Release Note for the Cisco 4700 Series Application Control Engine Appliance

February 28, 2011

Note The most current Cisco documentation for released products is available on Cisco.com.

Contents

This release note applies to the following software versions for the Cisco 4700 Series Application Control Engine (ACE) appliance:

- A4(1.1)
- A4(1.0)

For information on the ACE appliance features and configuration details, see the ACE documentation located on www.cisco.com at:

http://www.cisco.com/en/US/products/ps7027/tsd_products_support_series_home.html

This release note contains the following sections:

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

New Software Features in Version A4(1.1)

The A4(1.1) software release provides the new features described in the following sections:

Increasing SSL Header Insert Max Header Size to 2048 Bytes

In earlier releases, the maximum size of the SSL header that you can insert is 512 bytes. Per CSCtg72737, in software release A4(1.1), the maximum SSL header that you can insert has been increased to 2048 bytes to accommodate header insert with large SSL certificates. For complete details about header insert, see the Cisco Application Control Engine Module Server Load-Balancing Configuration Guide.

Monitoring and Displaying the Network Processor Buffer Usage

When the ACE is processing very heavy network traffic, the internal buffers of a network processor (NP) may reach their capacity. If this happens, the ACE may become unresponsive and require a manual reload. Per CSCtj84786, CSCtj83501, and CSCtj83515, to set threshold levels for the NP buffers in the active and the standby ACEs and cause the active ACE to reboot if the thresholds are reached or exceeded, use the **buffer threshold** command in configuration mode in the Admin context. The ACE checks the status of NP buffer usage every five seconds to initiate the reload action if the buffer threshold is configured and reached, and to generate syslogs if necessary. If the buffer threshold command is configured and if the NP buffer usage reaches or exceeds the threshold, the ACE reloads.

In a redundant configuration, a switchover occurs and the former standby ACE becomes the active ACE. In the absence of this command, the automatic reload feature is disabled. You can also use this command in a stand-alone ACE. The syntax of this command is:

buffer threshold active *number1* **standby** *number2* **action reload**

The keywords and arguments are:

- **active** *number1*—Specifies the buffer threshold for the active redundant ACE or stand-alone ACE as a percentage. Enter 50, 75, 88, 95, or 100. There is no default value. In a redundant configuration, if the buffer usage of any NP reaches or exceeds the threshold and each of the NP's buffer usage in the standby ACE is below the configured standby threshold, the active ACE reboots and a switchover occurs. For a standalone ACE, if any of the NP's buffer usage exceeds the active value, then the ACE reboots.
- **standby** *number2*—Specifies the buffer threshold for the standby redundant ACE. Enter 10, 20, 30, 40, or 50. There is no default value. In a redundant configuration, if the active ACE buffer usage reaches or exceeds the configured active threshold and the standby ACE buffer usage reaches or exceeds the standby threshold, the active ACE does not reboot and no switchover occurs. For a reload and a switchover to occur, the standby buffer usage of all NPs must be less than the configured standby threshold value.
- **action reload**—Specifies that the ACE reloads when the buffer utilization exceeds the configured threshold. In a redundant configuration, a switchover occurs upon reload of the active ACE.

For example, to specify the active NP buffer utilization threshold as 88 percent and the standby NP buffer utilization threshold as 40 percent, enter the following command:

```
host1/Admin(config)# buffer threshold active 88 standby 40 action reload
```

Displaying the NP Buffer Usage

You can display the buffer usage of each NP by using the show np number buffer usage command in Exec mode. The syntax of this command is:

show np *number* **buffer usage**

The *number* value specifies the number of the NP for which you want to display buffer usage statistics. Enter 1.

Table 1 describes the fields in the **show np buffer usage** command output when the buffer threshold command is configured.

Table 1 Output Fields of the show np buffer usage Command

Field	Description
Total Internal Buffer	Total initial internal buffer space in bytes.
Internal Buffer Used	Amount of used buffer space in bytes.
Percentage of Buffer Used	Amount of used buffer expressed as a percentage of the total initial buffer space.

Table 1 Output Fields of the show np buffer usage Command

Field	Description
Automatic reload	Status of the automatic reload feature: • Enabled—**buffer threshold** command is configured • Disabled— **buffer threshold** command is *not* configure.
Active buffer threshold	Configured buffer usage threshold in the active ACE. This field is available only when the **buffer threshold** command is configured.
Standby buffer threshold	Configured buffer usage threshold in the standby ACE. This field is available only when the **buffer threshold** command is configured.

Related Syslogs

The following system log messages (syslogs) are generated when the buffer usage crosses 50 percent, 75 percent, 88 percent, 95 percent, and 100 percent

The following warning syslog is generated when the buffer usage goes above the 50 percent threshold and falls below the 25 percent threshold:

```
%ACE-4-443003:Available NP 1 buffer reached above 75 percent threshold, Total
buffer:155648, Available Buffer:155015.
```

The following warning syslog is generated once when the buffer usage crosses the 50 percent threshold. The subsequent generation of this 50 percent syslog occurs only when the buffer usage goes below 25 percent and again crosses the 50 percent threshold.

```
%ACE-4-443003:Available NP 1 buffer reached below 50 percent threshold, Total buffer:
155648, Available Buffer: 75013
```

The following error syslogs are generated when the NP buffer usage crosses the 75 percent and 88 percent, respectively. The subsequent generation of these syslogs occurs once in five minutes if the same condition persists.

```
%ACE-3-443004:Available NP 1 buffer reached below 25 percent threshold, Total
buffer:155648, Available Buffer:15011
```

The following critical syslogs are generated when the NP buffer usage crosses 95% and 100%, respectively. The subsequent generation of these syslogs is once in 5 minutes if the same condition persists.

```
%ACE-2-443005:Available NP 1 buffer reached below 5 percent threshold, Total
buffer:155648, Available Buffer:7014
```

An alert syslog is generated when the reload action occurs based on the configured **buffer threshold** command as follows:

```
%ACE-1-443006:Available NP %d buffer reached below %d percent threshold, reload started
```

Related SNMP Changes

The ciscoL4L7BufferUtilizationTable was added to CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB. Use the The following SNMP OIDs in the ciscoL4L7BufferUtilizationTable to display the NP buffer usage and percentage of buffer usage:

- crlNetworkProcessor—Index that refers to the network processor number
- crlBufferUsageValue—Absolute buffer usage of an NP
- crlPercentageBufferUsage—Percentage of buffer usage in decimal format to allow historical information to be collected
- crlPercentageBufferUsageDisplay—percentage buffer usage in string format

Clearing TCP Connections in the CLSRST State

Per CSCtk08879, you can clear all TCP connections in a context that are in the CLOSE_RESET (CLSRST) state. Sometimes, these connections may appear to be stuck and do not close after a day or more. To close such connections, use the **clear conn state clsrst** command in Exec mode. The syntax of this command is:

clear conn state clsrst

For example, to clear all connections in the CLSRST state in the current context, enter the following command:

```
host1/Admin# clear conn state clsrst
```

Reserving Admin Context Resources

When you are configuring resource allocations for the ACE, it is possible to allocate 100 percent of the resources to non-Admin contexts. Such resource allocation starves the Admin context of resources so that it is no longer reachable with ICMP, Telnet, SNMP, or SSH, and can cause other issues as well.

Per CSCtf69300, to prevent Admin context resource starvation, the ACE reserves minimum resources for Admin context. The following Admin context reserved resources are displayed in the output of the **show resource usage** command:

Concurrent connections : 100 conns

Management Connections : 100 conns

Throughput Rate : 10 Mbps

Management Traffic rate: 10 Mbps

Connection Rate : 100 conns/sec

The ACE generates the following syslog to warn you when any resource allocation configuration results in less than the guaranteed allocation to the admin context:

```
%ACE-4-504004:Admin context is not guaranteed of one or more resources. Admin context
might get starved of these resources, leading to denial of some of the services.
```

Increasing the Number of Secondary IP Addresses

Per CSCtj96748, the maximum number of secondary IP addresses on a VLAN interface has been increased from 4 to 15. Use the **show interface internal seciptable** command to display the interface manager's view of the secondary addresses under an interface. For complete details about configuring secondary IP addresses, see the *Cisco Application Control Engine Module Routing and Bridging Configuration Guide*.

Configuring a Timeout for CRL Downloads

Prior to this release, if the ACE does not receive the complete certificate revocation list (CRL) in a timely manner from a CRL server or the server does not close the connection, the ACE continues to wait for the data to arrive. While it is waiting for the CRL data, the ACE keeps the socket connection with the server open until the TCP connection with the server is closed because of inactivity. The TCP inactivity timer value could be as large as an hour. There is no way to clear this already established connection with the CRL server even if the static CRL is removed from the configuration.

Per CSCsw73920, you can use the **crypto crl-params timeout** command to configure a CRL data download timeout for static CRLs. This command specifies the maximum wait time for the ACE to retrieve the CRL data from a server. The syntax of this command is as follows:

crypto crl-params *crl_name* **timeout** *number*

The keywords and arguments are:

- *crl_name*—Name of an existing CRL. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
- **timeout** *number*—Specifies the time in seconds that the ACE waits for the CRL data before closing the connection with the server. For static CRLs, enter an integer from 2 to 300. For best-effort CRLs, the timeout is 60 seconds and not user-configurable. If the ACE does not receive the entire CRL data within the timeout limit, the ACE closes the socket connection with the server. For static CRLs, you can abort the CRL data download by removing the static CRL from the configuration.

For example, to configure a 200-second CRL download timeout for CRL1, enter the following command:

host1/Admin(config)# **crypto crl-params CRL1 timeout 200**

When the CRL data download timeout expires and the download is aborted, the ACE generates a syslog to log the event as follows:

```
%ACE-6-253008: CRL crl_name could not be retrieved, reason: crl data dnld timeout error
```

The *crl_name* variable indicates the name of an existing CRL whose download was aborted because the CRL download timeout expired.

Bypassing HTTP Strict Header Parsing

By default, with HTTP 1.1, the ACE performs strict header parsing, which may cause a reset (RST) to be sent to the client and the server when the ACE is unable to parse the encrypted packet over a CONNECT request. This issue is not seen with HTTP 1.0 because the ACE skips the header parsing.

Per CSCtj68302, to prevent a reset from being sent to the client and the server, the ACE bypasses the HTTP parsing after a CONNECT request is received. The ACE uses this pass-through action when there is a match on a **port misuse** configuration with a pass-through action and a CONNECT request.

You can configure this feature in either of the following two ways:

1. Create a Layer 7 class map for tunneling protocols and the policy-map action as pass through using the **passthrough log** command as follows:

   ```
   class-map type http inspect match-any c2
     2 match port-misuse tunneling
   policy-map type inspect http all-match SECURITY
     class c2
       passthrough log
   ```

2. Create a **match** statement for tunneling protocols and the policy-map action as passthrough using the passthrough log command in a Layer 7 inspect policy

   ```
   policy-map type inspect http all-match SECURITY
     match m1 port-misuse tunneling
       passthrough log
   ```

When a CONNECT request matches this action, the HTTP passthrough field is incremented. The ACE also generates a syslog for this feature. For example:

```
%ACE-5-415025: HTTP Tunnel detected -  PortMisuse CONNECT from vlan2534:25.34.1.100/36430
to vlan2634:26.34.1.100/80 Connection 0x9
```

Skipping a Malformed Cookie in an HTTP Flow

Note This feature was originally introduced in software version A3(2.7) with the **cookie-error-ignore** command. In software version A4(1.1) and later, the **cookie-error-ignore** command is deprecated. If you are upgrading from version A3(2.7) and have the **cookie-error-ignore** command in your configuration, you will receive a command exec error during the upgrade process. In a redundant configuration, the standby ACE will remain in the WARM_COMPATIBLE state until you manually change the command configuration to the new syntax that is described below. The functionality of this command has not changed; only the command name has changed.

By default, when the ACE finds a malformed cookie in an HTTP flow, it stops parsing the remaining packets and drops the flow to Layer 4. You can use the **parsing non-strict** command in parameter map HTTP configuration mode to configure the ACE to ignore malformed cookies in a request and continue parsing the remaining packets in the flow. The syntax of this command is as follows:

parsing non-strict

For example, to configure the ACE to ignore a malformed cookie and continue parsing the packets in the flow, enter the following commands:

```
host1/Admin(config)# parameter-map http HTTP_PARAMMAP
host1/Admin(config-parammap-http)# parsing non-strict
```

To reset the ACE behavior to the default of stopping the parsing of packets in a flow when it finds a malformed cookie, enter the following command:

```
host1/Admin(config-parammap-http)# no parsing non-strict
```

Disabling Connection Replication

By default, connection replication is enabled. There may be times when you want to disable it. Per CSCte70082, to disable connection replication, use the **ft connection-sync disable** command in configuration mode in any context. The syntax of this command is:

ft connection-sync disable

Initially, after you disable connection replication, the active ACE does not synchronize connections to the standby ACE. After a bulk sync:

- New connections are not synchronized
- Connections are not updated in a periodic scan
- Connections that are already synchronized on the standby are not torn down

If you enable connection replication after a bulk sync occurs, the ACE takes the following actions:

- New connections are synced immediately
- Existing connections are synced in the next periodic cycle (in approximately 3 to 4 minutes)

Sticky replication is disabled by default and you can configure it on a per sticky group basis. The **replicate sticky** command takes precedence over the **ft connection-sync disable** command, so new client connections can be load balanced to the same server even when connection replication is disabled.

Note the following caveats with stickiness when connection replication is disabled:

- The sticky database is not always in sync on the standby. With connection replication disabled, sticky connections on the active close normally, but on the standby the connections time out according to the idle timeout setting.
- When sticky entries are approaching their expiration time, it is possible to have a zero active-conns-count on the standby and still have active connections on the active ACE. This condition can lead to sticky entries that are not present after a switchover.

For example, to disable connection replication, enter the following command:

```
host1/Admin(config)# ft connection-sync disable
```

To reenable connection replication after you have disabled it, enter the following command:

```
host1/Admin(config)# no ft connection-sync disable
```

Configuring a Probe under a Redirect Server

Per CSCtg31164, You can configure a probe under a redirect server to assess the health of the physical server that is referenced in the probe. When you configure a probe on a redirect server, the ACE considers the state of the real server that is referenced in the probe when it makes a load-balancing decision. You can configure only probes with an IP address in routed mode under a redirect server, redirect server farm, or redirect server under a redirect server farm by using the **ip address** *ip_address* **routed** command. You cannot associate a scripted probe with a redirect server.

The following configuration is an example of configuring a probe under a redirect server:

```
probe tcp t1
  ip address 10.25.25.18 routed
  interval 10
  passdetect interval 10
  open 49
probe tcp t3
  ip address 10.5.55.5 routed
  interval 10
  passdetect interval 10
  open 1
probe tcp t4
  interval 10
  passdetect interval 10
  open 1
rserver redirect r1
  probe t3
  webhost-redirection http://192.168.12.15/index.html 302
  inservice

serverfarm redirect sf1
  probe t3
  rserver r1
    probe t1
    inservice
  rserver r2
    inservice
```

Note When the ACE incrementally synchronizes a probe configuration under a redirect server to an older software release that does not have the ability to probe a redirect server, the configuration is synchronized but the probe remains inactive on the older software version.

If you attempt to add a probe without an IP address in routed mode to a redirect server, the ACE displays the following error message:

```
Error: Only Probe in routed mode can be configured under a redirect server
```

If you try to remove the **ip address** *ip_address* **routed** option from a probe that is associated with a redirect server, the ACE displays the following error message:

```
Error: Cannot remove ip address option from a probe associated with redirect server
```

Retaining Retcode and Inband Health Monitoring Statistics when a Real Server Goes from the Operational to the Inactive State

In software releases prior to software release A4(1.1), when a real server transitions from the OPERATIONAL state to the INACTIVE state because of an ARP failure, a probe failure, and so on, the inband health monitoring counters and the retcode counters are reset as shown by the output of the **show serverfarm** *name* **inband** and s**how serverfarm** *name* **retcode** commands.

Per CSCtf33526, the ACE now retains the retcode and inband health monitoring statistics when a real server transitions from the OPERATIONAL state to the INACTIVE state.

Displaying NP-Related Details in the show serverfarm Command

Per CSCtf55662, you can display the state of a real server on a per network processor (NP) basis by entering the **show serverfarm** *name* **np** command in Exec mode. The syntax of this command is as follows:

show serverfarm *name* **np**

For the *name* argument, enter the name of an existing server farm as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

For example, enter:

```
host1/Admin# show serverfarm sf1 np
```

Table 1 describes the fields in the **show serverfarm** *name* **np** command output when the buffer threshold command is configured.

Table 2 Output Fields of the show serverfarm name np Command

Field	Description
serverfarm	Name of the server farm
type	Server farm type: host or redirect
total rservers	Total number of real servers in the server farm
real	Name and IP address of the real server
NP*n*	Operational state of the real server for the NP. Possible states are: • OPERATIONAL • RETCODE-FAILED • INBAND-FAILED • DISABLED—Control plane failure (for example, PROBE-FAILED or ARP-FAILED) or the real server is OUTOFSERVICE

This output can be useful for checking the state of a real server per NP in case the real server is dropping only some connections.

Displaying and Clearing Specific Sticky Information

Per CSCtg55173, the **show sticky database** and **clear sticky database** commands allows you to display or clear specific sticky information, respectively. Previously, you could display or clear specific sticky information.

For the **show sticky database** command, you can display the following information:

- Entry count totals or additional detail information for all existing and new **show sticky database** commands through the **count** and **detail** options. Note that these options are mutually exclusive.
- IP netmask sticky database entries for specific a source or destination IP address and subnet mask. The syntax of the command is as follows:

  show sticky database [**type**] **ip-netmask source | destination** [**ip** *ip_address* **netmask** *subnet_mask*] [**count | detail**]

- IP netmask sticky database entries for both specific source and destination IP addresses and subnet masks. The syntax of the command is as follows:

  show sticky database [**type**] **ip-netmask both** [**source** *source_ip_address* **netmask** *subnet_mask* **destination** *dest_ip_address* **netmask** *subnet_mask*] [**count | detail**]

- Entries that expire within a specified minimum and maximum range in seconds. The syntax of this command is as follows:

  show sticky database time-to-expire min *seconds* **max** *seconds* [**count | detail**]

  For the *seconds* argument, enter a number from 0 to 3932100.

- Active entries between a connection count. The syntax of this command is as follows:

  show sticky database active-conn-count min *count* **max** *count* [**count | detail**]

  For the *count* argument, enter a number from 0 to 4294967295.

For the **clear sticky database** command, you can clear the following information:

- Active entries between a connection count. The syntax of this command is as follows:

  clear sticky database active-conn-count min *count* **max** *count*

  For the *count* argument, enter a number from 0 to 4294967295.

- Entries that expire within a specified minimum and maximum range in seconds. The syntax of this command is as follows:

  clear sticky database time-to-expire min *seconds* **max** *seconds*

  For the *seconds* argument, enter a number from 0 to 3932100.

- All sticky group types. The syntax of this command is as follows:

  clear sticky database type

- Specified hash key. The syntax of this command is as follows:

  clear sticky database type hash-key *hash_key*

- All sticky entries of type HTTP cookie. The syntax of this command is as follows:

  clear sticky database type http-cookie

- Entries with a specific source or destination IP address and subnet mask. The syntax of this command is as follows:

  clear sticky database [**type**] **ip-netmask source | destination** [**ip** *ip_address* **netmask** *subnet_mask*]

- Entries with a specific source and destination IP addresses and subnet masks. The syntax of this command is as follows:

  clear sticky database [**type**] **ip-netmask both** [**source** *source_ip_address* **netmask** *subnet_mask* **destination** *dest_ip_address* **netmask** *subnet_mask*]

Displaying the Hit Count for a Sticky Entry

The s**how sticky database detail** command now includes the sticky-hit-count field to display the total number of times that a sticky entry is hit. Previously, the only way determine whether the sticky entry was refreshed was to check the timer. However, it did not provide the exact number of times that the entry was hit.

Displaying the Current and Total Sticky Connection to a Real Server

Per CSCtj23462, the new sticky-conns field in the output of the **show serverfarm detail** command displays the current and total connections stuck to each real server due to sticky. Previously, the ACE displayed only the total number of active connections and total connections for every real server.

Checking the Syntax of Generated XML Output

Per CSCtj93478, the XML agent on the ACE checks the XML output that the ACE generates before sending it to the client. If the output contains incorrect syntax including unsupported characters, the agent displays the following error message:

```
Generated XML was not well-formed.  Possible workaround: retry XML request using text mode
response instead.
```

Displaying Appliance Hardware and Operating Environment Information

Per CSCti64505, the **show environment** [**temperature**] command displays the information for the ACE appliance hardware and operating environment. In software version A3(2.2), this command was disabled.

The fields for this command include the following:

- CPU Temp
- Ambient Temp
- RTC Battery

- CPU Fan
- DIMM Fan
- PCI Fan

Filtering the Running Configuration Based on the Name of the Object

Per CSCtj11147, the **show running-config** command has a new *name* option to filter the running-config file based on the name of the object. The syntax of this command is as follows:

show running-config *object* [*name*]

For example:

```
host1/Admin# show running-config rserver rs1
host1/Admin# show running-config serverfarm sf1
```

New Network Processor Hardware Interrupt Syslog in Version A4(1.1)

The ACE generates a syslog when a network processor (NP) fatal hardware interrupt error occurs. The format of the syslog is as follows:

%ACE-2-199009: NP Fatal Error: *error_text* detected, Contact Cisco TAC

The *error_text* variable can be any of the following NP interrupt errors:

- DDR/DRAM LMC0 Double bit error
- System Packet Interface (SPI) Error
- Packet Input Processing (PIP) Error
- L2 Tag ECC SEC/DED error
- L2 Data ECC SEC/DED error
- DDR ECC SEC/DED error
- Packet Order/work unit error (POW)
- Input Packet data unit error (IPD)
- Packet output processing error (PKO)
- Free Pool Unit Error (FPA)
- Input/ Output Busing/Bridging Error
- Key Memory unit error

New Counter for Fragmentation Reassembly Timeout

Per CSCtj59957, a new counter has been added for the fragmentation reassembly timeout. A TCP reassembly timeout can cause a TCP connection to be unexpectedly reset. Prior to software version A4(1.1), there was no way to know that a reassembly timeout was the root cause of a TCP reset because of the lack of a statistic. To display the Reassembly timeouts counter, enter the following command:

```
host1/Admin# show np 1 me-stats "-s tcp" | inc Reassembly
```

New Software Features in A4(1.0)

The ACE software version A4(1.0) release contains expanded features and functions. The new features include the following:

- Inband health monitoring (see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Guide*)
- SIP logging enhancement (see the *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*)
- Sticky enhancements (see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Guide*)
- Syslog enhancements (see the *Cisco 4700 Series Application Control Engine Appliance System Message Guide*)
- SNMP enhancements (see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*)

Also, the following features provides parity with the ACE module:

- Administration features (see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*):
  - Backup and restore of configuration files, licenses, SSL certificates and keys, and checkpoints
  - Large configuration download optimization
  - SNMP MIB and trap enhancements
- Server load-balancing features (see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Guide*):
  - Reverse IP stickiness
  - Failaction reassign across VLANs
  - Hit count per URI
  - KAL-AP Tags per VIP
- Security features (see the *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*)

  Switch mode (bridged connection timeout)
- SSL features (see the *Cisco 4700 Series Application Control Engine Appliance SSL Configuration Guide*):
  - Bulk import of SSL certificates
  - CRL checking of SSL server certificates
  - HTTP insertion of SSL session, client, and server header information
  - LDAP CRL support
  - Sample SSL certificate and key
  - Ignore authentication failures due to CDP errors
  - SSL redirect on SSL session setup failure
- Secondary IP address support for multiple subnets on the same VLAN (see the *Cisco 4700 Series Application Control Engine Appliance Routing and Bridging Configuration Guide*)

Available ACE Licenses

By default, the ACE supports the following features and capabilities:

- Performance: 1 gigabit per second (Gbps) appliance throughput
- Virtualization: 1 admin context and 5 user contexts
- Secure Sockets Layer (SSL): 1000 transactions per second (TPS)
- Hypertext Transfer Protocol (HTTP) compression: 100 megabits per second (Mbps)
- Application Acceleration: 50 connections

You can increase the performance and operating capabilities of your ACE product by purchasing one of the licensing options.

You can order your ACE product by either of these methods:

- Ordering a license bundle. Each license bundles includes the ACE appliance and a series of software licenses.
- Ordering separate license options.

You must have the Admin role in the Admin context to perform the tasks of installing, removing, and updating the license. You can access the **license** and **show license** commands only in the Admin context.

Table 3 ACE Licensing Bundles

License Model	Description	Upgrade Path
ACE-4710-0.5F-K9	This license bundle includes the following items: • ACE 4710 appliance • 0.5-Gbps throughput license (ACE-AP-500M-LIC) • 100-Mbps compression license (ACE-AP-C-100-LIC) • 100 SSL transactions per second (TPS) license (ACE-AP-SSL-100-K9) • Application acceleration license (50 connections) (ACE-AP-OPT-50-K9)	You have the option to upgrade to the 1-Gbps, 2-Gbps, or 4-Gbps bundle. Start the upgrade with ACE-4710-BUN-UP1=.
ACE-4710-1F-K9	This license bundle includes the following items: • ACE 4710 appliance • 1-Gbps throughput license (ACE-AP-01-LIC) • 500-Mbps compression license (ACE-AP-C-500-LIC) • 5000 SSL TPS license (ACE-AP-SSL-05K-K9) • Application acceleration license (50 connections) (ACE-AP-OPT-50-K9)	You have the option to upgrade to the 2-Gbps or 4-Gbps bundle. Start the upgrade with ACE-4710-BUN-UP2=.

Table 3 ACE Licensing Bundles (continued)

License Model	Description	Upgrade Path
ACE-4710-BAS-2PAK	This license bundle includes the following items: • Two ACE 4710 appliances • 1-Gbps throughput license (ACE-AP-01-LIC) ACE-4710-BAS-2PAK also includes the following default options: • 1000 SSL TPS • 100-Mbps compression • 5 virtual contexts • Application acceleration (50 connections)	You have the option to upgrade to the 2-Gbps or 4-Gbps bundle. Start the upgrade with ACE-4710-BUN-UP2=. Two upgrade licenses are required for upgrading two units of the ACE-4710-BAS-2PAK bundle.
ACE-4710-2F-K9	This license bundle includes the following items: • ACE 4710 appliance • 2-Gbps throughput license (ACE-AP-02-LIC) • 1-Gbps compression license (ACE-AP-C-1000-LIC) • 7500 SSL TPS license (ACE-AP-SSL-07K-K9) • Application acceleration license (50 connections) (ACE-AP-OPT-50-K9)	You have the option to upgrade to the 4-Gbps bundle. Start the upgrade with ACE-4710-BUN-UP3=.
ACE-4710-4F-K9	This license bundle includes the following items: • ACE 4710 appliance • 4-Gbps throughput license (ACE-AP-04-LIC) • 2-Gbps compression license (ACE-AP-C-2000-LIC) • 7500 SSL TPS license (ACE-AP-SSL-07K-K9) • Application acceleration license (50 connections) (ACE-AP-OPT-50-K9)	This is the highest value bundle.
ACE-4710-BUN-UP1	0.5 to 1-Gbps throughput bundle upgrade license	See the Upgrade Path outlined above.
ACE-4710-BUN-UP2	1 to 2-Gbps throughput bundle upgrade license	See the Upgrade Path outlined above.
ACE-4710-BUN-UP3	2 to 4-Gbps throughput bundle upgrade license	See the Upgrade Path outlined above.

Table 4 ACE Licensing Options

Feature	License Model	Description
Performance Throughput	Default	1-Gbps throughput.
	ACE-AP-500M-LIC	0.5-Gbps throughput.
	ACE-AP-01-LIC	1-Gbps throughput.
	ACE-AP-02-LIC	2-Gbps throughput.
	ACE-AP-04-LIC	4-Gbps throughput.
	ACE-AP-02-UP1	Upgrade from 1-Gbps to 2-Gbps throughput.
	ACE-AP-04-UP1	Upgrade from 1-Gbps to 4-Gbps throughput.
	ACE-AP-04-UP2	Upgrade from 2-Gbps to 4-Gbps throughput.
Virtualization	Default	1 admin/5 user contexts.
	ACE-AP-VIRT-020	1 admin/20 user contexts.
SSL	Default	1000 TPS.
	ACE-AP-SSL-05K-K9	5000 TPS.
	ACE-AP-SSL-07K-K9	7500 TPS.
	ACE-AP-SSL-UP1-K9	Upgrade from 5000 TPS to 7500 TPS.
HTTP Compression	Default	100-Mbps.
	ACE-AP-C-500-LIC	500-Mbps.
	ACE-AP-C-1000-LIC	1-Gbps.
	ACE-AP-C-2000-LIC	2-Gbps.
	ACE-AP-C-UP1	Upgrade from 500-Mbps to 1 Gbps.
	ACE-AP-C-UP2	Upgrade from 500-Mbps to 2 Gbps.
	ACE-AP-C-UP3	Upgrade from 1 Gbps to 2 Gbps.
Application Acceleration Feature Pack License	ACE-AP-OPT-LIC-K9	Application acceleration and optimization. By default, the ACE performs up to 50 concurrent connections. With the application acceleration and optimization software feature pack installed, the ACE can provide greater than 50 concurrent connections. This license increases the operating capabilities of the following features: • Delta optimization • Adaptive dynamic caching • FlashForward • Dynamic Etag

ACE demo licenses are available through your Cisco account representative. A demo license is valid for only 60 days. At the end of this period, you must update the demo license with a permanent license to continue to use the ACE software. To view the expiration of a demo license, from the CLI, use the **show license usage** command in Exec mode. If you need to replace the ACE appliance, you can copy and install the licenses onto the replacement appliance.

Ordering an Upgrade License and Generating a Key

This section describes the process that you use to order an upgrade license and to generate a license key for your ACE. To order an upgrade license, follow these steps:

Step 1 Order one of the licenses from the list in the "Available ACE Licenses" section using any of the available Cisco ordering tools on cisco.com.

Step 2 When you receive the Software License Claim Certificate from Cisco, follow the instructions that direct you to the following Cisco.com website:

- If you are a registered user of cisco.com, go to the following location:

  http://www.cisco.com/go/license

- If you are not a registered user of cisco.com, go to the following location:

  http://www.cisco.com/go/license/public

Step 3 Enter the Product Authorization Key (PAK) number found on the Software License Claim Certificate as your proof of purchase.

Step 4 Provide all the requested information to generate a license key. Once the system generates the license key, you will receive a license key e-mail with an attached license file and installation instructions.

Step 5 Save the license key e-mail in a safe place in case you need it in the future (for example, to transfer the license to another ACE).

For information on installing and managing ACE licenses:

- From the ACE appliance CLI, see Chapter 3, Managing ACE Software Licenses, in the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.
- From ACE appliance Device Manager, see Chapter 2, Configuring Virtual Contexts, in the *Cisco 4700 Series Application Control Engine Appliance Device Manager GUI Configuration Guide*.

Performing Software Upgrades and Downgrades

This section describes how to perform software upgrades and downgrades. It contains the following topics:

- Upgrading Your ACE Software in a Redundant Configuration
- Downgrading Your ACE Software in a Redundant Configuration

Upgrading Your ACE Software in a Redundant Configuration

This procedure assumes that your ACE appliances are configured as redundant peers to ensure that there is no disruption to existing connections during the upgrade process. In the following procedure, the active ACE is referred to as ACE-1 and the standby ACE is referred to as ACE-2.

This section includes the following topics:

- Before You Begin
- Upgrade Procedure

Before You Begin

Before you upgrade your ACE software, be sure that your ACE configurations meet the upgrade prerequisites in the following sections:

- Changing the Admin Password
- Changing the www User Password
- Removing the duplex Command from the ACE Configuration
- Removing the Underscore Character from a Hostname
- Creating a Checkpoint
- Copying the Startup Configuration of Each Context

Note To upgrade from software version A1(8a) to A4(1.0), you must first upgrade software version A1(8a) to A3(2.6). Then, upgrade software version A3(2.6) to A4(1.0).

Changing the Admin Password

Before you upgrade to ACE software version A3(1.0) or higher, you **must** change the default Admin password if you have not already done so. Otherwise, after you upgrade the ACE software, you will only be able to log in to the ACE through the console port.

Caution If you do not change the Admin password prior to upgrading to ACE software version A3(1.0) or higher, configuration synchronization may fail and the context may not be in the STANDBY_HOT state.

For details on changing the default Admin password, do one of the following:

- From the CLI, see Chapter 1, Setting Up the ACE, in the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.
- From the Device Manager GUI, see Chapter 1, Overview, in the *Cisco 4700 Series Application Control Engine Appliance Device Manager GUI Configuration Guide*.

Note If your ACE is managed by the Cisco Application Networking Manager (ANM) software, you **must** change the Admin password on the ANM in the Primary Attributes page instead of the ACE CLI. From the ANM, click the **Change Password** button on Primary Attributes page (**Config > Devices > System > Primary Attributes**).

Changing the www User Password

Before you upgrade the ACE software, you **must** change the default www user password if you have not already done so. Otherwise, after you upgrade the ACE software, the www user will be disabled and you will not be able to use Extensible Markup Language (XML) to remotely configure an ACE until you change the default www user password.

For details on changing a user account password, see Chapter 2, Configuring Virtualization, in the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*. In this case, the user would be **www**.

Caution If you do not change the www user password prior to upgrading the ACE software, configuration synchronization may fail and the context may not be in the STANDBY_HOT state.

Removing the duplex Command from the ACE Configuration

As a result of a **duplex** command syntax change between A3(2.1) and A3(2.2) (per CSCta56623), if your ACE configuration includes one or more Gigabit Ethernet ports that are configured for full or half duplex operation, before you upgrade from A3(2.1) to A3(2.2), or A3(2.2) to software version A3(2.3) or later, you must first remove the duplex configuration from the startup-configuration file on both the active ACE and standby (peer) ACE.

Perform the following configuration change on both the active ACE and standby (peer) ACE before you begin the upgrade procedure:

a. Use the **no** form of the **duplex** command in interface configuration mode to remove the duplex configuration from all configured Gigabit Ethernet ports.

b. Save changes from the running-configuration file to the startup-configuration file.

After you complete the upgrade procedure, you can update the duplex settings for the configured Gigabit Ethernet ports using software version A3(2.3) or later. See Chapter 1, Configuring Ethernet Interfaces, in the *Cisco 4700 Series Application Control Engine Appliance Routing and Bridging Configuration Guide.*

Removing the Underscore Character from a Hostname

Before you upgrade the ACE appliance software from A3(2.0) to A4(1.0) as a result of addressing CSCsr90184, the underscore character (_) is no longer allowed in the hostname. As a result of this change, if you do not modify a hostname by removing the underscore character (_), after you perform an upgrade the standby ACE will remain in the STANDBY_COLD state because the configuration cannot synchronize with the illegal character.

Creating a Checkpoint

We strongly recommend that you create a checkpoint of the running-configuration of each context in your ACE. A checkpoint creates a snapshot of your configuration that you can later roll back to in case a problem occurs with an upgrade and you want to downgrade the software to a previous release. Use the **checkpoint create** command in Exec mode in each context for which you want to create a configuration checkpoint and name the checkpoint. For details about creating a checkpoint and rolling back a configuration, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

Copying the Startup Configuration of Each Context

In addition to creating a checkpoint of the running-configuration of each context in your ACE, we also strongly recommend that you copy the startup configuration of each context to either:

- The disk0: file system on your ACE.
- An TFTP, FTP, or SFTP server.

Having a backup of the startup configuration of each context ensures that you can recover your ACE should an issue arise during the upgrade procedure. In that case, you can then downgrade and restore the existing startup configuration to your ACE.

Upgrade Procedure

To upgrade your ACE software in a redundant configuration, follow these steps:

Note Ensure that the preempt command is disabled before the upgrade procedure begins.

Step 1 Log in to both the active and standby ACEs. The Exec mode prompt appears at the CLI. If you are operating in multiple contexts, observe the CLI prompt to verify that you are operating in the Admin context. If necessary, log directly in to, or change to the Admin context.

```
ACE-1/Admin#
```

Step 2 Save the running configurations of every context by entering the **write memory all** command in Exec mode in the Admin context of each ACE.

```
ACE-1/Admin# write memory all
```

Step 3 Create a checkpoint in each context of both ACEs by entering the **checkpoint create** command in Exec mode.

```
ACE-1/Admin# checkpoint create ADMIN_CHECKPOINT
ACE-1/Admin# changeto C1
ACE-1/C1# checkpoint create C1_CHECKPOINT
```

Step 4 Copy the new software image to the image directory of each ACE (active and standby) by entering the **copy ftp**, **copy sftp**, or the **copy tftp** command in Exec mode. For example, to copy the image with the name c4710ace-t1k9-mz.A4_1_0.bin through FTP, enter:

```
ACE-1/Admin# copy ftp://server1/images//c4710ace-t1k9-mz.A4_1_0.bin image:
Enter source filename[/images/c4710ace-t1k9-mz.A4_1_0.bin]?
Enter the destination filename[]? [c4710ace-t1k9-mz.A4_1_0.bin] File already exists, do
you want to overwrite?[y/n]: [y]
Enter hostname for the ftp server[server1]?
Enter username[]? user1
Enter the file transfer mode[bin/ascii]: [bin] Enable Passive mode[Yes/No]: [Yes] no
Password:
```

Step 5 Ensure that the new software image is present on both the active and standby ACEs by entering the **dir** command in Exec mode. For example, enter:

```
ACE-1/Admin# dir image:c4710ace-t1k9-mz.A4_1_0.bin
35913728  Oct 25 2010 01:17:01 c4710ace-t1k9-mz.A4_1_0.bin

          Usage for image: filesystem
                 828182528 bytes total used
                  54165504 bytes free
                 882348032 bytes total
```

Step 6 Verify the current BOOT environment variable and configuration register setting by entering the **show bootvar** command in Exec mode. For example, enter:

```
ACE-1/Admin# show bootvar
BOOT variable = "image:c4710ace-t1k9-mz.A4_1_0.bin"
Configuration register is 0x1
```

Step 7 Remove the existing image from the boot variable on ACE-1 by entering the **no boot system image:***ACE_image* command in configuration mode. For example, to remove the A3(2.1) image, enter:

```
ACE-1/Admin# configure
Enter configuration commands, one per line. End with CNTL/Z.
ACE-1/Admin(config)# no boot system image:c4710ace-t1k9-mz.A3_2_1.bin
```

Step 8 Configure ACE-1 to autoboot from the latest ACE appliance image. To set the boot variable and configuration register to 0x1 (perform auto boot and use startup-config file), use the **boot system image:** and **config-register** commands in configuration mode. For example, enter:

```
ACE-1/Admin(config)# boot system image:c4710ace-t1k9-mz.A4_1_0.bin
ACE-1/Admin(config)# config-register 0x1
ACE-1/Admin(config)# exit
ACE-1/Admin# show bootvar
BOOT variable = "image:c4710ace-t1k9-mz.A4_1_0.bin"
Configuration register is 0x1
```

Step 9 On the standby ACE appliance (ACE-2), perform the following:

- Enter the **show running-config** command and ensure that all the changes made in the active ACE (ACE-1) are also reflected on the standby ACE.
- Enter the **show bootvar** command to verify that the boot variable was synchronized with ACE-1.

Step 10 Verify the state of each ACE by entering the **show ft group detail** command in Exec mode. Upgrade the ACE that has its Admin context in the STANDBY_HOT state (ACE-2) first by entering the **reload** command in Exec mode.

```
ACE-2/Admin# reload
This command will reboot the system
Save configurations for all the contexts. Save? [yes/no]: [yes]
```

After ACE-2 boots up, it may take a few minutes to reach the STANDBY_WARM state again. Configuration synchronization is still enabled and the connections through ACE-1 are still being replicated to ACE-2.

Note We do not recommend that you make any changes to the ACE-1 configuration. At this point in the upgrade procedure with ACE-2 in the STANDBY_WARM state, any incremental commands that you add to the ACE-1 configuration may not be properly synchronized to the ACE-2 configuration. To make any changes to ACE-1, disable incremental sync on ACE-1 and manually synchronize the changes to ACE-2.

Step 11 After the standby ACE reboots, log in and perform the following actions to verify the state of the standby ACE:

- Enter the **show version** command in Exec mode to verify that the appliance has properly rebooted with the latest ACE appliance software image.
- Enter the **show ft group detail** command in Exec mode to verify that the standby ACE has recovered to a STANDBY_HOT state. If the standby ACE is running software release A3(2.2) or later, the state is STANDBY_WARM.

Step 12 Perform a graceful failover of all contexts from ACE-1 to ACE-2 by entering the **ft switchover all** command in Exec mode on ACE-1. ACE-2 becomes the new active ACE and assumes mastership of all active connections with no interruption to existing connections.

```
ACE-1/Admin# ft switchover all
```

Step 13 Upgrade ACE-1 by reloading it. Verify that ACE-1 enters the STANDBY_WARM state (this action may take several minutes) by entering the **show ft group detail** command in Exec mode.

Because the standby ACE has changed its state to either STANDBY_COLD or STANDBY_HOT, the configuration mode is enabled. The configuration is synchronized from ACE 2 (currently active) to ACE-1. If ACE-1 is configured with a higher priority and **preempt** is configured on the FT group, ACE-1 reasserts mastership after it has received all configuration and state information from ACE-2, making ACE-2 the new standby. ACE-1 becomes the active ACE once again.

```
ACE-1/Admin# reload
This command will reboot the system
Save configurations for all the contexts. Save? [yes/no]: [yes]
```

Step 14 Verify that ACE-1 is in the ACTIVE state and ACE-2 is in the STANDBY_WARM state by entering the **show ft group detail** command in Exec mode.

Downgrading Your ACE Software in a Redundant Configuration

If you need to downgrade your ACE software from version A4(1.0) to an earlier ACE software version, use the procedure that follows. This procedure assumes that your ACEs are configured as redundant peers to ensure that there is no disruption to existing connections during the downgrade process. In the following procedure, the active ACE is referred to as ACE-1 and the standby ACE is referred to as ACE-2.

Before You Begin

Note the following considerations before you begin the downgrade process:

- Before you downgrade your ACE software, ensure that the following conditions exist:
  - Identical versions of the previous software image resides in the image: directory of both ACEs.
  - The active ACE has a higher priority than the standby ACE and **preempt** is enabled on the FT group if you want the active ACE to remain active after the downgrade procedure.
- If your ACE includes the 0.5-Gbps bundled license (ACE-4710-0.5F-K9) that is available with software version A3(2.0) or higher, ensure that you first uninstall the 0.5-Gbps bundle prior to downgrading to an earlier ACE software release. The ACE defaults to the 1-Gbps license.

Note If you have installed one of the other available ACE license bundles (see Table 3) or individual upgrade license options (see Table 4) in addition to the 0.5-Gbps bundled license, and you downgrade to an earlier software version without first uninstalling those bundled licenses or individual upgrade licenses, the ACE may not downgrade properly to the original system defaults. In this case, you may observe an inconsistent behavior in the system defaults of the ACE.

- If your ACE includes the 5-to-20 user context upgrade license (ACE-AP-VIRT-020-UP) that is available with software version A3(2.0) or higher, ensure that you first uninstall the 5-to-20 user contexts license prior to downgrading to an earlier ACE software release. The ACE defaults to 1 admin context and 5 user contexts.

Note If your ACE includes more than 5 user contexts configured, when you downgrade to an earlier ACE software release the ACE will default to 1 admin context and 5 user contexts. In this case, the ACE will randomly remove the additional user contexts that have been configured. The ACE will delete the configuration associated with those additional contexts, including SSL certification/keys and scripted probe files.

If this is an issue, we recommend that you copy the start-up configuration file, running-configuration file, and SSL certificate and key pair files of each context prior to uninstalling the 5-to-20 user contexts license.

See the "Copying Files" section of the *Cisco 4700 Series Application Control Engine Appliance Administration Guide* for details on how to use the **copy** command to save configuration files or objects.

See the *Cisco 4700 Series Application Control Engine Appliance SSL Configuration Guide* for details on how to use the **crypto export** command to export SSL certificate and key pair files to a remote FTP, SFTP, or TFTP server.

Downgrade Procedure

To downgrade your A4(1.0) software to an earlier ACE software version in a redundant configuration, follow these steps:

Step 1 If you have previously created checkpoints in your running-configuration files (highly recommended), roll back the configuration in each context on each ACE to the check-pointed configuration. For example:

```
ACE-1/Admin# checkpoint rollback CHECKPOINT_ADMIN
ACE-1/Admin# changeto C1
ACE-1/C1# checkpoint rollback CHECKPOINT_C1
```

Do the same on the other ACE. For information about creating checkpoints and rolling back configurations, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

Step 2 Configure ACE-1 to automatically boot from the earlier ACE software image. To set the boot variable and configuration register to 1, use the **boot system image:** and **config-register** commands in configuration mode. For example, enter:

```
ACE-1/Admin# config
ACE-1/Admin(config)# boot system image:c4710ace-mz.A3_2_6.bin
ACE-1/Admin(config)# config-register 1
ACE-1/Admin(config)# exit
ACE-1/Admin#
```

You can set up to two images through the **boot system** command. If the first image fails, the ACE tries to boot from the second image.

Note Use the **no boot system image:***ACE_image* command to remove the configured A3(x.x) boot variable.

Step 3 Verify that the boot variable was synchronized to ACE-2 by entering the following command on ACE-2:

```
ACE-2/Admin# show bootvar
BOOT variable = "disk0:c4710ace-mz.A3_2_6.bin"
Configuration register is 0x1
host1/Admin#
```

Step 4 Verify the state of each ACE by entering the **show ft group detail** command in Exec mode. Downgrade the ACE that has its Admin context in the STANDBY_HOT state (ACE-2) first by entering the **reload** command.

```
ACE-2/Admin# reload
This command will reboot the system
Save configurations for all the contexts. Save? [yes/no]: [yes]
```

When ACE-2 loads the startup-configuration file, you may observe a few errors if you did not roll back the configuration to a checkpoint. These errors are harmless and occur because the ACE software does not recognize the A4(1.0) commands in the startup-configuration file.

Note Dynamic incremental sync is automatically disabled while the active ACE is running software version A4(1.0) and the standby ACE is running software version A3(2.x).

Step 5 Perform a graceful failover of all contexts from ACE-1 to ACE-2 by entering the **ft switchover all** command in Exec mode on ACE-1. ACE-2 becomes the new active ACE and assumes mastership of all active connections with no interruption to existing connections.

```
ACE-1/Admin# ft switchover all
```

Step 6 Reload ACE-1 with the same ACE software version as ACE-2. Again, you may observe a few errors as ACE-1 loads the startup-configuration file.

```
ACE-1/Admin# reload
```

After ACE-1 boots up, it assumes the role of standby and enters the STANDBY_HOT state (this may take several minutes). You can verify the states of both ACEs by entering the **show ft group detail** command in Exec mode. Because the standby ACE has changed its state to either STANDBY_COLD or STANDBY_HOT, the configuration mode is enabled. The configuration is synchronized from ACE 2 (currently active) to ACE-1. If ACE-1 is configured with a higher priority and **preempt** is configured on the FT group, ACE-1 reasserts mastership after it has received all configuration and state information from ACE-2, making ACE-2 the new standby. ACE-1 becomes the active ACE once again.

Step 7 Enter the **write memory all** command in both ACEs to save the running-configuration files in all configured contexts to their respective startup-configuration files. This action will eliminate future errors when the ACEs reload their startup-configuration files.

Supported Browsers for ACE Appliance Device Manager

The ACE appliance Device Manager is supported on the following browsers:

- Microsoft Internet Explorer 6.0 or 7.0 with Service Pack 2 on Windows XP or Windows Vista
- Firefox 3.5 on Windows XP, Windows Vista, Windows 7, or Red Hat Enterprise Linux

All browsers require cookies and DHTML (JavaScript) to be enabled.

ACE Operating Considerations

The ACE operating considerations are as follows:

- Starting with software version A4(1.0) , the default connection inactivity timeout settings for the ACE have changed to the following values:
  - ICMP—2 seconds
  - TCP—3600 seconds (1 hour)
  - HTTP/SSL—300 seconds
  - UDP—10 seconds

  The default HTTP and SSL ports (80 and 443) now have a default inactivity timeout of 300 seconds.
- Starting with software version A4(1.0), it is no longer necessary to configure a resource class in the Admin context to allocate resources for stickiness. You can still allocate sticky resources if you wish, but skipping this step will not affect sticky functionality.
- When redundant ACEs lose connectivity, for example due to a network interruption, and they attempt to reestablish their connection, if you enter the **show ft** command during this time, the response for this command may be delayed.
- In a redundant configuration, dynamic incremental sync is a form of config sync that copies configuration changes that you make on the active ACE to the standby ACE when the two ACEs are running the same version of software and when both ACEs are up. When you upgrade from one major release of ACE software to another major release (for example, from A3(2.0) to A4(1.0)), dynamic incremental sync is automatically disabled only while the active ACE is running software version A4(1.0) and the standby ACE is running software version A3(2.0). See Table 5. We recommend that you do not make any configuration changes during this time and that you do not keep the ACEs in this state for a long time. However, if you must make configuration changes while the ACEs are in split mode, ensure that you manually synchronize to the standby ACE any configuration changes that you make on the active ACE. After you complete the software upgrade of both ACEs, a bulk sync occurs automatically to replicate the entire configuration of the new active ACE to the new standby ACE. At this time, dynamic incremental sync will be enabled again. For details about config sync, see Chapter 6, “Configuring Redundant ACEs” in the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

Table 5 Feature Availability for Redundancy when the Active and the Standby ACEs Are Running Different Major Software Versions

Active	Standby	Bulk Sync	Dynamic Incremental Sync	Connection Replication
A3(2.x)	A4(1.0)	Yes	Yes	Yes
A4(1.0)	A3(2.x)	Yes	No	Yes

- In version A1(8.0), the ACE introduces the STANDBY_WARM and WARM_COMPATIBLE redundancy states to handle any CLI incompatibility issue between peers during the upgrading and downgrading of the ACE software. When you upgrade or downgrade the ACE software in a redundant configuration with different software version, the STANDBY_WARM and WARM_COMPATIBLE states allow the configuration and state synchronization process to continue on a best-effort basis. This basis allows the active ACE to synchronize configuration and state information to the standby ACE even though the standby ACE may not recognize or understand the CLI commands or state information. These states allow the standby ACE to come up with best-effort support. In the STANDBY_WARM state, as with the STANDBY_HOT state, configuration mode is disabled on the standby ACE and configuration and state synchronization continues. A failover from the active ACE to the standby ACE based on priorities and preempt can still occur while the standby is in the STANDBY_WARM state.

  When redundancy peers run on different version images, the SRG compatibility field of the **show ft peer detail** command output displays WARM_COMPATIBLE instead of COMPATIBLE. When the peer is in the WARM_COMPATIBLE state, the FT groups on standby go to the STANDBY_WARM state instead of the STANDBY_HOT state.

  The following software version combinations indicate whether the SRG compatibility field displays WARM_COMPATIBLE (WC) or COMPATIBLE (C):

Note Per CSCtd68223 for software release A3(2.6), an SRG update is not required with every release. By default, releases are considered compatible unless they are explicitly declared as incompatible.

	Standby ACE Software Version										
Active ACE Software Version	**A1(7.0) or less**	**A1(8.0)**	**A3(1.0)**	**A3(2.0)**	**A3(2.1)**	**A3(2.2)**	**A3(2.3)**	**A3(2.4)**	**A3(2.5)**	**A3(2.6)**	**A4(1.0)**
A1(7.0) or less	C	C	C	C	C	C	C	C	C	C	C
A1(8.0)	C	C	WC	WC	WC	WC	WC	WC	WC	WC	WC
A3(1.0)	C	WC	C	C	C	C	WC	WC	WC	WC	WC
A3(2.0)	C	WC	C	C	C	C	WC	WC	WC	WC	WC
A3(2.1)	C	WC	C	C	C	C	WC	WC	WC	WC	WC
A3(2.2)	C	WC	C	C	C	C	WC	WC	WC	WC	WC
A3(2.3)	C	WC	WC	WC	WC	WC	C	WC	WC	WC	WC
A3(2.4)	C	WC	WC	WC	WC	WC	WC	C	WC	WC	WC
A3(2.5)	C	WC	WC	WC	WC	WC	WC	WC	C	WC	WC
A3(2.6)	C	WC	WC	WC	WC	WC	WC	WC	WC	C	WC
A4(1.0)	C	WC	WC	WC	WC	WC	WC	WC	WC	WC	C

ACE Documentation Set

You can access the ACE appliance documentation on www.cisco.com at:

http://www.cisco.com/en/US/products/ps7027/tsd_products_support_series_home.html

For information about installing the Cisco ACE 4710 appliance hardware, see the following documents on Cisco.com:

Document Title	Description
Cisco 4710 Application Control Engine Appliance Hardware Installation Guide	Provides hardware information for installing the Cisco ACE 4710 appliance.
Regulatory Compliance and Safety Information for the Cisco 4710 Application Control Engine Appliance	Provide regulatory compliance and safety information for the Cisco ACE 4710 appliance.

To familiarize yourself with the ACE appliance software, see the following documents on Cisco.com:

Document Title	Description
Release Note for the Cisco 4700 Series Application Control Engine Appliance	Provides information about operating considerations and caveats for the ACE.
Cisco 4700 Series Application Control Engine Appliance Quick Start Guide	Describes how to use the ACE appliance Device Manager GUI and CLI to perform the initial setup and VIP load-balancing configuration tasks.

For detailed configuration information on the ACE appliance Device Manager, see the following software documents on Cisco.com:

Document Title	Description
Cisco 4700 Series Application Control Engine Appliance Device Manager GUI Configuration Guide	Describes how to use the ACE appliance Device Manager. The Device Manager resides in Flash memory on the ACE appliance to provide a browser-based graphical user interface for configuring and managing the ACE.

For detailed configuration information on the ACE CLI, see the following software documents on Cisco.com:

Document Title	Description
Cisco 4700 Series Application Control Engine Appliance Administration Guide	Describes how to perform the following administration tasks on the ACE: • Setting up the ACE • Establishing remote access • Managing software licenses • Configuring class maps and policy maps • Managing the ACE software • Configuring SNMP • Configuring redundancy • Configuring the XML interface • Upgrading the ACE software
Cisco 4700 Series Application Control Engine Appliance Application Acceleration and Optimization Configuration Guide	Describes the configuration of the application acceleration and optimization features of the ACE. It also provides an overview and description of the application acceleration features and operation.
Cisco 4700 Series Application Control Engine Appliance Command Reference	Provides an alphabetical list and descriptions of all CLI commands by mode, including syntax, options, and related commands.
Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide	Describes how to perform the following ACE security configuration tasks: • Security access control lists (ACLs) • User authentication and accounting using a Terminal Access Controller Access Control System Plus (TACACS+), Remote Authentication Dial-In User Service (RADIUS), or Lightweight Directory Access Protocol (LDAP) server • Application protocol and HTTP deep packet inspection • TCP/IP normalization and termination parameters • Network Address Translation (NAT)
Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Guide	Describes how to configure the following server load-balancing tasks on the ACE: • Real servers and server farms • Class maps and policy maps to load balance traffic to real servers in server farms • Server health monitoring (probes) • Stickiness • Firewall load balancing • TCL scripts

Document Title	Description
Cisco 4700 Series Application Control Engine Appliance SSL Configuration Guide	Describes how to configure the following Secure Sockets Layer (SSL) tasks on the ACE: • SSL certificates and keys • SSL initiation • SSL termination • End-to-end SSL
Cisco 4700 Series Application Control Engine Appliance System Message Guide	Describes how to configure system message logging on the ACE. This guide also lists and describes the system log (syslog) messages generated by the ACE.
Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide	Describes how to operate your ACE in a single context or in multiple contexts.
Cisco CSS-to-ACE Conversion Tool User Guide	Describes how to use the CSS-to-ACE conversion tool to migrate Cisco Content Services Switches (CSS) running-configuration or startup-configuration files to the ACE.

Software Version A4(1.1) Resolved Caveats, Open Caveats, and Command Change

This release note includes resolved and open defects that have a severity level of Sev1, Sev2, and customer-use Sev 3. The following sections contain the resolved and open caveats, command changes, and revised system messages in software version A4(1.1):

Software Version A4(1.1) Resolved Caveats

The following resolved caveats apply to ACE software version A4(1.1).

- **CSCte91850, CSCtj30082**—When the NPs on the ACE are in a combination of RETCODE-FAILED and INBAND-HM-FAILED state due to a traffic pattern that hashes connections to specific NPs, the **show serverfarm** *name* command displays the real servers as OPERATIONAL but they will not process any connections. Workaround: Enter the **no inservice command** and then enter the **inservice** command to restore the real server to a working state.
- **CSCth07619**—When you apply or modify ACLs or object groups to an ACE that has operated for a long time and undergone many ACL configuration changes, issues in the ACL object group expansion during the configuration download may cause an unexpected traffic drop. The **show interface** command displays a non-zero download failure counter, similar to the following:

  ```
  Access-group download failures : 8
  ```

  Workaround: Remove and readd the object group.
- **CSCth08116**—When you configure the **expect regex** command on HTTP or HTTPS probes with a long regex string and the web page parsed by the probe is longer than 100 kbytes with the matched string at the bottom of the page, the probes may fail. Workaround: Configure a basic HTTP probe that does not match a regular expression.
- **CSCth15305** (**CSCtg37325**)—During normal ACE operating conditions, the configuration manager becomes unresponsive and the ACE generates a core file. Workaround: None.
- **CSCth20813**—In a multi-threaded code, some calls are unsafe and may cause the ACE to reboot. Workaround: None.
- **CSCth26795**—When you configure the **mac-address autogenerate** command with the **ip dhcp relay** command on an interface, the ACE appliance fails to relay the DHCP request to the configured server and the counters displayed by the **dhcp relay statistics** command do not increment. Workaround: Remove the **mac-address autogenerate** command from the interfaces and reboot the ACE.
- **CSCth39505** (**CSCth39502**)—The ACE divides the sticky table and cookies between its two IXP network processors (NPs). If a connection on one NP uses a cookie with a hash that resolves to the other NP, the NPs must perform additional inter-IXP messaging to process the cookie. In a default TCP connection configuration, if the server sends 32K or more of data in less than 10 milliseconds (msec), a zero window may result on the backend. Some server TCP stacks may inadvertently introduce a 5-second delay in this situation. The ACE should advertise a non-zero window to the sending server when the buffers are released. Workaround: You can configure the **set tcp wan-optimization rtt 0** command to apply TCP optimizations to packets for the life of a connection. However, this command results in increased resource consumption.

- **CSCth59247**—When you configure long and complex regular expressions in new or existing commands, the ACE does not allow you to make any additional changes and may become unresponsive for a long duration of time. Workaround: Shorten the regular expressions in the commands.
- **CSCth63553** (**CSCth63549**)—The standby ACE may have a higher number of connections than the active ACE. Workaround: Configure a shorter connection inactivity timeout.
- **CSCth64338**—If you configure TCP probes with small intervals and set the termination mode as forced, the TCP probe stops firing if the server sends an RST after the TCP handshake. Workaround: Remove and readd the faulty probe from the real server.
- **CSCth64381**—When you attempt to log in to the ACE using remote authentication with a username that has special characters that are not supported by the ACE, the securityd process becomes unresponsive and the ACE reboots. Workaround: Do not log in to the ACE with usernames with special characters that are not supported by the ACE.
- **CSCth72928**—When you include object groups in an ACL configuration, the hash value shown in output of the **show acl detail** command may not match the hash value in the ACL merge output. Workaround: None.
- **CSCth84690, CSCth78715**—When you configure a large number of NAT pools and they are in use and receiving traffic, if you change the configuration to a smaller number of NAT pools, the ACE delays the release of the older NAT translation resources. For this issue to occur, the ACE must have active NAT translation objects (xlates) that are in use. The cause of this issue is the queued-up reap messages that prevent the xlate from being reaped. In this case, the configuration rollback reduced 2k lines of NAT pools to a one-line NAT pool. The ACE generates one reap message per line for each removed NAT pool. Workaround: To avoid this issue, consider either of the following:
  - During configuration rollback, if the new configuration deletes a large number of NAT pools in one big pool but still keep the overall dynamic pool, remove the entire dynamic pool and readd it when required.
  - Set up a clean checkpoint that has an empty configuration. Perform a rollback to the first configuration and then perform a rollback to the second configuration. In this case, an overall reap message cleans the resource.

  Either of the workarounds can prevent a large number of reap messages from being produced and queued, which can cause the slow release of system resources.
- **CSCth89247**—When you place interfaces up and down several times or configure several interfaces or static routes, some interfaces or static routes may not work properly and connectivity to peers may be lost. Workaround: None.
- **CSCti11185**—If the client or server retransmits a packet and the remote end exceeds the acceptable window size, the ACE incorrectly drops the retransmission packet and increments the [Drops] fp TCP window left edge counter. Workaround: Disable normalization or correct the client or server to honor the window sizes.
- **CSCti11896**—The ACE treats the deny function inside a management policy or class map as a SKIP. The ACE does not deny the traffic. Instead, it skips the class map and tries to match another one. Workaround: None.
- **CSCti25263**—If the same SNMP request identifier is used in previous SNMP GET and GET NEXT requests to the ACE and an SNMP agent is polling the ACE, the ACE may incorrectly respond to the SNMP request. Workaround: Perform the following:
  a. Change the SNMP agent to use unique SNMP Request Identifiers for each SNMP request.
  b. Wait at least 10 seconds between SNMP requests that use the same SNMP request identifier.

- **CSCti34985**—A sticky entry that was synced initially to the standby with the **replicate sticky** command gets synced back to the new standby after a switchover even after removing the **replicate sticky** command. Workaround: None.
- **CSCti40433**—When the client sends a SYN on an existing Layer 7 connection, the ACE responds to a TCP SYN with an ACK, and an incorrect ACK sequence number. Workaround: None.
- **CSCti40456**—The ACE does not reset a SYN on an existing Layer 7 connection. The SYN is for an existing L7 connection and the sequence number is within the receive window. Workaround: None.
- **CSCti52534**—When you are converting a CSS configuration to an ACE configuration and the input CSS configuration contains the **ssl urlrewrite** command and the associated references for SSL certificates and keys, the resulting converted ACE configuration does not have **ssl urlrewrite** and the SSL proxy configuration does not have certificate and file names. Workaround: Manually add the missing configuration.
- **CSCti53513**—When you configure the default class (class-default) as the only class map in a load-balancing policy with features that use regular expressions (for example, compression), the **show service-policy** command does not display the Regex dnld status field and its value. Workaround: None.
- **CSCti61725 (CSCsz37412)**—When the software and license on the ACE are compatible, ANM does not display their compatibility status. The XML **show ft peer 1 detail** command on the ACE is not correct. Workaround: None.
- **CSCti66770, CSCth37401**—When the ACE receives a cookie string that contains many cookies and encounters a space character in the cookie value, it stops processing the cookies. Spaces are not permitted in the cookie name or cookie value. Persistence or stickiness fail. Workaround: None.
- **CSCti68403**—In a redundant configuration, after you reload the standby ACE, the SSH Keys on the standby are not always synchronized with the SSH keys on the active. Workaround: None.
- **CSCti72204**—After correcting a license mismatch on the standby ACE, the standby displays the following error message: Running cfg sync enabled : Disabled with sh ft group detail command. Configuration changes are still replicated to the standby ACE from the active ACE. Workaround: Reboot the standby ACE.
- **CSCti74520**—When sending malformed requests, SSHD may become unresponsive. This issue has occurred when running testcase 4738 of the Codenomicon SSHV2 test tool. Workaround: None.
- **CSCti76678**—When you change the default destination port for an HTTP probe, the probe does not append the port to the Host tag in the HTTP request and the ACE receives an HTTP/1.1 404 Not Found error. Workaround: Configure the probe with the **header Host header-value** command to specify and append the destination port to the host in the HTTP request.
- **CSCti84218 (CSCtb03138)**—If you configure SNMP traps on a VLAN that has either the IP address or the peer IP address missing and redundancy is enabled, the active ACE does not synchronize the SNMP traps to the standby ACE. The **show ft group detail** command displays the following error:

  ```
  Error "Incremental Sync Failure: snmp config sync to sby."
  ```

  Workaround: Configure both an IP address and a peer IP address on the interface VLAN that you are using as the trap source.
- **CSCti88468**—After you enter a **show** command at the CLI, the ACE may write a VSH core file when you enter an SSL **crypto** command. The VSH core file does not cause the ACE to reboot. Workaround: None.

- **CSCti90240**—In a redundant configuration, after the **show resource usage all** command is executed either by ANM or by using a script at bootup time, command parse errors are seen on the console of the standby and the context enters the STANDBY_COLD state. Workaround: After the bootup is finished, resynchronize the configuration using the **ft auto-sync running-config** command.
- **CSCti96864**—When you perform dynamic configurations of usernames in multiple contexts and enter the **no username** *name* command in a user context, the ACE module unexpectedly reboots and generates an SNMP core file. Workaround: None.
- **CSCtj07489**—When you configure a policy map that references another policy map on the ACE, if the checkpoint rollback or restore operation removes these recursively referenced policy maps during context deletion while the operation loads another context, the cfgmgr process may become unresponsive. This is especially risky when all context policy maps are removed which can occur during a restore operation. Workaround: None.
- **CSCtj13489**—Occasionally, when the FT TCP channel needs to be set up multiple times because it keeps getting torn down, its state eventually becomes TL_SETUP/FT_VLAN_DOWN or TL_ERROR/FT_VLAN_DOWN. This issue can be caused by intermittent network outages or other conditions that create the need to set up the FT channel several times back-to-back. Workaround: Manually toggle the FT VLAN.
- **CSCtj18925**—When you configure many servers with active/active NIC teaming, the ACE arp_mgr service may consume 100% of the CPU due to the ARP flood caused by teaming mode. Workaround: Reduce ARP traffic. Always use active/standby NIC teaming.
- **CSCtj25377**—While trying to obtain the hit count for an SNMP walk, the ACE may reboot and create a core file similar to cfgmgr_log.954.tar.gz. Workaround: None.
- **CSCtj27947**—After you stop network traffic, the active connection count for an IP static sticky entry remains because static sticky entries never expire. Workaround: None.
- **CSCtj30486**—Deleting and adding the **access-group** or the **service-policy** command multiple times under an interface mode may cause a leaf node leak and an action node leak, which can be observed by entering the following command: **show np 1 access-list resource**. Workaround: Delete then readd the interface.
- **CSCtj45039**—When you configure a Session Initiation Protocol (SIP) probe for health monitoring (HM), the ACE may incorrectly display the probe as down due to the ACE using the same Call ID for multiple probe instances to different configured real servers. Workaround: Configure the ACE with a different probe type.
- **CSCtj56049**—After a period of dynamic configuration, the configuration of a sticky serverfarm may fail when you are using the Command Line Interface (CLI) or XML. Workaround: Reload the ACE.
- **CSCtj62369**—When the application acceleration and optimization features of the ACE are configured, the integrated packet capture utility may not capture traffic from all interfaces even when the capture is configured to capture from all interfaces. Workaround: None.
- **CSCtj67137**—When you configure a probe on a real server of type host and the probe's state changes from FAILED to SUCCESS, the ACE should send the cesRserverStateChange SNMP trap. Currently, the SNMP trap that the ACE sends is inconsistent as follows:
  - When a probe state changes from SUCCESS to FAILED, the ACE generates the cesRserverStateChange SNMP trap.
  - When a probe state changes from FAILED to SUCCESS, the ACE generates the cesRserverStateUp trap.

  Workaround: None.

- **CSCtj68302**—When the ACE load balances clients towards the HTTP proxies, the ACE resets proxied SSL connection; an RST on the Client Hello. This issue may be associated with HTTP/1.1 in the CONNECT request or response. Workaround: You can configure HTTP/1.0 on the client and server. Do not inspect the HTTP connections.
- **CSCtj71370**—When real servers under a server farm are configured with the max conn command and the maximum connections limit is reached, sticky entries with a time to expire of 0 are seen on the ACE. The ACE does not remove these sticky entries because the active connection count is not 0. Workaround: None.
- **CSCtj75527**—With an aggressive sticky expiry timer of one minute, IP sticky and dynamic HTTP cookie traffic, and a sticky database of approximately 200,000 entries, the ACE may become unresponsive in LbSticky_ReturnExpiredEntries after five to six hours. Workaround: Configure a sticky expiry timer of 10 minutes or more.
- **CSCtj80791**—When SIP inspection is enabled and back-to-back SIP traffic (INVITE) occurs about 4 to 5 microseconds apart with 50 to 250 calls a second or with a high rate of traffic (800 to 900 calls a second) and inspection enabled, the ACE may leak network address translations (xlates), which can cause the ACE to drop the traffic. Workaround: Avoid back-to-back UDP packets for SIP INVITE with the same five-tuple and the same call ID across a few microseconds or, if possible, disable NAT for the SIP flows.
- **CSCtj84609**—When there is a high degree of control plane kernel stress with a large configuration and multiple scripts polling various ACE stats in a tight loop, memory corruption may occur. As a result, the ACE may reboot because the kernel becomes unresponsive.The ACE displays the “Unable to handle kernel paging request” message and generates a crashinfo file. Workaround: None.
- **CSCtj92423**—While you are modifying the probe **expect status** command at the CLI, sometimes the ACE may keep the old expect status values and also add the new probe expect status values to the configuration. Workaround: Log in to the CLI, remove the old **expect status** command, and synchronize the context by entering the **ft auto-sync** command. For details about the **ft auto-sync** command, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.
- **CSCtk01918**—When the ACE is configured with access control lists, object groups, and DHCP, an ACL merge failure may occur when you apply the configuration to an interface. This issue can cause the configuration to be incomplete and needs to be manually removed. Workaround: None.
- **CSCtk03294**—When you configure the ACE with a port-channel link, the redundancy heart beat is always sent on one interface only because of the load-balancing mechanism. If that interface goes up and down because of port-hashing convergence, the heart beat may be dropped during 2 to 4 seconds. Both ACEs may then become active /active during that time. This issue is a limitation of the current redundancy implementation. Workaround: Ensure that the heart beat interval is no too aggressive and avoid configuring carrier delay on PO interfaces.
- **CSCtk06591**—If the ACE is configured to get the time via the Network Time Protocol (NTP) and the actual time on the ACE is set incorrectly, a demo license can be installed and work correctly until the ACE is rebooted. Workaround: Set the time correctly using the **clock set** command.
- **CSCtk08750**—If you attempt to log in with a username that contains some special characters, the ACE inserts random text in the login prompt. This behavior occurs only with certain special characters that are invalid for a username. Workaround: Do not create or use a username with invalid characters.
- **CSCtk09730**—A Linux kernel file system error log was observed during bootup of the ACE. Workaround: None.
- **CSCtk11720**—When you are troubleshooting the ACE, the data plane (DP) console logs are difficult to obtain. Workaround: None.

- **CSCtk14790**—When you configure TACACS with the **aaa authentication login default group tacacs local** command, the first attempt to SSH to the ACE fails. A second SSH attempt with the same username is successful. If you enter the **no username** *name* command, the original behavior will occur again and you will have to SSH in twice to be successful again. Workaround: SSH to the ACE twice.
- **CSCtk30688**—When a Layer 7 policy is configured with a sticky server farm, the StickyConns counter in the **show serverfarm detail** command may overflow. Workaround: None.
- **CSCtk52854**—The time that is required to run the **show tech** [**details**] diagnostic command may take hours with a heavily configured ACE. Workaround: None.
- **CSCtk53132**—During bootup (initialization), the ACE running A4(1.0) may not boot properly although a A3(2.x) image boots and the system operates normally. Workaround: RMA the ACE. In this case, the new ACE will boot.
- **CSCtk66025**—When stickiness is configured, the ACE may become unresponsive after running traffic for several days because the sticky link list is corrupted. Workaround: None.
- **CSCtk69726**—If inband health checking and return code (retcode) checking are configured together under a server farm, a real server may become stuck in the INBAND FAILED or RETCODE FAILED state even after the configured resume time has elapsed. Workaround: None.
- **CSCtk76045**—In a redundant configuration, replicated dynamic sticky entries are seen on the standby even without dynamic sticky enabled. This behavior can occur when cookie insert is enabled on the sticky group with the **replicate sticky** command and a new request hitting the static cookie insert entry is replicated to the standby as dynamic. Workaround: None.
- **CSCtk96341**—The **duplex** command fails when playing the startup-config or when syncing to an ACE running another software release. For example, if a configuration containing the duplex full command was saved while running software version A3(2.x), the startup-config would be incompatible with other releases.
- **CSCtk97888**—If the lbconn structure's stickyKey is set to INVALID, the decrement operation fails at a few places and the sticky connection counter under a server farm displays an incorrect value. Workaround: None.
- **CSCtl03624**—When the **conn max** command is configured at the parent real server level and traffic is flowing, the ACE may consider the real server to be in the MAXCONNS state in the control plane, while the real server is actually in the OPERATIONAL state in the data plane. Workaround: Remove and then readd the real server to reset the real server state.
- **CSCtl07204**—When a very high rate of traffic is flowing through the ACE in multiple contexts and using most of the load-balancing features, sticky statistics may become corrupted and display as a very large value in the **show resource usage** and the **show stats sticky** command output. Workaround: Enter the **clear stats** command to clear the counters.
- **CSCtl48284**—When the **replicate sticky** command is configured on the sticky group in a reverse sticky configuration, the standby ACE may become unresponsive with a seg fault/sig 11 error message. Workaround: None.
- **CSCtl52592**—In a redundant configuration, if a switchover occurs after a Telnet or FTP connection was established on the active ACE, the connection becomes stuck. Workaround: Use the **clear conn** command to clear the connection after the switchover.
- **CSCtl60176**—If an internal software load-balancing structure is not initialized properly for point to multipoint (PTMP) traffic, sticky connections may appear under a server farm even though sticky is not configured. Workaround: None.
- **CSCtl69234**—The **count** and the **detail** options are not available for the **show sticky ip-netmask both** command because of missing XML code. Workaround: None.

- **CSCtl71859**—When an object group for a service is configured in a security ACL and a VIP is configured that fits within the network of the object group and also ends in a (multiple of 8) .7 and is the only VIP in that address range, the wrong virtual server may be hit when traffic is sent to that VIP. For example, the VIP ends in .7 and there are no other VIPs ending in the .1 to .6 range. Workaround: Add another VIP with an IP address that ends in a value which is within six numbers lower of any VIP that ends in a (multiple of 8) .7 and that has no other VIPs in that byte range. For example: If the VIP ends in .7 and has no other VIPs in the .1 to .6 range, then add a VIP in that range. If the VIP ends in .15, then add a VIP that ends in the .8 to .14 range, and so on.
- **CSCtl76866**—When you send an HTTP HEAD request on the same TCP connection, the ACE does not forward the HEAD request. Workaround: Disable persistence rebalance.
- **CSCtl81479**—In a redundant configuration, if a SIP caller repeatedly holds and then resumes the call thereby causing a high rate of SIP packets to enter the ACE, eventually, the ACE may drop one of more of these SIP packets, which can result in a dropped call. Workaround: None.
- **CSCtl92031**—When an improper TCP client requests data from the ACE, but never accepts all of it, resulting in a connection on the ACE that is continuously probing the client TCP receive window (TCP.RCV_WND), traffic to the ACE may fail due to high network processor buffer utilization that is contained in a small number of extremely long-lived TCP connections. In some buggy client TCP implementations, the client continues to send non-zero length segments even while advertising a zero window. Another type of buggy client may indefinitely send FIN segments to the ACE even while advertising a zero window. In both the non-zero segment and the FIN cases, the ACE consumes one buffer for each packet until the connection is closed or the client advertises a non-zero window. Workaround: To identify the connections in the connection table, enter the **show conn detail** command and search for connections that are idle (for hours or more) on the outbound side but not idle on the inbound side. To recover the buffers for an offending flow, clear the flow by entering the following command: **clear conn flow** *protocol source_ip source_port dest_ip dest_port*.
- **CSCtn16600**—In a redundant configuration with sticky configured, if you disable connection replication by entering the **no ft conn-sync** command, the standby ACE may become unresponsive. Workaround: None.

.Software Version A4(1.1) Open Caveats

The following open caveats apply to ACE software version A4(1.1).

- **CSCsu40160**—When the ACE configuration has more than 500 service policies and you can ping all VIP addresses, some VIP addresses are not served at all. Workaround: None.
- **CSCsu55909**—In a redundant configuration, when you configure the ACE with 20 contexts, apply it to the active ACE, and then bring up the standby ACE with the configuration, the active ACE transitions into the Cold state with the following error:

  ```
  Error on Standby device when applying configuration file replicated from active
  ```

  Workaround: First bring up the active and standby ACEs individually and then enable redundancy.
- **CSCsv62417**—In some instances, the virtual MAC address is used for both the client-side VIP addresses and server-side NAT pools. With an FT VLAN configuration, the virtual MAC address is used as the source MAC for both client- and server-side packets. This behavior can cause issues in specific network topologies where the client-side and server-side end up learning the same MAC address over two ports. Without the FT VLAN, the internal MAC address is used. Workaround: Use the **mac address autogenerate** command to enable the autogeneration of a MAC address.

- **CSCsx06085**—When you enable UDP boost on the ACE, the server-initiated traffic fails because the destination port changes to the source port value. Workaround: Disable UDP boost.
- **CSCsz71578**—When you apply a service policy globally and then add the VLANs, the ACE displays ACL-merge errors for newly added VLANs and traffic does not flow through them. Workaround: Remove the global service policy and then reconfigure it.
- **CSCsz88519**—When you configure a TCP-based syslog server and the syslog server application on the remote system is down even though it can be reached from the ACE appliance, the ACE becomes unresponsive and most of its commands either time out or respond slowly. Workaround: Either bring the syslog server application up or remove the configuration for the TCP-based syslog server.
- **CSCta87584**—Connections may get dropped intermittently when you use persistence rebalance in a configuration and a rebalance is performed across traffic policies. This behavior typically occurs in a configuration with two different server farms that both contain the same real server with different ports, and the server farms are attached to two different Layer 7 load-balancing policy maps. Workaround: None.
- **CSCtc50852**—When many new clients that are directly connected send a burst of traffic, you may see a drop in traffic for a short time because the ACE takes time to resolve the ARPs. Also, mac-miss drop messages occur during this time. Workaround: The issue does not occur when the ARPs for the clients are already present in the ARP cache table.
- **CSCtd42287**— When the ACE is running with the maximum limit of 8K static entries and you remove a service policy from an interface and quickly readd it, the ACE removes the statements from the NAT policies. Workaround: Provide ample time between removing a service policy from an interface and then readding it.
- **CSCte76618**—When traffic traverses the ACE module with the same source and destination port and dynamic NAT for that traffic is enabled, the ACE performs an implicit PAT. This behavior interrupts some sessions. This problem does not occur when NAT is not involved. Workaround: If possible, disable dynamic NAT.
- **CSCte76958** (**CSCsr21689**)—The first packet of a TCP, UDP, or ICMP connection may not be captured; however, the remaining packets are captured for the same flow. This behavior can occur when you have the packet capture function configured for a specific ACL and for Layer 7 load-balanced traffic. Workaround: None.
- **CSCtf54230**—When Layer 2 connected real servers are in the arp-failed state and probes are attached to all of them or the ACE is running a high rate traffic that generates many mac-miss IPCP messages, FT may appear to fail after several hours. Workaround: Remove the real servers in the arp_failed state or make sure that most of the real servers are UP.
- **CSCtg17350**—When you configure the Acceleration and Optimization features on the ACE, the integrated packet capture utility may not capture traffic from all interfaces, even when you configure the capture to capture from all interfaces. Workaround: None.
- **CSCtg31975**—A system admin account in the ACE software may allow an authenticated user to inject shell commands. This account does require authentication. Workaround: None.
- **CSCtg53126**—When you attempt to delete a server farm with the **no serverfarm host** command, the ACE displays the following error message:

  ```
  Error: serverfarm 'serverfarm_name' is in use. Cannot delete!
  ```

  The configuration manager thinks the server farm is still applied to the load-balance policy. Workaround: None.
- **CSCtg67860**—When you configure multiple track probes in two user contexts and enter the **show cfgmgr internal table track-probe** command, the ACE becomes unresponsive due to a Cfgmgr process failure. Workaround: None.

- **CSCtg76150**—When you configure an inline match statement that has a special character or space in its name under an Layer 7 policy, the checkpoint rollback fails. Workaround: Do not configure inline match statements with special characters or spaces.
- **CSCtg87927, CSCtf42007**—When you apply a real server to multiple server farms and the server recovers from a probe failure, it does not receive any new connections on any of the server farms. The **show probe** and **show serverfarm** commands indicate the real server is operational but does not have any current connections. Workaround: Remove the real server from service. Then, place it in service.
- **CSCtg87855** (**CSCtg87843**)— After you change the configuration in a large ACE configuration and enter **show** commands, the CLI becomes unresponsive for a period of time. In this case, the **show processes cpu | include cfgmgr** command displays one of the configuration manager (cfgmgr) processes consuming CPU resources. After you apply the configuration change, the cfgmgr CPU usage goes to zero, and the CLI becomes unresponsive. Workaround: Wait until the cfgmgr completes its previous operation before entering the **show** command.
- **CSCtg96456**—When you configure the maximum number of the VIP statements in a single class map of 254 and then delete one of the VIP statements, the ACE cannot add a match VIP address in a single class map and displays the following message:

  ```
  Error: Exceeded maximum match item limit for the class-map
  ```

  Workaround: Remove the class map and the reconfigure it again with all of the VIP addresses.
- **CSCth01552**—When you configure a large number of directly connected real servers on the ACE and they are in the DOWN state, ARP resolution may fail intermittently for the directly connected hosts. Workaround: Transition the directly connected hosts to the UP state or decrease the number of directly connected hosts.
- **CSCth04993**—When you configure an ACE interface with single NAT IP address in the NAT pool and the ACE receives SIP UDP traffic, it resets subsequent SIP TCP traffic. Workaround: Perform either of the following:
  - Perform a checkpoint rollback to a non-SIP configuration and then to the existing configuration.
  - Increase the number of IP addresses in the NAT pool.
- **CSCth07709**—When performing the **snmpwalk** or **snmpbulkwalk** command for any object on the ACE, occasionally the ACE displays an Unknown user name error. The frequency of this occurrence can increase by having three contexts on the ACE. Workaround: None.
- **CSCth16258**—The **snmpwalk** or **bulkwalk** command on the SSL proxy MIB always returns a timeout. Currently, there is no tnrpc call to fetch data. The number of statistics has increased to string parsing and is taking more time. The default timeout is one second and it is not responding within one second. Workaround: Increase the timeout value.
- **CSCth23304** (**CSCth12446**)—When the ACE is using a 1-Gbps throughput license, the throughput output displayed through the **show resource** command is rounded to the nearest thousand. For example, a value of 134217728 is rounded to 134217000. This issue does not occur with other throughput licenses. Workaround: Install a throughput license that is not 1 Gbps and then uninstall the license.
- **CSCth23432**—When you delete a certificate from a full image directory on the ACE and reboot the ACE, the ACE is not accessible from the XML interface and the Device Manager GUI does not work. Also, when the image directory is full, the ACE cannot generate a certificate. Workaround: Delete some data from the image directory and reboot the ACE, which will allow the creation of the certificate.

- **CSCth24647**—When the FT interface VLAN number is lower than the other interface numbers and these interfaces require the downloading of large configurations, an API timed out error occurs when applying the startup configuration. Workaround: Enter the **no ft auto-sync running-config** command and then enter the **ft auto-sync running-config** command.
- **CSCth55362**—When the ACE performs a configuration rollback, existing classes in a policy are not reordered according to the new configuration. The running configuration has a policy that contains several classes. The checkpoint contains that policy with some or all the classes in a different order. After performing the rollback, the order of the classes stays as it was in the running configuration.

  Workaround: Perform either of the following:

  - Remove the policy that was changed during the rollback and then perform the rollback.
  - If there are many similar policies in the configuration, perform a rollback to an empty configuration and then rollback to the desired configuration.
- **CSCth67961** (**CSCsy66327**)—When you enter the **show snmp group** command from any context other than the Admin context, it does not display any output. Workaround: None.
- **CSCth74700**—Connectivity to the real server may be lost when you configure the following:
  - A client and server side VLAN on the ACE
  - A real server and ensure that it is Layer 2 reachable
  - A static route with a /32 mask to reach the real server through another interface

  Workaround: Remove and reconfigure the real server.
- **CSCti28255**—When a real server state transitions to UP from a probe-failed or ARP-failed state, the ACE generates the CISCO-ENHANCED-SLB-MIB:cesRserverStateUp trap. However, if the real server goes down due to a probe-failed or ARP-failed state, the ACE generates the CISCO-ENHANCED-SLB-MIB:cesRserverStateChange trap. Workaround: None.
- **CSCti40456**—The ACE does not reset a SYN on an existing L7 connection. The SYN is for an existing L7 connection and the sequence number is within the receive window. Workaround: None.
- **CSCti68421**—If the ACL merge resources are almost exhausted and you add a configuration statement that places the resources over the limit, the ACE may drop traffic on the VLAN interface in which the configuration statement applies. Workaround: To restore service, remove the last configuration change that you made. To determine the current ACL merge resource status, enter the **show np 1 access-list resource** command in the Admin context and the s**how acl-merge merged-list vlan** *number* **in non-redundant** command in the context or VLAN where you will apply the configuration change.
- **CSCti68449**—The **show xlate** command displays thousands of entries. However, the **show resource usage** command displays zero peak and zero current. Workaround: Reboot the ACE.
- **CSCti76373** (**CSCsu08736**)—When you download the DTD file shipped with ACE and check the definitions for features such as CRL, authgroup, DNS, RTSP, and SIP, some of the XML tags definitions are not available. Workaround: None.
- **CSCti85064**—Occasionally when the ACE is under high control plane (CP) stress with a high rate of CP syslog traffic at logging Level 7, the CP becomes sluggish. If the data plane becomes unresponsive, the ACE console become unresponsive and the ACE reboots by the SME process without creating any dataplane core files. Workaround: Avoid CP syslogs at level 7 with a high rate of traffic, or enable only fast path syslogs.
- **CSCtj00826**—If the ACE is running a large number of HTTP or HTTPS probes when probing a file approximately a megabyte in size, the ACE reboots. The following message may precede the reboot:

```
System running low on direct mapped memory
Please issue 'show system kcache' to diagnose further
```

Workaround: Reduce the size of the file being probed when running a large number of probes on the ACE.

- **CSCtj12692**—When you configure the ACE with 4000 sticky groups and do not allocate a sticky resource class, the resource values of the sticky are the default of a minimum of 0 and a maximum of unlimited. When the sticky database has 800,000 entries and you create a sticky resource class to a minimum value equal to 20 percent and apply it to the context, the ACE becomes unresponsive after a few minutes because it becomes unresponsive in the LB module at the function LbSticky_ReturnOldestEntry. Workaround: Do not change the resource class when you configure a large number of sticky groups and the database is full with active entries.
- **CSCtj30825**—When you configure a large number of ICMP probes and directly connected hosts on the ACE, ARP resolution fails intermittently for the directly connected hosts. Workaround: Decrease the number of ICMP probes or change the ICMP probes to TCP or UDP-based probes.
- **CSCtj91896**—Soon after you configure a TCP probe and the probe becomes active, the server may send out-of-band data to the ACE, which causes the ACE to become unresponsive and to produce an hm_core file. Workaround: None.

Software Version A4(1.0) Resolved Caveats, Open Caveats, and Command Change

This release note includes resolved and open defects that have a severity level of Sev1, Sev2, and customer-use Sev 3. The following sections contain the resolved and open caveats, command changes, and revised system messages in software version A4(1.0):

Note Some caveats may have more than one number. A number in parenthesis is a caveat number that was associated with the previous A3(X) software release that now has another number for A4(1.0).

Software Version A4(1.0) Resolved Caveats

The following resolved caveats apply to ACE software version A4(1.0).

- **CSCsw58665**—If you initially configure a real server as a Layer 2 real server, and then the interface goes down or is deleted from the configuration, the real server may transition to an ARP_FAILED state and remain in this state after it becomes a Layer 3 real server. Workaround: Reconfigure the real server.
- **CSCta74000**—The ACE may fail to download a certificate revocation list (CRL). In some cases, the CRL fails to download when it is reapplied to the SSL proxy that is being used in certain VIPs if the previous applications to the SSL proxy had failed to download the same CRL at the point when the CRL server was down. When this situation occurs, the ACE stops downloading the CRL. Workaround: Unconfigure and then configure the CRL again.
- **CSCtb15306**—When expired CRLs are in use and the **expired-crl reject** command is configured in an SSL parameter map, the SSL process on the ACE control plane may become unresponsive. Workaround: Do not reconfigure VIPs while traffic is flowing.
- **CSCtb62478** (**CSCtf50924**)—When you configure 0.0.0.0/0 as the first VIP on the ACE, all subsequent VIPs inside the **show cfgmgr internal table vip** command matches 0.0.0.0/0. This command table becomes corrupted with 0.0.0.0/0 as the first VIP. Workaround: Do not configure 0.0.0.0/0 as the first VIP.
- **CSCtc77095**—When you configure a scripted probe that sends an XML request to the interface of the ACE (from another ACE) and executes the **show service-policy** command, the output of the **show proc cpu** command shows that the CPU of the control plane (CP) is almost always at approximately 90% usage and that the XML CP processes are consuming those cycles. Workaround: Instead of sending an XML request, send a RAW request and turn XML output on before executing the **show service-policy** command as follows:

  ```
  xml_cmd=<request_raw>xml-show on%0ashow service-policy</request_raw>
  ```

  The resulting XML output will have an extra exec_command node in the response for the **xml-show on** command, but the show service-policy response will be the same as with the XML request.
- **CSCtc82308**—TFTP file upload may timeout and fail for files more than 32 MB in size. Workaround: None.
- **CSCtd00348** (**CSCtf02311**)—When you configure NAT for DNS VIP traffic, the rewrite for an A record with a third-party address may not occur. The ACE forwards the DNS query response from the server with the original A-record address. This issue occurs only with the third-party address for

which the ACE fails to find the route. Workaround: You can prevent this issue by adding a static route for the third-party subnet through the following command, **ip route** *third-party-subnet mask gateway.*

- **CSCtd03068**—When you enter the **dir image:** command, its output displays incorrect used space and free space. It includes the internal file system space for the free and used space calculation. Workaround: None.
- **CSCtd18366** (**CSCtf28699**)—When you enable the server-connection reuse feature, and a real server becomes unreachable or the outbound interface is shutdown, a few dataplane connection entries may become stuck in a race condition and cannot be used by the ACE. Workaround: Reboot the ACE to recover the resources.
- **CSCtd74263** (**CSCte76795**)—After you change the resource-class configuration and traffic is successfully passing through the ACE, the compression statistics displayed by the **show service-policy** command do not update. Workaround: None.
- **CSCtd90778**—When you configure an ACE in a user context in a very large configuration with 10 contexts and multiple SSL certificates, the ACE may reboot and generate a CFGMGR core dump file. Workaround: None.
- **CSCte02072**—When the first load-balancing policy attached to a VIP in a user context is not configured with any server farms to load balance the requests, the ACE determines that the load for the VIP is 0 and the GSS determines it is offline. Workaround: Make the state of the first server farm attached to that VIP as UP.
- **CSCte19514**—Checkpoint rollback may fail with certain configurations. Workaround: None.
- **CSCte52355**—When you enable XML, the XML output is not seen for the **show serverfarm** *name* **retcode details** command. Workaround: None.
- **CSCte55851** (**CSCtf06483**)—When you configure HTTP inspection with SSL termination and Layer 7 load balancing, and add inband TCP and retcode health monitoring configurations to the same server farm while HTTP and HTTPS traffic passes through the ACE, the ACE may reboot due to the HTTP inspection engine accessing an invalid session state. Workaround: Disable the HTTP inspection feature.
- **CSCte62256** (**CSCte81895**)—When you configure HTTP inspection with the URL logging feature and change the HTTP inspection configuration while traffic is passing through the inspection engine, the ACE may reboot due to an inspection engine misbehavior. Workaround: Disable the URL logging feature.
- **CSCte76543** (**CSCte98511**)—When you configure the ACE with the maximum number of elements or match source statements and you add or remove match statements, match item object entries leak. Workaround: None.
- **CSCte79904**— If a large number of real servers are down in the ARP failed state, the CLI on the ACE appears to be less responsive. Workaround: None.
- **CSCte97036**—When you configure two or more probes to a server farm, the probe instance is not created after entering the **no inservice** command, removing one of the probes on the server arm and entering the inservice command on the real server. Workaround: None.
- **CSCte98195** (**CSCtf33109**)—When you configure a real server with the **fail-on-all** command in a server farm and more than one probe fails, the real server is in the OPERATIONAL state. If you remove the **fail-on-all** command from the server, it remains stuck in this state. The real server should transition to the PROBE-FAILED state. This issue also occurs when you configure a server farm with the **fail-on-all** command because the fail-on-all action applies to all real servers in the server farm. Workaround: Enter the **no inservice** command followed by **inservice** command to restore the real server and transition it to the PROBE-FAILED state even when one probe fails.

- **CSCtf01673**—When low connection limits or rate limits are applied to the parent real server, such that the limits are easily hit with regular traffic patterns, some real servers get stuck in the stopped list until the configuration changes are done. When the parent real server hits the limits, the associated real server is moved to the stopped list. When the real server comes back into service (for example, it comes out of the MAXCONNS state), some of the associated real servers are not removed from the stopped list. Workaround: Stop the traffic and move the real server out of service and then bring it back into service.
- **CSCtf04897**—If stickiness is not configured under a RADIUS policy map, policy-map entries are not cleared upon RADIUS response, and RADIUS requests may be unevenly load balanced because of false retransmission issues. Workaround: Configure a sticky server farm under the RADIUS Layer 7 policy map.
- **CSCtf08812**—TCP or UDP configured port ranges are being inherited for non-TCP non-UPD protocols when configured inside an object group right after a TCP or UDP range. Workaround: Configure the ACL directly without using the object group.
- **CSCtf12034**—In a large multiple context configuration, the arp_mgr becomes unresponsive while applying the configuration. Workaround: None.
- **CSCtf12749**—When using a custom role configuration on the ACE, some Admin commands are not accessible. Workaround: Use the Admin role.
- **CSCtf15879**—When the CSS2ACE tool converts a CSS configuration to the ACE appliance, the **persistence reset remap** command does not convert properly. Workaround: None.
- **CSCtf19783** (**CSCte37312**)—If you delete disk0 without the filename and you assign a filename on ACE, it deletes the entire disk0 directory rather than the file. If the directory is empty and you enter a dummy filename, it deletes the disk0 directory and disk0 cannot be used after that. The disk0 directory is lost and is not created until the next reboot of the ACE. Workaround: Reboot the ACE.
- **CSCtf23571**—When you use the XML management protocol to query the ACE for context configuration, the ACE generates invalid XML output for the **show context** command when you enter this command in a user context. Workaround: Enter the **show context** command in the Admin context.
- **CSCtj28940**—When you add a new real server under a server farm when traffic is hitting the active ACE in a redundant configuration, some real servers under the server farm may display additional numbers for the current connection count after the traffic stops. Workaround: After the traffic stops, remove and readd the real server.
- **CSCtf31062**—The previously configured inband health monitoring threshold was retained. The new threshold is seen as -1 on the data plane. Workaround: None.
- **CSCtf33301** (**CSCtf39663**)—When you configure the **send-data** command with a length greater than four characters inside a finger probe, the probe fails. When you configure the **expect regex** command with ".*" string, the probe also fails. Workaround: Configure the probe with a send-data length that is less than 4 characters.
- **CSCtf37639** (**CSCtg03038**)—When you configure an invalid OID in an SNMP probe, the probe fails due to parse error for the configured OID. Each failing SNMP probe leaks one socket. Eventually, the socket resources for health monitoring are exhausted causing all the probes on the system to fail with Out of Sockets errors. Workaround: Correct the OID under the SNMP probe and reboot the ACE.
- **CSCtf38880** (**CSCtf94950**)—When you remove a class map with a sticky load-balancing policy, the ACE removes sticky groups from other policies that are still using them. Workaround: Removing and adding the sticky group to the policy should download the correct configuration.

- **CSCtf40842** (**CSCtg31255**)—When you change the cookie name of an HTTP-cookie sticky group, the name does not change. Workaround: Remove the cookie group. Then, reapply it to the policy map.
- **CSCtf79958** (**CSCtg46244**)—When the ACE has a high rate of SIP calls per second and the SIP inspection engine encounters any errors due to resource allocation failures, the ACE may reboot. This issue occurs only when the SIP inspection engine encounters failures in the initial packet processing, for example, memory allocation, object allocation, and inspection configuration version mismatch failures. Workaround: Disable the SIP inspection feature, if possible.
- **CSCtf82525** (**CSCtd19335**)—If RADIUS traffic is being sent and you enter the **show conn rserver** *rserver_name* command, the outstanding messages in the load-balancing queue build up over time, which causes the ACE to become unresponsive eventually. This issue is not seen with the **show conn** command. Workaround: Do not use the **show conn rserver** command.
- **CSCtf86417**—When you configure the ACE module for Role-Based Access Control (RBAC) using custom domains and roles, and you log in to the ACE as a user with a user-configured domain and role, some commands do not work. Workaround: Use the specific versions of the **show rserver** *name* and **show serverfarm** *name* commands.
- **CSCtf89530**—In a redundant configuration, the standby ACE may become unresponsive upon reboot and displays the following message: “Service name:cfgmgr(948) has terminated on receiving signal 11." Workaround: None.
- **CSCtf89544**—When you configure a server-farm NAT on the ACE and remove a policy map, the ACE does not remove the association between the interface and NAT. Workaround: To remove the association between the interface and NAT, first remove the Layer 3 rules and then remove the policy map.
- **CSCtg24769** (**CSCtg53196**)—When you configure the **ip options clear** or **ip options clear-invalid** command, and the ACE receives packets that contain the IP options, it drops the packets. Workaround: None.
- **CSCtg27617** (**CSCtg27611**)— When you configure the IP relay agent on the ACE VLAN interfaces, due to the fix for CSCtb60599, the ACE DHCP relay agent forwards DHCP unicast packets which is incorrect. Workaround: None.
- **CSCtg43059**—When you enter the s**how telnet maxsession** *context_name* command, where the *context_name* argument is an existing or nonexisting context, the ACE generates a VSH core file in the core directory with a sig 11, Segmentation fault and then displays an internal error during command execution error message. Workaround: None.
- **CSCtg43315**—If you configure a SIP probe with an IP address, the probes are correctly sent to this address but the payload still contains the real server IP address. Workaround: None.
- **CSCtg43402** (**CSCtg43409**)—When you configure DHCP-related changes on the VLAN and BVI interfaces, the ACE becomes unresponsive due to a cfgmgr termination. Workaround: None.
- **CSCtg53426**—The ACE does not bridge the TCN-BPDU. The ACE does not have a way to handle TCN-BPDU and considers TCN-BPDU as an invalid BPDU packet and drop it because of bad Ethernet frame length. Workaround: None.
- **CSCtg65914**—When you modify a NAT pool under an interface configuration, the following error may be logged and can be displayed using the **show logging** command:

  ```
  Sep 4 2009 12:34:03 ace/ace: %ACE-1-106028: WARNING: Unknown error while processing
  service-policy. Incomplete rule is currently applied on interface vlan953. Manual roll
  back to a previous access rule configuration on this interface is needed.
  ```

  You may also see Service download failures in the **show interface** command output. Workaround: Remove and then reapply the NAT pool configuration.

- **CSCtg68475** (**CSCtg70470**)—After you add multiple ACE configurations and then remove them by deleting contexts, the ACE becomes unresponsive. The backtrace indicates a WeightBucket-related operation. Workaround: None.
- **CSCtg72700**—This issue is due to an open SIP data channel pinhole facing the client direction. When you allocate a valid port range from 1025 to 65535 for the PAT port and the ACE performs an implicit PAT, the ACE includes the 5060 and 5061 control ports. If the ACE uses these two ports and the next packet matching these pinholes is a new call control packet instead of data, the ACE mishandles the new control packet and promotes the pinhole.

  The traffic itself is not interrupted. However, when the ACE releases the resource, since it handled this control packet and the flow as a pinhole promoted data channel (although it does not affect classification in which the flow is still treated as SIP control or inspection), it does not send it for load balancing to release the policy map entry and eventually a resource leak occurs. Workaround: None.
- **CSCtg84721** (**CSCtg84678**)—When you attempt to log in to the ACE console with a username containing an @ character, the login attempt fails. For example, if you use the user@cisco username, as soon as you type the @ character, the ACE deletes everything before the character. Workaround: Perform either of the following:
  - Log in to the ACE over SSH.
  - Cause a failed login attempt on the console first before attempting to login with a username with an @ character.
- **CSCtg96108** (**CSCtg96913**, **CSCtg45244**)—When traffic is flowing through the ACE and you change the configuration with respect to the real server, probe and clearing statistics, weight bucket for the real server may become corrupted causing the ACE to reboot. This is an one-time occurrence. Workaround: None.
- **CSCth04943**—The **show** commands output may not display the configured interface description for the physical ports. Workaround: None.
- **CSCth13081** (**CSCth13078**)—When you configure multiple interfaces to share the same multi-match policy, you cannot ping a VIP defined on the ACE. Workaround: Removing and reapplying the class map in the multi-match policy may clear this issue.
- **CSCth24111**—When you enter the **show logging message all** command on the ACE, it displays the unnecessary log messages (5123456, 6101005, 6101006, 6101007, 2888006, and 6101004). Workaround: None.
- **CSCth24858**—After running the Device Manager GUI for more than a few months or a year, it cannot deploy a configuration to the ACE. There is no impact on the ACE load balancing. It continues to work. Workaround: Enter the **dm reload** command from the ACE CLI to restart the Device Manager.
- **CSCth26460**—When you configure the following commands, you cannot define a user role group different from the default Network-Monitor group, even if the group has the same permissions, especially the Permit-Monitor group:
  - **snmp-server user** *name* **r1**, where **r1** is a previously defined role. It writes on the running configuration.
  - **snmp-server user** *name* **Network-Monitor**

  Workaround: None.

- **CSCth34168**—When transparent probes are configured, the ACE may incorrectly use the wrong real server's MAC address if a new probe is sent to another real server before the previous probe completes. For example, suppose that the ACE sends a TCP SYN (probe A) to the real server with the MAC address ending with 1a:0d. The real server will respond with a SYN-ACK. If the ACE sends another probe to a different real server (for example, one whose mac address ends in 15:2d) before probe A completes, the ACE may use the MAC address ending with 15:2d for the ACK instead of the MAC address ending with 1a:0d for probe A. The real server will send a TCP RST in response. Workaround: Use the real server's physical IP address as the probe destination address.
- **CSCth36734**—If more than one pair of redundant ACE appliances are on the same network using the same VLANs and there are more than 21 redundant contexts configured among the ACE pairs, it is not possible to choose Fault Tolerant Group IDs in a manner in which they are not reused. Since the VMAC, the MAC address to alias IP and VIPs, is based on the FT group ID, reusing FT group IDs leads to MAC address collisions. This problem occurs because the allowable FT group IDs are 1 to 21. To allow a second pair of ACEs on the same network, additional FT Group IDs from 21 to 42 would be required. Workaround: Use fewer than 21 redundant contexts. Use separate VLANs for each ACE pair.
- **CSCth38238**—In both FT or non-FT configurations, when you add a new entry to the object group, the expected behavior is to expand. If you add a new entry after removing and adding the first access list where the object group is associated, it does not expand. Workaround: Remove the access list and readd it.
- **CSCth40276** (**CSCth13221**)—When TCP probes are sent to specific services which may cause unusual TCP sequences to occur, the ACE may run out of sockets for the probes. The output for the **show probe detail** command displays the following:

  ```
  Internal error: Out of sockets
  ```

  Workaround: Increase the open timer for the probes to increase the time it takes before the ACE runs out of sockets. If you reboot the ACE while the problem is occurring, it temporarily clears this issue.
- **CSCth53019**—When you configure a role with the real-inservice feature and assign this role to a user, this user cannot use the **inservice standby** command. Workaround: Instead of the real-inservice feature, configure the server farm feature in the role.
- **CSCth55161**—When TACACS+ is configured, the ACE does not account for configuration mode commands that contain sensitive information (for example, keys and passwords). Such commands do not appear in the local ACE accounting log nor in the TACACS server accounting log. In the ACE accounting log, there are descriptive entries (for example, “deleted user”). In the supervisor engine accounting log, the commands are accounted for, but the sensitive information is masked. Workaround: None.
- **CSCth56535**—When the ACE performs RADIUS load balancing on thousands of requests per second over one connection, the ACE reboots. Workaround: Reduce the request rate or spread the requests over more connections.
- **CSCth59667** (**CSCth06234**)—When you configure a match statement in a match-all class map, you cannot modify the statement. Workaround: Remove the class map from the associated Layer 3 policy and then modify the match statement.
- **CSCth76771**—When you configure the UDP port equal to 5060 (**udp eq 5060**) on the active ACE, it appears as the **udp eq sip** command in the **show run** command in the active and the standby ACEs. When a bulk synchronization occurs, the standby ACE does not recognize the command and transitions to the Cold state. UDP equal to 5060 is not standard port on the ACE. Workaround: Use the **tcp-udp eq 5060** command.

- **CSCti02047**—When the ACE is using SSL client authentication and is oversubscribed beyond capacity, HTTPS probes fail even after traffic has failed over to the standby ACE. The connections become stuck. Workaround: Do not allow the ACE to be oversubscribed. Clear the connections and allow the connections to continue.
- **CSCti42268**—When you configure a match source address and traffic is sent from that source address, a loadbalance (LB) crash is seen in the policy selection. Workaround: None.
- **CSCti56408**—When you change the value of the **limit-resource all minimum** command, the ACE may start rate-limiting traffic at a different throughput level from the level that the **show resource usage** command displays. Workaround: None.
- **CSCti68103**—When selecting a bridged VLAN as the SNMP server trap source, the ACE uses the BVI internal interface ID for the agent address instead of the BVI interface IP address. Workaround: Use a non-bridged VLAN.
- **CSCti73595**—In software version A4(1.0), the **crypto rehandshake enabled** command was added at the context level allowing you to enable SSL rehandshake for all VIPs in the current context. When you upgrade from software version A3(x) and the **crypto rehandshake enabled** command is configured in the Admin context, this command is added to all existing contexts on the standby ACE running software version A4(1.0). You can downgrade the software version from A4(1.0) to A3(x). However, incremental synchronization of this command is blocked between these versions to avoid the system SSL rehandshake behavior change. Bulk synchronization is still allowed from software version A4(1.0) to A3(x). If the command is enabled in the Admin context, it is copied to the A3(x) ACE and SSL rehandshake is enabled on all contexts. If the command is enabled in the user contexts, the cmd exec error message occurs on the standby ACE. However, the HA state stays in standby warm. Workaround: None.
- **CSCti95325**—Under normal operating conditions, the ACE core server could become unresponsive and the resulting core files would not be packaged, compressed, and stored in the core directory. The ACE does not reboot. Workaround: Use the diagnostic dplug to manually retrieve the files from the /var/tmp directory.
- **CSCtj05727**—When you use the Device Manager to create a probe expect status with a minimum and maximum value of 100 and then change the minimum value to 300 and maximum value to 600, the previous expect status of 100 is not removed and the new expect status is added in the CLI. Workaround: Log in to the CLI and remove the old **expect status** command and synchronize the context.
- **CSCtj19641**—When you configure a looped backup real server and the ACE receives traffic, if both real servers are not usable because of maximum connection failures, the ACE reboots due to an infinite loop. Workaround: None.

Software Version A4(1.0) Open Caveats

The following open caveats apply to ACE software version A4(1.0).

- **CSCsu40160**—When the ACE configuration has more than 500 service policies and you can ping all VIP addresses, some VIP addresses are not served at all. Workaround: None.
- **CSCsu55909**—In a redundant configuration, when you configure the ACE with 20 contexts, apply it to the active ACE, and then bring up the standby ACE with the configuration, the active ACE transitions into the Cold state with the following error:

  ```
  Error on Standby device when applying configuration file replicated from active
  ```

  Workaround: First bring up the active and standby ACEs individually and then enable redundancy.

- **CSCsv62417**—In some instances, the virtual MAC address is used for both the client-side VIP addresses and server-side NAT pools. With an FT VLAN configuration, the virtual MAC address is used as the source MAC for both client- and server-side packets. This behavior can cause issues in specific network topologies where the client-side and server-side end up learning the same MAC address over two ports. Without the FT VLAN, the internal MAC address is used. Workaround: Use the **mac address autogenerate** command to enable the autogeneration of a MAC address.
- **CSCsx06085**—When you enable UDP boost on the ACE, the server-initiated traffic fails because the destination port changes to the source port value. Workaround: Disable UDP boost.
- **CSCsz71578**—When you apply a service policy globally and then add the VLANs, the ACE displays ACL-merge errors for newly added VLANs and traffic does not flow through them. Workaround: Remove the global service policy and then reconfigure it.
- **CSCsz88519**—When you configure a TCP-based syslog server and the syslog server application on the remote system is down even though it can be reached from the ACE appliance, the ACE becomes unresponsive and most of its commands either time out or respond slowly. Workaround: Either bring the syslog server application up or remove the configuration for the TCP-based syslog server.
- **CSCta87584**—Connections may get dropped intermittently when you use persistence rebalance in a configuration and a rebalance is performed across traffic policies. This behavior typically occurs in a configuration with two different server farms that both contain the same real server with different ports, and the server farms are attached to two different Layer 7 load-balancing policy maps. Workaround: None.
- **CSCtc50852**—When many new clients that are directly connected send a burst of traffic, you may see a drop in traffic for a short time because the ACE takes time to resolve the ARPs. Also, mac-miss drop messages occur during this time. Workaround: The issue does not occur when the ARPs for the clients are already present in the ARP cache table.
- **CSCtd42287**— When the ACE is running with the maximum limit of 8K static entries and you remove a service policy from an interface and quickly readd it, the ACE removes the statements from the NAT policies. Workaround: Provide ample time between removing a service policy from an interface and then readding it.
- **CSCte76618**—When traffic traverses the ACE module with the same source and destination port and dynamic NAT for that traffic is enabled, the ACE performs an implicit PAT. This behavior interrupts some sessions. This problem does not occur when NAT is not involved. Workaround: If possible, disable dynamic NAT.
- **CSCte76958** (**CSCsr21689**)—The first packet of a TCP, UDP, or ICMP connection may not be captured; however, the remaining packets are captured for the same flow. This behavior can occur when you have the packet capture function configured for a specific ACL and for Layer 7 load-balanced traffic. Workaround: None.
- **CSCte96191**—On a rare occasion, the route manager becomes unresponsive on the standby ACE when you attempt configuration changes similar to the following on the active ACE:
  - Remove a service policy from local to global and global to local.
  - Remove or add VIPs in a Layer 3 class map which traffic is hitting.
  - Perform a checkpoint rollback.

  Workaround: None.
- **CSCtf54230**—When Layer 2 connected real servers are in the arp-failed state and probes are attached to all of them or the ACE is running a high rate traffic that generates many mac-miss IPCP messages, FT may appear to fail after several hours. Workaround: Remove the real servers in the arp_failed state or make sure that most of the real servers are UP.

- **CSCtg17350**—When you configure the Acceleration and Optimization features on the ACE, the integrated packet capture utility may not capture traffic from all interfaces, even when you configure the capture to capture from all interfaces. Workaround: None.
- **CSCtg31975**—A system admin account in the ACE software may allow an authenticated user to inject shell commands. This account does require authentication. Workaround: None.
- **CSCtg53126**—When you attempt to delete a server farm with the **no serverfarm host** command, the ACE displays the following error message:

  ```
  Error: serverfarm 'serverfarm_name' is in use. Cannot delete!
  ```

  The configuration manager thinks the server farm is still applied to the load-balance policy. Workaround: None.
- **CSCtg67860**—When you configure multiple track probes in two user contexts and enter the **show cfgmgr internal table track-probe** command, the ACE becomes unresponsive due to a Cfgmgr process failure. Workaround: None.
- **CSCtg76150**—When you configure an inline match statement that has a special character or space in its name under an Layer 7 policy, the checkpoint rollback fails. Workaround: Do not configure inline match statements with special characters or spaces.
- **CSCtg84721** (**CSCtg84678**)—When you attempt to log in to the ACE console with a username containing an @ character, the login attempt fails. For example, if you use the user@cisco username, as soon as you type the @ character, the ACE deletes everything before the character. Workaround: Perform either of the following:
  - Log in to the ACE over SSH.
  - Cause a failed login attempt on the console first before attempting to login with a username with an @ character.
- **CSCtg87927, CSCtf42007**—When you apply a real server to multiple server farms and the server recovers from a probe failure, it does not receive any new connections on any of the server farms. The **show probe** and **show serverfarm** commands indicate the real server is operational but does not have any current connections. Workaround: Remove the real server from service. Then, place it in service.
- **CSCtg87855** (**CSCtg87843**)— After you change the configuration in a large ACE configuration and enter **show** commands, the CLI becomes unresponsive for a period of time. In this case, the **show processes cpu | include cfgmgr** command displays one of the configuration manager (cfgmgr) processes consuming CPU resources. After you apply the configuration change, the cfgmgr CPU usage goes to zero, and the CLI becomes unresponsive. Workaround: Wait until the cfgmgr completes its previous operation before entering the **show** command.
- **CSCtg92971**—When the ACE uses an archive with the restore feature that has domain add-object configurations, the restore feature fails with the configurations. Workaround: Manually remove the affected configurations from the archive and restore it with a new archive file. After the restore is complete, you can reapply the manually removed configurations.
- **CSCtg96456**—When you configure the maximum number of the VIP statements in a single class map of 254 and then delete one of the VIP statements, the ACE cannot add a match VIP address in a single class map and displays the following message:

  ```
  Error: Exceeded maximum match item limit for the class-map
  ```

  Workaround: Remove the class map and the reconfigure it again with all of the VIP addresses.

- **CSCth01552**—When you configure a large number of directly connected real servers on the ACE and they are in the DOWN state, ARP resolution may fail intermittently for the directly connected hosts. Workaround: Transition the directly connected hosts to the UP state or decrease the number of directly connected hosts.
- **CSCth04993**—When you configure an ACE interface with single NAT IP address in the NAT pool and the ACE receives SIP UDP traffic, it resets subsequent SIP TCP traffic. Workaround: Perform either of the following:
  - Perform a checkpoint rollback to a non-SIP configuration and then to the existing configuration.
  - Increase the number of IP addresses in the NAT pool.
- **CSCth07619**—When you apply or modify ACLs or object groups to an ACE that has operated for a long time and undergone many ACL configuration changes, issues in the ACL object group expansion during the configuration download may cause an unexpected traffic drop. The **show interface** command displays a non-zero download failure counter, similar to the following:

  ```
  Access-group download failures : 8
  ```

  Workaround: Remove and readd the object group.
- **CSCth07709**—When performing the **snmpwalk** or **snmpbulkwalk** command for any object on the ACE, occasionally the ACE displays an Unknown user name error. The frequency of this occurrence can increase by having three contexts on the ACE. Workaround: None.
- **CSCth08116**—When you configure the **expect regex** command on HTTP or HTTPS probes with a long regex string and the web page parsed by the probe is longer than 100 kbytes with the matched string at the bottom of the page, the probes may fail. Workaround: Configure a basic HTTP probe that does not match a regular expression.
- **CSCth15305** (**CSCtg37325**)—During normal ACE operating conditions, the configuration manager becomes unresponsive and the ACE generates a core file. Workaround: None.
- **CSCth16258**—The **snmpwalk** or **bulkwalk** command on the SSL proxy MIB always returns a timeout. Currently, there is no tnrpc call to fetch data. The number of statistics has increased to string parsing and is taking more time. The default timeout is one second and it is not responding within one second. Workaround: Increase the timeout value.
- **CSCth20813**—In a multi-threaded code, some calls are unsafe and may cause the ACE to reboot. Workaround: None.
- **CSCth23304** (**CSCth12446**)—When the ACE is using a 1-Gbps throughput license, the throughput output displayed through the **show resource** command is rounded to the nearest thousand. For example, a value of 134217728 is rounded to 134217000. This issue does not occur with other throughput licenses. Workaround: Install a throughput license that is not 1 Gbps and then uninstall the license.
- **CSCth23432**—When you delete a certificate from a full image directory on the ACE and reboot the ACE, the ACE is not accessible from the XML interface and the Device Manager GUI does not work. Also, when the image directory is full, the ACE cannot generate a certificate. Workaround: Delete some data from the image directory and reboot the ACE, which will allow the creation of the certificate.
- **CSCth24647**—When the FT interface VLAN number is lower than the other interface numbers and these interfaces require the downloading of large configurations, an API timed out error occurs when applying the startup configuration. Workaround: Enter the **no ft auto-sync running-config** command and then enter the **ft auto-sync running-config** command.

- **CSCth26795**—When you configure the **mac-address autogenerate** command with the **ip dhcp relay** command on an interface, the ACE appliance fails to relay the DHCP request to the configured server and the counters displayed by the **dhcp relay statistics** command do not increment. Workaround: Remove the **mac-address autogenerate** command from the interfaces and reboot the ACE.
- **CSCth37401**—When the ACE receives HTTP traffic containing special characters in the cookie value, it does not properly parse the cookie. The ACE accepts a space inside the cookie value. However, a quoted string containing the comma (,) character inside the string may cause a parsing error. Based on RFC2068, special characters are not legal in the cookie value and are not allowed inside a quoted string. Refer to the following information from RFC2068:

```
token   = 1*<any CHAR except CTLs or tspecials>
    tspecials      = "(" | ")" | "<" | ">" | "@"
                   | "," | ";" | ":" | "\" | <">
                   | "/" | "[" | "]" | "?" | "="
                   | "{" | "}" | SP | HT
```

  Workaround: Do not use special characters inside the cookie value.
- **CSCth39505** (**CSCth39502**)—The ACE divides the sticky table and cookies between its two IXP network processors (NPs). If a connection on one NP uses a cookie with a hash that resolves to the other NP, the NPs must perform additional inter-IXP messaging to process the cookie. In a default TCP connection configuration, if the server sends 32K or more of data in less than 10 milliseconds (msec), a zero window may result on the backend. Some server TCP stacks may inadvertently introduce a 5-second delay in this situation. The ACE should advertise a non-zero window to the sending server when the buffers are released. Workaround: You can configure the **set tcp wan-optimization rtt 0** command to apply TCP optimizations to packets for the life of a connection. However, this command results in increased resource consumption.
- **CSCth53131**—When you add a class map to a configuration with a large number of class maps and the ACE fails to add it to the running configuration, the ACE displays an error message that does not describe the actual issue. Workaround: None.
- **CSCth55362**—When the ACE performs a configuration rollback, existing classes in a policy are not reordered according to the new configuration. The running configuration has a policy that contains several classes. The checkpoint contains that policy with some or all the classes in a different order. After performing the rollback, the order of the classes stays as it was in the running configuration. Workaround: Perform either of the following:
  - Remove the policy that was changed during the rollback and then perform the rollback.
  - If there are many similar policies in the configuration, perform a rollback to an empty configuration and then rollback to the desired configuration.
- **CSCth59247**—When you configure long and complex regular expressions in new or existing commands, the ACE does not allow you to make any additional changes and may become unresponsive for a long duration of time. Workaround: Shorten the regular expressions in the commands.
- **CSCth63553** (**CSCth63549**)—The standby ACE may have a higher number of connections than the active ACE. Workaround: Configure a shorter connection inactivity timeout.
- **CSCth64338**—If you configure TCP probes with small intervals and set the termination mode as forced, the TCP probe stops firing if the server sends an RST after the TCP handshake. Workaround: Remove and readd the faulty probe from the real server.

- **CSCth64381**—When you attempt to log in to the ACE using remote authentication with a username that has special characters that are not supported by the ACE, the securityd process becomes unresponsive and the ACE reboots. Workaround: Do not log in to the ACE with usernames with special characters that are not supported by the ACE.
- **CSCth67961** (**CSCsy66327**)—When you enter the **show snmp group** command from any context other than the Admin context, it does not display any output. Workaround: None.
- **CSCth74700**—Connectivity to the real server may be lost when you configure the following:
  - A client and server side VLAN on the ACE
  - A real server and ensure that it is Layer 2 reachable
  - A static route with a /32 mask to reach the real server through another interface

  Workaround: Remove and reconfigure the real server.
- **CSCth78715**—When you remove a NAT pool and quickly readd it with a new pool, if the IP addresses in the new pool overlap or are in common with the IP addresses in the removed pool and traffic is hitting the policy and there are active NAT allocations corresponding to the policy being removed, the ACE performs NAT or PAT allocation incorrectly.

  For example, NAT allocation is seen for PAT policy and PAT allocation is seen with NAT policy. The issue is due to the ACE freeing active NAT allocations incorrectly to the wrong pool. Workaround: When you replace a NAT policy with a new policy with an overlapping address or range, ensure that current NAT allocations time out or are removed before adding a new policy that reuses some of the same IP addresses.
- **CSCth84690**—When you configure a large number of NAT pools and they are in use and receiving traffic, if you change the configuration to a smaller number of NAT pools, the ACE delays the release of the older NAT translation resources. For this issue to occur, the ACE must have active NAT translation objects (xlates) that are in use. The cause of this issue is the queued-up reap messages that prevent the xlate from being reaped. In this case, the configuration rollback reduced 2k lines of NAT pools to a one-line NAT pool. The ACE generates one reap message per line for each removed NAT pool. Workaround: To avoid this issue, consider either of the following:
  - During configuration rollback, if the new configuration deletes a large number of NAT pools in one big pool but still keep the overall dynamic pool, remove the entire dynamic pool and readd it when required.
  - Set up a clean checkpoint that has an empty configuration. Perform a rollback to the first configuration and then perform a rollback to the second configuration. In this case, an overall reap message cleans the resource.

  Either of the workarounds can prevent a large number of reap messages from being produced and queued, which can cause the slow release of system resources.
- **CSCth89247**—When you place interfaces up and down several times or configure several interfaces or static routes, some interfaces or static routes may not work properly and connectivity to peers may be lost. Workaround: None.
- **CSCti11185**—If the client or server retransmits a packet and the remote end exceeds the acceptable window size, the ACE incorrectly drops the retransmission packet and increments the [Drops] fp TCP window left edge counter. Workaround: Disable normalization or correct the client or server to honor the window sizes.
- **CSCti11896**—The ACE treats the deny function inside a management policy or class map as a SKIP. The ACE does not deny the traffic. Instead, it skips the class map and tries to match another one. Workaround: None.

- **CSCti25263**—If the same SNMP request identifier is used in previous SNMP GET and GET NEXT requests to the ACE and an SNMP agent is polling the ACE, the ACE may incorrectly respond to the SNMP request. Workaround: Perform the following:
  a. Change the SNMP agent to use unique SNMP Request Identifiers for each SNMP request.
  b. Wait at least 10 seconds between SNMP requests that use the same SNMP request identifier.
- **CSCti28255**—When a real server state transitions to UP from a probe-failed or ARP-failed state, the ACE generates the CISCO-ENHANCED-SLB-MIB:cesRserverStateUp trap. However, if the real server goes down due to a probe-failed or ARP-failed state, the ACE generates the CISCO-ENHANCED-SLB-MIB:cesRserverStateChange trap. Workaround: None.
- **CSCti40433**—When the client sends a SYN on an existing Layer 7 connection, the ACE responds to a TCP SYN with an ACK, and an incorrect ACK sequence number. Workaround: None.
- **CSCti40456**—The ACE does not reset a SYN on an existing L7 connection. The SYN is for an existing L7 connection and the sequence number is within the receive window. Workaround: None.
- **CSCti53513**—When you configure the default class (class-default) as the only class map in a load-balancing policy with features that use regular expressions (for example, compression), the **show service-policy** command does not display the Regex dnld status field and its value. Workaround: None.
- **CSCti64563**—When you configure access control lists (ACLs) in the ACE, using the **access-list** *name* **resequence** command to renumber the line numbers may cause an ACL merge error and the access-list configuration fails to download to an interface. Workaround: Do not use the **access-list** *name* **resequence** command when you are configuring ACLs.
- **CSCti66770**—When the ACE receives a cookie string that contains many cookies and encounters a space character in the cookie value, it stops processing the cookies. Spaces are not permitted in the cookie name or cookie value. Persistence or stickiness fail. Workaround: None.
- **CSCti68347**—When you use the **system internal snapshot** command to force a cfgmgr core, the ACE generates a core dump. However, the backtrace does not provide correct information. Workaround: None.
- **CSCti68421**—If the ACL merge resources are almost exhausted and you add a configuration statement that places the resources over the limit, the ACE may drop traffic on the VLAN interface in which the configuration statement applies. Workaround: To restore service, remove the last configuration change that you made. To determine the current ACL merge resource status, enter the **show np 1 access-list resource** command in the Admin context and the s**how acl-merge merged-list vlan** *number* **in non-redundant** command in the context or VLAN where you will apply the configuration change.
- **CSCti68449**—The **show xlate** command displays thousands of entries. However, the **show resource usage** command displays zero peak and zero current. Workaround: Reboot the ACE.
- **CSCti73091**—When you configure access lists to be shared among multiple features, if you remove and readd the same access lists within the same download frame, the ACL line numbers go out of synchronization among the features. The ACE adds the line duplications for the access list to only one of the features. When you enable acl merge debug on the ACE, the ACE displays the following ACL Merge errors:

```
ACL-MERGE-ERROR:Duplicate lineno: lineno already exists
ACL-MERGE-ERROR:list insertion failure
```

Workaround: If the error has already occurred:

a. Remove the access groups from the features.

b. Remove and readd the access lists

c. Readd the access groups to the features.

If the error has not occurred, wait from 5 to 10 seconds between removing and readding the same access list.

- **CSCti74520**—When sending malformed requests, SSHD may become unresponsive. This issue has occurred when running testcase 4738 of the Codenomicon SSHV2 test tool. Workaround: None.
- **CSCti76373** (**CSCsu08736**)—When you download the DTD file shipped with ACE and check the definitions for features such as CRL, authgroup, DNS, RTSP, and SIP, some of the XML tags definitions are not available. Workaround: None.
- **CSCti76678**—When you change the default destination port for an HTTP probe, the probe does not append the port to the Host tag in the HTTP request and the ACE receives an HTTP/1.1 404 Not Found error. Workaround: Configure the probe with the **header Host header-value** command to specify and append the destination port to the host in the HTTP request.
- **CSCti85064**—Occasionally when the ACE is under high control plane (CP) stress with a high rate of CP syslog traffic at logging Level 7, the CP becomes sluggish. If the data plane becomes unresponsive, the ACE console become unresponsive and the ACE reboots by the SME process without creating any dataplane core files. Workaround: Avoid CP syslogs at level 7 with a high rate of traffic, or enable only fast path syslogs.
- **CSCti90916**—When you configure DNS load balancing and sticky on the ACE, DNS load balancing fails. Workaround: Do not configure sticky for DNS load balancing.
- **CSCti96864**—When you perform dynamic configurations of usernames in multiple contexts and enter the **no username** *name* command in a user context, the ACE module unexpectedly reboots and generates an SNMP core file. Workaround: None.
- **CSCtj00826**—If the ACE is running a large number of HTTP or HTTPS probes when probing a file approximately a megabyte in size, the ACE reboots. The following message may precede the reboot:

```
System running low on direct mapped memory
Please issue 'show system kcache' to diagnose further
```

Workaround: Reduce the size of the file being probed when running a large number of probes on the ACE.

- **CSCtj07489**—When you configure a policy map that references another policy map on the ACE, if the checkpoint rollback or restore operation removes these recursively referenced policy maps during context deletion while the operation loads another context, the cfgmgr process may become unresponsive. This is especially risky when all context policy maps are removed which can occur during a restore operation. Workaround: None.
- **CSCtj12692**—When you configure the ACE with 4000 sticky groups and do not allocate a sticky resource class, the resource values of the sticky are the default of a minimum of 0 and a maximum of unlimited. When the sticky database has 800,000 entries and you create a sticky resource class to a minimum value equal to 20 percent and apply it to the context, the ACE becomes unresponsive after a few minutes because it becomes unresponsive in the LB module at the function LbSticky_ReturnOldestEntry. Workaround: Do not change the resource class when you configure a large number of sticky groups and the database is full with active entries.
- **CSCtj18925**—When you configure many servers with active/active NIC teaming, the ACE arp_mgr service may consume 100% of the CPU due to the ARP flood caused by teaming mode. Workaround: Reduce ARP traffic. Always use active/standby NIC teaming.

- **CSCtj30082**—When the NPs on the ACE are in a combination of RETCODE-FAILED and INBAND-HM-FAILED state due to a traffic pattern that hashes connections to specific NPs, the **show serverfarm** *name* command displays the real servers as OPERATIONAL but they will not process any connections. Workaround: Enter the **no inservice** command and then enter the **inservice** command to restore the real server to a working state.
- **CSCtj30825**—When you configure a large number of ICMP probes and directly connected hosts on the ACE, ARP resolution fails intermittently for the directly connected hosts. Workaround: Decrease the number of ICMP probes or change the ICMP probes to TCP or UDP-based probes.
- **CSCtj45039**—When you configure a Session Initiation Protocol (SIP) probe for health monitoring (HM), the ACE may incorrectly display the probe as down due to the ACE using the same Call ID for multiple probe instances to different configured real servers. Workaround: Configure the ACE with a different probe type.
- **CSCtj68302**—When the ACE load balances clients towards the HTTP proxies, the ACE resets proxied SSL connection; an RST on the Client Hello. This issue may be associated with HTTP/1.1 in the CONNECT request or response. Workaround: You can configure HTTP/1.0 on the client and server. Do not inspect the HTTP connections.
- **CSCtj80208**— In a redundant configuration, the active ACE is running software version A4(1.0) with a full configuration and the standby ACE is running software version A3(2.X) with a user context that has a blank configuration. When you attempt to restore the configuration on the standby ACE for the user context, the active ACE reboots. Workaround: When restoring the configuration, trigger a bulk synchronization instead of an incremental synchronization by entering the **no ft auto-sync** command followed by the **ft-auto sync** command.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.