# Enhancing System Performance Using Clock Synchronization and Web Caching in Oracle Solaris 11.3

**Part No: E57652**
November 2016

ORACLE

Enhancing System Performance Using Clock Synchronization and Web Caching in Oracle Solaris 11.3

**Part No: E57652**



**Documentation Accessibility**

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

**Access to Oracle Support**

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

**Référence: E57652**



**Accessibilité de la documentation**

Pour plus d'informations sur l'engagement d'Oracle pour l'accessibilité à la documentation, visitez le site Web Oracle Accessibility Program, à l'adresse `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

**Accès aux services de support Oracle**

Les clients Oracle qui ont souscrit un contrat de support ont accès au support électronique via My Oracle Support. Pour plus d'informations, visitez le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` ou le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` si vous êtes malentendant.

# Contents

# Using This Documentation

- **Overview** – Describes how to use the clock synchronization and web caching services to enhance system performance.
- **Audience** – Technicians, system administrators, and authorized service providers
- **Required knowledge** – Basic and some advanced network administration skills.

## Product Documentation Library

Documentation and resources for this product and related products are available at http://www.oracle.com/pls/topic/lookup?ctx=E53394.

## Feedback

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

♦ ♦ ♦ CHAPTER 1

# Introduction to Clock Synchronization and Web Caching

This chapter provides an overview about clock synchronization and web caching services. It covers the following topics:



## Overview of Clock Synchronization

Clock synchronization software synchronizes time across multiple systems in a network. Oracle Solaris uses the Network Time Protocol (NTP) and the Precision Time Protocol (PTP) to synchronize the system clock. You can also use the `rdate` command while using the `cron` utility to synchronize system clocks.

You must not run NTP and PTP on the same system simultaneously. Also, you must configure only a single instance of the NTP or PTP service on a system.

---

**Note -** Do not use the `rdate`, `ntpdate`, or `date` command to set the date and time while NTP is running. However, you can run the `ntpdate` command with the `-q` and `-d` options as it does not set the time.

---

### Network Time Protocol Overview

NTP is an open source software from the University of Delaware that is included in the Oracle Solaris software. The `ntpd` daemon sets and maintains the system time of day. The `ntpd` daemon is a complete implementation of the version 4 standard as defined by RFC 5905. You can use the `svc:/network/ntp:default` service to start the `ntpd` daemon.

The `ntpd` daemon reads the `/etc/inet/ntp.conf` file at system startup. See the `ntp.conf`(4) man page for information about configuration options. Sample `ntp.conf` files are available at `/etc/inet/ntp.server` and `/etc/inet/ntp.client` on a system.

Note the following when using NTP in your network:

- The `ntpd` daemon uses minimal system resources.
- An NTP client synchronizes automatically with an NTP server when it boots. If the NTP client becomes unsynchronized, the client resynchronizes again when the client contacts a time server.
- If you use the NTP service on a virtualized SPARC system, you must run the NTP service in the global zone, logical domain, control domain, and kernel zone.
- You cannot run the NTP service on both global zone and non-global zone at the same time.
- By default, you cannot run the NTP service on a non-global zone because a non-global zone does not have sufficient privileges. However, if the NTP service is not running on the global zone, you can configure a non-global zone with the privileges required to run the NTP service.
- Avoid configuring exactly two NTP servers as this might lead to clock hopping.
- You must use only one NTP server to set the system time and keep it correct. However, for setting system time accurately, you can use a minimum of four NTP servers.
- Use local reference clock only when necessary.

Additional documentation for the NTP service is available at `/usr/share/doc/ntp/index.html` on a system running the Oracle Solaris 11 release.

For information about procedures for administering NTP, see "Managing the Network Time Protocol" on page 17. For instructions about installing NTP while configuring OpenStack on Oracle Solaris, see "How to Install and Configure Network Time Protocol" in *Installing and Configuring OpenStack (Havana) in Oracle Solaris*.

## Required Files for NTP

The NTP service requires the files listed in the following table.

**TABLE 1** Required NTP Files

| File Name | Function |
|---|---|
| `/etc/inet/ntp.client` | Sample configuration file for NTP clients and servers. |
| `/etc/inet/ntp.conf` | Lists configuration options for NTP. |
| `/etc/inet/ntp.keys` | Contains the NTP authentication keys.<br>**Note -** This is an optional file and is not delivered by the NTP package. |
| `/etc/inet/ntp.leap` | Leap seconds configuration file. This is an optional file and is not delivered by the NTP package.<br>**Note -** This is an optional file and is not delivered by the NTP package. |
| `/etc/inet/ntp.server` | Contains additional configuration instructions for some NTP servers. |
| `/usr/lib/inet/ntpd` | NTP daemon. For more information, see the `ntpd(1m)` man page. |
| `/usr/sbin/ntpdate` | Utility to set the local date and time, based on NTP. For more information, see the `ntpdate(1m)` man page. |

| File Name | Function |
|---|---|
| /usr/sbin/ntpdc | NTP query program for the ntpd daemon. For more information, see the ntpdc(1m)man page. |
| /usr/sbin/ntpq | NTP query program. For more information, see the ntpq(1m) man page. |
| /usr/sbin/ntptime | Program to display or set the kernel time variables. For more information, see the ntptime(1m) man page. |
| /usr/sbin/ntptrace | Program to trace NTP hosts back to the master NTP server. For more information, see the ntptrace(1m) man page. |
| /usr/sbin/ntp-keygen | Program used to generate public and private keys for NTP. For more information, see the ntp-keygen(1m) man page. |
| /var/ntp/ntpstats | Directory for holding NTP statistics. |
| /var/ntp/ntp.drift | Sets the initial frequency offset on NTP servers. |

# Precision Time Protocol Overview

The PTP software synchronizes system time across multiple systems in a broadcast domain, such as a local area network (LAN). Oracle Solaris PTP software is implemented as the ptpd daemon, which is based on the public domain software available at https://github.com/ptpd/ptpd. It implements PTP Version 2 as defined in the IEEE standard 1588-2008.

The ptpd daemon can use the hardware assistance capability provided by any compatible Network Interface Card (NIC) and its driver to timestamp the PTP packets.

You can use the svc:/network/ptp:default service to start the ptpd daemon. You can configure a system as a PTP slave or a PTP master.

- **PTP slave** – Runs the ptpd daemon in slave mode. A PTP slave synchronizes the system clock to a master clock present in the subnet.
- **PTP master** – Runs the ptpd daemon in master mode. Other systems in the slave mode can synchronize their clock to the PTP master.

The state of the ptpd daemon can be slave, master, or initializing.

By default, the service management facility starts the PTP service as a slave and binds the PTP service to the first interface that is up and running. For more information about the Service Management Facility, see the smf(5) man page.

The ptpd daemon uses the /var/log/ptp.log file to record the following information:

- Timestamp of the PTP log entry
- State of the ptpd daemon
- Clock ID

For task information, refer to “Managing the Precision Time Protocol” on page 18.

# Overview of Network Cache and Accelerator

The Network Cache and Accelerator (NCA) increases web server performance by maintaining an in-kernel cache of web pages that are accessed during HTTP requests. This in-kernel cache uses system memory to significantly increase performance for HTTP requests that are normally handled by web servers. Using system memory to hold web pages for HTTP requests increases web server performance by reducing the overhead between the kernel and the web server. NCA provides a sockets interface through which any web server can communicate with NCA with minimal modifications.

In situations where the requested page is retrieved from the in-kernel cache (cache hit), performance improves dramatically. In situations where the requested page is not in the cache (cache miss) and must be retrieved from the web server, performance is also significantly improved.

This product is intended to be run on a dedicated web server. If you run other large processes on a server that runs NCA, problems can result.

NCA logs all cache hits. This log is stored in binary format to increase performance. The `ncab2clf` command can be used to convert the log from binary format to common log format (CLF).

The Oracle Solaris release includes the following enhancements:

- Sockets interface.
- Support for vectored sendfile, which provides support for AF_NCA. See the `sendfilev`(3EXT) man page for more information.
- New options for the `ncab2clf` command that support the ability to skip records before a selected date (`-s`) and to process a specified number of records (`-n`).
- `logd_path_name` in `ncalogd.conf` can specify either a raw device, a file, or a combination of the two.
- Support for a web server to open multiple AF_NCA sockets. With multiple sockets, you can have different web servers that run on one server.
- A new configuration file, `/etc/nca/ncaport.conf`, to manage the IP addresses and ports that NCA uses. If web server does not provide native support for the AF_NCA socket, use this file and the NCA socket utility library to convert an AF_INET socket to an AF_NCA socket.

For task information on managing and administering web cache servers, refer to “Managing Web Cache Servers Task Map” on page 23 and “Administering the Caching of Web Pages” on page 25.

# NCA Architecture

The NCA feature includes the following components.

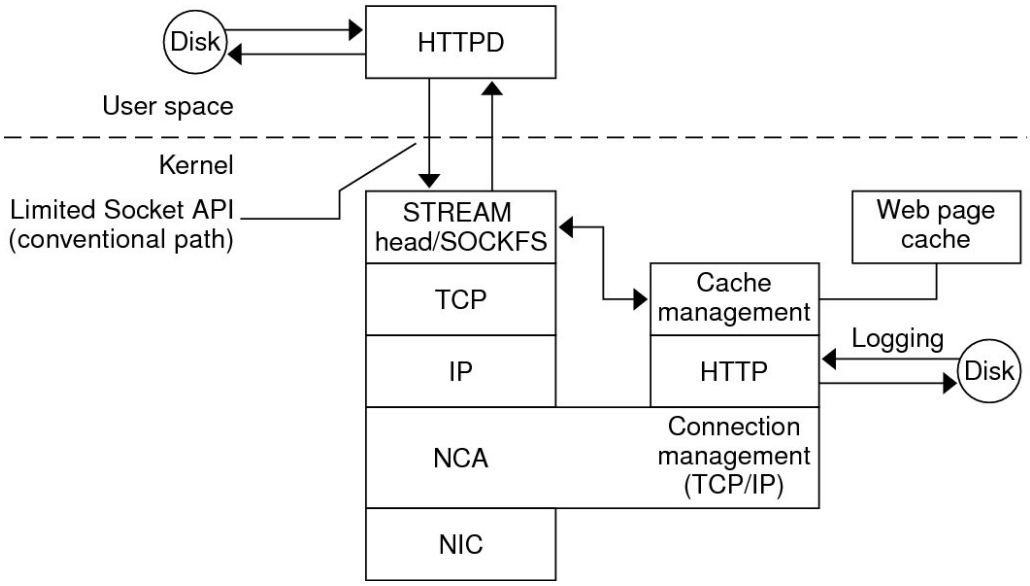
- Kernel module, `ncakmod`
- Web server, `httpd`

The kernel module `ncakmod` maintains the cache of web pages in system memory. The module communicates with a web server, `httpd`, through a sockets interface. The family type is PF_NCA.

The kernel module also provides a logging facility that logs all HTTP cache hits. NCA logging writes HTTP data to the disk in binary format. NCA provides a conversion utility for converting binary log files to common log format (CLF).

The following figure shows the flow of data for the conventional path and the path that is used when NCA is enabled.

**FIGURE 1** Data Flow With the NCA Service




## NCA to Httpd Request Flow

The request flow between the client and the web server proceeds as follows:

1. An HTTP request is made from the client to the web server.
2. If the page is in cache, the in-kernel cache web page is returned.
3. If the page is not in cache, the request goes to the web server to retrieve or update the page.
4. Whether the page is cached depends on the HTTP protocol semantics that are used in the response, or not. If the Pragma: No-cache header is included in the HTTP request, the page is not cached.
5. The page is returned to the client

# Required Files for NCA

The following table lists the files that are necessary to support the NCA feature. Many of these files are ASCII, but some of the files are binary.

**TABLE 2** NCA Files

| File Name | Function |
|---|---|
| `/dev/nca` | Path name for the NCA device. |
| `/etc/hostname.*` | File that lists all physical interfaces that are configured on the server. |
| `/etc/hosts` | File that lists all host names that are associated with the server. Entries in this file must match entries in `/etc/hostname.*` files for NCA to function. |
| `/etc/init.d/ncakmod` | Script that starts the NCA server. This script is run when a server is booted. |
| `/etc/init.d/ncalogd` | Script that starts NCA logging. This script is run when a server is booted. |
| `/etc/nca/nca.if` | File that lists the interfaces on which NCA is run. See the `nca.if(4)` man page for more information. |
| `/etc/nca/ncakmod.conf` | File that lists configuration parameters for NCA. See the `ncakmod.conf(4)` man page for more information. |
| `/etc/nca/ncalogd.conf` | File that lists configuration parameters for NCA logging. See the `ncalogd.conf(4)` man page for more information. |
| `/etc/nca/ncaport.conf` | File that lists the IP addresses and the ports for NCA. See the `ncaport.conf(4)` man page for more information. |
| `/system/volatile/nca_httpd_1.door` | Door path name. |
| `/usr/bin/ncab2clf` | Command that is used to convert data in the log file to the common log format. See the `ncab2clf(1)` man page for more information. |
| `/usr/lib/net/ncaconfd` | Command that is used to configure NCA to run on multiple interfaces during boot. See the `ncaconfd(1M)` man page for more information. |
| `/usr/lib/nca_addr.so` | Library that uses AF_NCA sockets instead of AF_INET sockets. This library must be used on web servers that |

| File Name | Function |
| --- | --- |
| | use AF_INET sockets. See the ncad_addr(4) man page for more information. |
| /var/nca/log | File that holds the log file data. The file is in binary format, so do not edit it. |

♦ ♦ ♦ CHAPTER 2

# Managing Clock Synchronization

Many databases and authentication services require system clocks to be kept synchronized within a network. This chapter covers the following related topics:



## Managing the Network Time Protocol

The procedures in this section describe how to set up and use the NTP service. You can set up a Oracle Solaris system as an NTP server or an NTP client.

### ▼ How to Set Up NTP on a Oracle Solaris System

1. **Become an administrator.**

   For more information, see "Using Your Assigned Administrative Rights" in *Securing Users and Processes in Oracle Solaris 11.3*.

2. **Copy the `ntp.client` file to use as a template for the `ntp.conf` file.**

   ```
   # cd /etc/inet
   # cp ntp.client ntp.conf
   ```

3. **Make site-specific changes to the `ntp.conf` file as needed.**

4. **(Server-only) Add information from the `ntp.server` file to the `ntp.conf` file.**

5. **Start the `ntpd` daemon.**

   ```
   # svcadm enable ntp
   ```

### ▼ How to Enable NTP Logging

1. **Become an administrator.**

   For more information, see "Using Your Assigned Administrative Rights" in *Securing Users and Processes in Oracle Solaris 11.3*.

2. **Enable logging.**

   ```
   # svccfg -s svc:/network/ntp:default setprop config/verbose_logging = true
   ```

   See the `svccfg`(1M) man page for more information.

3. **Update the SMF repository and restart the service.**

   ```
   # svcadm refresh svc:/network/ntp:default
   # svcadm restart svc:/network/ntp:default
   ```

4. **Verify that logging has been enabled.**

   ```
   # svcprop -p config/verbose_logging svc:/network/ntp:default
   true
   ```

### ▼ How to Display the SMF Properties Associated With the NTP Service

- **List the SMF properties by using the `svcprop` command.**

  - To list all of the properties associated with the NTP service:

    ```
    # svcprop svc:/network/ntp:default
    ```

  - To list all of the properties in the `config` property group:

    ```
    # svcprop -p config svc:/network/ntp:default
    ```

## Managing the Precision Time Protocol

You can use the PTP service, `svc:/network/ptp:default`, to set up an interface as a PTP master or a PTP slave. The procedures in this section describe how to set up the PTP service for clock synchronization.

## How to Install PTP

1. **Become an administrator.**

   For more information, see "Using Your Assigned Administrative Rights" in *Securing Users and Processes in Oracle Solaris 11.3*.

2. **Verify whether the PTP package is installed.**

   ```
   # pkg info ptp
   ```

3. **Install the PTP package if it is not installed.**

   ```
   # pkg install ptp
   ```

## How to Set Up an Interface as a PTP Master

1. **Become an administrator.**

   For more information, see "Using Your Assigned Administrative Rights" in *Securing Users and Processes in Oracle Solaris 11.3*.

2. **Assign a system as the PTP master.**

   ```
   # svccfg -s svc:/network/ptp:default setprop config/node_type=master
   ```

3. **Enable an interface to listen to the PTP packets.**

   ```
   # svccfg -s svc:/network/ptp:default setprop config/listen_ifname=interface-name
   ```

4. **Determine whether the PTP service is enabled by using the `svcs` command.**

   - If the PTP service is not enabled on the master system, enable it.

     ```
     # svcadm enable svc:/network/ptp:default
     ```

   - If the PTP service is already enabled, restart the PTP service.

     ```
     # svcadm restart svc:/network/ptp:default
     ```

## How to Set Up an Interface as a PTP Slave

1. **Become an administrator.**

For more information, see "Using Your Assigned Administrative Rights" in *Securing Users and Processes in Oracle Solaris 11.3*.

2. **Enable an interface to listen to the PTP packets.**

```
# svccfg -s svc:/network/ptp:default setprop config/listen_ifname=interface-name
```

3. **Assign the interface as a PTP slave.**

```
# svccfg -s svc:/network/ptp:default setprop config/node_type=slave
```

4. **Enable the PTP service on the slave system.**

```
# svcadm enable svc:/network/ptp:default
```

## How to Enable PTP Logging

1. **Become an administrator.**

   For more information, see "Using Your Assigned Administrative Rights" in *Securing Users and Processes in Oracle Solaris 11.3*.

2. **Enable PTP logging.**

```
# svccfg -s svc:/network/ptp:default setprop config/enable_logging=true
```

   For more information, see the `svccfg`(1M) man page.

3. **Restart the PTP service.**

```
# svcadm restart svc:/network/ptp:default
```

# Identifying Whether a NIC Provides PTP Hardware Assistance

PTP can use the hardware assistance capability provided by any compatible NIC to improve the clock synchronization accuracy.

To determine whether a NIC provides hardware assistance to the `ptpd` daemon, issue the following command:

```
# dladm show-linkprop -p ptp
```

If the `ptp` property value that is displayed in the `VALUE` field of the output is `1` (one), then the corresponding NIC provides hardware assistance to the `ptpd` daemon.

You can configure the `ptpd` daemon to use the hardware assistance that is provided by a NIC. For more information, see "How to Enable the PTP Service to Use the PTP Hardware in a NIC" on page 21.

**EXAMPLE 1** Displaying the PTP Property of NICs in a System

```
# dladm show-linkprop -p ptp
LINK  PROPERTY PERM VALUE EFFECTIVE DEFAULT POSSIBLE
net1  ptp      r-   0     0         0       --
net2  ptp      r-   0     0         0       --
net0  ptp      r-   0     0         0       --
net3  ptp      r-   0     0         0       --
net6  ptp      r-   0     0         0       --
net7  ptp      r-   0     0         0       --
net4  ptp      r-   1     1         0       --
net5  ptp      r-   0     0         0       --
```

This example displays the `ptp` property value for the interface cards in the system. The integer 1 in the `VALUE` field for `net4` indicates that `net4` can provide hardware assistance to the `ptpd` daemon.

## How to Enable the PTP Service to Use the PTP Hardware in a NIC

1. **Become an administrator.**

   For more information, see "Using Your Assigned Administrative Rights" in *Securing Users and Processes in Oracle Solaris 11.3*.

2. **Ensure that the PTP service is enabled.**

   ```
   # svcs -l  svc:/network/ptp:default
   ```

3. **Check whether any of the NICs support PTP.**

   ```
   # dladm show-linkprop -p ptp
   ```

4. **If a NIC is found, configure the PTP service to use the PTP hardware.**

   ```
   # svccfg -s svc:/network/ptp:default setprop config/use_hw=true
   ```

5. **Restart the PTP service.**

```
# svcadm restart svc:/network/ptp:default
```

# Synchronizing the Date and Time From Another System

The following procedure describes how to update the current time without having to set up NTP.

## ▼ How to Synchronize the Date and Time From Another System

1. **Become an administrator.**

   For more information, see "Using Your Assigned Administrative Rights" in *Securing Users and Processes in Oracle Solaris 11.3*.

2. **Reset the date and time to synchronize with another system.**

   **# rdate** *other-system-name*

3. **Verify that you have reset your system's date correctly by using the `date` command.**

   The output should show a date and time that matches that of the other system.

**Example 2** Synchronizing Date and Time From Another System

This example shows how to use `rdate` to synchronize the date and time of one system with another. In this example, the system `earth`, running several hours behind, is reset to match the date and time of the server `mars`.

```
earth# date
Tue Jun  3 11:08:27 MDT 2014
earth# rdate mars
Tue Jun  3 14:06:37 2014
earth# date
Tue Jun  3 14:06:40 MDT 2014
```

♦ ♦ ♦ CHAPTER 3

# Managing Web Cache Servers

This chapter provides the procedures for using Network Cache and Accelerator in the Oracle Solaris 11 release.



To improve security between two applications, you may want to look at Chapter 3, "Web Servers and the Secure Sockets Layer Protocol" in *Securing the Network in Oracle Solaris 11.3*.

## Managing Web Cache Servers Task Map

The following table describes the tasks that are needed to use NCA.

| Task | Description | For Instructions |
|---|---|---|
| Planning for NCA | A list of issues to be resolved before you enable the use of NCA. | "Planning for NCA" on page 23 |
| Enabling NCA | Steps to enable in-kernel caching of web pages on a web server. | "How to Enable Caching of Web Pages" on page 25 |
| Disabling NCA | Steps to disable in-kernel caching of web pages on a web server. | "How to Disable Caching of Web Pages" on page 27 |
| Administering NCA logging | Steps to enable or disable the NCA logging process. | "How to Enable or Disable NCA Logging" on page 28 |
| Loading the NCA socket library | Steps to use NCA if the AF_NCA socket is not supported. | "Loading the Socket Utility Library for NCA" on page 28 |

## Planning for NCA

This section discusses the issues that need to be resolved before starting the NCA service.

## System Requirements for NCA

To support NCA, the system must meet these requirements:

- 256 Mbytes RAM must be installed.
- The Oracle Solaris release must be installed.
- Support for a web server which has native support for NCA or a web server whose startup script has been modified to use the Socket Utility Library for NCA:
  - Apache web server, ships with the Oracle Solaris release
  - Oracle iPlanet Web Server
  - Zeus web server available from Zeus Technology, `http://www.zeus.com`

This product is intended to be run on a dedicated web server. The running of other large processes on a server that runs NCA can cause problems.

## NCA Logging

You can configure the NCA service to log web activity. Generally, NCA logging should be enabled if the web server logging is enabled.

## Interpositioning Library for Daemon Support of the Door Server

Many web servers use AF_INET sockets. By default, NCA uses AF_NCA sockets. To correct this situation, an interpositioning library is provided. The new library is loaded in front of the standard socket library, `libsocket.so`. The library call `bind()` is interposed by the new library, `ncad_addr.so`. Suppose that the status is enabled in `/etc/nca/ncakmod.conf`. The version of Apache that is included with the Solaris 9 and Solaris 10 release is already set up to call this library. If you are using IWS or Netscape servers, see "Loading the Socket Utility Library for NCA" on page 28 to use the new library.

## Multiple Instance Support

Systems that have NCA installed often need to run multiple instances of a web server. For example, a single system might need to support a web server for outside access as well as web administration. To separate these web servers, you would configure each web server to use a separate port.

# Administering the Caching of Web Pages

This section provides procedures to enable or disable parts of the NCA service.

## ▼ How to Enable Caching of Web Pages

1. **Become an administrator.**

   For more information, see "Using Your Assigned Administrative Rights" in *Securing Users and Processes in Oracle Solaris 11.3*.

2. **Register the interfaces by adding the names of each of the physical interfaces in the `/etc/nca/nca.if` file.**

   See the `nca.if`(4) man page for more information. For example:

   ```
   # cat /etc/nca/nca.if
   hme0
   hme1
   ```

   Each interface must have an accompanying `hostname.`*interface-name* file and an entry in `/etc/hosts` file for the contents of `hostname.`*interface-name*.

   To start the NCA feature on all interfaces, place an asterisk, `*`, in the `nca.if` file.

3. **Enable the `ncakmod` kernel module by Changing the `status` entry in `/etc/nca/ncakmod.conf` to `enabled`.**

   ```
   # cat /etc/nca/ncakmod.conf
   #
   # NCA Kernel Module Configuration File
   #
   status=enabled
   httpd_door_path=/system/volatile/nca_httpd_1.door
   nca_active=disabled
   ```

   See the `ncakmod.conf`(4) man page for more information.

4. **(Optional) Enable NCA logging by changing the `status` entry in `/etc/nca/ncalogd.conf` to `enabled`.**

   Change the `status` entry in `/etc/nca/ncalogd.conf` to `enabled`.

   ```
   # cat /etc/nca/ncalogd.conf
   #
   # NCA Logging Configuration File
   ```

```
#
status=enabled
logd_path_name="/var/nca/log"
logd_file_size=1000000
```

You can change the location of the log file by changing the path that is indicated by the `logd_path_name` entry. The log file can be a raw device or a file. See the `ncalogd.conf`(4) man page for more information about the configuration file.

5. **(Optional) Define ports for multiple instance support by adding the port numbers in the `/etc/nca/ncaport.conf` file.**

   The following example causes NCA to monitor port 80 on all configured IP addresses.

```
# cat /etc/nca/ncaport.conf
#
# NCA Kernel Module Port Configuration File
#
  .
  .
ncaport=*/80
```

6. **For x86 only: Increase the virtual memory size by using the `eeprom` command to set the `kernelbase` of the system.**

```
# eeprom kernelbase=0x90000000
# eeprom kernelbase
kernelbase=0x90000000
```

   The second command verifies that the parameter has been set.

   **Note -** By setting the `kernelbase`, you reduce the amount of virtual memory that user processes can use to less than 3 Gbytes. This restriction means that the system is not ABI compliant. When the system boots, the console displays a message that warns you about noncompliance. Most programs do not actually need the full 3–Gbyte virtual address space. If you have a program that needs more than 3 Gbytes, run the program on a system that does not have NCA enabled.

7. **Reboot the server.**

**Example 3** Using a Raw Device as the NCA Log File

The `logd_path_name` string in `ncalogd.conf` can define a raw device as the place to store the NCA log file. The advantage to using a raw device is that the service can run faster because the overhead in accessing a raw device is less.

The NCA service tests any raw device that is listed in the file to ensure that no file system is in place. This test ensures that no active file systems are accidentally written over.

The following example shows how to prevent this test from finding a file system, run the following command. The example command destroys part of the file system on any disk partition that had been configured as a file system. In this example, `/dev/rdsk/c0t0d0s7` is the raw device that has an old file system in place.

```
# dd if=/dev/zero of=/dev/rdsk/c0t0d0s7 bs=1024 count=1
```

After running the `dd` command, you can then add the raw device to the `ncalogd.conf` file.

```
# cat /etc/nca/ncalogd.conf
#
# NCA Logging Configuration File
#
status=enabled
logd_path_name="/dev/rdsk/c0t0d0s7"
logd_file_size=1000000
```

**Example 4** Using Multiple Files for NCA Logging

The `logd_path_name` string in `ncalogd.conf` can define multiple targets as the place to store the NCA log file. The second file is used when the first file is full. The following example shows how to select to write to the `/var/nca/log` file first and then use a raw partition.

```
# cat /etc/nca/ncalogd.conf
#
# NCA Logging Configuration File
#
status=enabled
logd_path_name="/var/nca/log /dev/rdsk/c0t0d0s7"
logd_file_size=1000000
```

## ▼ How to Disable Caching of Web Pages

1. **Become an administrator.**

   For more information, see "Using Your Assigned Administrative Rights" in *Securing Users and Processes in Oracle Solaris 11.3*.

2. **Disable the `ncakmod` kernel module by changing the `status` entry in `/etc/nca/ncakmod.conf` to `disabled`.**

   ```
   # cat /etc/nca/ncakmod.conf
   # NCA Kernel Module Configuration File
   #
   status=disabled
   httpd_door_path=/system/volatile/nca_httpd_1.door
   nca_active=disabled
   ```

See the ncakmod.conf(4) man page for more information.

3. **Disable NCA logging by changing the `status` entry in `/etc/nca/ncalogd.conf` to `disabled`.**

```
# cat /etc/nca/ncalogd.conf
#
# NCA Logging Configuration File
#
status=disabled
logd_path_name="/var/nca/log"
logd_file_size=1000000
```

See the ncalogd.conf(4) man page for more information.

4. **Reboot the server.**

## How to Enable or Disable NCA Logging

You can set NCA logging after NCA has been enabled. See "How to Enable Caching of Web Pages" on page 25 for more information.

1. **Become an administrator.**

   For more information, see "Using Your Assigned Administrative Rights" in *Securing Users and Processes in Oracle Solaris 11.3*.

2. **Change NCA logging.**

   To permanently disable logging, you need to change the status in `/etc/nca/ncalogd.conf` to `disabled` and reboot the system. See the ncalogd.conf(4) man page for more information.

   - **To disable logging:**

     ```
     # /etc/init.d/ncalogd stop
     ```

   - **To enable logging:**

     ```
     # /etc/init.d/ncalogd start
     ```

## Loading the Socket Utility Library for NCA

Follow this process only if your web server does not provide native support of the AF_NCA socket.

In the startup script for the web server, add a line similar to the following example to cause the library to be preloaded.

```
LD_PRELOAD=/usr/lib/ncad_addr.so /usr/bin/httpd
```

## How to Add a New Port to the NCA Service

1. **Become an administrator.**

   For more information, see "Using Your Assigned Administrative Rights" in *Securing Users and Processes in Oracle Solaris 11.3*.

2. **Add a new port entry to `/etc/nca/ncaport.conf`.**

   The following example adds port `8888` on IP address `192.168.84.71`. See the `ncaport.conf(4)` man page for more information.

```
# cat /etc/nca/ncaport.conf
#
# NCA Kernel Module Port Configuration File
#
  .
  .
ncaport=*/80
ncaport=192.168.84.71/8888
```

3. **Start a new web instance.**

   You must include a web address in the file that contains the NCA port configurations before a web server can use the address for NCA. If the web server is running, it must be restarted after the new address is defined.

# Index

## U



## V



## W