Release Note for the Cisco Application Control Engine Module (Software Version A4(1.1))

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 releases for the Cisco Application Control Engine Module (ACE), model ACE30 (ACE30_MOD_K9):

- A4(1.0)
- A4(1.1)

For information on the ACE module features and configuration details, see the ACE documentation located at:

http://www.cisco.com/en/US/products/ps6906/tsd_products_support_model_home.html

This release note contains the following sections:

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

Chassis, Supervisor Engine, and Cisco IOS Support for the ACE30 Module

Table 1 and Table 2 summarize the chassis, supervisor engine model, and Cisco IOS version support for the ACE30 module in the Catalyst 6500E series switch and the Cisco 7600 series router, respectively.

Table 1 Chassis, Supervisor Engine, and IOS Support for the ACE 30 in a Catalyst 6500 Series Switch with a Multilayer Switch Feature Card (MSFC3)

Catalyst 6500 Series Switch Chassis	Supervisor Engine Model	Minimum Required IOS Version
6503E	WS-SUP720-3B	12.2(33)SXI4 (or later)
6504E	WS-SUP720-3BXL	
6506E	VS-S720-10G-3C(=)	
6509E	VS-S720-10G-3CXL(=)	
6509-V-E		
6513		

Table 2 Supervisor Engine, Route Switch Processor (RSP), and IOS Support for the ACE30 in a Cisco 7600 Series Router with an MSFC3

Cisco 7600 Series Router Chassis	Supervisor Engine or RSP	Minimum Required IOS Version
7603	WS-SUP720-3B	15.0(1)S (or later)
7604	WS-SUP720-3BXL	
7609	RSP720-3C-GE(=)	
7613	RSP720-3CXL-GE(=)	
7603-S	RSP720-3C-10GE	
7604-S	RSP720-3CXL-10GE	
7606-S		
7609-S		

Virtual Switching System Support

The ACE30 running ACE software version A4(1.0) and installed in a Catalyst 6500 series switch running IOS software version 12.2(33)SXI4 or later supports the Virtual Switching System (VSS). VSS is a system virtualization technology that allows the pooling of multiple Catalyst 6500 switches into a single virtual switch for increased operational efficiency by simplifying the network. Inter-chassis Supervisor switchover (SSO) boosts non-stop communication. For more information about VSS, see the *Cisco IOS Version 12.2(33)SXI4 Configuration Guide*.

ACE Module Troubleshooting Wiki

The ACE documentation set now includes the ACE Module Troubleshooting Wiki. This wiki is a collaborative site that describes the basic procedures and methodology to assist you in troubleshooting the most common problems that you may encounter while you are operating your ACE.

As a registered user of Cisco.com, we strongly encourage you to add content to this site in the form of troubleshooting tips, procedures, or even entire sections. When you add content to the site, you should adhere to the format that has been established for the wiki. To access the ACE Module Troubleshooting Wiki on Cisco DocWiki, click the following URL:

http://docwiki.cisco.com/wiki/Cisco_Application_Control_Engine_(ACE)_Troubleshooting_Guide

New Software Features in Version A4(1.1)

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

- Using Data Path Online Diagnostics
- Increasing SSL Header Insert Max Header Size to 2048 Bytes
- Monitoring and Displaying the Network Processor Buffer Usage
- Clearing TCP Connections in the CLSRST State
- Reserving Admin Context Resources
- Increasing the Number of Secondary IP Addresses
- Configuring a Timeout for CRL Downloads
- Bypassing HTTP Strict Header Parsing
- Skipping a Malformed Cookie in an HTTP Flow
- Disabling Connection Replication
- Configuring a Probe under a Redirect Server
- Retaining Retcode and Inband Health Monitoring Statistics when a Real Server Goes from the Operational to the Inactive State
- Displaying NP-Related Details in the show serverfarm Command
- Displaying and Clearing Specific Sticky Information
- Displaying the Current and Total Sticky Connection to a Real Server
- Checking the Syntax of Generated XML Output
- Filtering the Running Configuration Based on the Name of the Object
- New Network Processor Hardware Interrupt Syslog in Version A4(1.1)
- New Counter for Fragmentation Reassembly Timeout

Using Data Path Online Diagnostics

Per CSCth10125, software release A4(1.1) introduces a new online diagnostic called TestNPLoopback that tests the control plane and the data plane of the ACE30. This test is one of several diagnostics that run automatically at bootup and it is initiated by the supervisor engine. You can also run this diagnostic and the others from the supervisor engine CLI.

Before the TestNPLoopback test can run, the supervisor sends an SCP message to the ACE to configure a special loop-back VLAN or to configure a shared memory space with the VLAN ID that the NPs can access. The VLAN exists internally between the ACE and the supervisor engine and you cannot modify it. The ACE ACKs that the test configuration is complete to the supervisor. If the ACE software does not send an ACK to the supervisor, after three failed retries, the supervisor resets the ACE.

The supervisor engine sends four specially marked diagnostic packets each with a different MAC address to the network processors (NPs) in the ACE30 daughter cards. The NPs must loop back the packets to the supervisor within 200 ms. If the supervisor does not receive the looped-back packet within the allotted time, it declares the test as failed. Upon any failure of the test, a syslog message is printed, error logs are recorded in the System Event Archive (SEA) logs, and an SCP message is sent to the ACE to indicate which NPs failed the test. The ACE decides whether to reset the module.

Enabling and Disabling Bootup Diagnostics

You can disable all bootup diagnostics by entering the following command from the supervisor engine in configuration mode:

```
c6k(config)# no diagnostic bootup level
```

To reenable bootup diagnostics, enter the following command:

```
c6k(config)# diagnostic bootup level complete | minimal
```

Running On-Demand Diagnostics

You can run any ACE bootup diagnostic test or all tests on demand at any time from the supervisor engine in Exec mode by entering the following command:

```
c6k#diagnostic start module number1 test number2 | name | all
```

The arguments are:

- *number1*—The module number
- *number2* | *name*—The number or the name of the test

Note that for each test you can enter either the test number or the test name.

To specify the number of repetitions for the on-demand tests, enter the following command:

```
c6k#diagnostic ondemand iterations number
```

For the *number* argument, enter an integer from 1 to 999.

To set the test parameters, enter the following command:

```
c6k#diagnostic ondemand test-parameter module number1 test number2 | name
```

Enter the module number and either the test number or the test name.

Stopping a Running Test

To stop a running diagnostic test, enter the following command in Exec mode:

```
c6k#diagnostic stop module number
```

For the *number* argument, enter the module number.

Health Monitoring Diagnostics

The health-monitoring diagnostics run in the background to monitor system health. You can configure the time interval between health-monitoring tests by entering the following command in configuration mode:

```
c6k(config)#diagnostic monitor interval module number1 {test number2 | name} hh:mm:ss
```

The arguments are:

- **interval**—Time period between health-monitoring tests
- **module** *number1*—Module number
- **test** *number2* | *name*—Number or name of the test
- *hh:mm:ss*—Test repeat interval in hours, minutes, and seconds

To configure the failure threshold for the health-monitoring diagnostics, enter the following command:

```
c6k(config)#diagnostic monitor threshold module number1 test number2 failure count number3
```

The keywords and arguments are:

- **threshold**—Specifies the health-monitoring failure threshold
- **module** *number1*—Module number
- **test** *number2* | *name*—Number or name of the test
- **failure count** *number3*—Number of test failures required to mark the test as failed

You can run a single health-monitoring test on demand by entering the following command:

```
#c6k#diagnostic start module number1 test number2 | name | all
```

You can disable an individual health-monitoring diagnostic or all health-monitoring diagnostics by entering the following command:

```
c6k(config)#no diagnostic monitor module number1 test number2 | name | all
```

Displaying ACE Diagnostic Failures on the Supervisor Engine

You can display all test failures from the supervisor engine by entering the following command:

```
c6k#show diagnostic result module number1 test number2
```

For each test failure, the supervisor displays a specific error code that indicates the reason for the failure. In the failure event, an SCP message is sent to notify the application about the failure. This notification allows the application to take appropriate action. For the ACE30, the CP collects core dumps on all the NPs and then resets the module.

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, 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 an integer from 1 to 4.

Table 3 describes the fields in the **show np buffer usage** command output when the buffer threshold command is configured.

Table 3 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.
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 2 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 2 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 A2(3.3) 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 A2(3.3) 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 3 describes the fields in the **show serverfarm** *name* **np** command output when the buffer threshold command is configured.

Table 4 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.
```

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 Version A4(1.0)

The A4(1.0) software release provides the following new features:

- HTTP compression of server responses (up to 6 Gbps)
- Inband health monitoring
- Probe port inheritance
- SSL cipher-base load balancing
- Support of SSL certificates signed with SHA-2 hashing algorithms (SHA-224 through SHA-512) for certificate verification in data plane SSL offload
- Sticky enhancements
- Syslog enhancements
- SNMP enhancements

ACE Operating Considerations

- 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.
- 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 A2(3.0) to A4(1.0), bulk sync, dynamic incremental sync, and connection replication are automatically disabled only while the active ACE is running software version A4(1.0) and the standby ACE is running software version A2(3.0). 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 an extended period of 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 Application Control Engine Module Administration Guide*.

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

Active	Standby	Bulk Sync	Dynamic Incremental Sync	Connection Replication	Comments
A2(3.0)	A4(1.0)	Yes	Yes	Yes	—
A4(1.0)	A2(3.0)	No	No	No	Functionality not supported due to architectural differences between the ACE20 and the ACE30 hardware

- During an upgrade to software version A4(1.0) in a redundant configuration, we recommend that you do not run the two ACEs with different versions of software (split mode) for an extended period of time. However, if you must remain in split mode for a period of time to make configuration changes, we strongly recommend that you disable configuration synchronization (config sync) by entering the following command:

  ```
  host1/Admin(con)# no ft auto-sync running-config
  ```

  When you have finished making configuration changes to the active ACE, reenable config sync by entering the following command:

```
host1/Admin(con)# ft auto-sync running-config
```

After you reenable config sync, the ACE automatically synchronizes the configuration changes from the active ACE to the standby ACE.

- We strongly recommend that you do not make any CLI changes when the ACE modules in a redundant configuration are running different software versions. Unexpected results may occur. Remove any new feature commands before performing a downgrade on the ACE.
- In software version A4(1.0), all four of the network processors (NPs) must transition into the retcode or inband failed state before the ACE marks the real server as RETCODE-FAILED or INHAND-HM-FAILED, respectively, and places it on the reactivate list for recovery. Note that the following may occur:
  - When some NPs are in the retcode failed state and the other NPs are in the inband failed state due to a traffic pattern that hashes connections to specific NPs, the real servers are in the OPERATIONAL state as displayed by the **show serverfarm** *name* command because the NPs are deadlocked waiting until the other NPs reach the retcode or inband failed state, respectively.
  - When some NPs are in the retcode or inband failed state due to a traffic pattern that hashes only to some NPs and not to the other NPs, the real servers are left in the OPERATIONAL state until all NPs transition into the retcode or inband failed state, respectively.

  When the traffic distribution is uniform across all NPs, these issues do not occur.
- The ACE requires a route back to the client before it can forward a request to a server. If the route back to the client is not present, the ACE cannot establish a flow and drops the client request. Make sure that you configure the appropriate routing to the client network on the ACE VLAN where the client traffic enters the ACE module.
- When you downgrade the ACE software, the features and commands of the higher release are lost because they are not supported by the lower release.
- Per CSCsz87533, the outbound UDP connection may timeout shortly after the ACE receives a RADIUS request, but before it gets the response for this request from the server. This situation can cause the ACE to improperly forward subsequent RADIUS traffic. If the server is not expected to initiate connections through the ACE, we recommend that you apply an inbound ACL on the server interface to block these connections.
- When redundant ACEs lose connectivity (for example, because of a network interruption) and they attempt to reestablish their connection, if you enter the **show ft peer** or **show ft group** command during this time, the response to this command may be delayed.
- If you are using the Application Networking Manager (ANM) to manage an ACE module and you configure a named object at the ACE CLI, ANM does not support all of the special characters that the ACE CLI supports for a named object. If you use special characters that ANM does not support, you may not be able to import or manage the ACE using ANM.

  When naming ACE objects (such as a real server, virtual server, parameter map, class map, health probe, and so on) for use with ANM, enter an alphanumeric string of 1 to 64 characters, which can include the following special characters: underscore (_), hyphen (-), dot (.), and asterisk (*). Spaces are not allowed.
- When you remove a NAT pool configuration, wait more than five seconds before adding a NAT pool with the same ID.
- The Account Expiry field for the **show user-account** command displays the date, if any, when the user account expires. This date is based on Coordinated Universal Time (UTC/GMT) which the ACE keeps internally. If you use the **clock timezone** command to configure a UTC offset, this field displays the UTC date and does not reflect the date with the offset as displayed by the **show clock** command.

Software Version A4(1.1) Resolved Caveats and Open Caveats

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

Software Version A4(1.1) Resolved Caveats

The following resolved caveats apply to 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.
- **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.
- **CSCth07619** (**CSCtg30362**)—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 re-add 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 KB 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**—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 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** (**CSCtg85460**)—The ACE divides the sticky table and cookies between its four 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-NP messaging to process the cookie. In a default TCP connection configuration, if the server sends 32 KB or more of data in fewer 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.

- **CSCth46984**—When you assign VLANs to the ACE module in a Cisco Catalyst SUP-2T VSS configuration, error messages flood the supervisor console. Workaround: None.
- **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 (CSCtf01034)**—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 re-add 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 2 K 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, do 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 re-add 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 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 (CSCth75707)**—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 (CSCsv82779)**—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** (**CSCth41583), CSCth37401** (**CSCth21361**)—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 fails. 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 test case 4738 of the Codenomicon SSHV2 test tool. Workaround: None.
- **CSCti76422 (CSCth69782)**—When you configure a VIP on the ACE, the ARP entry is inconsistent but the connections are working. 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 (CSCte81257)—**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 (CSCth66757)**—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.

- **CSCtj20521**—If the %EARL-SWITCH_BUS_IDLE error occurs in the chassis, the supervisor declares the ACE as MajFail and the LCPFW process stops responding. The **show proc** command does not display the LCPFW process. The **reload** command on the ACE does not work. Workaround: None.

- **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.
- **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 (CSCti13494)**—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.
- **CSCtj68574**—When the ACE is processing a high rate of concurrent SSL traffic with session ID reuse, header insert, and a small session cache timeout configured, the ACE may reload. Workaround: There is no effective workaround. However, keeping the session cache timeout value at approximately 1800 to 3600 seconds can reduce the possibility of this issue occurring.
- **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 Application Control Engine Module 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.

- **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.
- **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.
- **CSCtk18904**—When you are using the CLI to save the output of the **show tech** [**details**] command to disk, the command output may become truncated. Workaround: Do not save **show** command output to a file. Instead, log the remote session to the ACE30 and save the output that way.
- **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.
- **CSCtk65341**—When the ACE is configured with a primary VLAN interface as a server VLAN, it does not load balance traffic to the real servers on a secondary VLAN. Workaround: Reload the ACE after configuration and then the ACE load balances the traffic correctly.
- **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.
- **CSCtk93650, CSCtj81469**—When there is a high rate (1000 calls per second with one request per connection) of SIP calls over TCP, a proxy-related resource leak is observed. With a lower rate of SIP TCP traffic (approximately 400 calls per second), no resource leak is observed. Workaround: Reduce the number of SIP calls per second to a lower rate.
- **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 software version A4(1.1):

- **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 8 K static entries and you remove a service policy from an interface and quickly re-add it, the ACE removes the statements from the NAT policies. Workaround: Provide ample time between removing a service policy from an interface and then re-adding it.
- **CSCte76618** (**CSCsy31553**)—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.
- **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.
- **CSCtg87855** (**CSCtg22592**)—After you make a change to 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 drops to zero, and the CLI becomes unresponsive. Workaround: Wait until the cfgmgr process completes its previous operation before entering the **show** command.
- **CSCtg87895 (CSCtg22592)**—After you make a change to 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 drops to zero, and the CLI becomes unresponsive. Workaround: Wait until the cfgmgr process completes its previous operation before entering the show command.
- **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.
- **CSCth07709**—When performing the **snmpwalk** or **snmpbulkwalk** command for any object on the ACE, occasionally the ACE displays an Unknown username 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.
- **CSCth20813**—In a multi-threaded code, some calls are unsafe and may cause the ACE to reboot. Workaround: None.
- **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** (**CSCso76154**)—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 the ACE performs 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.
- **CSCti29333** (**CSCti08045**)—Intermittently, a race condition can occur when the ACE is using the same VIP to listen on two different ports with persistence rebalance that is also load balancing to the same real server with port redirection on the backend using the same port. The ACE resets the connection.

  For example, the ACE has the following configuration:

  ```
  vip 192.168.100.20: 443
  vip 192.168.100.20: 80
  rserver 10.10.10.20: 81
  ```

  The first connection enters on port 443. The ACE creates a second connection on port 80 while the first connection is still open. When the ACE attempts to set up the outbound flow for port 80, the race condition can occur. The ACE sees that the second flow has a redundant connection causing it to drop the flow. You can see the Drop [redundant connection]: counter increment in -socm. Workaround: Make sure that the VIP real servers are listening on different ports, for example:
  - VIP 192.168.100.20:443, real server 10.10.10.20:81
  - VIP 192.168.100.20:80, real server 10.10.20:82

  Do not have more than one VIP redirecting to the same port number on the same server on the backend. You could also use different real servers for each VIP port pair.
- **CSCti68421** (**CSCtc80207**)—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** (**CSCtf43237**)—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**—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 load-balancing 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.
- **CSCtj62399 (CSCsr76812)**—When you configure the ACE with Layer 7 load balancing, TCP connection may be disrupted. Packets arrive at the client in reverse order or packets are forced to be re-sent. Workaround: None.
- **CSCtj63378 (CSCtb55845)**—When a Virtual Switching System is configured on two Catalyst 6500 series switches, active-active redundancy is configured on the two ACEs in separate chassis, and you run stateless UDP traffic through the ACEs, some connections may fail. A trace shows that the successful flows use the ACE virtual MAC as the destination and the unsuccessful flows use the physical interface MAC of the standby ACE. A display of the default route and the svclc RHI routes shows two entries for the VIP in question. If you enter the **show ip route** command, the preferred route is the standby interface instead of the alias IP address. Workaround: None.
- **CSCtj63624 (CSCth52830)**—The supervisor reboots the ACE module due to a diagnostic failure. The last boot reason on the ACE is unknown and the ACE does not generate core files. The supervisor engine logs indicate the following:

```
date_time UTC: %LINK-5-CHANGED: Interface TenGigabitEthernet2/1, changed state  to
administratively down
date_time UTC: %LINEPROTO-5-UPDOWN: Line protocol on Interface  TenGigabitEthernet2/1,
changed state to down
date_time UTC: %OIR-SP-3-PWRCYCLE: Card in module 2, is being power-cycled off
(Diagnostic Failure)
date_time UTC: %LINK-SP-5-CHANGED: Interface TenGigabitEthernet2/1, changed  state to
administratively down
date_time UTC: %C6KPWR-SP-4-DISABLED: power to module in slot 2 set off  (Diagnostic
Failure)
date_time UTC: %SNMP-5-MODULETRAP: Module 2 [Down] Trap
date_time UTC: %LINEPROTO-SP-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet2/1, changed state to down
date_time UTC: %DIAG-SP-3-INVALID_TEST: Invalid test: TestRwEngineOverSubscription
date_time UTC: SP:  TestRwEngineOverSubscription is not valid for Module 2
```

  Workaround: None.

- **CSCtj65189 (CSCtb72635)**—When you run a script for the **show tech detail** command on an ACE that has 4000 BVI and 4000 VLAN interfaces configured, the ACE may become unresponsive. Workaround: None.

- **CSCtj65372 (CSCsy23268)**—The ACE may send probe traffic with the source IP address of the alias IP address instead of the local interface IP address. This issue occurs on the active ACE only. Workaround: None.
- **CSCtj65408 (CSCth99982)**—When you configure an ECHO TCP probe with send-data and regular expression (regex) values, the probe always passes even if the server sends a regex that does not match the sent-data value. Workaround: You can use a TCP probe with send-data and regex values as required instead of an ECHO TCP probe.
- **CSCtj65475 (CSCso82657)**—While moving a VLAN from a Cisco Firewall Services Module (FWSM) to an ACE or from an ACE to an FWSM, IP routing is not updated on the ACE to reflect the change. This behavior occurs when you are making a change to the **svclc** commands and the **shut** and **no shut** commands on the ACE interfaces. Workaround: None.
- **CSCtj65486 (CSCtg93332)**—When you configure the **mac-address autogenerate** command on the client VIP interface in bridge mode, traffic to VIP starts failing. Workaround: Delete the client side interface and re-add it.
- **CSCtj65501 (CSCth94715)**—When you configure multiple contexts in an FT configuration and configure probes for each context but you configure one context with an FT track probe, if you remove these contexts from the FT configuration and delete them, health monitoring may become unresponsive. Workaround: None.
- **CSCtj65628 (CSCsv80430)**—When you configure RBAC on an ACE with a custom role and domain, any permit rule allows all **show** commands to be entered regardless of the configured permissions. Workaround: None.
- **CSCtj65631 (CSCsx13061)**—When you perform a checkpoint rollback in a specific order or execute a match and no match statement under a class map, ACL memory is leaked and some entries configured in the ACL are not removed from the interface. Workaround: Remove the interface and re add it, or do not perform a rollback in the specific order mentioned in the steps to reproduce of the bug description.
- **CSCtj65634 (CSCsx28587)**—When the maximum ACL merge instance limit of 8191 is reached and then freed, ACL merge will not occur. Also, after reaching the maximum limit of instances, if you remove the outbound ACL from the interface, the policy action nodes are not released. Workaround: None.
- **CSCtj65642 (CSCsx55228)**—When you remove an entry with an object group from an ACL which is associated as a global access group and then re-add it, an ACL merge errors occur and disallowed traffic goes through the ACE. Workaround: Unconfigure and then reconfigure the access group.
- **CSCtj65644 (CSCsz19782)**—When you convert the configuration from a non-full proxy to a full proxy configuration for full proxied new connections and you add new VIPs for load balancing, traffic to these VIPs do not go through the ACE. Workaround: Reboot the ACE.
- **CSCtj65646 (CSCsz22742)**—When you copy a large configuration to the running-configuration file, an API timeout error may occur. Workaround: None.
- **CSCtj65668 (CSCth15050)**—When you place a VIP in a Layer 3 policy map out of service, the ACE does not remove the VSERVER-related ARP entries from the ARP cache. Workaround: Clear ARP to clear all ARP entries.
- **CSCtj65673 (CSCsz85367)**—When you configure and unconfigure access lists in a loop, the ACE experiences a memory leak. Workaround: Do not configure and unconfigure access lists in a loop.
- **CSCtj65676 (CSCta13446)**—When you remove and then reapply the **inspect ftp** command, the ACE drops connections. Workaround: None.
- **CSCtj65682 (CSCta39372)**—When you perform repetitive checkpoint rollbacks, the ACE becomes unresponsive after 5 to 6 hours. Workaround: None.

- **CSCtj65685 (CSCta73571)**—When you configure the **ft track** command for an interface that is constantly down and then attempt a checkpoint rollback from a large configuration to an empty configuration, the rollback ends prematurely, resulting in a partial rollback. The ACE, however, indicates that the rollback is complete. Workaround: Attempt the rollback once again. If it fails again, configure the **ft track** command with a greater difference between the active and standby priority settings.
- **CSCtj65687 (CSCtb00726)**—If the VIP address conflicts with the shared interface address across contexts, the standby ACE goes into the cold state with the **show ft config-error** command displaying the following error message:

  ```
  interface vlan number
  Error: Global Policy applied, conflicts with VIP, NAT or Interface IP in shared
  interface!
  ```

  Workaround: Do not configure a VIP address with the same address as the shared interface IP address on which the service policy is configured.
- **CSCtj65690 (CSCtb28077)**—When you add the **nat dynamic** *pool id* **vlan** *vlan-id* command to a Layer 3 rule (combination of Layer 3 policy map and Layer 3 class map), which already has one dynamic NAT pool configured. For example:

  ```
  policy-map multi-match pm1
  class vip1
  nat dynamic 1 vlan 731
  ```

  This configuration already contains one dynamic NAT statement. If you add another statement for NAT dynamic, that configuration will not be downloaded. Dynamic NAT configuration is not downloaded to Data Plane and dynamic NAT does not work. Workaround: Remove and add the service policy under the client interface.
- **CSCtj65693 (CSCtb32537)**—The **ip name-server** command is seen in the standby mode even after removing it in active mode. This issue happens in redundant configuration. Workaround: None.
- **CSCtj65895 (CSCsz67761)**—When a network error, such as a network interface going down, occurs during the bulk importing of crypto files, the temporary storage space for imported crypto files is not gracefully released. Some of the temporary files remain in the temporary storage area until the system is reloaded. Bulk import procedures do not perceive network failures or inactivity if the transfer of the files has begun. Workaround: None.
- **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 and Open Caveats

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

Software Version A4(1.0) Resolved Caveats

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

- **CSCsz49543, CSCtj68287 (CSCte26173)**—During periodic XML queries on ACE for **show** commands, such as **show ft group status**, the ACE places the bash core files in the core: directory. Some files are unpackaged and other files are mispackaged as VSH core files. Workaround: None.
- **CSCsz80038 (CSCsz92540)**—If the configuration contains inline match statements under a policy map, the check point rollback fails. For example:

  policy-map type inspect http all-match http-match

  match test strict-http

  reset

  Workaround: Remove all the inline match statements before doing the checkpoint rollback.
- **CSCtc21997**—When configuring a threshold for the **retcode** command, the minimum value for the *threshold* value should be 2 on the module. Workaround: None.
- **CSCtc52785**—When an HTTP or HTTPS probe fetches files that are larger than 8 KB, the **show probe** *probe_name* **detail** command for HTTPS and HTTP probe types displays no data in the Last Status Code field. Workaround: None.
- **CSCtc56023**—After changing the ports under a probe, the ACE may not initialize the probe and the statistics may get carried forward if multiple real servers have the same real server stamped with different ports. Port changes include:
  - Changing explicitly configured port to another port
  - Explicitly configuring a port to the **no port** default on a probe

  Workaround: Unconfigure and reconfigure all the same real server instances.
- **CSCtd00348**—When you configure NAT for DNS VIP traffic and the ACE cannot find a route for a third-party address, the ACE may not rewrite the A-record with the third party address. Therefore, the DNS query response from the server is forwarded with the original A-record address. Workaround: Configure a static route for the third-party subnet (for example, **ip route** *third_party_subnet subnet_mask gateway*).
- **CSCtd02062**—ARP entries for newly configured hosts or interfaces may not appear in the ARP table. When a large number of interfaces are deleted, for example, a rollback from a configuration having a large number of interfaces to a blank configuration and if the interface or real server configuration is immediately tried after the rollback succeeds, the ACE may take some time to add the ARP entries to the ARP table. Workaround: None.

- **CSCtd03068**—When you enter the **dir image:** command, the command output shows incorrect used space and free space because the ACE includes internal file system space in the free and used space calculation. This is a cosmetic issue only. Workaround: None.
- **CSCtd17908 (CSCth85288)**—When a real server that is Layer 2 connected to the ACE and in the ARP_FAILED state is moved to one hop away (for example, you shut down or deleted the corresponding interface and now it is reachable through a gateway), the real server's state does not return to OPERATIONAL. Workaround: Unconfigure and reconfigure the given real server.
- **CSCtd19640**—When you add and then delete the shared primary VLAN, traffic from the client or the server in a secondary VLAN that needs to be routed or bridged through the ACE fails. Workaround: Reload the ACE.
- **CSCtd38326**—After 16 K server farms are created, the client authentication redirect feature is accepted by the CLI, but connections are failing. The ACE is not validating the server farm ID availability while configuring the feature. To test for this problem, enter the **sh cfgmgr internal table** *serverfarm_name* **count** command. Workaround: The maximum number of server farms has been used and some need to be removed before new client authentication redirects can be added.
- **CSCtd39652**—When you interrupt the **show system internal mts buffer** command by pressing CTRL-c before the command completes, you may observe an mts buffer leak. Workaround: Exit from the current VSH session and log in again.
- **CSCtd45685**—Deleting a user context that has a sample cert and key can cause a memory leak in the itasca-ssl process. Workaround: None.
- **CSCtd51502**—If a domain name consists of more than 15 characters, the **show kalap udp all** command may show only the first 15 characters of the name. Workaround: None. Enter the **show run** command to see the full name of the domain.
- **CSCtd61399**—You may be observe that SSL client authentication requests are failing for a few requests that are sent immediately after the ACE boots up. Workaround: None.
- **CSCtd89844**—When 250 contexts are added and then removed and, subsequently, new contexts are added to a configuration, the **backup** command fails for a newly created context with no configuration in the probe script component with an error similar to the following:

  ```
  host1/Admin# show backup errors
  Context:ctx235
  Component:Probe scripts
  Error: Error, probe gpp1.tcl not found in disk0: or probe
  ```

  Workaround: None.
- **CSCtd90778**—While trying to add and delete match items under a load-balancing policy using copy and paste, config manager may become unresponsive. Workaround: Add and delete match items manually without using copy and paste.
- **CSCte19514**—Checkpoint rollback may fail with certain configurations. Workaround: None.
- **CSCte36785**—The archive restoration may complete successfully for archives with invalid licenses or with licenses not supported by the version. Workaround: None.
- **CSCte50124**—Checkpoint rollback may fail sometimes with the following error: "no NOTE: Configuration mode has been disabled on all sessions." This is a cosmetic error and has no impact on functionality. Workaround: None.
- **CSCte52355**—When XML output is enabled, no XML output is seen for the **show serverfarm** *serverfarm_name* **retcode details** command. Workaround: None.

- **CSCte55851**—When HTTP inspection is configured along with SSL termination and Layer 7 load balancing and HTTP and HTTPS traffic is passing through the ACE, adding inband TCP and retcode health monitoring configurations to the same server farm may cause a system reload because the HTTP inspection engine is accessing an invalid session state. Workaround: Disable HTTP inspection.
- **CSCte69958 (CSCsu22856)**— When you configure VIPs with sticky and the ACE resets new connection requests to these VIPs, the ACE displays the following **show** command output:
  - The **show stats sticky** command displays over 400,000 active sticky entries.
  - The **show conn count** command displays approximately 10,000 active connections.
  - The **show sticky database detail** command displays a large number of sticky entries, the active-conn-count field with 0 and the time-to-expire (secs) field with 0.

  Workaround: Clear the sticky database in the affected context.
- **CSCte76638**—When RTSP load balancing or RTSP inspection is configured, RTSP connections that contain a request message from the RTSP server are dropped by the ACE. Workaround: None.
- **CSCte79904**—If a large number (2000 or more) of real servers are down in the ARP_FAILED state, the CLI on the ACE appears to be less responsive. Workaround: None.
- **CSCte93954 (CSCsy98701)**—When you configure two ACEs as FT pairs that are replicating sticky entries and enter **show** commands on the active ACE, the standby ACE generates a load-balancing core file. Workaround: None.
- **CSCte97036**—When two or more probes are configured on a server farm, the ACE does not create the probe instance after you enter no inservice, remove one of the probes on the server farm, and then enter inservice on the real server. Workaround: None.
- **CSCte98195 (CSCtf33100)**—A real server configured under a server farm that is configured with more than one failing probe (PROBE-FAILED state) and the **fail-on-all** option may remain in the OPERATIONAL state even after you remove the **fail-on-all** option. Workaround: To restore the real server to move to the PROBE-FAILED state even if only one probe fails, enter the **no inservice** command followed by the **inservice** command.
- **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 configuration changes are done. When the parent real server hits the limits, the associated real servers are moved to stopped list. When this real server comes back into service (for example, it comes out of maxconn), some of the associated reals 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**—If you configure a non-TCP or non-UDP protocol (for example, ASP) in an object group immediately following a TCP or UDP port range, traffic may not match the ACL. Workaround: Configure the ACL directly without using an object group.
- **CSCtf12034**—The arp_mgr process may become unresponsive while you are applying a large multi-context configuration. Workaround: None.
- **CSCtf12749**—When you use a custom role in the ACE, certain commands may not be accessible even as read only. Workaround: Use the Admin role.

- **CSCtf15879**—When converting a CSS configuration to an ACE configuration, the CSS-to-ACE conversion tool does not properly convert the **persistence reset remap** command. Workaround: None.
- **CSCtf15949**—The CSS-to-ACE conversion tool attaches probes to a real server and to server farms of type redirect in the ACE configuration. However, the ACE does not allow probes to be attached to redirect server farms or real servers. Workaround: None.
- **CSCtf19783**—If you delete disk0: without the filename and you assign a filename on the ACE, it deletes the whole disk0: directory rather than just the file. If the directory is empty now and you enter a dummy filename, it deletes the disk0: directory; hence disk0: cannot be used after that. The disk0: directory is lost and is not created until the next reload of the ACE. Workaround: Reload the ACE.
- **CSCtf23244**—When a PAT pool that is associated with an interface is changed to a NAT pool, it is not downloaded to the data plane. The **show nat nat-pool** command reflects the updated changes, but the **show nat policies** command still reflects the old configuration, referencing it as PAT. This problem occurs only when you change a PAT configuration to NAT or a NAT configuration to PAT back-to-back. Workaround: Remove the configurations from the interface and apply the NAT configuration again.
- **CSCtf23571**—When you enter the **show context** command in a user context, the ACE may generate invalid XML output for the command. Workaround: Enter the command from the Admin context.
- **CSCtf25239**—When you are converting a service that accesses a page for a keepalive using the CSS-to-ACE conversion tool, the tool does not convert the IP address. Workaround: None.
- **CSCtf26876**—The CSS-to-ACE conversion tool may not properly convert catch-all rules from the CSS. Workaround: None.
- **CSCtf31292**—When a user context is configured for redundancy and its configuration mode is locked, the **restore** command fails with an error. For example:

```
host1/Admin# show restore errors
%ACE-7-111009: User 'admin' executed cmd: sh restore errors
Context: CTX1
Component:Running-cfg
 Below diff could not be applied
--
no NOTE: Configuration mode has been disabled on all sessions
no NOTE: Configuration mode has been disabled on all sessions
```

  Workaround: None.

- **CSCtf31299**—Headers are not inserted after a Layer 7 HTTP policy is activated to do so. Replacing the existing Layer 7 load-balancing policy in the multi-match policy with the Layer 7 HTTP policy with header insertion does not activate header insertion. Workaround: Remove and re-add the multi-match policy with the Layer 7 HTTP header insert policy already included in it.
- **CSCtf33301** (**CSCtf39655**)—When you configure the **send-data** command with a length that is greater than four characters inside a finger probe, the probe fails. When you configure the **expect regex** command with the ".*" string, the probe also fails. Workaround: Configure the probe with a **send-data** length that is fewer than 4 characters.
- **CSCtf37639**—If an SNMP probe is configured with an invalid OID, probes eventually start failing with the "Internal Error: Out of Sockets" message. Workaround: Change the OID for the SNMP probe to a valid one.
- **CSCtf49106**—When preempt is configured on the ACE and the Catalyst 6500 series switch with the active ACE is reloaded, the ACE may not correctly replicate connections after rebooting and becoming active again and it may drop some connections. Workaround: If possible, disable preempt.

- **CSCtf49108**—When packet capture has been running from 15 minutes to several hours, the ARP entries fail to refresh, which causes the ACE to drop the connections. The **show ft peer detail** command output displays the peer state as FSM_PEER_STATE_TL_ERROR. This sequence of events causes redundancy to fail and network access to the ACE starts to fail. Workaround: Reload the ACE.
- **CSCtf79958 (CSCtg46241)**—During a high rate of Session Initiation Protocol (SIP) calls per second and during the initial processing of packets, if the SIP inspection engine encounters resource allocation failures such as memory allocation, object allocation, or inspection configuration version mismatch failures, the ACE may reboot. Workaround: Disable the SIP inspection feature, if possible.
- **CSCtf86417**—When the ACE module is configured for Role-Based Access Control (RBAC) using custom domains and roles and you log in with a username that has a user-configured domain and role, some commands do not work, but it is not clear why. Workaround: Use the specific forms of the **show rserver** *name* and **show serverfarm** *name* commands.
- **CSCtf87870**—Because the SNMP agent on ACE is read only, the snmpTargetSpinLock MIB object is not supported and has been removed from the ACE software. The MIB definition of snmpTargetSpinLock from SNMP-TARGET-MIB is as follows:
  - snmpTargetSpinLock OBJECT-TYPE
  - SYNTAX TestAndIncr
  - MAX-ACCESS read-write
  - STATUS current
  - DESCRIPTION

  This object is used to facilitate modification of table entries in the SNMP-TARGET-MIB module by multiple managers. In particular, it is useful when modifying the value of the snmpTargetAddrTagList object.

  Workaround: None.
- **CSCtf87898**—When the gslb_proto process receives a signal 11 or SIGSEGV, it does not create a core dump when it becomes unresponsive because of a segmentation fault. Workaround: None.
- **CSCtf89460**—When the UDP booster feature is enabled, every first packet is not forwarded to the real server on each NP. So, two packets are dropped per session. Workaround: Disable UDP booster.
- **CSCtf89505**—When you are manipulating an ACL, especially if you are removing it, the ACE may become unresponsive. Workaround: None.
- **CSCtf89480**—The syntax for configuring a class map with XML has changed. The correct syntax is:

  <class-map match-type='match-all' name='vip-cm'>

  <match_virtual-addr seq-num='2' virtual-address='10.10.10.52' protocol-type='tcp' operator='eq' port-tcp-name='www'/>

  </class-map>
- **CSCtf89525**—The syntax for configuring a sticky HTTP cookie via XML has changed. The correct syntax is:

  <sticky http-cookie='STDCOOKIE' sticky-group-name='hstk'>

  <cookie config-type='offset' offset-value='4' length='100'/>

  </sticky>

- **CSCtf89530**—In a redundant configuration, the standby ACE may become unresponsive upon reboot and display the following message: “Service name:cfgmgr(948) has terminated on receiving signal 11." Workaround: None.
- **CSCtf89544**—You may not be able to delete an interface even after you delete the associated policy map. When you remove the policy map directly, the association between the interface and NAT is not removed. Workaround: Remove the Layer 3 rules first and then remove the policy map. When you remove the Layer 3 rules, the association between the interface and NAT is removed.
- **CSCtf91681**—When the ACE is bridging packets from one VLAN to another and IGMP snooping is in use on the Catalyst 6500 series switch, all IPv4or IPv6 multicast traffic is not bridged or forwarded through the ACE module even though the ACE has ACLs to permit the traffic. The problem occurs even if there is a functioning IGMP snooping mrouter port in both vlans. Workaround: Disabling IGMP Snooping on the Catalyst 6500 causes the packets to flood and the ACE successfully bridges them from one VLAN to another.
- **CSCtf93893**—The sysmgr process may become unresponsive because of memory corruption that occurs while the ACE is booting. The memory corruption may not appear for a period of time until the process hits the corrupted area and then fails. Workaround: None.
- **CSCtg18762**—When redundant ACEs are running in split mode (running two different versions of software), secondary IP addresses configured under the interface on the active ACE may sync to the standby ACE as primary IP addresses. This problem occurs only when configuring the commands incrementally. This problem is not seen during bulk synchronization. Workaround: None.
- **CSCtg20931**—If you configure two entries in an ACL that use the same object group and that has everything else the same except the protocol, you may observe a duplicate line number error and the hosts in an object group are not downloaded. Workaround: Configure the entries under two different ACLs.
- **CSCtg21646**—When the ACE is configured with the **xml-show on** command and there is a policy map with a sticky server farm and action, the sticky server farm is duplicated in the XML output. Workaround: The XML output is correct if you remove the action from the policy.
- **CSCtg33663**—After configuring the **drop** option under a Layer 7 policy map, the ACE may reboot. When the policy has **drop** configured as the action, the ACE drops any request that hits this policy and increments some context counters (rejections and ACL denied). Rejections is a 64-bit counter and ACL denied is a 32-bit counter. For both counters, the LB_INCR_CONTEXT_STATS64 macro is used. When the macro is used for a 32-bit counter, the ACE may reload because of a signal 4 illegal instruction. Workaround: Remove the **drop** statement under the policy.
- **CSCtg37080**—You may observe that HTTP parameter map changes are not downloaded for an HTTP inspection policy. As a result, the secondary cookie delimiter and the secondary cookie start does not work for the inspection policy. Workaround: None.
- **CSCtg43059**—When you enter the **show 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.
- **CSCtg43402**—If you change the DHCP configuration for an interface and change the ACE mode of operation to bridge mode, cfgmgr may become unresponsive. Workaround: None.
- **CSCtg44508**—When SIP load balancing is configured and SYN RSTs have been received by the ACE, the **show serverfarm** command output does not show any connection failure for SYN RSTs. Workaround: None.
- **CSCtg45934**—After the **match** statement limit is reached and you delete some **match** statements, you cannot add a new **match** virtual statement under a class map. Workaround: Delete the last match statement and then add a new one.

- **CSCtg51515**—When client authentication, best-effort CRL, and the **cdp-error ignore** command are configured and the client sends a certificate that has no CDPs and that should fail client authentication for some reason other than a revocation check (for example, a bad issuer), the connection fails on the first attempt as expected, but, after a few reconnection attempts, starts to pass. Workaround: Either use a static CRL or disable the **cdp-error ignore** command.
- **CSCtg53426**—The ACE does not bridge TCN-BPDUs; it considers them invalid BPDU packets and drops them because of a bad Ethernet frame length. Workaround: None.
- **CSCtg56490**—When you have a large configuration with many **match http** statements in Layer 7 class maps, the **show service-policy detail** command output loops continuously. Workaround: None.
- **CSCtg69713**—When a real server is in the RETCODE FAILED state and a probe, which fails, is added to that real server, the real server assumes the OPERATIONAL state after **resume** *seconds* have elapsed. Instead, the real server should be in the DISABLED state on the data plane. Workaround: None.
- **CSCtg72700**—The 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, because the ACE handled this control packet and the flow as a pinhole-promoted data channel, which does not affect classification in that the flow is still treated as a SIP control or inspection flow, when it releases the resource, the ACE does not send the packets for load balancing to release the policy map entry. Eventually, a resource leak occurs. Workaround: None.
- **CSCtg75545 (CSCth02932)**—When you enter the **show np 1 me-stats | memory | status** or **show tech-support** commands in the user context, the ACE displays an error message. Workaround: Enter these commands in the Admin context.
- **CSCth12667**—If the class-default class map is the only class that is configured in the load-balancing policy, when you remove class-default from the configuration, traffic does not stop flowing. Workaround: Do not remove the class-default class map from the load-balancing policy if it is the only class attached to the policy.
- **CSCth24111**—When you enter the **show logging message all** command on the ACE module, the command output displays a log message that is specific to the ACE appliance. Workaround: None.
- **CSCth26460**—When you are creating an SNMP user or an SNMP community attached to a created role that is equivalent to Network-Monitor, you cannot attach a group other than the default Network Monitor group to an SNMP user or SNMP community even though there is no indication in the CLI help string that this is the only acceptable role. Workaround: None.
- **CSCth30569 (CSCth30569)**—When you apply a large multi-context configuration, the arp_mgr service in ACE becomes unresponsive. Workaround: None.
- **CSCth32609 (CSCtg83716)**—When you enable DNS inspection and a DNS response hits a PAT policy map, the ACE drops the response. Workaround: None.
- **CSCth38238**—In a redundant configuration with a network type object group, after adding a new entry to an object group that is associated with two different ACLs, the new entry may not appear in the expansion of one or both ACLs, although it should appear in both. Workaround: Create a second object group exactly like the first one, but with a new name and the new entry you want to add. Then add to each ACL that references the original object group a new line that references the new object group. Now you can remove the line from the ACL that referenced the original ACL. All the entries in the new object group should now appear when the ACL is expanded.

- **CSCth34168**—If transparent probe traffic is destined to multiple real servers using a single probe address and is interleaved (alternated with other probe traffic to the same IP address), the ACE may become confused about the destination MAC address. The problem does not happen if a probe runs from start to finish without interruption from any other probe traffic to the same probe address. Workaround: Send the probes to the real server physical IP address.
- **CSCth39220**—When there are multiple Layer 3 rules with static sticky entries, the ACE does not download the entries to the data plane for both case-sensitive and case-insensitive types. Workaround: Apply the entire configuration first and then add the static sticky entries to the sticky group.
- **CSCth48841 (CSCth75674)**—When the SCP HW watchdog on the ACE fails to detect the timer expiry, the Catalyst 6500 supervisor power cycles the ACE with an SCP keepalive failure message. The watchdog may fail to detect the timer expiry when the internal counters overflow. The SCP HW watchdog mechanism detects when the ACE becomes unresponsive and collects the core files in error case scenarios, which prevents the power cycling by the Catalyst 6500 supervisor. On very rare occasions, the watchdog may fail to detect the timer expiry. Workaround: None.
- **CSCth53019**—A user with a role that contains the real-inservice feature cannot enter the **inservice standby** command. Workaround: configure **feature serverfarm** instead of **feature real-inservice** in the role.
- **CSCth55161**—The ACE does not account for config mode commands that contain sensitive information, for example, keys and passwords. The commands are not in the local ACE accounting log nor on the TACACS server accounting log if TACACS is configured. In the ACE accounting log there are descriptive entries such as “deleted user.” However, there is no workaround for the TACACS accounting side of the problem. Testing the supervisor engine shows that 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.
- **CSCti02047 (CSCth74249)**—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 all connections and then allow connections to continue.
- **CSCti06274**—When ICMP packets are sent to the ACE with an IP header that contains IP options, invalid connections are seen for nonexistent or invalid hosts. Workaround: None.
- **CSCti21425**—When you enter the **show ipcp** command while the system is in a stressed state, you may see the “proc_file_read: Apparent buffer overflow” error on the console. There is no actual buffer overflow and this is only a display issue. Workaround: None.
- **CSCti42268**—When **match source-address** is configured in a class map and traffic is sent from that source address, the ACE may become unresponsive because of an error in the load-balancing function. Workaround: None.
- **CSCti43744**—When the last NAT pool under an interface is removed and multiple NAT pools are added at the same time using copy and paste, the ACE does not download the NAT pool to the data plane. Workaround: Do not copy and paste such a configuration. Remove the NAT pool first and then, after waiting for some time, add it back.
- **CSCti44478**—When the control plane is stressed and there is a high rate of syslogs being generated, the kernel may become unresponsive at the buf_alloc_hdr() instruction. Workaround: Change the syslog level/severity to 4 or below to relieve the stress on the control plane.

- **CSCti56408**—A configuration change in the **limit-resource all minimum** percentage may cause the ACE to start rate-limiting traffic at a different throughput level than what is indicated by the **show resource usage** command. Workaround: None.
- **CSCti68103**—When selecting a bridged VLAN (VLAN part of BVI) as the SNMP-server trap-source and the SNMP v1 trap is sent with an agent IP address 0.0.0.x., the ACE uses the BVI internal interface ID to fill in 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. When you configure this command, SSL rehandshake is enabled for all VIPs in the current context. When you upgrade from A2(1.6a) or later, if the **crypto rehandshake enabled** command is configured in the Admin context, on the standby ACE that is running the A4(1.0) software image, the command is added to all existing contexts. A downgrade from A4(1.0) to A2(x) is currently blocked; thus, there is not a downgrade issue. If the CLI is enabled in user contexts, a 'cmd exec error' occurs on the standby; however, the redundancy state stays in STANDBY_WARM.
- **CSCth76771**—Configuring **udp eq sip** causes the standby ACE to enter the STANDBY_COLD state. UDP port 5060 is not a standard port in the ACE. Workaround: Configure **tcp-udp eq 5060** instead.
- **CSCti87496**—When the Admin context is not part of the FT group and different resources are allocated, if the active ACE has available resources and then you configure some static sticky entries, the standby ACE does not go to the STANDBY_COLD state if a standby context is starved of all resources. Workaround: Do not starve the standby ACE of all resources.
- **CSCtj19641**—When you configure a looped backup real server, both real servers are not usable (for example, because of maximum connection failures), and the ACE receives traffic, the ACE reboots because of an infinite loop. Workaround: None.
- **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 re-add the real server.

Software Version A4(1.0) Open Caveats

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

- **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 8 K static entries and you remove a service policy from an interface and quickly re-add it, the ACE removes the statements from the NAT policies. Workaround: Provide ample time between removing a service policy from an interface and then re-adding it.
- **CSCte76618** (**CSCsy31553**)—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.
- **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.
- **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.
- **CSCtg87855** (**CSCtg22592**)—After you make a change to 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 drops to zero, and the CLI becomes unresponsive. Workaround: Wait until the cfgmgr process completes its previous operation before entering the **show** command.
- **CSCtg87895 (CSCtg22592)**—After you make a change to 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 drops to zero, and the CLI becomes unresponsive. Workaround: Wait until the cfgmgr process 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.
- **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.
- **CSCth07619** (**CSCtg30362**)—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 re-add the object group.
- **CSCth07709**—When performing the **snmpwalk** or **snmpbulkwalk** command for any object on the ACE, occasionally the ACE displays an Unknown username 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 KB 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**—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.
- **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 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** (**CSCth21361**)—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** (**CSCtg85460**)—The ACE divides the sticky table and cookies between its four 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-NP messaging to process the cookie. In a default TCP connection configuration, if the server sends 32 KB or more of data in fewer 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.
- **CSCth46984**—When you assign VLANs to the ACE module in a Cisco Catalyst SUP-2T VSS configuration, error messages flood the supervisor console. Workaround: None.
- **CSCth53131** (**CSCsy05318**)—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** (**CSCso76154**)—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 the ACE performs 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 (CSCtf01034)**—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 re-add 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 re-add 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 2 K 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, do 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 re-add 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 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 (CSCth75707)**—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 (CSCsv82779)**—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.
- **CSCti29333** (**CSCti08045**)—Intermittently, a race condition can occur when the ACE is using the same VIP to listen on two different ports with persistence rebalance that is also load balancing to the same real server with port redirection on the backend using the same port. The ACE resets the connection.

  For example, the ACE has the following configuration:

  ```
  vip 192.168.100.20: 443
  vip 192.168.100.20: 80
  rserver 10.10.10.20: 81
  ```

  The first connection enters on port 443. The ACE creates a second connection on port 80 while the first connection is still open. When the ACE attempts to set up the outbound flow for port 80, the race condition can occur. The ACE sees that the second flow has a redundant connection causing it to drop the flow. You can see the Drop [redundant connection]: counter increment in -socm. Workaround: Make sure that the VIP real servers are listening on different ports, for example:

  - VIP 192.168.100.20:443, real server 10.10.10.20:81
  - VIP 192.168.100.20:80, real server 10.10.20:82

  Do not have more than one VIP redirecting to the same port number on the same server on the backend. You could also use different real servers for each VIP port pair.

- **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.

- **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.
- **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** (**CSCth41583**)—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 back trace does not provide correct information. Workaround: None.
- **CSCti68421** (**CSCtc80207**)—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** (**CSCtf43237**)—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 re-add 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 re-add the access lists.
  c. Re-add the access groups to the features.

  If the error has not occurred, wait from 5 to 10 seconds between removing and re-adding the same access list.
- **CSCti74520**—When sending malformed requests, SSHD may become unresponsive. This issue has occurred when running test case 4738 of the Codenomicon SSHV2 test tool. Workaround: None.
- **CSCti76373**—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.
- **CSCti76422 (CSCth69782)**—When you configure a VIP on the ACE, the ARP entry is inconsistent but the connections are working. 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.

- **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.

- **CSCti96864** (**CSCte81257)—**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.

- **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.

- **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 load-balancing 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 (CSCth66757)**—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.

- **CSCtj20521**—If the %EARL-SWITCH_BUS_IDLE error occurs in the chassis, the supervisor declares the ACE as MajFail and the LCPFW process stops responding. The **show proc** command does not display the LCPFW process. The **reload** command on the ACE does not work. Workaround: None.

- **CSCtj25006 (CSCth77963)**—When you upgrade ACE to software version A2(2.4), the ACE logs the following message after the reboot message:

  ```
  %ACE-4-901001 kernel: Cannot find mapfile.
  ```

  Workaround: None.

- **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.
- **CSCtj62399 (CSCsr76812)**—When you configure the ACE with Layer 7 load balancing, TCP connection may be disrupted. Packets arrive at the client in reverse order or packets are forced to be re-sent. Workaround: None.
- **CSCtj62639 (CSCtb30178)**—If you configure a RADIUS client Layer 7 policy map and continuously send accounting On/Off packets for 12 hours, the system fails. Workaround: None.
- **CSCtj63378 (CSCtb55845)**—When a Virtual Switching System is configured on two Catalyst 6500 series switches, active-active redundancy is configured on the two ACEs in separate chassis, and you run stateless UDP traffic through the ACEs, some connections may fail. A trace shows that the successful flows use the ACE virtual MAC as the destination and the unsuccessful flows use the physical interface MAC of the standby ACE. A display of the default route and the svclc RHI routes shows two entries for the VIP in question. If you enter the **show ip route** command, the preferred route is the standby interface instead of the alias IP address. Workaround: None.
- **CSCtj63624 (CSCth52830)**—The supervisor reboots the ACE module due to a diagnostic failure. The last boot reason on the ACE is unknown and the ACE does not generate core files. The supervisor engine logs indicate the following:

  ```
  date_time UTC: %LINK-5-CHANGED: Interface TenGigabitEthernet2/1, changed state  to
  administratively down
  date_time UTC: %LINEPROTO-5-UPDOWN: Line protocol on Interface  TenGigabitEthernet2/1,
  changed state to down
  date_time UTC: %OIR-SP-3-PWRCYCLE: Card in module 2, is being power-cycled off
  (Diagnostic Failure)
  date_time UTC: %LINK-SP-5-CHANGED: Interface TenGigabitEthernet2/1, changed  state to
  administratively down
  date_time UTC: %C6KPWR-SP-4-DISABLED: power to module in slot 2 set off  (Diagnostic
  Failure)
  date_time UTC: %SNMP-5-MODULETRAP: Module 2 [Down] Trap
  date_time UTC: %LINEPROTO-SP-5-UPDOWN: Line protocol on Interface
  TenGigabitEthernet2/1, changed state to down
  date_time UTC: %DIAG-SP-3-INVALID_TEST: Invalid test: TestRwEngineOverSubscription
  date_time UTC: SP:  TestRwEngineOverSubscription is not valid for Module 2
  ```

  Workaround: None.
- **CSCtj65189 (CSCtb72635)**—When you run a script for the **show tech detail** command on an ACE that has 4000 BVI and 4000 VLAN interfaces configured, the ACE may become unresponsive. Workaround: None.
- **CSCtj65372 (CSCsy23268)**—The ACE may send probe traffic with the source IP address of the alias IP address instead of the local interface IP address. This issue occurs on the active ACE only. Workaround: None.

- **CSCtj65408 (CSCth99982)**—When you configure an ECHO TCP probe with send-data and regular expression (regex) values, the probe always passes even if the server sends a regex that does not match the sent-data value. Workaround: You can use a TCP probe with send-data and regex values as required instead of an ECHO TCP probe.
- **CSCtj65475 (CSCso82657)**—While moving a VLAN from a Cisco Firewall Services Module (FWSM) to an ACE or from an ACE to an FWSM, IP routing is not updated on the ACE to reflect the change. This behavior occurs when you are making a change to the **svclc** commands and the **shut** and **no shut** commands on the ACE interfaces. Workaround: None.
- **CSCtj65486 (CSCtg93332)**—When you configure the **mac-address autogenerate** command on the client VIP interface in bridge mode, traffic to VIP starts failing. Workaround: Delete the client side interface and re-add it.
- **CSCtj65501 (CSCth94715)**—When you configure multiple contexts in an FT configuration and configure probes for each context but you configure one context with an FT track probe, if you remove these contexts from the FT configuration and delete them, health monitoring may become unresponsive. Workaround: None.
- **CSCtj65628 (CSCsv80430)**—When you configure RBAC on an ACE with a custom role and domain, any permit rule allows all **show** commands to be entered regardless of the configured permissions. Workaround: None.
- **CSCtj65631 (CSCsx13061)**—When you perform a checkpoint rollback in a specific order or execute a match and no match statement under a class map, ACL memory is leaked and some entries configured in the ACL are not removed from the interface. Workaround: Remove the interface and re add it, or do not perform a rollback in the specific order mentioned in the steps to reproduce of the bug description.
- **CSCtj65634 (CSCsx28587)**—When the maximum aclmerge instance limit of 8191 is reached and then freed, ACL merge will not occur. Also, after reaching the maximum limit of instances, if you remove the outbound ACL from the interface, the policy action nodes are not released. Workaround: None.
- **CSCtj65642 (CSCsx55228)**—When you remove an entry with an object group from an ACL which is associated as global access group and then re-add it, merge errors occur and nonallowed traffic goes through the ACE. Workaround: Unconfigure and then reconfigure the access group.
- **CSCtj65644 (CSCsz19782)**—When you convert the configuration from a non-full proxy to a full proxy configuration for full proxied new connections and you add new VIPs for load balancing, traffic to these VIPs do not go through the ACE. Workaround: Reboot the ACE.
- **CSCtj65646 (CSCsz22742)**—When you copy a large configuration to the running-configuration file, an API timeout error may occur. Workaround: None.
- **CSCtj65668 (CSCth15050)**—When you place a VIP in a Layer 3 policy map out of service, the ACE does not remove the VSERVER-related ARP entries from the ARP cache. Workaround: Clear ARP to clear all ARP entries.
- **CSCtj65673 (CSCsz85367)**—When you configure and unconfigure access lists in a loop, the ACE experiences a memory leak. Workaround: Do not configure and unconfigure access lists in a loop.
- **CSCtj65676 (CSCta13446)**—When you remove and then reapply the **inspect ftp** command, the ACE drops connections. Workaround: None.
- **CSCtj65682 (CSCta39372)**—When you perform repetitive checkpoint rollbacks, the ACE becomes unresponsive after 5 to 6 hours. Workaround: None.

- **CSCtj65685 (CSCta73571)**—When you configure the **ft track** command for an interface that is constantly down and then attempt a checkpoint rollback from a large configuration to an empty configuration, the rollback ends prematurely, resulting in a partial rollback. The ACE, however, indicates that the rollback is complete. Workaround: Attempt the rollback once again. If it fails again, configure the **ft track** command with a greater difference between the active and standby priority settings.
- **CSCtj65687 (CSCtb00726)**—If the VIP address conflicts with the shared interface address across contexts, the standby ACE goes into the cold state with the **show ft config-error** command displaying the following error message:

  ```
  interface vlan number
  Error: Global Policy applied, conflicts with VIP, NAT or Interface IP in shared
  interface!
  ```

  Workaround: Do not configure a VIP address with the same address as the shared interface IP address on which the service policy is configured.
- **CSCtj65690 (CSCtb28077)**—When you add the **nat dynamic** *pool id* **vlan** *vlan-id* command to a Layer 3 rule (combination of Layer 3 policy map and Layer 3 class map), which already has one dynamic NAT pool configured. For example:

  ```
  policy-map multi-match pm1
  class vip1
  nat dynamic 1 vlan 731
  ```

  This configuration already contains one dynamic NAT statement. If you add another statement for NAT dynamic, that configuration will not be downloaded. Dynamic NAT configuration is not downloaded to Data Plane and dynamic NAT does not work. Workaround: Remove and add the service policy under the client interface.
- **CSCtj65693 (CSCtb32537)**—The **ip name-server** command is seen in the standby mode even after removing it in active mode. This issue happens in redundant configuration. Workaround: None.
- **CSCtj65895 (CSCsz67761)**—When a network error, such as a network interface going down, occurs during the bulk importing of crypto files, the temporary storage space for imported crypto files is not gracefully released. Some of the temporary files remain in the temporary storage area until the system is reloaded. Bulk import procedures do not perceive network failures or inactivity if the transfer of the files has begun. Workaround: None.
- **CSCtj68302 (CSCti13494)**—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.
- **CSCtj68574**—When the ACE is processing a high rate of concurrent SSL traffic with session ID reuse, header insert, and a small session cache timeout configured, the ACE may reload. Workaround: There is no effective workaround. However, keeping the session cache timeout value at approximately 1800 to 3600 seconds can reduce the possibility of this issue occurring.
- **CSCtj80208**—In a redundant configuration, the active ACE30 is running A4(1.0) and the standby ACE20 is running A2(3.x). In this split mode, dynamic incremental sync is automatically disabled. After a switchover for a single user context that is configured only on the ACE30, when you try to restore a local backup of the user context that was taken on the ACE30 to the ACE20, dynamic incremental sync is enabled because the ACE20 is now active for the user context and the ACE30 reboots. Workaround: Disable dynamic incremental sync before you restore the user context configuration by entering the no ft auto-sync command. After the restore completes, enter the ft auto-sync command to trigger a bulk sync.

- **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.
- **CSCtj81469**—When there is a high rate (1000 calls per second with one request per connection) of SIP calls over TCP, a proxy-related resource leak is observed. With a lower rate of SIP TCP traffic (approximately 400 calls per second), no resource leak is observed. Workaround: Reduce the number of SIP calls per second to a lower rate.

Available ACE Licenses

By default, the ACE supports virtualization with one Admin context and five user contexts, 4 gigabits per second (Gbps) module bandwidth, 1 Gbps compression, and 1,000 SSL transactions per second (TPS). You can increase the number of default user contexts, module bandwidth, and SSL TPS by purchasing the licenses shown in Table 6.

Table 6 ACE30 License Bundles

License Bundle	Product ID (PID)	License File	Description
Base (default)	ACE30-BASE-04-K9	None required	4 Gbps bandwidth 1 Gbps compression 1,000 SSL TPS 5 Virtual Contexts
Base to 4 Gbps 4 Gbps Bundle	ACE30-MOD-UPG1= ACE30-MOD-04-K9	ACE30-MOD-UPG1 ACE30-MOD-04-K9	4 Gbps bandwidth 6 Gbps compression 30,000 SSL TPS 250 Virtual Contexts
4 Gbps to 8 Gbps 8 Gbps Bundle	ACE30-MOD-UPG2= ACE30-MOD-08-K9	ACE30-MOD-UPG2 ACE30-MOD-08-K9	8 Gbps bandwidth 6 Gbps compression 30,000 SSL TPS 250 virtual contexts
8 Gbps to 16 Gbps 16 Gbps Bundle	ACE30-MOD-UPG3= ACE30-MOD-16-K9	ACE30-MOD-UPG3 ACE30-MOD-16-K9	16 Gbps bandwidth 6 Gbps compression 30,000 SSL TPS 250 virtual contexts

You can also obtain an ACE demo license for each license bundle. You can get a demo license that is valid for 30 or 90 days. At the end of this period, you will need to update the demo license with a permanent license to continue to use the ACE software. To view the expiration of the demo license, use the **show license usage** command in Exec mode. If you need to replace the ACE module, you can copy and install the licenses onto the replacement module.

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

Ordering an Upgrade License and Generating a License Key

This section describes the process to order an upgrade license and to generate a license key for your ACE. To order an upgrade license, perform the following 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 cisco.com website. As a registered user of cisco.com, go to this URL:

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

Step 3 Enter the Product Authorization Key (PAK) number found on the license certificate as your proof of purchase.

Step 4 Provide all the requested information to generate a license key.

Step 5 After the system generates the license key, you will receive a license key e-mail with an attached license file and installation instructions. 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 about installing and managing ACE licenses, refer to Chapter 3, Managing ACE Software Licenses, in the *Cisco Application Control Engine Module Administration Guide*.

Upgrading Your ACE Software in a Redundant Configuration

To upgrade you ACE software to version A4(1.0), you must also migrate your ACE10 or ACE20 module to a new ACE30 module. For details about migrating to an ACE30 and upgrading your software to A4(1.0), see the procedure in the *Cisco Application Control Engine (ACE30) Module Installation Note*.

Downgrading Your ACE Software in a Redundant Configuration

If you need to downgrade your ACE software from version A4(1.0) to an earlier supported ACE software version (version A2(3.x) or A2(1.6a) or later), use the procedure in the *Cisco Application Control Engine (ACE30) Module Installation Note*.

ACE Documentation Set

In addition to this document, the ACE documentation set includes the following publications:

Document Title	Description
Cisco Application Control Engine Module Hardware Installation Note	This guide provides information for installing the ACE into the Catalyst 6500 series switch and the Cisco 7600 series router.
Cisco Application Control Engine Module Getting Started Guide	This guide describes how to perform the initial setup and configuration tasks for the ACE.
Cisco Application Control Engine Module Administration Guide	This guide describes how to perform administration tasks on the ACE, including initial setup, establish remote access, configure class maps and policy maps, manage the ACE software, configure SNMP, define system message logging, configure redundancy, and upgrade your ACE software.
Cisco Application Control Engine Module Virtualization Configuration Guide	This guide provides instructions on how to operate your ACE in a single-context or in multiple-contexts. Multiple-contexts use the concept of virtualization to partition your ACE into multiple virtual devices or contexts.

Document Title	Description
Cisco Application Control Engine Module Routing and Bridging Configuration Guide	This guide provides instructions for configuring the routing and bridging features of the ACE. This guide provides a routing overview and describes how to perform ACE configuration tasks, including: • Configuring VLANs • Configuring routing • Configuring bridging • Configuring Address Resolution Protocol (ARP) • Configuring Dynamic Host Configuration Protocol (DHCP)
Cisco Application Control Engine Module Server Load-Balancing Configuration Guide	This guide describes how to perform ACE server load-balancing configuration tasks, including: • Server health monitoring • Real servers and server farms • Stickiness • Class maps and policy maps to load-balance traffic to real servers in server farms • Firewall load balancing • TCL scripts
Cisco Application Control Engine Module Security Configuration Guide	This guide describes how to perform ACE security configuration tasks, including: • Security access control lists (ACLs) • User authentication and accounting using a TACACS+, RADIUS, or LDAP server • Application protocol and HTTP deep packet inspection • TCP/IP normalization and termination parameters • Network address translation (NAT)
Cisco Application Control Engine Module SSL Configuration Guide	This guide describes how to perform ACE SSL configuration tasks, including: • SSL certificates and keys • SSL initiation • SSL termination • End-to-end SSL
Cisco Application Control Engine Module System Message Guide	Describes how to configure system message logging on the ACE. This guide lists and describes the system log messages generated by the ACE.
Cisco Application Control Engine Module Command Reference	This reference provides an alphabetical list of all command line interface (CLI) commands including syntax, options, and related commands.

Document Title	Description
Cisco CSM-to-ACE Conversion Tool User Guide	Describes how to use the CSM-to-ACE conversion tool to migrate Cisco Content Switching Module (CSM) running-configuration or startup-configuration files to the ACE.
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.
Cisco Application Control Engine (ACE) Troubleshooting Guide	Describes the procedures and methodology in wiki format to troubleshoot the most common problems that you may encounter during the operation of your ACE.
Cisco Application Control Engine (ACE) Configuration Examples Wiki	Provides examples of common configurations for load balancing, security, SSL, routing and bridging, virtualization, and so on.

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.