user of a deferred session had to wait before gaining access to the server.After the initial rejection, the user is prevented from returning to the site for a specified amount of time. If a session is allocated, this is the minimum delay that can be scheduled. You can set this time interval with the directive `HPACRejectedExclusionTime`. The default is “300” seconds. For example, to specify that the user will have to wait 120 seconds before he can again try to access the site, use the following directive in your configuration file:

```
HPACRejectedExclusionTime 120
```

Creating an Allocation Page for Rejected Sessions. The following is the default contents of the deferral (allocation) page:

Server Busy

```
We are sorry our server is busy, and in order to ensure adequate
levels of service to our current visitors, we cannot serve you at
this time. We have allocated you a position in line and will serve
you as soon as we can.

You will automatically enter the site in mm:ss (minutes:seconds).
```

The page has three parts, which can be set independently. The first part is the title (Server Busy). You can change the title with the `HPACDeferralTitle` directive. To set the title to "Site Temporarily Unavailable," use the following directive in your configuration file:

```
HPACDeferralTitle Site Temporarily Unavailable
```

The second part of the deferral page is an explanatory message, which can be set with the `HPACDeferralMessage` directive. An informative message is likely to span several lines, in which case you have to escape the newline character on all but the last line. For example,

```
HPACDeferralMessage     We are sorry, our server is busy. In order \
                        to ensure adequate levels of service to \
                        our current visitors, we cannot serve you \
                        at this time. We have allocated you a \
                        position in line and will serve you as \
                        soon as we can.
```

The third part is the countdown line, which can be set with the `HPACDeferralEnterMsg` directive. For example:

```
HPACDeferralEnterMsg  Time left:
```

Logging HP AdmissionControl Information

Saving Information to the Server Access Log. HP AC admission decisions can be saved to the server's access log, by adding the "%{HPAC}n" format option to the `LogFormat` directive. For example:

```
LogFormat %h %l %u %t \%r\ %>s %b %{HPAC}n
```

The effect of this option is to append one of the words listed below to the log message:

rejected	The request was rejected
basic	The request was processed as part of a basic priority session
priority	The request was processed as part of a high priority session
deferred	The request was deferred to a future time slot
redirected	The request was redirected to another server

Logging Statistics to a File. The statistics displayed on the `HP AdmissionControl Statistics` web page can be logged to a file. You can turn on statistics logging with the `HPACStatsLogging` directive. The default for this directive is "off." For example:

```
HPACStatsLogging on
```

In addition, you can specify the time interval between log updates with the `HPACLogUpdateInterval` directive. The default for this directive is "300" seconds. You can specify the log file with the `HPACStatsLogfile` directive.

For example, to specify that the log file *apache_home*`/var/log/stats.hpac` is updated every 600 seconds, use the following directives:

```
HPACLogUpdateInterval 600

HPACStatsLogfile var/log/stats.hpac
```

The log update interval has to be a multiple of 5 seconds. For example, if you set the interval to 1 second, the update will take place after 5 seconds. If you set the interval to 7 seconds, the update will take place after 10 seconds.

If logging is enabled, but the log file has not been specified, the default log file is *apache_home*`/var/log/hpac.log` (or *apache_home*`/logs/hpac.log`, depending on the layout of *apache_home*) .

NOTE

The `HPACStatsLogging`, `HPACLogUpdateInterval` and `HPACStatsLogfile` directives set global AC parameters, therefore they should be used outside virtual host configuration blocks. They are ignored inside the virtual host configuration blocks.

A log entry consists of a number of comma separated fields, as follows:

```
07/Oct/1998:19:30:00,virtual.host.com,15,0,0,0,0,0,0,0,
181,0,0,0.5,0.00,92
```

The first field is the update time (GMT) and the second field is the name of the virtual host to which the statistics refer. The table below lists the remaining fields.

Table 2-7 HP AC for Apache Log File Statistics

Statistic Name	Example Value
Basic Sessions	15
Priority Sessions	0
Redirected Sessions	0
Sessions Rejected	0
Sessions Rejected Again	0
Sessions Timed Out	0
Sessions Too Long	0

Statistic Name	Example Value
Bad MD5 Requests	0
Basic Requests	181
Priority Requests	0
Management Requests	0
Load	0.5
Percentage Priority Requests	0.00
Last Allocation Delay	92

Other Configuration Considerations

This section covers tasks beyond basic configuration:

Admission Control and Response Caching. To control session admissions, HP AC tracks the session state by including cookies in HTTP responses. For the session tracking mechanism to work properly, server responses can no longer be cached. This, in turn, impacts the performance of the server.

You can alleviate the problem by specifically allowing caching of certain mime types, short of allowing a session to be fully served from cached responses. Good candidates for caching are mime types representing objects embedded in an HTML document (for example, images, sounds).

To turn on caching, use the `HPACMimeCaching` directive. The default for the directive is “off.” For example, to turn mime caching on, use the following directive in your configuration file:

```
HPACMimeCaching on
```

With mime caching on, the HP AC allows caching of the following mime types:

audio/basic	image/gif	image/x-photo-cd
audio/midi	image/ief	video/quicktime
audio/x-wav	image/ifsimage/jpeg	video/x-mpeg2
audio/x-liveaudio	image/tiff	video/x-msvideo
audio/x-pn-realaudio	image/wavelet	
image/fif	image/vnd	

You can turn off caching of individual mime types in this list with the `HPACMimeNocache` directive. For example, assuming that mime caching is on, the following directive turns off caching for the specified mime types:

```
HPACMimeNocache video/x-mpeg2 audio/x-pn-realaudio
```

You can add to the default list of mime types that can be cached with the `HPACMimeCache` directive. For example, if mime caching is on, the following directive adds the specified mime types to the list of mime types that can be cached:

```
HPACMimeCache image/x-rgb image/x-xpixmap
```

NOTE If the list of mime types passed to the `HPACMimeNocache` and `HPACMimeCache` directives is too long to fit on one line, the newline character must be escaped on all but the last line.

The caching commands specified in the configuration file have no effect if a document cannot be cached in the first place (for instance, documents created dynamically).

System Resources Sharing Among Virtual Hosts. By default, each virtual host equally shares the system resources. However, this does not guarantee equal use of the resources. Virtual hosts hosting active sites may use more than their fair share of system resources, at the expense of other virtual hosts. A more equitable use of system resources can be achieved using one of the techniques described below.

You can influence the access of virtual servers to system resources by using different load thresholds for the virtual hosts. For instance, you could set the load threshold lower for virtual hosts that have a tendency to use most of the system resources. Conversely, you can set the load threshold higher, or even turn off admission control, for virtual hosts that have little impact on the system resources.

You can use the `HPACShareUnits` directive to give more weight to some of the virtual hosts. The default for this directive is "1." For example, to give more weight to some of the virtual hosts, use the following directive in your configuration file:

```
HPACShareUnits 2
```

To understand the effect of this command, assume that you have three virtual hosts, A, B and C: A is assigned one share of system resources, B is assigned two shares and C is assigned three shares. (There are a total of six shares.) This amounts to assigning 17% of system resources to A (1 / 6 * 1), 33% to B (1 / 6 * 2) and 50% to C (1 / 6 * 3).

The assigned share of system resources is used to compute the actual priority threshold for each virtual host from the server-wide priority threshold. You can set the value for the server-wide priority threshold with `HPACAdmitPriorityThreshold`. The default for this directive is "0.9.". For example, to set the server-wide priority threshold to .75, use the following directive in your configuration file:

```
HPACAdmitPriorityThreshold 0.75
```

The setting above will allow up to 75% of all sessions to be priority sessions. Beyond this threshold, even priority sessions are rejected. The value set with directive is used to compute the priority threshold for individual hosts, taking into account the assigned share (see `HPACShareUnits` above).

The assigned share is also used to give priority to under-represented virtual hosts, when virtual host isolation is in effect. Virtual host isolation is turned on with the `HPACVHostIsolation` directive. The default for this directive is "off." For example, to turn on virtual host isolation, use the following directive in your configuration file:

```
HPACVHostIsolation on
```

With this option in effect, the admission controller raises the priority of new sessions for those virtual hosts that contribute less than their assigned share to the system load.

Global Parameters. Most HP AC configuration directives set values for parameters that affect individual virtual hosts. A few of them set values for parameters that affect all virtual hosts. These directives are:

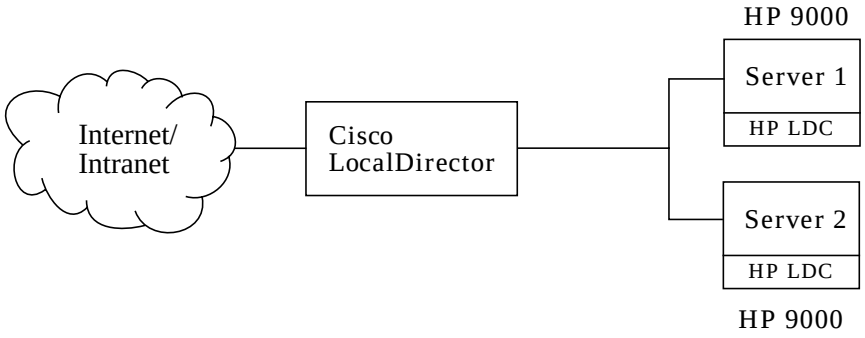
`HPACAdmitPriorityThreshold`	`HPACStatsLogfile`
`HPACIsolateDamping`	`HPACStatsLogging`
`HPACLoadDamping`	`HPACVHostIsolation`
`HPACLogUpdateInterval`	

The directives setting global AdmissionControl parameters should be used outside virtual host configuration blocks. Inside virtual host configuration blocks, the directives are ignored and the parameters they try to set revert to default values.

3 HP LocalDirector Controller

What is HP LocalDirector Controller?

HP LocalDirector Controller (HP LDC) works with Cisco LocalDirector by automatically generating the information needed by Cisco LocalDirector to load balance TCP/IP traffic across multiple servers. HP LDC, specifically the HP LocalDirector Control daemon (`ldc_agt`), must be configured and running on each system that is managed by Cisco LocalDirector. Information regarding Cisco LocalDirector can be found at the URL `http://www.cisco.com/warp/public/751/lodir/`.



The information generated by HP LDC is referred to as “weights” in this document. The weights help Cisco LocalDirector determine which system has the resources to process an incoming request.

Initial weights are generated by the Webstone benchmark tool. Webstone generates traffic to a system and calculates the throughput based on getting different-sized static pages in three minutes. The throughput is used to calculate the initial weights.

HP LDC adjusts the weights depending on CPU usage and system load. Both the CPU usage and system load (measured by a one minute average job queue) must reach their configured thresholds before the weights are lowered. The weights will range between one and the initial weights.

Installing HP LocalDirector Controller

HP LocalDirector Controller (HP LDC) is part of the HP Domain ServiceControl (HP DSC) product. You do not need to load the entire HP DSC product if you only want to use HP LDC.

Installation Requirements

Hardware Requirements

- HP 9000 computer system
- 32 MB of memory
- CD-ROM drive to load the software

Software Requirements

- HP-UX 10.20 or 11.0
- HP DESMS
- An HTTP server such as Netscape Enterprise or FastTrack Server version 3.0 or later
- A web browser that supports JDK 1.1, such as Communicator 4.06 or Microsoft Internet Explorer 4.0

Other Requirements

- A system already running Cisco LocalDirector version 2.1 or later

Installing the Software

To install HP LDC, run `swinstall` (as root), double-click on the bundle J1592AA to view the software, and select the HP LDC software.

Configuring Cisco LocalDirector

Because HP LocalDirector Controller sends information to Cisco LocalDirector using SNMP traps, the *snmp-server host* parameter must be configured in the Cisco LocalDirector.

On a system managed by Cisco LocalDirector, run **`netstat -rn`** and check the routing table information. Use the IP address associated with the Cisco LocalDirector gateway to configure the *snmp-server host* parameter

Refer to Cisco LocalDirector's manuals for information on setting this parameter and other configuration information.

Configuring HP LocalDirector Controller

There are two components you need to configure before using HP LDC: the HP LDControl server and the HP LDControl daemon.

You must configure HP LDC using the HP Domain Enterprise Management System (HP DESMS). Instructions on how to start HP DESMS are included in this manual. For more information on HP DESMS, please refer to the *Getting Started with HP Domain Software* manual.

Starting HP DESMS

To start HP DESMS, do the following:

1. Start the HP administration server. Type the following:

   `/opt/hpwebsuite/start-admin`

2. Start a browser that supports frames, is Java-enabled, and supports JDK 1.1.

3. Go to the URL

   `http://`*`hostname`*`:8181`

   where *hostname* is the name of the system on which you are running the HP administration server.

   Reload this page if you have visited this page prior to this installation.

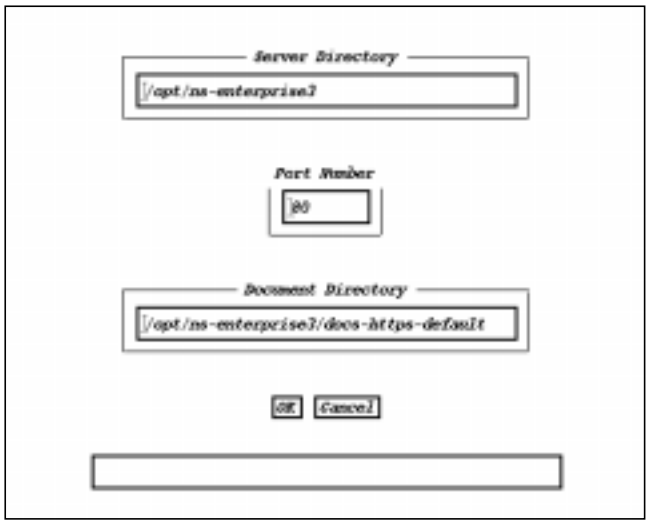
4. Enter the following administration user (server) ID and password:

   User ID: **`hpadmin`**
   Password: **`hpadmin`** (you may have changed this during the setup process)

If you are starting HP DESMS for the first time, the page to configure the HP LDControl daemon is displayed.

Configuring the HP LDControl Server

After starting HP DESMS, click on “Service Control” from the side menu and then “Server Configuration.” The following page displays:



Set the following parameters to configure the HP LDControl server:

Table 3-1 HP LDControl Server Configurable Parameters

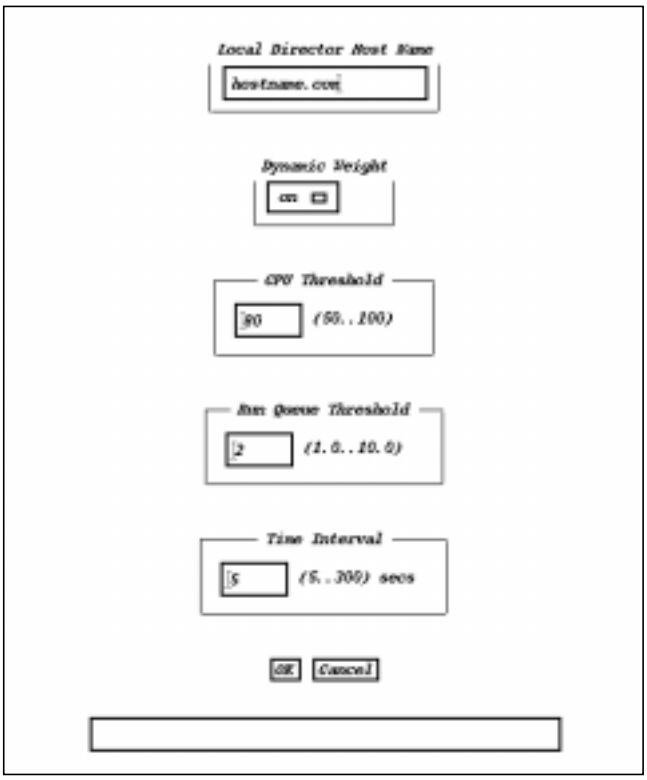
Parameter	Description
Server Directory	The home directory of the web server. For example, `/opt/ns-enterprise3`.
Port Number	The port number used by the web server. This must be a non-SSL port number. For example, `80`.
Document Directory	The document root directory of the web server. For example, `/opt/ns-enterprise3/docs-https-default`.

The HP LDControl daemon must be started/restarted for these values to take effect. See “Starting and Stopping the HP LDControl Daemon” on page 55 for more information on starting HP LDC.

NOTE The web server configured in the `/etc/hpldc/webstone/conf/server-list` file must be running before the HP LDControl daemon is started.

Configuring the HP LDControl Daemon

After starting HP DESMS, select “Service Control” from the side menu and then “Configuration.” The following page displays:



Set the following parameters to configure the HP LDControl daemon:

Table 3-2 HP LDControl Daemon Configurable Parameters

Parameter	Description
LocalDirector Hostname	The hostname of the system on which Cisco LocalDirector is running.
Dynamic Weight	Starts/Stops the HP LDControl daemon. When activated, the daemon will monitor the system and adjust the weights, if necessary. When deactivated, the HP LDControl daemon sends the initial weights to Cisco LocalDirector and exits.

Parameter	Description
CPU Threshold	The highest percentage the CPU usage should reach before the weight of the server is automatically decreased. Note that the run queue threshold (average load) must also be reached before the weights are adjusted. Default: 80 Range: 50 - 100% (integer only)
Run Queue Threshold	The highest amount the average load should reach before the weight of the server is automatically decreased. Note that the CPU usage threshold must also be reached before the weights are adjusted. Default: 2 Range: 1.0 - 10.0 (real number)
Time Interval	How often, in seconds, the thresholds are checked and adjustments are made, if needed, to the weights. Default: 5 seconds Range: 5 - 300 seconds (integer only)

Click on “OK” to save your changes. The values are saved in the file `/etc/opt/hpldc/conf/ldc.conf`.

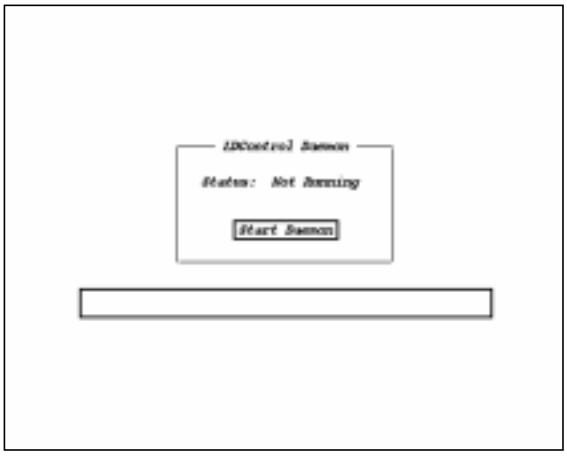
NOTE

The web server configured in the `/etc/hpldc/webstone/conf/server-list` file must be running before the HP LDControl daemon is started.

Starting and Stopping the HP LDControl Daemon

The HP LDControl daemon can be started and stopped from HP DESMS. Select “Service Control” from the side menu and then “Start/Stop Daemon.” A page similar to the following displays (what is displayed depends on the status of the HP LDControl daemon: running or not running):

NOTE The web server configured in the `/opt/hpldc/webstone/conf/server-list` file must be running before the HP LDControl daemon is started.



To start or stop the HP LDControl daemon from the command line, type:

`/opt/hpldc/bin/ldc_agt`

Configuring a System with More than One LAN Card

If the system on which you are running the web server has more than one LAN card, you must set the *snmp-server host* and *real* parameters in Cisco LocalDirector. Do the following:

1. On the system with multiple LAN cards, run **`netstat -rn`** and check the routing table information. Use the IP address associated with the Cisco LocalDirector gateway to configure the *snmp-server host* parameter of Cisco LocalDirector.
2. On the system with multiple LAN cards, run **`nslookup`** ***`local_hostname`*** and use this IP address to configure the *real* parameter of Cisco LocalDirector.

Refer to Cisco LocalDirector's manuals for information on setting these parameters.

Troubleshooting the HP LD Controller

General Troubleshooting

If an error occurs, check the following two log files for error messages, causes, and recommended actions:

1. `/var/opt/hpldc/ldc.log`
2. `/var/opt/hpldc/webstone.log`

Problems Accessing the HP LD Controller from HP DESMS

Table 3-3 Browser Error Message and Action

Error Message	Action
Applet ConfApplet can't start.	The browser that you are using to administer the system must support JDK 1.1 in order to run HPLDC. Two browsers that support JDK 1.1 are Netscape Navigator 4.05 and Microsoft Internet Explorer 4.0.

HP LDControl Daemon

If the HP LDControl daemon dies, check for the following error messages in the `/var/opt/hpldc/ldc.log` file. Complete the listed actions for the specified messages.

Table 3-4 HP LDControl Daemon Error Log Messages and Actions

Error Message	Action
Cannot open file *filename*.	Check that the file *filename* exists and that the HP LDControl daemon has write permission to its directory.

Error Message	Action
Server might be down. Initial weight set to 0. Exiting.	1. Make sure the web server is running on the system. Restart/Start the web server and then restart the HP LDControl daemon. 2. Check the parameters in the file `/etc/hpldc/webstone/conf/server-list`. 3. In `/etc/passwd`, check for the following entry: `webstone:trKI3jiXvewTw:33:1::/tmp:/sbin/sh` If this entry does not exist, add it to the file. 4. If the web server is running, make sure it is using a non-SSL port. The HP LDControl daemon must use a non-SSL port to generate the initial weight.
Cannot send weight to LocalDirector.	1. The *snmp-server host* parameter must be set on the system running Cisco LocalDirector. Refer to Cisco LocalDirector's manual for more information on setting this parameter. 2. Check that *LDHostname* is set to the system running Cisco LocalDirector in the `/etc/opt/hpldc/conf/ldc.conf` file.

A HP AdmissionControl Configurable Parameters

HP AdmissionControl Configurable Parameters for Netscape

You can modify the behavior of the HP AC modules by setting the appropriate parameters in your Netscape configuration file: `/opt/ns-`*server_name*`/`*server_id*`/config/hpac/config.ac`.

Table A-1 HP AC Configurable Parameters for Netscape

Parameter	Range/Type	Default	Description
admit.always	N/A	N/A	Configures HP AC to always accept sessions.
admit.load	N/A	N/A	Sets the "Admit Sessions" to use the load threshold.
admit.load.threshold	0.0 <= x	2.0	Sets the load threshold for admitting a session.
admit.priority.damping	0.0 <= x <= 1.0	0.001	The damping factor used to compute the priority percentage. Larger values make the controller more responsive to recent activity.
admit.priority.threshold	0.0 <= x <= 1.0	0.9	The value of the priority fraction when priority requests are rejected (0.9 = 90% priority percentage).
admit.shutdown	N/A	N/A	Sets the "Admit Sessions" to shutdown.
admit.shutdown.delay	0 <= n (integer)	600	Sets how much time before HP AC shuts down and rejects all (new and remaining) sessions.
cluster.disable	N/A	N/A	Disables clustering. The system will not try to open the `hpac-cluster` port.
cluster.domain	string		The domain used to limit the scope of the cluster over which the client-side cookies can be shared.
cluster.group	string	default	Sets the cluster group.

Parameter	Range/Type	Default	Description
cluster.keepalive.interval	1 <= n (integer)	60	The number of seconds between status broadcasts.
cluster.keepalive.misses	1 <= n (integer)	3	The number of missed status broadcasts before a server is identified as down.
cluster.TTL	0 <= n (integer)	0	Sets the cluster TTL which is the number of redirections allowed before rejecting the session.
cookie.password	string	N/A	Sets the password used in creating the MD5 digest.
deferral.enterMsg	string	You will automatically enter the site in .	Part of the allocation page message served when a session is rejected.
deferral.message	string	We are sorry our server is busy, and in order to ensure adequate levels of service to our current visitors, we cannot serve you at this time. We have allocated you a position in line and will serve you as soon as we can.	Part of the allocation page message served when a session is rejected.
deferral.title	string	Server Busy .	Part of the allocation page message served when a session is rejected.
endsession.duration	0 <= n (integer)	0	Sets, in seconds, the maximum session duration
endsession.requestInterval	0 <= n (integer)	300	Sets, in seconds, the maximum interval between requests

Parameter	Range/Type	Default	Description
isolate.damping	0.0 <= x <= 1.0	0.001	The damping factor used to compute the share of resources being used by each virtual server. Larger values make the controller more responsive to recent activity.
isolate.pattern	string	N/A	The pattern used to identify virtual servers. If provide, HP AC will isolate traffic to each virtual server.
load.damping	0.0 <= x <= 1.0	0.1	The damping factor used to compute the web server load. Larger values make the controller more responsive to recent activity.
log.file	string	N/A	The full path name of the HP AC log file. The statistics from the HP AdmissionControl Statistics web page are logged to this file.
log.interval	1 <= n (integer)	600	How often, in seconds, the statistics are logged to the log.file.
mime.cache	N/A	See “Defaults Already Configured in config.ac” on page 64.	The web server should cache the specified mime types.
mime.nocache	N/A	N/A	The web server should cache all but the specified mime types.
mime.type	string	N/A	Specifies the mime type used by the caching policy.
reject.error	N/A	Server Temporarily Unavailable	Sets the response to a rejected session to the “Server Temporarily Unavailable” error message. This message is not configurable.
reject.excludeTime	0 <= x	300	Sets how long, in seconds, the user is prevented from returning to the site.

Parameter	Range/Type	Default	Description
reject.external	N/A	Server Temporarily Unavailable	Sets the response to a rejected session to use an external function or application. Currently, it will only serve the “Server Temporarily Unavailable” error message.
reject.future	N/A	N/A	Sets the response to a rejected session to a `countdown` web page.
reject.future.rate	1 <= n (integer)	10	Set the number of sessions that can be admitted each minute.
reject.page	N/A	N/A	Sets the response to a rejected session to a customizable web page.
reject.page.path	string	N/A	The full path and file name of the customizable web page.
shlib.initialize	string	N/A	The name of the function that initializes the library.
shlib.library	string	N/A	The file name of the shared library.
shlib.loadMetric	string	N/A	The name of the function used as the load metric.
shlib.release	string	N/A	The name of the function that releases resources allocated by the library.
shlib.reject	string	N/A	The name of the function used when the reject policy is set to External.
shlib.sessionState	string	N/A	The name of the function that modifies the session state. This function may change the priority of sessions or end sessions.

Defaults Already Configured in config.ac

The following are defaults that have been configured in the /opt/ns-*server_name*/*server_id*/config/hpac/config.ac file:

```
# Warning, manual changes to this file will be
# overwritten by changes made
# via the Admission Control Policy screen.
mime.cache # a list of likely cache candidates follows
mime.type audio/basic
mime.type audio/midi
mime.type audio/x-wav
mime.type audio/x-liveaudio
mime.type audio/x-pn-realaudio
mime.type image/fif
mime.type image/gif
mime.type image/ief
mime.type image/ifs
mime.type image/jpeg
mime.type image/tiff
mime.type image/wavelet
mime.type image/vnd
mime.type image/x-photo-cd
mime.type video/mpeg
mime.type video/quicktime
mime.type video/x-mpeg2
mime.type video/x-msvideo
```

HP AdmissionControl Configurable Parameters for the Apache Web Server

You can modify the behavior of the HP AC modules by placing the appropriate directives (commands) in your Apache configuration file(s): either `httpd.conf`, `srm.conf`, or `access.conf`. These configuration files can be found in *apache_home*`/etc/` (or in *apache_home*`/conf/`, if you used the older installation layout.)

Table A-2 HP AC Configurable Parameters for the Apache Web Server

Parameter	Argument	Default	Description
HPACAdmissionControl	On or Off	On	Turns admission control on or off.
HPACAdmitLoadThreshold	x > 0.0 (real number)	2.0	Sets the load threshold beyond which no new session is admitted.
HPACAdmitPriorityThreshold	0 <= x <= 1.0 (real number)	0.9	Sets the upper limit for the percentage of priority requests that can be admitted. (for example, 0.9 means that 90% of all requests admitted can be priority requests.) Beyond this limit, even priority requests will be rejected.
HPACCookieDomain	the string following the hostname in a fully qualified domain name (see description)	the domain extracted from the fully qualified domain name of the web server running the admission controller	Sets the domain over which cookies will be shared. For example, the domain for host `www.software.hp.com` is `.software.hp.com`
HPACCookiePassword	string	N/A	Sets the password used to create the MD5 digest for the cookie.

Parameter	Argument	Default	Description
HPACDeferralEnterMsg	string	You will automatically enter the site in	Sets the heading for the time counter on the deferral page.
HPACDeferralMessage	string	We are sorry, our server is busy. In order to ensure adequate levels of service to our current visitors, we cannot serve you at this time. We have allocated you a position in line and will serve you as soon as we can.	Sets the descriptive message displayed on the deferral page. If the message takes several lines, the newline character should be escaped on all but the last line. (For example: We are sorry, our server is \ busy. In order to ensure ...)
HPACDeferralTitle	string	Server Busy	Sets the title of the deferral page.
HPACDeferredAdmitRate	n >= 1 (integer)	10	Sets the rate (per minute) at which deferred sessions will be admitted to the server.
HPACIdleSessionTimeout	n >= 0 (integer)	300	Sets the time interval (in seconds) that can elapse between successive requests of a session before the session is considered idle (that is, next request from the same user agent will be the start of a new session.).
HPACIsolateDamping	0 < x <=1.0 (real number)	.001	Sets the damping factor used to compute the share of resources used by each virtual server. Larger values make the controller more responsive to recent activity.
HPACLoadDamping	0 <= x <= 1.0 (real number)	0.1	Sets the damping factor used to compute the web server load. Note: larger values make the controller more responsive to recent activity.

Parameter	Argument	Default	Description
HPACLogUpdateInterval	n > 0 (integer)	600	Sets the time interval (in seconds) between statistics log updates. Note: the granularity of the time interval is 5 seconds (that is, if the interval is set to one second, the update will take place after five seconds; if set to six seconds, the update will take place after 10 seconds, etc.).
HPACMimeCache	a list of one or more space-separated mime type strings	audio/basic audio/midi audio/x-wav audio/x-liveaudio audio/x-pn-realaudio image/fif image/gif image/ief image/ifs image/jpeg image/tiff image/wavelet image/vnd image/x-photo-cd video/quicktime video/x-mpeg2 video/x-msvideo	Sets the mime types the server can cache (all other mime types are not cached). Note: If the list takes several lines, the newline character should be escaped on all but the last line.
HPACMimeCaching	on/off	off	Turns mime caching on or off.
HPACMimeNocache	a list of one or more space-separated mime type strings	all, except those listed in the default list for HPACMimeCache	Removes mime types from the list of mime types the server can cache. Note: If the list takes several lines, the newline character should be escaped on all but the last line.

Parameter	Argument	Default	Description
HPACRedirectURL	[http://]**host [:port]**	N/A	Sets the URL of an alternate site where rejected requests can be redirected. Note: the alternate site should be a mirror of the site that redirected the request, otherwise redirection will not work.
HPACRejectPagePath	file path	N/A	Sets the path of the file containing the document to be displayed when a request is rejected and the rejection policy is *rejectpage*. The path can be absolute or relative to the web server root.
HPACRejectedExclusionTime	n > 0 (integer)	300	Sets the time interval (in seconds) to elapse before a rejected session can be considered again for admission.
HPACRejectionPolicy	defer | reject | rejectpage	reject	Sets the rejection policy. If the policy is *reject* (default), users whose requests are rejected will see the message returned by the server for the HTTP_SERVICE_ UNAVAILABLE code. If the policy is *rejectpage*, the document in the file set by HPACRejectPath is returned. If the policy is *defer*, a deferral page showing the time the user has to wait before gaining access is displayed.
HPACSessionDuration	n >= 0 (integer)	0	Sets the maximum duration (in seconds) of a session. When set to 0 (default), the session never expires.

Parameter	Argument	Default	Description
HPACShareUnits	n > 0 (integer)	1	Sets the number of units of server resources a virtual host is entitled to use. (A unit is calculated as 1.0/total_share_units). This number is used to compute the percentage of the web server's total resources a virtual host is allowed to use. For instance, if the share units assigned to three virtual hosts A, B and C are 1, 2 and 3, then A can use up to 17% of the server's resources (1/6 * 1), B can use up to 33% of the server's resources (1/6 * 2) and C can use up to 50% (1/6 * 3) of the server's resources.
HPACStatsLogfile	file path	*apache_home* `/var/log/hpac.log` | *apache_home* `/logs/hpac.log` (depending on the *apache_home* layout)	Sets the path of the file to which the admission control statistics are logged. The path can be absolute, or relative to the web server root.
HPACStatsLogging	on/off	off	Turns statistics logging on or off.
HPACVHostIsolation	on/off	off	Turns on or off virtual host isolation. When virtual host isolation is on, new sessions belonging to under-represented virtual hosts are admitted at priority level.

HP AdmissionControl Configurable Parameters for the Apache Web Server