

HP-UX NSA HTTP B.11.23.01.01 Release Notes

HP-UX 11i version 2 (11.23)

Edition 1003

Documentation Web Site: <http://www.docs.hp.com>



i n v e n t

Manufacturing Part Number: 5971-4797

October 2003

U.S.A.

© Copyright 2003 Hewlett-Packard Development Company L.P.

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.

U.S. Government License

Proprietary computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Copyright © 2003 Hewlett-Packard Development Company L.P. All rights reserved. Reproduction, adaptation, or translation of this document without prior written permission is prohibited, except as allowed under the copyright laws.

Trademark Notice

UNIX® is a registered trademark of The Open Group.

Intel® and Itanium® are registered trademarks of Intel Corporation.

HP-UX NSA HTTP B.11.23.01.01 Release Notes

Announcement

The HP-UX NSA HTTP B.11.23.01.01 product enables NSA (Network Server Accelerator) functionality for the HTTP protocol on HP-UX 11i version 2 (11.23). NSA HTTP improves Web server performance by maintaining an in-kernel cache of recently accessed web pages. When NSA HTTP is activated, web page requests (HTTP GET requests) are serviced directly from the data cache in the kernel. Serving web pages from the in-kernel cache instead of passing the requests to a user-space application tremendously improves web server performance.

What's in this Version

NSA HTTP B.11.23.01.01 includes the following new features:

- Support for HP-UX 11i version 2 (HP-UX 11.23)
 - Virtual Web server support
 - Optional binary format logging
 - Utility to convert binary format log files to ASCII Common Log Format (CLF), a de facto industry standard used by many Web server vendors
-

NSA HTTP Components

HP-UX NSA HTTP includes the following components:

- Administrative Utility (**nsahttp**)
- Configuration File (**/etc/rc.config.d/nsahttpconf**)
- Startup Script (**/sbin/init.d/nsahttp**)
- Dynamically Loadable Kernel Module (DLKM, **nsad**)

Administrative Utility (**nsahttp**)

HP-UX NSA HTTP provides the **nsahttp** administrative utility. This utility can display statistics about NSA HTTP performance, list the TCP ports registered to use NSA HTTP, and display other configuration and statistical information. This includes:

- The total number of TCP connection requests received for the registered NSA HTTP ports.
 - The number of HTTP cache hits, which corresponds to the number of HTTP GET requests that NSA HTTP serviced from its cache.
 - The number of HTTP cache misses, which corresponds to the number of HTTP GET requests that NSA HTTP could not service from its cache.
 - The current size of the HTTP cache in bytes.
-

You can also use the `nsahttp` utility to configure operating settings for the NSA HTTP service, including the following items:

- TCP port number for NSA registration and deregistration
- maximum system memory usage for the URI data cache
- idle HTTP TCP connection timeout value
- NSA HTTP cache entry timeout
- maximum URI data size (maximum web page size) that can be cached by the NSA HTTP service
- HTTP access logging options
 - access logging enabled or disabled
 - ASCII or binary log file format
 - log file location
- statistics collection
- debug level for event logging

You can also use `nsahttp` to convert binary HTTP access log files to ASCII Common Log Format (CLF), a de facto industry standard used by many log servers.

Configuration File

The `/etc/rc.config.d/nsahttpconf` configuration file stores NSA HTTP configuration information to be used at system startup time and each time NSA HTTP is activated. NSA HTTP can be enabled or disabled automatically at system startup depending on the setting of the `NSAHTTP_ENABLE` flag in the `/etc/rc.config.d/nsahttpconf` file. In addition, the `/etc/rc.config.d/nsahttpconf` file contains all/any NSA HTTP settings to be used in conjunction with the NSA HTTP startup script.

When delivered with NSA HTTP product, the `/etc/rc.config.d/nsahttpconf` file contains default values for all NSA HTTP options. If an option is not set in the `/etc/rc.config.d/nsahttpconf` file, NSA HTTP will use the default value, as listed in the *nsahttp* (1) man page.

For details on configuring `/etc/rc.config.d/nsahttpconf`, refer to the *nsahttp* (1) man page.

NSA HTTP Components

Startup Script

The `/sbin/init.d/nsahttp` file is the startup script used to activate NSA HTTP at system startup time. The system will activate NSA HTTP at system startup time if the `NSAHTTP_ENABLE` flag is set to 1 in the NSA HTTP configuration file (`/etc/rc.config.d/nsahttpconf`).

NOTE Do not modify the `/sbin/init.d/nsahttp` script file. This file is delivered with the product and may be replaced in future product releases.

DLKM

NSA HTTP includes a DLKM, `nsamod`. The `nsamod` DLKM is used to spawn an NSA HTTP service daemon, `nsad`. An `nsad` daemon is activated for every socket listening on the TCP port registered with NSA HTTP. If logging is enabled, `nsad` logs HTTP access events to the log file, which by default is `/var/nsa/nsahttp_log.pid` where `pid` corresponds to the process ID of the `nsad` process. The `nsad` kernel daemon is also used to establish TCP connections for NSA HTTP registered TCP ports and servicing cache requests.

System Requirements

Hardware Requirements

HP-UX Integrity system (Intel® Itanium®-based system).

OS Platform and Version Compatibility

HP-UX 11i version 2 (B.11.23).

Software Requirements

The system must have standard HP-UX 11i version 2 core products.

HP-UX NSA HTTP B.11.23.01.01. You can obtain HP-UX NSA HTTP B.11.23.01.01 from the HP Software Depot at <http://software.hp.com>. Specify NSA HTTP Release Depot for HP-UX 11i version 2.

Other Requirements

None.

Disk Space Required for Installation

This product requires approximately 500 Kbytes of disk space.

Installing, Activating and Configuring NSA HTTP

This section contains procedures for installing and activating HP-UX NSA HTTP B.11.23.01.01. For information on deactivating and deinstalling HP-UX NSA HTTP, refer to “Deactivating and Deinstalling NSA HTTP” on page 10.

Installing NSA HTTP

1. Go to the HP Software Depot website, www.software.hp.com. Search for the Network Server Accelerator product using the keyword NSAHTTP. Select HP-UX 11i version 2 for the Software Specification.

2. Download the depot to a local directory, such as /tmp. The depot name is NSAHTTP-IPF.depot.

3. Install HP-UX NSA HTTP with the swinstall utility by executing the following command:

```
swinstall -s absolute_path_of_depot NSAHTTP
```

For example:

```
swinstall -s /tmp/NSAHTTP-IPF.depot NSAHTTP
```

4. Verify that the HP-UX NSA HTTP software is installed by executing the following command:

```
swlist | grep NSAHTTP
```

The output should show the following message:

```
NSAHTTP B.11.23.01.01 NSA HTTP Bundle for HP-UX 11i version 2
```

5. Verify that the DLKM module delivered with HP-UX NSA HTTP (nsamod) is installed and loaded by executing the following command:

```
kcmodule -q nsamod -P state
```

The output should show the following message:

```
state loaded
```

Activating NSA HTTP

1. Verify the settings in the NSA HTTP configuration file, /etc/rc.config.d/nsahttpconf. This configuration file is delivered with the default settings for NSA HTTP. By default, this file configures TCP port 80 (the IANA registered port number for WWW HTTP) to be registered for NSA HTTP.

Edit the /etc/rc.config.d/nsahttpconf file, if needed.

2. Execute the following command to register the TCP port(s) specified in the /etc/rc.config.d/nsahttpconf file:

```
/sbin/init.d/nsahttp start
```

3. Stop the Web server (such as the Apache Web server) you want to use with the NSA HTTP service.
4. Restart the Web server you want to use with the NSA HTTP service.
5. Once the Web server is restarted, there will be one `nsad` kernel daemon for each socket listening on a port registered with NSA HTTP. You can verify this with the following command:

```
ps -ef | grep nsad | grep -v grep
```

Activating NSA HTTP at System Startup

1. Configure the `/etc/rc.config.d/nsahttpconf` with the operating parameters for the NSA HTTP service or use NSA HTTP default values.
2. Set the `NSAHTTP_ENABLE` flag to 1 in the `/etc/rc.config.d/nsahttpconf` file. This causes the system to activate NSA HTTP automatically at system startup time. (This is the default behavior of NSA HTTP, so unless the setting of `NSAHTTP_ENABLE` has been previously altered, no action is required.) The entry will be:

```
NSAHTTP_ENABLE=1
```

Deactivating and Deinstalling NSA HTTP

This section contains procedures for deactivating and deinstalling HP-UX NSA HTTP.

Deactivating NSA HTTP

1. Stop the Web server being used with the NSA HTTP service.
2. Deregister the NSA HTTP application port used by the web server (the default port number is 80, or otherwise configured in `/etc/rc.config.d/nsahttpconf`):

```
nsahttp -D -p port_num
```

3. Restart the Web server.

Deinstalling NSA HTTP

Follow the procedure listed below to deinstall NSA HTTP.

NOTE Although the NSA HTTP kernel module, `nsamod`, is a DLKM, there are cases when deinstalling NSA HTTP on a system where the Web server was serving a local Web client may cause the `swremove` utility to reboot the system. For more information, refer to “Known Problems and Workarounds” on page 11.

1. Stop the Web server being used with the NSA HTTP service.
 2. Deregister the NSA HTTP application port used by the web server (the default port number is 80, or otherwise configured in `/etc/rc.config.d/nsahttpconf`):
- ```
nsahttp -D -p port_num
```
3. Restart the Web server.
  4. If you want to retain any NSA HTTP log files in the `/var/nsa` directory, copy the files to a backup medium or move them to another directory, such as `/tmp`. Removing the NSA HTTP product in the next step will also remove the `/var/nsa` directory.
  5. Remove the NSA HTTP product by executing the following command:

```
swremove -x autoreboot=true NSAHTTP
```

The `swremove` utility requires the `-x autoreboot=true` option because the NSA HTTP product includes a DLKM (`nsamod`), and it cannot determine if a reboot is required at the time you issue the `swremove` command. In most cases, no reboot is necessary.

---

## Limitations

NSA HTTP cache size management is not currently integrated with file system buffer cache management. If the NSA HTTP product is installed, HP suggests that you verify and possibly decrease the size of the file system buffer cache.

By default, the NSA HTTP maximum cache size percentage is 50 (50% of available system memory). If the NSA HTTP maximum cache size percentage plus the minimum file system buffer cache percentage (`dbc_min_pct`) is 100 percent or more, it is possible to have all of system memory used for the NSA HTTP and file system caches. This will cause system performance to degrade. The default value for `dbc_min_pct` is 5 (5%).

You can change the NSA HTTP maximum cache size percentage by editing `/etc/rc.config.d/nsahttpconf` or using the `nsahttp` command. To change the file system buffer cache values, set the `dbc_min_pct` and `dbc_max_pct` system parameters with the `kctune` command. For more information, refer to the *ktune* (1M) man page.

---

## Known Problems and Workarounds

If both the Web server and the Web client are running on the same system, the NSA HTTP module, `nsamod`, may be busy even when no Web server is running. This condition may happen if the Web client sends an HTTP GET request but does not immediately retrieve the reply. In this case, `nsamod` will remain “busy” until the Web client reads the reply (for example, by completing a `recv()` request).

This behavior has no side effects unless you try to deinstall the NSA HTTP product while there is an un-read HTTP GET reply for a local Web client. Deinstalling the NSA HTTP product when the `nsamod` module is busy will cause the system to reboot.

To avoid a system reboot, execute the following command after deregistering the NSA HTTP ports (step 2 of the deinstallation process):

```
kcmodule nsamod=unused
```

If the above command successfully completes, you can use `swremove` to remove the NSA HTTP product without causing `swremove` to reboot the system.

## Documentation

If the above `kmodule` command is not successful and you still want to deinstall the NSA HTTP product, wait until all local Web clients have completed their transactions with the local Web servers. Terminate any local Web clients that are unable to complete transactions with local Web servers. Repeat the deinstallation procedure.

---

## Documentation

For usage information, refer to the *nsahttp* (1) man page. You can also get additional information from <http://docs.hp.com> under “Internet and Security Solutions.”