Release Note for the Cisco 4700 Series Application Control Engine Appliance

April 30, 2012

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

Contents

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

- A4(2.3)
- A4(2.2)
- A4(2.1a)
- A4(2.1)
- A4(2.0)

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

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

This release note contains the following sections:

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

New Software Features in Version A4(2.3)

Software version A4(2.3) provides the following new features:

- Support for NTPv3 Authentication
- Mitigating a Slowloris HTTP DoS Attack
- Closing a TCP Connection in a FIN_WAIT State
- Ability to Allow send-data to Support Carriage Return and Linefeed Characters
- Modifications to the show ip fib Command
- Extended Range of Supported Characters in a URL
- Ability for the ACE to Accept a User Account with an Expired Date
- Accessibility of Device Manager GUI Troubleshooting Tools from the ACE Appliance CLI

Note For a summary of CLI command and system message changes for software version A4(2.2), see the "Software Version A4(2.3) Resolved Caveats, Open Caveats, Command Changes, and System Log Messages" section.

Support for NTPv3 Authentication

The Network Time Protocol (NTP) synchronizes the ACE system clock to a time server. Per CSCtr62165, the ACE appliance now complies with the NTPv3 standard and supports NTPv3 authentication through the addition of a series of new **ntp** commands in configuration mode and a series of new **show ntp** commands in Exec mode.

For details on the use of NTP by the ACE appliance, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*, Chapter 1, Setting Up the ACE, the "Synchronizing the ACE with an NTP Server" section.

This section includes the following topics:

- Configuring NTP Authentication
- Enabling NTP Logging
- Displaying NTP Information

Configuring NTP Authentication

You can configure the ACE appliance to authenticate the time sources to which the local clock is synchronized. When you enable NTP authentication, the ACE appliance synchronizes to a time source only if the source carries one of the authentication keys specified by the **ntp trusted-key** command. The ACE appliance drops any packets that fail the authentication check and prevents them from updating the local clock.

Note NTP authentication is disabled by default.

To configure your ACE appliance for NT authentication using the new ntp commands included as part of software version A4(2.3), follow these steps:

Step 1 Use the **ntp authentication-key** command to define the authentication keys. The ACE appliance does not synchronize to a time source unless the source has one of these authentication keys and the key number is specified by the **ntp trusted-key** number command. The syntax of the **ntp authentication-key** configuration mode command is as follows:

ntp authentication-key *number* **md5** *md5-string*

To remove an NTP authentication key, use the **no** form of this command.

The keywords and arguments are as follows:

- **number**—Authentication key number. The range is from 1 to 65535.
- md5—The MD5 algorithm for authentication.
- *md5-string*—Enter up to a maximum of 16 alphanumeric characters for the MD5 string.

Step 2 Use the **ntp trusted-key** command in configuration mode to specify one or more keys (defined using the **ntp authentication-key** command) that the time source must provide in its NTP packets in order for the ACE appliance to synchronize to it. This command provides protection against accidentally synchronizing the ACE appliance to a time source that is not trusted. The syntax of the **ntp trusted-key** configuration mode command is as follows:

ntp trusted-key *number*

To remove the NTP trusted key, use the **no** form of this command.

The range for the *number* argument is from 1 to 65535.

Step 3 Use the **ntp authenticate** configuration mode command to enable or disable NTP authentication. NTP authentication is disabled by default. The syntax of the **ntp authenticate** configuration mode command is as follows:

ntp authenticate

To disable NTP authentication, use the **no** form of this command.

For example, to configure the ACE appliance to synchronize only to time sources that provide authentication key 42 in their NTP packets, enter:

```
host/Admin# config
host/Admin(config)# ntp authentication-key 42 md5 ExampleKey
host/Admin(config)# ntp trusted-key 42
host/Admin(config)# ntp authenticate
```

Enabling NTP Logging

You can enable NTP logging in order to generate system logs with significant NTP events. Use the **ntp logging** configuration mode command to turn on NTP logging for the ACE appliance.

Note NTP logging is disabled by default.

The syntax of the **ntp logging** configuration mode command is as follows:

ntp logging

To turn off NT logging on the ACE appliance, use the **no** form of this command.

For example, to enable NTP logging for the ACE appliance, enter:

```
host/Admin# config
host/Admin(config)# ntp logging
```

Displaying NTP Information

To display the new NTP configuration status and relevant information, use the **show ntp** command from Exec mode. Only users who are authenticated in the Admin context can use the **show ntp** command.

The syntax of the **show ntp** configuration mode command has been expanded as follows:

show ntp {**authentication-keys** | **authentication-status** | **logging-status** | **trusted-keys**}

The keywords are as follows:

- **authentication-keys**—Displays the configured NTP authentication keys.
- **authentication-status**—Displays the status of NTP authentication.
- **logging-status—**Displays the NTP logging status.
- **trusted-keys**—Displays the configured NTP trusted keys.

For example, enter:

```
host/Admin# show ntp authentication-keys
-----------------------------
 Auth key         MD5 String
-----------------------------
  1               ExampleKey

host/Admin# show ntp trusted-keys
Trusted Keys:1

host/Admin# show ntp logging-status
NTP logging enabled.

host/Admin# show ntp authentication-status
Authentication enabled.
```

Mitigating a Slowloris HTTP DoS Attack

Slowloris is an HTTP Denial of Service (DoS) tool written in PERL that is used to perform denial of service attacks against Apache-based servers (as well as other web services). Slowloris exhausts all available server connections by repeatedly initiating several hundred valid HTTP requests to the server and keeping these connections open using a minimal amount of TCP traffic to consume server resources. Once server resources are exhausted, the server is no longer able to respond to legitimate traffic.

Per CSCtu08459, you are now able to configure the ACE to mitigate a Slowloris HTTP DOS attack by including an HTTP parse timeout in your HTTP parameter map. With software version A5(1.2), the new **set max-parse-time** command has been added as protection from Slowloris DoS attacks. The default HTTP parsing timeout is set to 255 seconds, and if the ACE does not receive a GET request from the connection within 255 seconds, the HTTP parse timeout initiates and the ACE drops the connection and sends a reset to the client. You can increase this timeout maximum through the **set max-parse-time** command.

The syntax of this parameter map HTTP configuration mode command is as follows:

set max-parse-time *time*

The *time* argument is the time in seconds for the maximum length of the HTTP parsing timeout. Valid entries are 1 to 65535 seconds.

For example, to enter an HTTP parsing timeout of 200 seconds, enter the following:

```
host1/Admin(config)# parameter-map type http HTTP_MAP
host1/Admin(config-parammap-http)# set max-parse-time 200
```

Closing a TCP Connection in a FIN_WAIT State

You may be operating in an environment where connections do not close due to clients that fail to reply to a FIN from one or more real servers. This situation can result in the server continuing to handle the open connections (remaining in a FIN_WAIT_1 state), which, during high volume traffic, can result in the server running out of connections. As a result, the server maintains a high CPU load because it continues to wait for a FIN, ACK, or RST to close the connection. The server is unable to answer requests because it is handling the open connections.

Per CSCtr61749, the ACE now supports the ability to define a timeout in your connection parameter map for TCP connections that are in the FIN_WAIT_I state. The **set tcp timeout** command now includes the **fast-fin** option to specify the FIN timeout (in seconds). This command is available in the Admin context only.

The syntax of this parameter map connection configuration mode command is as follows:

set tcp timeout fast-fin *time*

The *time* argument is the time in seconds after which the ACE will send a timeout for TCP connections that are in a FIN_WAIT_1 state. Enter an integer from 1 to 4294967295. The default is no FIN timeout.

For example, to set a FIN timeout of 200 seconds, enter the following:

```
host1/Admin(config)# parameter-map type connection conn_para
host1/Admin(config-parammap-http)# set tcp timeout fast-fin 60
```

To return to the default state of no FIN timeout, enter the following:

```
host1/Admin(config-parammap-http)# no set max-parse-time
```

The **show parameter-map** command output now includes information on the state of the fast FIN timeout, as shown below:

```
host1/Admin# show parameter-map

 Number of parameter-maps: 2

 Parameter-map: CONN_MAP
 Description: -
 Type: connection
    nagle                              : disabled
    slow start                         : disabled
    buffer-share size                  : 32768
    inactivity timeout (seconds)       : 240
    reassembly timeout (seconds)       : 60
    embryonic timeout (seconds)        : 5
    ack-delay (milliseconds)           : 200
    WAN Optimization RTT (milliseconds): 65535
    half-closed timeout (seconds)      : 3600
    fast FIN timeout (seconds)         : disabled >>>>>>>>>>>>> This field has been added
    TOS rewrite                        : disabled
    syn retry count                    : 4
    TCP MSS min                        : 0
    TCP MSS max                        : 1460
    tcp-options drop range             : 0-0
    tcp-options allow range            : 0-0
    tcp-options clear range            : 1-255
    selective-ack                      : clear
    timestamp                          : clear
    window-scale                       : clear
    window-scale factor                : 0
    reserved-bits                      : allow
    random-seq-num                     : enabled
    SYN data                           : allow
    exceed-mss                         : drop
    urgent-flag                        : allow
    conn-rate-limit                    : disabled
    bandwidth-rate-limit               : disabled
```

Ability to Allow send-data to Support Carriage Return and Linefeed Characters

Per CSCts40548, the send-data under the TCP, ECHO, and UDP probes now allows the following combination of Carriage Return (CR) and Linefeed (LF) characters:

- \r\n
- \r\r
- \n\n
- Multiples of these (such as \r\n\r\n)

An example would be “send-data GET / HTTP/1.0\r\n\r\n”.

The conversion to CR,LF will be as follows :

- \r\n in send-data would be converted to CRLF while sending probe data to the server.
- \r\r in send-data would be converted to CRCR while sending probe data to the server.
- \n\n in send-data would be converted to LFLF while sending probe data to the server.

Separate entries such as \r and \n in send-data would not be converted to CR and LF. They will be sent as '\' followed by 'r', and '\' followed by 'n', respectively, similar to the process prior to the introduction of this enhancement in software version A4(2.3).

Modifications to the show ip fib Command

Per CSCtu37951, the overflow (V) flag now displays the legend explanation in the **show ip fib** command as displayed in the following output:

```
host1/Admin# show ip fib

FIB for Context Admin (RouteId 0)

   Codes: H - host,   I - interface
          S - static,      N - nat
          A - need arp resolve,      E - ecmp
          V - virtual server

Destination         Interface         EncapId  Flags
------------------------------------------------------------------------
224.0.0.0/3         N/A                 DROP   N/A [0x100]
127.1.0.0/16        vlan1                  1   SI [0x18]
25.25.25.0/24       vlan200                0   IA [0x30]
25.25.25.49/32      vlan200                3   H [0x3]
127.1.0.0/32        N/A                 DROP   N/A [0x10]
127.1.0.1/32        vlan1                  1   I [0x10]
25.25.25.86/32      vlan200                4   H [0x3]
25.25.25.214/32     N/A                 DROP   V [0xc00]
127.1.255.255/32    N/A                 DROP   N/A [0x10]
25.25.25.0/32       N/A                 DROP   N/A [0x10]
25.25.25.99/32      N/A                 DROP   N/A [0x10]
25.25.25.255/32     N/A                 DROP   N/A [0x10]
25.25.25.11/32      vlan200                5   H [0x3]
25.25.25.13/32      vlan200                2   H [0x3]
Total route entries = 14
```

Extended Range of Supported Characters in a URL

In software releases prior to A4(2.3), the ACE HTTP parser accepted characters in the range of 32 to 126 characters in the UTF-8 encoding schema for URLs. Per CSCts64534, with software release A4(2.3) the ACE has extended support for characters in the range from 128 to 255 (all characters) in the UTF-8 encoding schema for URLs. This extended range is allowed only when the **parsing non-strict** command is configured in the HTTP parameter map configuration mode.

Ability for the ACE to Accept a User Account with an Expired Date

You create a user and define the associated role and operating domains by using the **username** command in configuration mode. You can optionally specify an expiration date of the user account. In software releases prior to A4(2.3), when the user account is configured with a specified expiration date in the past (with reference to the ACE system clock), the ACE displays the error message "date should be in the future, expiry date wrong" and the configuration is then rejected. When operating in a redundant configuration, when the username expires, the expired configuration is not removed from the running-configuration file on the active ACE which can result in synchronization issues.

Per CSCtx45830, with software release A4(2.3), when the user account is configured with an expiry date in the past (with reference to the ACE system clock), the ACE displays the error message “User created with expiry date in the past, please edit to make it usable, which allows the configuration to be accepted. You can then modify the expiration date associated with the user account.

The change allows an expired “username” configuration to be accepted.

For example:

```
host1/Admin(config)# do show clock
Wed Mar 14 11:16:09 UTC 2012
host1/Admin(config)# username abcd pass cisco123 expire 2012-03-10 role Network-Monitor
domain default-domain
User created with expiry date in the past, please edit to make it usable
host1/Admin(config)#
```

Accessibility of Device Manager GUI Troubleshooting Tools from the ACE Appliance CLI

Per CSCtq28184, software version A4(2.3) now enables you to utilize the following troubleshooting tools on the Device Manager GUI directly from the ACE appliance CLI:

- Enable the Device Manager GUI (if it is not running) using the **dm enable** CLI command.
- Verify the health of the Device Manager using the **dm status** command.
- Restart the Device Manager using the **dm reload** command.
- Create and upload a lifeline to a remote TFTP server using the **dm lifeline** CLI command.

For details on troubleshooting the ACE appliance Device Manager GUI, see the *Cisco 4700 Series Application Control Engine Appliance Device Manager GUI Configuration Guide*, Chapter 16, Using ACE Device Manager Troubleshooting Tools.

Enabling the Device Manager GUI

By default, the ACE appliance Device Manager is always enabled. If you find that the ACE appliance Device Manager is no longer running, you can use the **dm enable** configuration mode command to restart the Device Manager GUI.

For example, enter:

```
host/Admin# config
host/Admin(config)# dm enable
```

If you need to stop the ACE appliance Device Manager, enter the **no dm enable** configuration mode command as follows:

```
host/Admin(config)# no dm enable
```

The **no dm enable** command will be included in the running-configuration file.

Note If you specify the **no dm-enable** command and save the updated running-configuration to the startup-configuration file, when you reload the ACE appliance, the Device Manager GUI will automatically be disabled. At that point, you must specify the **dm enable** configuration mode command to restart the Device Manager GUI.

Checking the ACE Appliance DM GUI Status

If you find that the ACE appliance Device Manager GUI appears to be inoperative, enter the **dm status** CLI command in Exec mode to verify the health of the Device Manager. The **dm status** command output indicates the status of the Device Manager: whether it is running or stopped. This status is reflected in the DM and MySQL fields of the status output.

Note You must be the global administrator to access the **dm status** CLI command. This command is only available to the global administrator.

For example, enter:

```
host1/Admin# dm status
DM ROOT:
DM HOME: /opt/CSCOanm
JAVA_HOME: /opt/CSCOanm/jre
MYSQL_HOME: /opt/CSCOanm/mysql
java is /opt/CSCOanm/jre/bin/java

DM : STOPPED (1230)
MySQL : STOPPED (1187)
```

If you see that the status is "STOPPED," restart the Device Manager by using the **dm reload** command. You must be the global administrator to access the **dm reload** command. Restarting the Device Manager does not impact ACE functionality; however, it may take a few minutes for the Device Manager to reinitialize as it reads the ACE CLI configuration.

For example, enter:

```
host1/Admin# dm reload
Are you sure you want to reload? [y/n]: y
Beginning Reload...
Reload done..
```

Reenter the **dm status** CLI command in Exec mode to verify that the status of the Device Manger is "RUNNING."

For example, enter:

```
host1/Admin# dm status
DM ROOT:
DM HOME: /opt/CSCOanm
JAVA_HOME: /opt/CSCOanm/jre
MYSQL_HOME: /opt/CSCOanm/mysql
java is /opt/CSCOanm/jre/bin/java

DM : RUNNING (1230)
MySQL : RUNNING (1187)
```

Creating a Lifeline Package from the ACE Appliance CLI

If you encounter issues with the ACE appliance Device Manager GUI (for example, when the Device Manager GUI is inoperative), use the **dm lifeline** CLI command from Exec mode to create and upload a lifeline to a remote TFTP server. The **dm lifeline** CLI command is useful when a lifeline cannot be generated from the ACE appliance Device Manager GUI.

Assumptions

- The ACE appliance is running.

- You have opened a case with Cisco technical support.
- You are the global administrator; the **dm lifeline** CLI command is only available to the global administrator.
- The TFTP server is reachable and is able to receive files from the ACE appliance.

Procedure

Note Your user role determines whether you can use this option.

Step 1 Log into the ACE by entering the login username and password at the following prompt:

```
host1 login: admin
Password: xxxxx
```

Step 2 Enter the **dm lifeline tftp** CLI command using the following syntax:

dm lifeline tftp host [*port*]

The keywords, arguments, and options are as follows:

- **host**—Specifies the TFTP network server.
- *port*—(Optional) Port number.

A file is created and uploaded to the specified TFTP server in the following format: anm-lifeline.tar.gz. The file is copied to the root directory of the TFTP server.

New Software Features in Version A4(2.2)

Software version A4(2.2) provides the following new features:

- Ability to Backup and Restore Only SSL Files Between ACEs
- Addition of the Normalization Stateless Function
- RADIUS-Attribute Sticky Group Enhancement
- ACE Probes Use the Interface MAC Address as the Source MAC Address
- Default SSL Handshake Support (Per RFC 5746)
- Configuring an SNMP Peer Engine ID for the Standby ACE
- Configuring an SNMP User Authentication Password for the Standby ACE
- Related SNMP Changes for A4(2.2)

Note For a summary of CLI command and system message changes for software version A4(2.2), see the "Software Version A4(2.2) Resolved Caveats, Open Caveats, Command Changes, and System Log Messages" section.

Ability to Backup and Restore Only SSL Files Between ACEs

Per CSCtq38074, the ACE now allows you to specify to backup only SSL files from your ACE and restore all SSL files to the new device. The redundancy configuration on the standby ACE synchronizes the configuration from the active ACE to the standby ACE.

During the restore process, the ACE does not create the missing contexts. The restore functionality will look at each context in the backup file and if the context is present in the ACE, SSL files will be restored. Otherwise, if the context does not exist the restore process is skipped for this context. The restore process then continues with the next context in the backup file.

The modified syntax of the **backup** and **restore** Exec mode commands is as follows:

backup [**all**] [**pass-phrase** *text_string*] [**ssl-only**] [**exclude** *component*]

restore {[**all**] **disk0:***archive_filename*} [**pass-phrase** *text_string*] [**ssl-only**] [**exclude** {**licenses** | **ssl-files**}]

The optional **ssl-only** keyword has been added to the CLI syntax of the **backup** and **restore** commands to enable you to specify exportable SSL files as part of the configuration file backup and restore processes. The nonexportable files are not supported by the back up operation and need to be restored manually.

Addition of the Normalization Stateless Function

The ACE uses TCP normalization to perform checks for Layer 4 packets that have invalid or suspect conditions. Per CSCtr31749, the **normalization stateless** command has been added to Interface mode primarily for use in DSR scenarios as well as a means to provide a certain level of protection against Distributed Denial of Service (DDoS) attacks on an interface during TCP connection creation. The **normalization stateless** command is applicable only to Layer 4 flows.

Note The **normalization stateless** command is for DSR TCP connections only and does not apply to UDP stateless connections.

When you specify the **normalization stateless** command, the ACE processes TCP connections on an interface as stateless connections that undergo TCP normalization checks (for example, TCP window, TCP state, TCP sequence number, and other normalization checks).

Only SYN packets are allowed to create a TCP connection once the connection is created. When the connection is created, Layer 4 normalization checks are relaxed. In this case, since only a SYN packet is allowed to create a connection, the ACE sends a reset (RST) when the connection ends. The **no normalization stateless** command disables the function.

```
lbmb1104-11/CTX1(config)# interface vlan 461
lbmb1104-11/CTX1(config-if)# normalization stateless
```

With the **normalization stateless** command, there are no additional counters in the ACE used to track when a stateless DSR TCP connection is denied or DDoS-protected. All encountered issues are summarized under the existing counters available with the **show np** command output. See the *Cisco Application Control Engine (ACE) Troubleshooting Guide* wiki for details on the **show np** command output:

show np 1 me-stats -snormalization

RADIUS-Attribute Sticky Group Enhancement

A RADIUS-attribute sticky group enables the ACE to stick client connections to the same real server based on a RADIUS attribute. By default, a sticky entry is always created on reception of an Accounting Start packet regardless of the subsequent ACK. “Accounting only” customer deployments require sticky entries to be validated by a response (ACK). After the sticky entry is created, if the real server fails to respond to or acknowledge the request, all subsequent requests must be re-load balanced excluding this real server.

Per CSCth52602, enhancements have been made to the RADIUS-attribute sticky group to optimize sticky entry creation for Accounting Only deployments during RADIUS load balancing. With this enhancement, a new option has been added in sticky RADIUS configuration mode (accessed through the **sticky radius framed-ip** command and the **sticky radius framed-ip username** command) to instruct the ACE to use a sticky entry only after it has been validated by a server response. In the case where no response has been received and the sticky entry has not been validated, the ACE will re-load balance, excluding the real server to which the RADIUS request was stuck initially.

At the end of service delivery, the client generates an Accounting Stop packet that describes the type of service that was delivered and statistics (optional). The Accounting Stop packet deletes the sticky entry immediately without waiting for the ACK.

The new option in sticky RADIUS configuration mode is as follows:

wait-for-ack

Use the **no** form of this command to return operation to the default behavior.

For example, to create a group for RADIUS-attribute stickiness that includes the “wait for ACK” function, enter the following command:

```
host1/Admin(config)# sticky radius framed-ip RADIUS_GROUP
host1/Admin(config-sticky-radius)# wait-for-ack
```

The **show sticky database detail Exec mode** command has also been modified to display the new Radius Wait-For-Ack entry. The states of this entry are either True or False.

For example, enter the following command:

```
host1/Admin# show sticky database detail
processor (0/3):             3
results index:               1 of 1
sticky group:                fip-uname-farm
sticky type:                 RADIUS
rserver:                     rs-01
realPort:                    0
timeout (secs):              86400
sticky-entry:                0x1b6e0438e29341a
internal entry-id:           0xc020000b
time-to-expire (secs):       86342
sticky-hit-count:            1
active-conn-count:           0
in-use reference count:      0
static entry:                FALSE
reverse entry:               FALSE
active entry:                TRUE
timeout-active-conns:        FALSE
created-from-HA-peer:        FALSE
HA-replicated-at-least-once: TRUE
Radius Wait-For-Ack:         TRUE <<<<<<

Total Sticky Entries: 1
```

ACE Probes Use the Interface MAC Address as the Source MAC Address

When an ACE-configured probe closes internally or times-out internally, a RST is generated. Per CSCtj65372, a change has occurred in this RST to have the source MAC address use the nterface MAC address instead of the current behavior of using the virtual MAC address. The inclusion of the interface MAC address allows both the active and standby ACEs in an HA pair to send the RST packet out with the source MAC as its respective interface MAC rather than a common virtual MAC address.

This changes impacts the following probes types: TCP, FTP, HTTP, and HTTPS.

Default SSL Handshake Support (Per RFC 5746)

With defect CSCtd21177, a PSIRT case was initiated. An industry-wide vulnerability exists in the Transport Layer Security (TLS) protocol that could impact any Cisco product that uses any version of TLS and SSL. The vulnerability exists in how the protocol handles session renegotiation and exposes users to a potential man-in-the-middle attack.

RFC 5746 defines the renegotiation indication extension which allows SSL/TLS to perform SECURED renegotiation.

Per CSCtq48352, this enhancement supports a secure handshake by default on the ACE, as defined by RFC 5746. By default the ACE now allows SECURED SSL/TLS renegotiation with a client and server that supports RFC 5746 and, by default, the ACE disallows UNSECURED SSL/TLS renegotiation with a client and server that do not support RFC 5746 (same as previous behavior).

The following two new statistics have been added to the s**how stats crypto server** and **show stats crypto client** commands:

- SSLv3 Secured Rehandshakes—Number of secured SSLv3 renegotiation handshakes that the ACE performed successfully with the client and server.
- TLSv1 Secured Rehandshakes—Number of secured TLSv1 renegotiation handshakes that the ACE performed successfully with the client and server.

Configuring an SNMP Peer Engine ID for the Standby ACE

In prior releases, the ACE allowed you to configure an SNMP engine ID that applied to both the active and standby ACE. Per CSCtq59860, you can configure a different engine ID for the standby ACE in a redundant configuration. The **snmp-server engineid** command in configuration mode includes the new **peer engineid** *peer_value* option. The syntax of this command is as follows:

snmp-server engineid *local_value* [**peer engineid** *peer_value*]

The *local_value* argument is the engine ID for the active ACE. If you do not enter the **peer engineid** *value_2* option, the *local_value* argument applies to both the active and standby ACEs.

To change the value of an engine ID, you must change both values. Otherwise, the ACE displays the following error message:

```
Enter valid value for engineid/peer engineid
Either both should be same or both should change
```

To change the *peer_value* argument, you must also change the *local_value* argument, or visa versa, for example:

```
host/Admin(config)# snmp-server engineid 1234567892 peer engineid 2234567891
host/Admin(config)# snmp-server engineid 2134567892 peer engineid 2324567891
```

To change a configuration in which the active and standby engine IDs are different to a value that is the same value for both engine IDs, you must enter a value that is different for both IDs, for example:

```
host/Admin(config)# snmp-server engineid 2134567892 peer engineid 2324567891
host/Admin(config)# snmp-server engineid 4567892213
```

When synchronization occurs in a redundant configuration, consider the following:

- When both the active and standby ACEs are running software version A4(2.2) and you configure different local and peer engine IDs on the active ACE, the active ACE sends the local engine ID as the peer ID to the standby ACE, and the peer engine ID as the local ID. For example, the running configuration on the ACEs will be similar to the following:
  - On the active ACE: `snmp-server engineid 2134567892 peer engineid 2324567891`
  - On the standby ACE: `snmp-server engineid 2324567891 peer engineid 2134567892`
- When the active ACE is running software version A4(2.2) and the standby ACE is running a software version less than A4(2.2) and you configure different local and peer engine IDs on the active ACE, the active ACE verifies that the software version on the standby ACE and sends only the peer engine ID as the local ID to the standby ACE. For example, the running configuration on the ACEs will be similar to the following:
  - On the active ACE: `snmp-server engineid 2134567892 peer engineid 2324567891`
  - On the standby ACE: `snmp-server engineid 2324567891`

- When the active ACE is running a software version less than A4(2.2) and the standby ACE is running software version A4(2.2) and since you can configure only one engine ID on the active ACE, the active ACE sends the engine ID to the standby ACE. The local and peer engine IDs on the standby ACE will have the same value. For example, the running configuration on the ACEs will be similar to the following:
  - On the active ACE: `snmp-server engineid 2134567892`
  - On the standby ACE: `snmp-server engineid 2134567892 peer engineid 2134567892`

Use the **no** form of this command to delete the SNMP engine IDs. If you delete one engine ID, the other engine ID is also deleted.

The **show snmp engineID** command has been modified to display the identification of the peer SNMP engine in addition to the local SNMP engine configured on the ACE. If you use the **show snmp engineID** command on the standby ACE, the local SNMP engine ID will be the peer engine ID presented in the active ACE.

For example, you can configure different SNMPv3 engine IDs for active and standby ACEs:

```
host1/Admin(config)# snmp-server engineid 1234567890 peer engineid 0987654321
host1/Admin(config)# do show snmp engineID
Local SNMP engineID: 1234567890
PEER SNMP engineID: 0987654321
```

Configuring an SNMP User Authentication Password for the Standby ACE

Per CSCtq60293, when you configure Simple Network Management Protocol (SNMP) user information, you can specify a peer privacy password for user authentication parameters or user encryption parameters. Upon a switchover from an active ACE to the standby ACE, the **snmp-server user** command privacy passwords synchronize between the active and standby ACEs.

The modified keywords, arguments, and options are as follows:

snmp-server user *user_name* [*group_name*] [**auth** {**md5** | **sha**} *local_password1* **peer** *peer_password1*] **[priv [aes-128]** *local_password2* **peer** *peer_password* 2**] [localizedkey**]]

- **peer** *peer_password1*—(Optional) Used for user authentication parameters to specify an authentication password for a peer user on a standby ACE. Enter an unquoted text string with no space and a maximum of 130 alphanumeric characters. The ACE automatically synchronizes the SNMP authentication password as the password for the CLI user on the standby ACE.

Note The peer password is optional; if you do not enter a peer password the ACE will use the local password for the peer user on a standby ACE.

The ACE supports the following special characters in a password: , . / = + - ^ @ ! % ~ # $ * ( ) .

- **peer***peer_password2* —(Optional) Used for user encryption parameters to specify a privacy password for a peer user on a standby ACE.

Note The peer password is optional; if you do not enter a peer password the ACE will use the local password for the peer user on a standby ACE.

Note the following specifications for the user encryption peer password:

  - The AES **priv** password can have a minimum of eight characters.

  - If the passphrases are specified in clear text, you can specify a maximum of 64 alphanumeric characters.
  - If you use the localized key, you can specify a maximum of 130 alphanumeric characters.

  Spaces are not allowed. The ACE supports the following special characters in a password: , . / = + - ^ @ ! % ~ # $ * ( ) .

By default, the ACE automatically creates an SNMP engine ID for the Admin context and each user context. The SNMP engine represents a logically separate SNMP agent. In prior releases, the ACE allowed you to configure an SNMP engine ID that applied to both the active and standby ACE. With software version A4(2.2), you can configure a different engine ID for the standby ACE in a redundant configuration (see the "Configuring an SNMP Peer Engine ID for the Standby ACE" section).

Included below are a set of running configuration examples that illustrate the interaction between the SNMP engine ID and SNMP user password configured for the the active and standby ACEs in a redundant configuration.

SNMP Engine ID is the Same for the Active and Standby ACEs and SNMP User Password is the Same for the Active and Standby ACEs

```
host1/Admin(config)# snmp-server engineid 1234567890 peer engineid 1234567890
host1/Admin(config)# snmp-server user usr1 auth md5 abcd12345 peer abcd12345
host1/Admin(config)# do show running-config | inc snmp
Generating configuration....
snmp-server engineid  1234567890 peer engineid 1234567890
snmp-server user usr1 Network-Monitor auth md5 0xea2410e3deaf422dab2ad979d406825
7 peer 0xea2410e3deaf422dab2ad979d4068257 localizedkey
```

SNMP Engine ID is the Same for the Active and Standby ACEs and SNMP User Password is Different for the Active and Standby ACEs

```
host1/Admin(config)# snmp-server engineid 1234567890 peer engineid 1234567890
host1/Admin(config)# snmp-server user usr1 auth md5 abcd12345 peer ghijk12345
host1/Admin(config)# do show running-config | inc snmp
Generating configuration....
snmp-server engineid  1234567890 peer engineid 1234567890
snmp-server user usr1 Network-Monitor auth md5 0xea2410e3deaf422dab2ad979d406825
7 peer 0x2285eb39064716bdae814e038bcba6c4 localizedkey
```

SNMP Engine ID is Different for the Active and Standby ACEs and SNMP User Password is the Same for the Active and Standby ACEs

```
host1/Admin(config)# snmp-server engineid 123456789010 peer engineid 0987654321
host1/Admin(config)# snmp-server user usr1 auth md5 abcd12345 peer abcd12345
host1/Admin(config)# do show running-config | inc snmp
Generating configuration....
snmp-server engineid  123456789010 peer engineid 0987654321
snmp-server user usr1 Network-Monitor auth md5 0x4d1d46812f0484674e98ba5757ed7aa
7 peer 0x95312cbb53b1ef8c8c556fa5a2378fa7 localizedkey
```

SNMP Engine ID is Different for the Active and Standby ACEs and SNMP User Password is Different for the Active and Standby ACEs

```
host1/Admin(config)# snmp-server engineid 123456789010 peer engineid 0987654321
host1/Admin(config)# snmp-server user usr1 auth md5 abcd12345 peer dfgh12345
host1/Admin(config)# do show running-config | inc snmp
Generating configuration....
snmp-server engineid  123456789010 peer engineid 0987654321
snmp-server user usr1 Network-Monitor auth md5 0x4d1d46812f0484674e98ba5757ed7aa
7 peer 0x30778af5b6239945f2bae806112676b3 localizedkey
```

Related SNMP Changes for A4(2.2)

Per CSCtl73658, the following two new MIB objects have been added to the CISCO-SLB-EXT-MIB to better track Layer 7 parsing failures:

- cslbxStatsL7ParserErrorRejects
- cslbxStatsMaxParseLenReject

The two new MIB objects are part of cslbxStatsTable.

Included below is a summary of the SNMP OIDs for these two objects:

- cslbxStatsMaxParseLenRejects OBJECT-TYPE:

```
SYNTAX        Counter32
UNITS         "connections"
MAX-ACCESS    read-only
STATUS        current
DESCRIPTION
   "The number of connections rejected because the length
   of an HTTP request or response header exceeded the
   maximum L7 parse length configured for the matching
   virtual server."
::= { cslbxStatsTableEntry 18 }
```

- cslbxStatsL7ParserErrorRejects OBJECT-TYPE:

```
SYNTAX        Counter32
UNITS         "connections"
MAX-ACCESS    read-only
STATUS        current
DESCRIPTION
   "The number of connections rejected because an
   error occurred while parsing the connection data
   at Layer 7."
::= { cslbxStatsTableEntry 20 }
```

New Software Features in Version A4(2.1)

Software version A4(2.1) provides the following new features and features merged from software version A4(1.1) as described in the "Software Version A4(1.1) Features Merged into A4(2.1)" section:

- CSCtn25620, the ACE now allows 1000 chain groups system-wide and the limit per context has been removed. Previously, eight SSL chain groups were allowed per context.
- Per CSCtl97681, the new **connection advanced-option default-override** command in configuration mode allows you to globally apply the inactivity and TCP half-closed connection timeout values of a parameter map in a context. For more information, see the "Globally Applying Parameter Map Inactivity and TCP Half-Closed Connection Timeout Values" section.
- Per CSCtn73473, the ACE provides SNMP supports for average CPU usage per network processor. The ciscoL4L7NpCpuUtilTable was added to CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB. The SNMP clrNpCpuUtilizationAverage OID in this table indicates the average CPU utilization of all sub-processors belonging to a network processor at that instance.
- Per CSCth45076, you are now able to ping a multicast ARP address from the ACE.
- Per CSCtk08915, the new **backup sticky** command in sticky cookie configuration mode enables the backup sticky feature for new connections to maintain persistence by providing backup persistence for the source IP address. For more information, see the "Configuring the Backup Sticky Feature" section.
- Per CSCtl23213, the **show np** *number* **me-stats "-c** *connection_id* **-v"** command displays the buffer usage per connection in the Buffer usage count field. This count includes the number of buffer particles for chains connected through user_data[0|1] and buffer particles used during setting up http-proxy, tcp-proxy, SSL, AI etc. and displaying the total count used for each.
- Per CSCtn23472, the **show np** *number* **me-stats "-c t** *number***"** command provides buffer monitoring and leak detection as part of the ucdump **-c** arguments. The **t** *number* option is the threshold number of buffer particles. Any connections that use buffer particles greater than the threshold number are displayed along their count, and idle time. This option also displays the total number of buffers used by the connections, and the total allocated buffers in the ACE.
- Per CSCtl89566, when you apply the **parsing non-strict** command in parameter map HTTP configuration mode, the ACE now accepts non-RFC requests with space and special characters in the HTTP headers, and parses them at Layer 7. For more information on this command as per software version A4(1.1), see the "Skipping a Malformed Cookie in an HTTP Flow" section.
- Per CSCtn61051, the **buffer threshold** command in configuration mode now handles external buffers in addition to internal buffers. Also, the **show np buffer usage** command output includes external buffer information. For more information about this command as per software version A4(1.1), see the "Monitoring and Displaying the Network Processor Buffer Usage" section.
- Per CSCtl72367, the connection limit of 4 million per real server has been removed from the ACE.
- Per CSCtn73488, the **show service-policy** command now includes the conns per second field that displays the connections per second at the virtual server level when you configure more than one VIP under a class map. When you configure one VIP under a class map, the connections per second field is displayed at the VIP level.
- Per CSCto13407, the ACE provides SNMP support for the slbVServerConnectionRate OID. This OID was added to the slbVServerInfoTable table and indicates the connections per second for the virtual server.
- Per CSCtn14041, the HTTP load-balancing limitation of 1024 entries per class map and 1024 entries per policy map has increased to 4096. The line number value for match statements has increased from 1024 to 4096.

- Per CSCtn43569, the ACE now queried the properties of the VM server and its average CPU usage in megahertz (MHz), and calculates the average CPU usage as a percentage. Previously, the ACE calculated the VM CPU load as a percentage of the total ESX server CPU usage instead of relative VM CPU usage. For more information, see the "DWS Support for VM Share" section.
- Per CSCtl53644, the **show interface vlan** *number* now accepts the range from 1 to 4095 to display the internal VLAN information. Previously, the range was 2 to 4094.
- Per CSCtn25383, the following level-3 error syslog message is generated for scripted probe failures:

  ```
  %ACE-3-251018: Scripted probe failed for server A.B.C.D, error message.
  ```

  For more information, see the "Software Version A4(2.1) System Log Messages" section.
- Per CSCtj65408, when you configure an echo TCP or UDP probe on the ACE and the server sends a regex that does not match the configured send-data value, the probe fails and the ACE generates the following syslog message:

  ```
  %ACE-3-251010: Health probe failed for server address on port number, Server response
  not matching with configured echo probe send-data
  ```

  Also the **show probe detail** command displays the following error message in the Last disconnect err field:

  ```
  Server response not matching with user configured send-data
  ```

  Previously, echo probes always passed including when the server sends a regex that does not match the configured send-data value.
- Per CSCtn93913, when an FE/BE MSS mismatch occurs, the ACE generates the following syslog message:

  ```
  %ACE-3-400001: MSS mismatch from A.B.C.D:E (M) to W.X.Y.Z:F (N) on interface
  IFVLAN_NAME
  ```

  For more information, see the "Software Version A4(2.1) System Log Messages" section.

  Also, for the FE/BE MSS mismatch, the **show np** *number* **me-stats "-snorm -M1"** command displays the new normalization statistic field, Fastpath MSS mismatch.
- Per CSCtn78101, the new **inspect non-persistence** command in parameter map HTTP configuration mode allows you to configure the ACE to bypass connection persistence inspection during HTTP transactions for use with smooth streaming deployments. Also, the inspect non-persistence field is added to the **show parameter-map** command. For more information, see the "Bypassing Inspection during HTTP Transactions" section.

Globally Applying Parameter Map Inactivity and TCP Half-Closed Connection Timeout Values

Per CSCtl97681, you can globally apply the inactivity and TCP half-closed connection timeout values of a connection parameter map in a context. The global timeout values override the default values for all the Layer 3 rules in the context. If you configure the timeout values for a specific parameter map, they override the global inactivity timeout values.

Before you can globally apply the connection timeout values, you must configure a connection parameter map that contains these values. You can configure this parameter map with either or both the inactivity and TCP half-closed connection timeouts. For example, to configure a connection parameter map with the inactivity and half-closed connection timeouts, enter the following:

```
host1/Admin(config)# parameter-map type connection TCP_MAP
```

```
host1/Admin(config-parammap-conn)# set timeout inactivity 7200
host1/Admin(config-parammap-conn)# set tcp timeout half-closed 1800
```

You cannot configure any additional parameters to this parameter map. If the parameter map is configured with parameters other than these connection timeouts, the ACE displays the following error message:

```
Error: Parameter map can't be applied globally.
```

After you configure the parameter map, you can globally apply it and its timeouts through the **connection advanced-option default-override** command in configuration mode. The syntax of the command is as follows:

connection advanced-option default-override *connection_parameter_map*

The *connection_parameter_map* argument is the name of connection parameter map name configured with the inactivity or half-closed connection timeout values, or both. For example, enter the following:

```
host1/Admin(config)# connection advanced-option default-override TCP_MAP
```

The **show service-policy** command indicates the global parameter map applied to Layer 3 rule by appending the (Global) tag to its name. The **show parameter map** command displays the globally-applied inactivity and half-closed connection timeouts by appending the (Global) tag appended to the timeout values.

To remove the global timeout values, enter the following:

```
host1/Admin(config)# no connection advanced-option default-override TCP_MAP
```

Configuring the Backup Sticky Feature

When primary persistence fails in the case of a browser not accepting cookies, the ACE may load balance the client requests on new connections to different servers. Per CSCtk08915, the backup sticky feature for new connections maintains persistence by providing backup persistence for the source IP address. For new connections on the first request, this feature selects a server based on any existing load-balancing predictor method and inserts a sticky entry based on client source IP address on the server response. When traffic for the session returns with a cookie, the ACE sends it back to the same server. When traffic returns without a cookie, the ACE sends it to the server that is assigned to the client source IP address.

To enable the backup sticky feature, use the **backup sticky** command in sticky cookie configuration mode. The syntax of this command is as follows:

backup sticky

For example, enter the following:

```
host1/Admin(config)# sticky http-cookie cisco.com GROUP3
host1/Admin(config-sticky-cookie)# backup sticky
```

Use the **no** form of the command to disable the backup sticky feature, as follows:

```
host1/Admin(config-sticky-cookie)# no backup sticky
```

DWS Support for VM Share

When creating a VM, the vCenter provides multiple controls for the VM CPU and memory allocation. These controls allow you to allocate a number of cores to the VM and also provide an option to provision a resource limit to limit the VM CPU utilization to a portion of the maximum available CPU power in megahertz (MHz). When you configure this option on the vCenter, the average CPU usage counter provided by the vCenter is calculated against the total CPU power for the ESX or ESXi host server. The ACE retrieves this counter but treats it incorrectly as the VM CPU usage percentage against its own allocated CPU resource limit.

Since the CPU utilization counter that the ACE obtains from the vCenter provides the CPU utilization of a VM as a percentage of the total ESX CPU, it works fine for the default case in which you allocate a VM with any number of cores and do not apply any resource limits (the default option). The ACE receives the correct CPU load values of the VM and the behavior for the feature works as expected. However if you provision resource limits to the VM, for example, limiting it to 50% of the maximum CPU, the counter value from the vCenter does not reflect accurate results. For example, if the VM uses all 50% of the allocated maximum CPU, the ACE should be receiving 100% as the VM CPU load. Instead, the ACE receives 50% which is the percentage of the total available ESX CPU utilization.

Per CSCtn43569, the ACE now queried the properties of the VM server and its average CPU usage in MHz, and calculates the average CPU usage as a percentage. When you create a VM with a CPU resource limit lower than the maximum limit in MHz, the CPU burst threshold that you configure on the ACE for the DWS feature now compensates for the incorrect value provided by the vCenter. The new CPU burst threshold on the ACE is based on the following formula:

> new burst threshold = expected burst threshold * VM CPU resource limit (MHz) / VM maximum resource limit (MHz)

Bypassing Inspection during HTTP Transactions

By default, when you configure an HTTP inspection policy, connection persistence inspection is enabled during HTTP transactions. However, this inspection can reduce the quality for video or MP4 content in streaming content deployments.

Per CSCtn78101, the **inspect non-persistence** command in parameter map HTTP configuration mode allows you to configure the ACE to bypass connection persistence inspection during HTTP transactions. Note that the ACE still inspects the initial packets (GET and response PDUs) in the same connections. The syntax of the command is as follows:

inspect non-persistence

For example, to configure this command, enter the following:

```
host1/Admin(config)# parameter-map http HTTP_PARAMMAP
host1/Admin(config-parammap-http)# inspect non-persistence
```

To reset the default behavior of enabling connection persistence inspection on an HTTP inspection policy, enter the following command:

```
host1/Admin(config-parammap-http)# no inspect non-persistence
```

To display whether the inspection persistence is enabled or disabled, see the inspect non-persistence field displayed by the **show parameter-map** command.

Software Version A4(1.1) Features Merged into A4(2.1)

The following features from software version A4(1.1) were merged into software version A4(2.1):

- 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
- Probing a Redirect Real 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

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 4700 Series Application Control Engine Appliance Server Load-Balancing Guide*.

Monitoring and Displaying the Network Processor Buffer Usage

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

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

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

The keywords and arguments are:

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

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

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

Displaying the NP Buffer Usage

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

show np *number* **buffer usage**

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

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

Table 1 Output Fields of the show np buffer usage Command

Field	Description
Total Internal Buffer	Total initial internal buffer space in bytes.
Internal Buffer Used	Amount of used buffer space in bytes.
Percentage of Buffer Used	Amount of used buffer expressed as a percentage of the total initial buffer space.
Automatic reload	Status of the automatic reload feature: • Enabled—**buffer threshold** command is configured. • Disabled— **buffer threshold** command is *not* configured.
Active buffer threshold	Configured buffer usage threshold in the active ACE. This field is available only when the **buffer threshold** command is configured.
Standby buffer threshold	Configured buffer usage threshold in the standby ACE. This field is available only when the **buffer threshold** command is configured.

Related Syslogs

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

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

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

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

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

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

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

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

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

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

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

Related SNMP Changes

Per CSCtk08401, 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 4700 Series Application Control Engine Appliance Routing and Bridging Configuration Guide*.

Configuring a Timeout for CRL Downloads

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

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

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

The keywords and arguments are:

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

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

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

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

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

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

Bypassing HTTP Strict Header Parsing

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

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

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

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

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

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

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

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

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

Skipping a Malformed Cookie in an HTTP Flow

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

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

parsing non-strict

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

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

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

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

Disabling Connection Replication

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

ft connection-sync disable

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

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

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

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

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

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

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

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

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

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

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

Probing a Redirect Real Server

Per CSCtg31164, you can configure and associate a probe under a redirect real server or 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 2 describes the fields in the **show serverfarm** *name* **np** command output when the buffer threshold command is configured.

Table 2 Output Fields of the show serverfarm name np Command

Field	Description
serverfarm	Name of the server farm
type	Server farm type: host or redirect
total rservers	Total number of real servers in the server farm

Table 2 Output Fields of the show serverfarm name np Command (continued)

Field	Description
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 not 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(2.0)

The ACE software version A4(2.0) release contains expanded features and functions. The new features include the following:

- Dynamic workload scaling (DWS) feature integrating the ACE with both the Cisco Nexus 7000 series switches that are running the Cisco Overlay Transport Virtualization (OTV) Data Center Interconnect (DCI) Technology and VMware vCenter Server 4.0 or later (see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Guide*)
- Per CSCtg31164, the ability to probe redirect servers, (see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Guide*)
- New licence bundles (see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*)

Available ACE Licenses

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

- Performance: 1 gigabit per second (Gbps) appliance throughput
- Virtualization: 1 admin context and 20 user contexts
- Secure Sockets Layer (SSL): 7500 transactions per second (TPS)
- Hypertext Transfer Protocol (HTTP) compression: 2 Gbps
- Application Acceleration: 100 connections

You can increase the performance and operating capabilities of your ACE product by purchasing one of the optional license bundles. You can order your ACE product by ordering a license bundle. Each license bundle includes the ACE appliance and a software license bundle.

Note Regardless of the license bundle you choose, the maximum application acceleration performance is fixed at 100 concurrent connections and is not configurable.

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

For more information on license bundles, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

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

Ordering an Upgrade License and Generating a Key

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

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

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

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

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

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

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

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

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

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

For information on installing and managing ACE licenses:

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

Performing Software Upgrades and Downgrades

For detailed information on performing an ACE appliance software upgrade or downgrade, see the *Upgrade/Downgrade Guide, Cisco ACE 4700 Series Application Control Engine Appliance*. You can find this document at the following location on www.cisco.com:

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

Supported Browsers for ACE Appliance Device Manager

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

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

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

ACE Operating Considerations

The ACE operating considerations are as follows:

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

  The default HTTP and SSL ports (80 and 443) now have a default inactivity timeout of 300 seconds.
- During an upgrade of two redundant ACEs from software version A4(1.0) to software version A4(2.x), while the two ACEs are in split mode with A4(1.0) running on the active ACE and A4(2.x) running on the standby, config sync is disabled because of a license incompatibility between the two releases. Do not make any configuration changes while the two ACEs are in split mode. If you make any configuration changes on the active ACE during this time, your changes are not synchronized to the standby and are lost. After you complete the upgrade, config sync is automatically reenabled and works normally. To avoid this license incompatibility issue, you can install a 20-virtual context license before you upgrade your ACEs to software version A4(2.x).
- In software version 4(2.0), the maximum number of concurrent connections for optimization is reduced to 100 connections. If the ACE startup configuration contains the **concurrent-connections** command in optimize configuration mode, consider the following:
  - If you upgrade the ACE from a version earlier than A4(2.0), the ACE software ignores the configured command and sets it to 100 connections.
  - If you downgrade the ACE to a version earlier than A4(2.0), the command is removed from the startup configuration and you must reconfigure it after the downgrade process is completed.
- Starting with software version A4(1.0), it is no longer necessary to configure a resource class in the Admin context to allocate resources for stickiness. You can still allocate sticky resources if you wish, but skipping this step will not affect sticky functionality.
- When redundant ACEs lose connectivity, for example due to a network interruption, and they attempt to reestablish their connection, if you enter the **show ft** command during this time, the response for this command may be delayed.
- In a redundant configuration, dynamic incremental sync is a form of config sync that copies configuration changes that you make on the active ACE to the standby ACE when the two ACEs are running the same version of software and when both ACEs are up. When you upgrade from one major release of ACE software to another major release (for example, from A3(2.0) to A4(1.0)) or later, dynamic incremental sync is automatically disabled only while the active ACE is running software version A4(1.0) and the standby ACE is running software version A3(2.0). See Table 3.

We recommend that you do not make any configuration changes during this time and that you do not keep the ACEs in this state for a long time. However, if you must make configuration changes while the ACEs are in split mode, ensure that you manually synchronize to the standby ACE any configuration changes that you make on the active ACE. After you complete the software upgrade of both ACEs, a bulk sync occurs automatically to replicate the entire configuration of the new active ACE to the new standby ACE. At this time, dynamic incremental sync will be enabled again. For details about config sync, see Chapter 6, "Configuring Redundant ACEs" in the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

Table 3 Redundancy Feature Availability Between Major ACE Software Versions

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

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

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

  The following software version combinations in Table 4 indicate whether the SRG compatibility field displays WARM_COMPATIBLE (WC) or COMPATIBLE (C):

Note By default, software versions are considered compatible unless they are explicitly declared as incompatible.

Table 4 Software Release Compatibility Matrix

Active ACE Software Version	Standby ACE Software Version												
	A3(2.1)	A3(2.2)	A3(2.3)	A3(2.4)	A3(2.5)	A3(2.6)	A3(2.7)	A4(1.0)	A4(1.1)	A4(2.0)	A4(2.1)	A4(2.2)	A4(2.3)
A3(2.1)	C	C	WC	WC	WC	WC	WC	WC	WC	WC	WC	WC	WC
A3(2.2)	C	C	WC	WC	WC	WC	WC	WC	WC	WC	WC	WC	WC
A3(2.3)	WC	WC	C	WC	WC	WC	WC	WC	WC	WC	WC	WC	WC
A3(2.4)	WC	WC	WC	C	WC	WC	WC	WC	WC	WC	WC	WC	WC
A3(2.5)	WC	WC	WC	WC	C	WC	WC	WC	WC	WC	WC	WC	WC
A3(2.6)	WC	WC	WC	WC	WC	C	WC	WC	WC	WC	WC	WC	WC
A3(2.7)	WC	WC	WC	WC	WC	WC	C	WC	WC	WC	WC	WC	WC
A4(1.0)	WC	WC	WC	WC	WC	WC	WC	C	WC	WC	WC	WC	WC
A4(1.1)	WC	WC	WC	WC	WC	WC	WC	WC	C	WC	WC	WC	WC
A4(2.0)	WC	WC	WC	WC	WC	WC	WC	WC	WC	C	WC	WC	WC
A4(2.1)	WC	WC	WC	WC	WC	WC	WC	WC	WC	WC	C	WC	WC
A4(2.2)	WC	WC	WC	WC	WC	WC	WC	WC	WC	WC	WC	C	WC
A4(2.3)	WC	WC	WC	WC	WC	WC	WC	WC	WC	WC	WC	WC	C

ACE Documentation Set

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

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

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

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

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

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

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

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

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

Document Title	Description
Cisco 4700 Series Application Control Engine Appliance Administration Guide	Describes how to perform the following administration tasks on the ACE: • Setting up the ACE • Establishing remote access • Managing software licenses • Configuring class maps and policy maps • Managing the ACE software • Configuring SNMP • Configuring redundancy • Configuring the XML interface • Upgrading the ACE software
Cisco 4700 Series Application Control Engine Appliance Application Acceleration and Optimization Configuration Guide	Describes the configuration of the application acceleration and optimization features of the ACE. It also provides an overview and description of the application acceleration features and operation.
Cisco 4700 Series Application Control Engine Appliance Command Reference	Provides an alphabetical list and descriptions of all CLI commands by mode, including syntax, options, and related commands.

Document Title	Description
Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide	Describes how to perform the following ACE security configuration tasks: • Security access control lists (ACLs) • User authentication and accounting using a Terminal Access Controller Access Control System Plus (TACACS+), Remote Authentication Dial-In User Service (RADIUS), or Lightweight Directory Access Protocol (LDAP) server • Application protocol and HTTP deep packet inspection • TCP/IP normalization and termination parameters • Network Address Translation (NAT)
Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Guide	Describes how to configure the following server load-balancing tasks on the ACE: • Real servers and server farms • Class maps and policy maps to load balance traffic to real servers in server farms • Server health monitoring (probes) • Stickiness • Firewall load balancing • TCL scripts
Cisco 4700 Series Application Control Engine Appliance SSL Configuration Guide	Describes how to configure the following Secure Sockets Layer (SSL) tasks on the ACE: • SSL certificates and keys • SSL initiation • SSL termination • End-to-end SSL
Cisco 4700 Series Application Control Engine Appliance System Message Guide	Describes how to configure system message logging on the ACE. This guide also lists and describes the system log (syslog) messages generated by the ACE.
Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide	Describes how to operate your ACE in a single context or in multiple contexts.
Cisco CSS-to-ACE Conversion Tool User Guide	Describes how to use the CSS-to-ACE conversion tool to migrate Cisco Content Services Switches (CSS) running-configuration or startup-configuration files to the ACE.

Software Version A4(2.3) Resolved Caveats, Open Caveats, Command Changes, and System Log Messages

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(2.3):

- Software Version A4(2.3) Resolved Caveats
- Software Version A4(2.3) Open Caveats
- Software Version A4(2.3) Command Changes
- Software Version A4(2.3) System Log Message Changes

Software Version A4(2.3) Resolved Caveats

The following resolved caveats apply to software version A4(2.3):

- **CSCtd33226**—The SNMP daemon can be very slow to respond (for example, a delay of approximately 10 to 15 minutes) when the ACE receives a malformed SNMP packet or there is a heavy utilization of SNMP polls. Workaround: None.
- **CSCtf28855**—If you configure the **no inservice standby** command under a real server, when you reboot the ACE, the running-configuration file incorrectly lists “inservice standby” in the configuration file. The running-configuration file should be the same as before and after the reboot of the ACE. Workaround: None.
- **CSCtg87855**—After you change the configuration in a large ACE configuration and enter **show** commands, the CLI becomes unresponsive for a period of time. In this case, the **show processes cpu | include cfgmgr** command displays one of the configuration manager (cfgmgr) processes consuming CPU resources. After you apply the configuration change, the cfgmgr CPU usage goes to zero, and the CLI becomes unresponsive. Workaround: Wait until the cfgmgr completes its previous operation before entering the **show** command.
- **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.
- **CSCti85313**—When using the **sticky-serverfarm** command to specify that all requests that match a Layer 7 policy map are load balanced to a sticky server farm, if a server farm goes down, the ACE fails to display the following system message:

  ```
  %ACE-5-441003: Serverfarm (name) failed in policy_map (policy_name) --> class_map
  (cmap_name) without backup. Number of failovers = count1, number of times back in
  service = count2
  ```

  Workaround: None.
- **CSCtj12692**—When you configure the ACE with 4000 sticky groups and do not allocate a sticky resource class, the resource values of the sticky are the default of a minimum of 0 and a maximum of unlimited. When the sticky database has 800,000 entries and you create a sticky resource class to a minimum value equal to 20 percent and apply it to the context, the ACE becomes unresponsive after a few minutes because it becomes unresponsive in the LB module at the function LbSticky_ReturnOldestEntry. Workaround: Do not change the resource class when you configure a large number of sticky groups and the database is full with active entries.

- **CSCtk12683**—All SSL probes on the ACE fail with the following reason: "No SYN/ACK returned from server." However, if you perform a trace, the trace shows that the TCP SYN from the ACE is not on the wire. This behavior is due to a configuration change that caused the access control list (ACL) to be downloaded to the internal VLAN 4095. The ACL failed, causing the Data Plane (DP) to reject the TCP SYN for the SSL probes being sent by the Control Plane (CP). Workaround: Reboot the ACE. If this action does not resolve the issue, try another configuration change to force the ACL to be downloaded again to the internal VLAN.
- **CSCto65861**—During normal ACE operating conditions, the ACE fails to reboot or to generate a file when the ha_mgr process in the ACE become unresponsive. Workaround: None.
- **CSCtq11972**—When you configure an Oscilloquartz NTP server with stratum 2, the ACE cannot synchronize its time with the NTP server. Workaround: None.
- **CSCtq63901**—When you configure long probe names, long server farm names, and long real server names, the probe server farm or real server length can become too large (greater than 128 bytes) and the ACE can encounter a problem parsing the ciscoSlbHealthMonMIBObjects MIB object. In this case, when the ACE attempt to poll the ciscoSlbHealthMonMIBObjects, an SNMP query timeout will occur or there will be missing probe information. Workaround: None.
- **CSCtq63912**—SNMP traps are not sent when the SNMP trap queue is full. When this situation occurs, the ACE displays the following error messages:

  ```
  snmpd[1027]: (ctx:9)send_notification: new: enqueueing notification........
  snmpd[1027]: (ctx:9)ERROR: notif_enqueue_tail : Size of the notif queue is more than
  the MAX size 250
  ```

  Software version A4(2.3) increased the queue size from 250 to 2000 and added new a counter in the **show snmp** command output to print the number of traps dropped because of a full SNMP queue. Workaround: None.
- **CSCtr40282**—Under normal operation conditions with regexp resources in use, the **clear stats resource-usage** command may fail to clear the regexp peak counter. Workaround: Reload the ACE.
- **CSCtr59322**—When performing a continuous snmpwalk on crlBufferUsageValue, this action may cause a memory leak. This issue can cause SNMP to keep allocating memory that is never released after stopping the script, eventually resulting in the ACE rebooting due to less free memory. Workaround: None.
- **CSCtr62530**—When a NAT pool is applied and then removed from a VLAN interface, these actions corrupt the Route table in the ACE. This issue happens when the same NAT pool is applied to multiple VLAN interfaces, and that NAT pool is removed from the first VLAN interface while it is still applied on the second VLAN interface. Workaround: None.
- **CSCtr79276**— The ACE does not work properly in one-arm mode with SIP and TCP when source NAT is enabled. SIP registrations and calls may fail depending on whether SIP Inspect is enabled. Workaround: None.
- **CSCtr96229**—With the ACE configured with several contexts, and one of the contexts has a resource class that contains sticky limits, the ACE reboots after you remove the resource class association from that context. The issue is related to the number of contexts configured in an ACE. When the load-balancing module in the ACE tries to remove sticky entries from the free list, it needs to check if there is a starving context that is waiting for resources, which can consume CPU time. Workaround: None.
- **CSCts07333**—During a configuration change on the ACE, the ACE reloaded because the cfgmgr becomes unresponsive. This behavior could be due to a memory corruption problem. Workaround: None.
- **CSCts09006**—Under normal operations with SNMP, the ACE unexpectedly reloads and generates a core file. Workaround: None.

- **CSCts44219**—The ACE is configured with access control lists (ACLs) which reference object groups. The ACL is part of a policy which is applied globally or to an interface. When dynamic changes are made to the ACL or object group, the following ACL merge error may occur:

  ```
  "%ACE-1-106028: WARNING: ACL Merge failed to add ACE..."    and this leave the service
  policy incomplete and can cause traffic to be mis-handled.
  ```

  Workaround: Perform one of the following actions:

  - Delete the ACL which logged the merge error, reconfigure the policy, and reapply.
  - Reboot the ACE.
- **CSCts45803**—Applying, detaching, and then reapplying a traffic policy to a specific VLAN interface or globally to all VLAN interfaces in the same context results in an "Error: Policy does not exist" error message. Workaround: None.
- **CSCts56552**—In a P2MP scenario, there are multiple SIP connections between the client and server and the connection is terminated with BYE. In this case, BYE should clean the entries for the connection in the ACE or the table will get full and a RESET will be sent to close the SIP session. Workaround: None.
- **CSCts68281**—With a configured HTTPS health probe, the ACE may display the following system error message:

  ```
  %ACE-3-400001: MSS mismatch from 10.0.5.193:443 (1380) to 127.1.2.34:64571 (1460) on
  interface vlan40
  ```

  Workaround: Remove the HTTPS probe from the server farm.
- **CSCts69941**—With a large configuration containing a large number of contexts, interfaces, and ACLs (including a merge of individual ACLs into one large ACL), the ACE can become unresponsive 10 to 15 minutes after booting. Workaround: Specify the **show np 1 access-list resource** command after you boot the ACE. Confirm if the Leaf Parameter nodes exceeds 400K and the policy action nodes exceeds 200K (recommended values are 200K and 100K, respectively). If one of these nodes exceeds the specified value, remove the merged ACLs and associated contexts until this threshold is not exceeded in the **show np 1 access-list resource** command output.
- **CSCts79939**—The following rewrite configuration does not successfully rewrite any instances of "http" under some scenarios:

  ```
  action-list type modify http REWRITE
    header rewrite response Location header-value "(.*)http(.*)" replace "%1https%2"
  ```

  While parsing the Location header, the ACE stops parsing after encountering any instance of the first letter in the match string ("h"). At that point, the ACE does not complete the match or perform the rewrite. Workaround: None.
- **CSCts98720**—In an application where the ACE is performing firewall load-balancing with two server farms (where one server farm is for user traffic and the other server farm is for BGP traffic sent to the firewalls), when performing failaction reassign and then undoing the failaction, the ACE incorrectly moves a user connection to the BGP dedicated server farm. Workaround: None.
- **CSCts99950**—With backend SSL configured on the ACE, the ACE may become unresponsive and generate a core file. Workaround: None.
- **CSCtt02508**—The end-to-end SSL TCP connection encounters issues while uploading a large (approximately 4.5 GB) file through an ACE VIP that is configured for end-to-end SSL. Simultaneous front and back-end traces show that the ACE brings the TCP window to zero on the client side but does not send any further data toward the server on the back-end side even though the last TCP window update from the server is 65K. The upload stops and never resumes after that. Workaround: None.

- **CSCtt06395**—The ACE fails to create sticky entries when HTTP content and HTTP request Header insert for load-balancing are configured on the ACE. In this case, sticky entries should be created in the **show sticky database** command output. Workaround: None.
- **CSCtt08380**—After experiencing packet loss, the ACE inconsistently sends ACKs. This behavior is due to the length of reassembly queue in TCP (32 buffer particle). With software version A4(2.3), this length has been tied to the size of rcv-wnd (typically 64 buffer particle). Workaround: None.
- **CSCtt14768**— The ACE may start dropping connections due to an unavailable buffer. This issue is related to improper handling of an HTTP GET request to the ACE VIP. The issue is verified only if you enable Layer 7 application inspection. You will notice the connection buffer utilization is slowly increasing. Workaround: Clear the connection to clear all stale connections and to release the buffer.

  PSIRT Evaluation:

  The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4.0/3.3:

  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:S/C:P/I:N/A:N/E:F/RL:OF/RC:C

  CVE ID CVE-2011-0956 has been assigned to document this issue.

  Additional information on Cisco's security vulnerability policy can be found at the following URL:

  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html
- **CSCtt24046**—When the ACE performs multiple simultaneous SNMP requests on the cpmProcessTable, this action may result in an SNMP timeout. Workaround: Perform only sequential SNMP requests on Cisco Process MIB.
- **CSCtt30579**—When you use the **show cfgmgr internal table slb-policy** command, the output incorrectly displays all the entries as invalid. Workaround: None.
- **CSCtt33804**—During a modification of an access control list (ACL) within a context, an ACL merge error may be reported on one or more of the interfaces where the ACL list is applied, leaving the interface in an inconsistent state. When this issue occurs, the following system message appears:

  ```
  %ACE-1-106028: WARNING: ACL Merge failed to locate specified ACL in context 10049.
  Error while processing service-policy. Incomplete rule is currently applied on
  interface vlan200. Configuration on this interface needs to be manually reverted
  ```

  Workaround: Perform one of the following actions:

  - Remove the offending lines one at a time from the ACL until the ACL can be successfully applied.
  - Reload the ACE.
- **CSCtt42497**—When performing Layer 7 server load balancing with a configuration that includes a combination of sticky, server connection reuse, and persistence-rebalance, bad HTTP requests may occur on the server as Layer 7 HTTP packets are sent out of order. Packets sent out of order cause the server to drop the packets or tag the request as malformed. Workaround: Disable the **server-conn reuse** command.
- **CSCtt61028**—In a redundant configuration, SSL probes may fail intermittently when the ACE is in standby mode. The active ACE does not encounter this issue. Workaround: Reload the ACE.
- **CSCts64847**—Only the default Admin user can run the **show environment temperature** command. If another user has an Admin role but is not the default Admin user, that user may not be able to specify this command and the ACE displays the following error:

  ```
  ACE/Admin# show environment temperature
  Could not open device at /dev/ipmidev or /dev/ipmi/0 or /dev/ipmidev/0:
  Not a directory
  ```

```
Get Device ID command failed
Unable to open SDR for reading
```

Workaround: Use the default Admin user to run the **show environment temperature** command.

- **CSCts67210**—In a redundant configuration, the ACE appliance allows only FT group numbers 1 to 63 to be configured; however, the ACE module supports FT group numbers 1 to 255. Workaround: None.
- **CSCtu10624**—Establishing a Telnet connection from the ACE to a remote device is silent with no indication of a successful connection or DNS resolution. When this situation occurs, the lines "trying ..." and "connected..." are not seen. Workaround: None.
- **CSCtu18281**—The restore process may fail if the Admin context in the backup configuration has TACACS authorization and the configuration is associated with a domain (**add-object** command). When this issue occurs, the restore process fails and the non-Admin contexts are not imported. However, for the Admin context, the configurations are properly applied. Workaround: Remove "domain TACACS" from the backup configuration and perform the restore.
- **CSCtu27310**—When operating the ACE in bridging mode, a DHCP client on a VLAN that is located "behind" the ACE is unable to obtain a lease from a DHCP server "in front of" the ACE. This behavior can occur with a Linux-based DHCP server. Workaround: Use a different DHCP server where the reply is broadcast instead of unicast.
- **CSCtu30517**—When you are operating the ACE in switch mode (the **switch-mode** command) or the ACE has been configured on a shared interface with syn-cookie enabled, when you use the **show syn-cookie** command you may find that the embryonic connections are not counted properly in the output. Workaround: None.
- **CSCtu33484**—When setting the idle timeout on the ACE, an extra second is added for every minute of idle operation. The connection disappears from the statistics on the configured time. When this occurs, the reset is not sent until the idle time plus the extra time expires. Workaround: None.
- **CSCtu34037**— User context configurations (including certificates and keys) are lost after the ACE reloads. When this issue occurs, the Admin context configuration is reduced to the minimal, initial configuration. This issue can occur when you specify the **reload** command, or if the FT link is interrupted by high CPU usage on the switch that the ACE is connected to. Workaround: None.
- **CSCtu34163**—Under normal operating conditions, you attempt to access the ACE through an SSH remote session and the ACE reboots and then generates an SSHD core file. Workaround: None.
- **CSCtu36146**—The ACE becomes unresponsive due to a configuration manager (Cfgmgr) process failure with the last boot reason: Service "cfgmgr." Workaround: None.
- **CSCtv17196**—The **show script code** command fails, stating an invalid call. Workaround: Reboot the ACE.
- **CSCtw54107**—The ACE requires the ability to display the hidden parameter of a server farm when using the **show cfgmgr internal table sfarm det** command.
- **CSCtw70949**—Currently, the **ucdump -w a** debugging command does not show the allocated buffers. This debugging command display incorrect output. Workaround: None.
- **CSCtw70955**—With DNS inspection enabled on the ACE, the ACE strips the checksum. This behavior does not effect functionality, and DNS queries are still resolved. You will not encounter this issue when DNS inspection is disabled. Workaround: None.

- **CSCtw79419**—An error occurs when you attempt to delete a server farm, and the ACE prevents you from performing the deletion. This behavior can occur when the ACE configuration manager still associates the server farm with a load-balancing policy. For example:

  ```
  ACE/1(config)# no serverfarm host 2081bancaPR
  Error: serverfarm 'SERVERFARM_X' is in use. Cannot delete!
  ```

  Workaround: Reboot the ACE.
- **CSCtw81056**—With a Layer 7 server load-balancing configuration with server-conn reuse enabled, you may find that intermittent client connections are reset. Traces show a Reset occurred from the backend server immediately after the ACE forwarded the client's GET request on the backend connection. Workaround: Initiate a failover to the standby ACE and reboot.
- **CSCtw84303**—The ACE downloads the CRL for the first time from the specified CRL download location. However, subsequent updates are not attempted after the ACE NextUpdate timer expires. Workaround: None.
- **CSCtx03563**—The ACE may produce large httpd logs over time when you use the XML interface. This operation can cause the file system to become full, resulting in the generation of messages such as: "write error: No space left on device." If you reload the ACE in this state, and you save the configuration when prompted, this action causes the ACE to wipe all configuration files. Workaround: Do not save the configuration on reload when prompted.
- **CSCtx20459**—When you specify the **show system resources** command, CPU states values are shown as "nan%". For example:

  ```
  ACE/Admin# show system resources
  Load average:   1 minute: 0.10   5 minutes: 0.05   15 minutes: 0.01
  Processes   :   5606 total, 1 running
  CPU states  :   nan% user,   nan% kernel,   nan% idle  <<<<<<<<<<<<<
  Memory usage:      5955K total,      1623K used,      4331K free
                       21K buffers,     858K cache
  Average ME Utilization Statistics
  ```

  Workaround: None.
- **CSCtx27638**—The ACE may suddenly display the following log message with no operational impact:

  ```
  %ACE-3-251006: Health probe failed for server x.x.x.x on port nnnnn, internal error:
  failed to setup a socket
  ```

  Workaround: None.
- **CSCtx32644**—When operating the ACE for approximately two days with the following set of scripts, syslogd may become unresponsive:
  - HTTP traffic hitting HTTP compression
  - Configuring changes using XML
  - Specifying SNMP commands in a loop
  - Sending HTTP traffic to a VIP using LDT
  - Running the clogin script from a server (nine instances from one server)
  - Specifying the **xml show** command in a loop

  Workaround: None.

- **CSCtx45830**—In a redundant configuration, the config sync process fails because of an expired user account configured on the ACE. This issue occurs when a user account is configured with a specified expiration date in the past (with reference to the ACE system clock), the ACE displays the error message "date should be in the future, expiry date wrong" and the configuration is then rejected. Workaround: Remove the expired user account from the active ACE configuration.
- **CSCtx53490**—In a redundant configuration, the ACE may generate a high volume of Generic Attribute Registration Protocols (GARP) which result in a high CPU load. In this situation, the he ACE will not stop sending the GARPs until you reload it. This behavior can occur under the following conditions:
  - The ACE is running software release A4(2.1) or later.
  - Your configuration includes: two ACEs in FT setup with FT preemption enabled, host tracking for a default-gateway of which the ARP can not be solved, and SNAT.
  - All ARP entries of real servers and default-gateway devices have the ARP entry type of VIP(SNAT) as "NAT" instead of "VSERVER".

  Workaround: To resolve this issue, address one or more of the configuration items listed above.
- **CSCtx58666**—The ACE displays the "internal error: failed to setup a socket" error message when it is unable to send a probe due to a network issue. Workaround: None.
- **CSCtx59909**—If you log into the ACE appliance Device Manager GUI using the "admin" username with custom role permissions within a context, when you attempt to change the configuration, you may see a popup window that displays the following error: "Failed to deploy config to device: Infringing CLI command: with reason: reached max checkpoint limit 10." Workaround: Do not use "admin" as the username within the sub-context. Any other username will not trigger this error message.
- **CSCtx92484**—During a Layer 7 file transfer is terminated after transferring approximately 16 kB of data. Workaround: Configure an HTTP parameter map and set the content-maxparse-length and header-maxparse-length to larger values. For example:

  ```
  parameter-map type http PM-HTTP
    persistence-rebalance
    set header-maxparse-length 65535
    set content-maxparse-length 65535
  ```
- **CSCtx96626**—In a redundant configuration, when multiple track priorities are configured in an FT track host configuration, you may find that some track states are TRACK_DOWN. In this case, the FT track priority is not properly decreasing as expected after the ACE reboots. Workaround: Reconfigure the FT track priority using the **probe** [*probe_name*] **priority [priority**] command or change all track states from TRACK_DOWN to TRACK_UP.
- **CSCty01285**—With the ACE configured for SSL termination with client authentication and OCSP, when the ACE makes an OCSP request to the OCSP server, the server responds with a certificate status of unknown. Workaround: Disable OCSP.
- **CSCty11329**—In a redundant configuration, while attempting to remove a virtual IP address from a class map, both the active and standby ACE appliances reboot and create a cfgmgr core file. Workaround: None.
- **CSCty24569**— Cross-site scripting (XSS) vulnerability in the Adobe Flex SDK 3.x and 4.x before 4.6 allows remote attackers to inject arbitrary web script or HTML from vectors related to the loading of modules from different domains. Workaround: None.

  PSIRT Evaluation:

  The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4.3/3.6:

https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:S/C:P/I:N/A:N/E:F/RL:OF/RC:C

CVE ID CVE-2011-2461 has been assigned to document this issue.

Additional information on Cisco's security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- **CSCty60596**—If you configure an ACE with the same VIP that listens on two separate ports, with both VIPs performing server-conn reuse using the same server farm, once one VIP receives the traffic this can result in operational issues with the other VIP. This behavior can occur because the ACE uses a real server ID to index to the reuse pool for sending the server connection to the pool or for retrieving server connection from the pool. Configuring the same server farm for both an HTTP policy and an HTTPS policy results in the ACE using identical real server IDs to index to the same reuse pool to store or retrieve the server connections for both HTTP and HTTPS traffic (ingress).

  Workaround: In order for the ACE to generate two different real server IDs for the same real server to separately serve the HTTP and HTTPS traffic, create a new server farm to contain the same real servers. Associate one server farm to the HTTP policy and another server farm to the HTTPS policy. The ACE will generate two different real server IDs for this real server because it is configured with two server farms. The server connections for HTTP traffic are stored to and retrieved from the reuse pool indexed by one real server ID, and server connections for HTTPS traffic are stored to and retrieved from the reuse pool indexed by a different real server ID.

Software Version A4(2.3) Open Caveats

The following open caveats apply to software version A4(2.3):

- **CSCth04993**—When you configure an ACE interface with single NAT IP address in the NAT pool and the ACE receives SIP UDP traffic, it resets subsequent SIP TCP traffic. Workaround: Perform either of the following:
  - Perform a checkpoint rollback to a non-SIP configuration and then to the existing configuration.
  - Increase the number of IP addresses in the NAT pool.
- **CSCth56931**—With FTP inspection enabled in the configuration and the **logging buffered** command enabled for debugging (level 7), the ACE reboots with the syslogd process creating a core file. Workaround: None.
- **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.
- **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.
- **CSCtk53923**—When you delete a user with the name “test”, the ACE may unexpectedly reboot. The last boot reason is Service “securityd.” Workaround: None.

- **CSCtk98620**—When you make multiple changes to an SSL parameter map and then specify the **show stats crypto client** command, the ACE configuration manager (cfgmgr) receives a signal 11 and the ACE becomes unresponsive. Workaround: None.
- **CSCtl04271**—After you remove a class map from a policy map, an ACL merge does not work. Workaround: Remove the service policy from the assigned interface and reapply the same policy.
- **CSCtn18486**—Performing a backup and restore of the ACE configuration can cause the ACE configuration manager (cfgmgr) to become unresponsive. This issue may be due to a kernel issue. Workaround: None.
- **CSCto94653**—With traffic flowing through the ACE, while creating a checkpoint of a running configuration on your ACE, you may find that the console hangs and that the ACE becomes unresponsive. Workaround: None.
- **CSCts36540**—In a redundant configuration, with multi-context sticky traffic, if you perform an FT switchover while under heavy traffic and the sticky database is full, the ACE will reboot. Workaround: Increase the sticky timeout value.
- **CSCtu01626**—The HTTP probe with a regex search string fails when the HTTP header is split into two packets. When this issue occurs, HTTP probes pass and fail intermittently. Workaround: The server needs to send the entire header in one receive packet and not split the header into two packets.
- **CSCua26437**—When the server response is chunked encoded and the VIP is configured for cookie-based sticky, the ACE may fail to forward the server response to the client. To determine if chunked encoding is present in the network, use the **show stats http | inc chunk** command to check if the HTTP chunks counter increases per context:

  ```
  ACE/Admin# show stats http | inc chunk
  HTTP chunks               : 0          , Pipelined requests       : 0
  ```

  Workaround: Use IP-based sticky.
- **CSCtu40720**—When using an HTTP probe on the ACE, if the response (not the header) contains "content-length: 0", the ACE fails the probe with an "Unrecognized or invalid response" error even if the response is 200 ok from the server. Workaround: If you remove the "-" from the content-length and just use "contentlength", the ACE accepts the server response and will not fail the HTTP probe. Another alternative is to use a "head" instead of a "get" on the URL request method.
- **CSCtx27765**—During a normal startup during initialization when the ACE is reloading, on occasion it may fail due to NAT initialization. Workaround: The ACE will reboot and work on the next reload.
- **CSCtx57994**—After performing a software upgrade or while using software version A4(2.2), the ACE rebroadcasts a non-IP logical-link control (llc) broadcast packet generated by an IBM server. As a result, this action causes the ACE to believe that the IBM server now resides off the ACE switchport. When this behavior occurs, you will see the following message:

  ```
  %MAC_MOVE-SP-4-NOTIF: Host <IBM-SERVER-MAC> in vlan XX is flapping between port
  <ACE-PORT> and port <SERVER-PORT>
  ```

  Workaround: If necessary, downgrade to an earlier version of ACE software.
- **CSCtx64126**—The ACE contains static ARP entries even though no static ARPs have been recently been configured. This issue may be related to static ARPs configured in the past and then removed. In this case, the ACE failed to remove the entries. Workaround: Readd the static ARP entry, then remove it. This action will remove the static ARP from the ACE.
- **CSCtx76894**—If you try to import a license while the /isan/ partition is full (due to CSCtx03563), the import will fail because the file copied in the partition is empty. This issue will also cause issues with the liccheck process when it tries to parse an empty file. Workaround: Reload the ACE and try to import the license again.

- **CSCtx81319**—An HTTPS probe that is configured with an open timeout value will fail to log a “no SYN/ACK'” failure if the SYN/ACK does not return from the probed real server within the specified open timeout value. When this situation occurs, the ACE continues to retransmit the SYN packet to the real server. After the interval timeout expires, the ACE logs a failure of the probe as “server reply timeout.” Workaround: None.
- **CSCty02827**—The NP ME in the ACE may become unresponsive and generate a core file, with the following reboot error: “NP 1 Failed: NP ME Hung.” Workaround: None.
- **CSCty08887**—The ACE resets a connection if the HTTP header is approximately 14K in length while the VIP configuration does not require HTTP parsing. Workaround: Create an HTTP parameter map that includes the **set header-maxparse-length** command followed by a proper value.
- **CSCty14193**—If the ACE receives an ACK with 1 greater than the current sequence number, the ACE responds with its own ACK instead of ignoring the received ACK. If the rate of these ACKs are high enough, this situation can lead to buffer depletion. Workaround: None.
- **CSCty25519**—While making multiple simultaneous changes to one or more server farms that use the same Layer 7 policy map (for example, putting multiple real servers in an inservice/no inservice state several times), HTTP requests from a client sometimes hit an incorrect Layer 7 policy map statement and are load balanced to incorrect server farms for a short period of time (during the time the change is processed). Workaround: In situations where there are administrative operational changes required, such as placing real servers in and out of service, instead of making **inservice** and **no inservice** changes on the ACE, configure the probes on the real servers in the server farm and make the probes fail.
- **CSCty43331**—Under a normal server load-balancing operation when you add or modify a virtual IP (VIP) address, you may find that the VIP addresses do not appear in the **show cfgmgr internal table icmp-vip** output. Workaround: Reload the ACE.
- **CSCty47743**—In a redundant configuration, if you configure a description under an interface that contains a valid ACE command, the bulk synchronization script may parse the description as a command, change it, and attempt to apply it to the configuration. For example:

  ```
  interface vlan X
    description Admin context Mgmt VLAN IP address
  ```

  On the standby ACE, the “IP address” section is parsed as an actual command and changed to the **peer ip address** command. When the ACE applies this command, it fails because the command is incomplete. The following config synchronization error appears:

  ```
  cdn-ace--2/Admin# sh ft config-error
  Tue Mar 6 22:56:56 CET 2012
  `peer ip address`
  *** Context 5: cmd parse error ***
  --
  *** Context 5: Config can not been applied fully. Please try again***
  ```

  Workaround: Remove or modify the description string. For example, insert a dash (-) or underscore (_) instead of using a space.
- **CSCty58098**—With the ACE configured with a class map containing wildcards within the regex expression match string this may result in inconsistency in the matching criteria. Workaround: None.
- **CSCty61047**—With a DHCPv6 relay configured on an interface, the DHCP relay does not function properly for IPv6 DHCP when using a wide-dhcp DHCP server. Workaround: None.
- **CSCtx64223, CSCtx96520**—When there are more than 255 characters in the SSL Subject (with 255 being the maximum value), certain characters in the SSL Subject are then omitted. Workaround: None.

- **CSCty74282**—In a configuration where you are configure KAL-AP on the ACE to allow communication between the ACE and the Global Site Selector (GSS), after performing a software upgrade to A4(x.x), with the ACE being actively probed using SNMP, the KAL-AP by VIP keepalives intermittently fail. Traces from the GSS show that the ACE reports a load of 0 intermittently for the VIPs which cause the GSS to report the VIPs as being offline. Workaround: Stop SNMP polling or use a KAL-AP tag with the address in the class map by using the **kal-ap-tag** command.
- **CSCtz01045**—The ACE may stop responding to the OPTIONS messages sent on the inbound leg of the transmission. OPTIONS messages are sent every three seconds. In this case, the TCP window size advertised by the TCP module of the ACE continues to decrement, and the connection resets when the TCP window size becomes zero. Workaround: None.

Software Version A4(2.3) Command Changes

Table 5 lists the command changes in software version A4(2.3).

Note For a summary of new features for software version A4(2.3), including the associated new or modified commands, see the "New Software Features in Version A4(2.3)" section.

Table 5 CLI Command Changes in Version A4(2.3)

Mode	Command and Syntax	Description
Exec	**dm** [**lifeline** | **reload** | **status**]	Per CSCtq28184 the **dm** command options are available in Exec mode to utilize the troubleshooting tools on the Device Manager GUI directly from the ACE appliance CLI. See the "Accessibility of Device Manager GUI Troubleshooting Tools from the ACE Appliance CLI" section for details.
	show ntp {**authentication-keys** | **authentication-status** | **logging-status** | **trusted-keys**}	Per CSCtr62165, the ACE appliance now complies with the NTPv3 standard and supports NTPv3 authentication through the addition of a series of new **show ntp** commands in Exec mode. See the "Displaying NTP Information" section for details.
	show ip	Per CSCtu37951, the overflow (V) flag now displays the legend explanation in the **show ip fib** command. See the "Modifications to the show ip fib Command" section for details.
Configuration	**ntp authenticate** **ntp authentication-key** *number* **md5** *md5-string* **ntp trusted-key** *number* **ntp logging**	Per CSCtr62165, the ACE appliance now complies with the NTPv3 standard and supports NTPv3 authentication through the addition of a series of new **ntp** commands in configuration mode. See the "Displaying NTP Information" section for details.

Table 5 CLI Command Changes in Version A4(2.3) (continued)

Mode	Command and Syntax	Description
Parameter map connection	**set tcp timeout fast-fin** *time*	Per CSCtr61749, the ACE now supports the ability to define a timeout in your connection parameter map for TCP connections that are in the FIN_WAIT_I state. The **set tcp timeout** command now includes the **fast-fin** option to specify the FIN timeout (in seconds). This command is available in the Admin context only. See the "Closing a TCP Connection in a FIN_WAIT State" for details.
Parameter map HTTP	**set max-parse-time** *time*	Per CSCtu08459, you are now able to configure the ACE to mitigate a Slowloris HTTP DOS attack by including an HTTP parse timeout in your HTTP parameter map. With software version A4(2.3), the new **set max-parse-time** command has been added as protection from Slowloris DoS attacks. The default HTTP parsing timeout is set to 255 seconds, and if the ACE does not receive a GET request from the connection within 255 seconds, the HTTP parse timeout initiates and the ACE drops the connection and sends a reset to the client. See the "Mitigating a Slowloris HTTP DoS Attack" for details.

Software Version A4(2.3) System Log Message Changes

Software version A4(2.3) includes the following system log (syslog) message changes.

251006

Error Message `%ACE-3-251006: Health probe failed for server A.B.C.D on port P, internal error: error message`

Per CSCtx58666, the "failed to setup a socket" error message has been removed as one of the possible values of the *error message* variable from syslog %ACE-3-251006.

251010

Error Message `%ACE-3-251010: Health probe failed for server A.B.C.D on port P, error message`

Per CSCtx58666, connection error message "Network or Host is unreachable" has been added as one of the possible values of the *error message* variable in syslog %ACE-3-251010.

Software Version A4(2.2) Resolved Caveats, Open Caveats, Command Changes, and System Log Messages

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(2.2):

- Software Version A4(2.2) Resolved Caveats
- Software Version A4(2.2) Open Caveats
- Software Version A4(2.2) Command Changes
- Software Version A4(2.2) System Log Messages

Software Version A4(2.2) Resolved Caveats

The following resolved caveats apply to software version A4(2.2):

- **CSCte79279**—When you display the statistics for a policy map using the **show service-policy summary** command, you may see "N/A" in the command output. For example:

  ```
  host1/Admin# show service-policy L4-policy summary
  cMap-Any                          17.1.1.10       any    any
  OUT-SRVC
  N/A
  ```

  Workaround: None.

- **CSCtg80762**—When you use a management tool for ACE XML formatting using a script, the ACE may add four extra lines to the XML output. You can see the extra lines when you run the **show service-policy detail** command. The failure is specific to the context where you have performed the formatting. Workaround: Divide the respective policy map where the VIP is configured.
- **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.
- **CSCtj01818**—When the ACE performs a configuration rollback after a configuration contained a large number of ACLs, the ACE may display the following system error message:

  ```
  %ACE-3-440003: Deletion failed for RedInfoTable
  ```

  This system message may appear you specify a **no associate context** command and **no ft group** command. Workaround: None.

- **CSCtj24719**—When the ACE has mixed TCP and UDP SIP traffic running at a high rate for five to six hours to a combination of Layer 7 and Layer 4 VIPs, the **show serverfarm** *name* command may display some real servers with current connections after the traffic has stopped and the connections have closed. Workaround: None.
- **CSCtk57750**—When you configure SNMP to poll the ACE for a configured class map, the correct information is not retrieved. Workaround: None.
- **CSCtn54768**—A HM socket leak can trigger an out-of-socket condition when the socket resource limit for HM is reached. When this issue occurs, probes fail due to the out-of-socket condition. You can verify this condition by using the **show hm-internal wrkthread-stats** command. Workaround: None.

- **CSCto02825**—The ACE allows users to configure inconsistent netmasks and fails to notify them of the inconsistency. For example, in this case the access-lists have inconsistent netmasks:

  ```
  access-list acl1 extended deny ip any 10.45.15.192 0.0.0.15
  access-list acl1 extended deny ip any 10.45.15.192 0.0.9.0
  ```

  Workaround: Manually unconfigure the objects (such as access-lists) that have an inconsistent netmask and then reconfigure them with consistent netmasks.

- **CSCto45906**—Each time that the standby ACE reboots, a context on it transitions to the STANDBY_COLD state and the ACE displays the following error:

  ```
  Error on Standby device when applying configuration file
  ```

  It is a timing issue due to the configuration size and total number of contexts. This issue can lead to a lot of Configuration Manager (CFGMGR) download processing which can lead to a command failure. CSCtn50357 is tracking the issue of the actual failing command that is not properly placed in the error logs. Workaround: Perform either of the following:

  - On the FT group for the context in the STANDBY_COLD state, enter the **no inservice** command followed by the **inservice** command.
  - Change the context FT group ID in the FT group to a higher number so that the context with the largest configuration does the configuration synchronization last.

- **CSCto81777**—When you use the CLI to configure a probe on the ACE, you cannot remove the **open** statement. You may also find that even if you did not configure values for probe interval, passdetect interval, and open timeout, those values appear in the ACE running configuration. Workaround: None.

- **CSCto94539**—When you configure probes on the ACE, they unexpectedly stop working and an out of socket condition is reported. Additional syslog will be provided to further troubleshoot this type of issue. Workaround: Take the probe out of service and place it back in service. If this action does not resolve the issue, remove the probe from the configuration and reconfigure it.

- **CSCtq12770**—When a port-channel interface is configured and you send an SNMP walk on the ifHighSpeed OID, it returns an invalid value. Workaround: None.

- **CSCtq24092**—When the ACE imports PEM-encoded SSL certificates or keys with line wrapping over 70 characters through a terminal, the ACE fails to install the certificate or key. Workaround: Import the certificate through FTP or TFTP.

- **CSCtq39716**—When the cesServerFarmRserverCurrentConns OID is polled through SNMP, it returns wrong values. For example:

  ```
  ACE/context# show rserver
   rserver              : server1, type: HOST
   state                : OPERATIONAL (verified by arp response)
   ---------------------------------
                                                  ----------connections-----------
         real                 weight state        current    total
     ---+---------------------+------+------------+----------+--------------------
     serverfarm: farm1
         172.21.31.3:0        8      OPERATIONAL  3          5809
  ```

  ```
  CISCO-ENHANCED-SLB-MIB::cesServerFarmRserverCurrentConns.1."farm1"."server1".0 =
  Counter64: 12884901891
  ```

  Workaround: Use the CLI to monitor this counter.

- **CSCtq38048**—If you find that a restore fails due to an error (for example, if you have nonexportable keys that are missing in the backup), the restore process halts and none of the remaining contexts are restored. This behavior typically occurs during restore due to nonexportable keys missing in the backup. Workaround: None.
- **CSCtq40340**—A half-opened connection (ESTAB/CLOSED) is created on the ACE. Upon receiving a SYN, the ACE sometimes fails to respond with the ACK for the SYN and silently drops the SYN. Without the ACK, the client continues to resend a SYN and the existing entry is never purged until the connection inactivity timer reaches the timeout for idle TCP connections. Workaround: None.
- **CSCtq64174**—After performing a reload of the ACE, you may find that the **no arp learned-mode enable** command is not shown in the **show running-config** command output. The **arp learned-mode enable** command is an ACE default, so it is shown in the running-configuration file only when the command is disabled; the **show running-config** command output displays “no arp learned-mode.” When an ACE reload occurs, this configuration is copied to the startup-config file. After an ACE reload when the startup-config file is applied to the ACE, the **no arp learned-mode** command generates an error because it is an incomplete command. Workaround: Specify the **no arp learned-mode enable** command in configuration mode, and then specify the **show running-config** command. The **no arp learned-mode enable** command should now appear in the **show running-config** command output.
- **CSCtq70223**—The ACE sends TACACS+ accounting information in two lines making it slightly more difficult to grep through. In the example shown below, “cmd=” is the start of the new line.

```
Mon May 23 11:49:26
2011 mnl-1slb-01 jwacase 3000 unknown stop task_id=/dev/pts/0_1306171095 stop_time=Mon
May 23 17:49:26 2011
    cmd=0:show runn service=none
```

  Workaround: None.

- **CSCtq73968**—In a redundant configuration, the active and standby ACEs display policy map statements in reverse order. For example:

  Active ACE:

```
policy-map type loadbalance first-match ERP-HCMTSTVIP-POLICY
  class class-default
    sticky-serverfarm NEW
    insert-http WL-Proxy-SSL header-value "true"
    insert-http WL-Proxy-Client-IP header-value "%is"
```

  Standby ACE:

```
policy-map type loadbalance first-match ERP-HCMTSTVIP-POLICY
  class class-default
    sticky-serverfarm NEW
    insert-http WL-Proxy-Client-IP header-value "%is"
    insert-http WL-Proxy-SSL header-value "true"
```

  Workaround: None.

- **CSCtq77675**—When using the ACE appliance Device Manager GUI, if you attempt to view the results of a virtual server (**Config > Operations > Virtual Servers)** by clicking the Oper State link of the virtual server (the blue and underlined Inservice link), the popup window will show details about a different virtual server. This issue may be due to configurations in which multiple class maps use similar names. Workaround: Use the **show service-policy detail** CLI command to check the details of the virtual server.

- **CSCtq80722**—When you configure a real server in service and have it remain inactive until the primary real server fails (the **inservice standby** command), the ACE config manager may become unresponsive and the ACE reboots. The following system messages may appear:

  ```
  %ACE-2-443001: System experienced fatal failure.Service name:cfgmgr(x) has terminated
  on receiving signal 8,system will not be reloaded
  %ACE-2-443001:System experienced fatal failure.Service name:cfgmgr(x) crashed, last
  core saved,system will not be reloaded
  %ACE-2-199006: Orderly reload started at xxx by System. Reload reason: Service
  "cfgmgr"
  ```

  This issue can occur when you use the leastconns, least-loaded, or response predictor to define how the ACE selects a real server in a server farm to service a client request. Workaround: Use the roundrobin predictor for the affected server farm.

- **CSCtr23456**—For Layer 7 connections, the ACE does not advertise the maximum segment size (MSS) configured for a connection parameter map through the **exceed-mss** command. Instead, the ACE echoes back the same MSS that the client advertised. Workaround: None.
- **CSCtr28457**—An ACL merge fails for certain VLANs that are in bridge groups; the global ACL fails to merge properly. This behavior occurs when the traffic is bridged on the ACE and is one hop away from the ACE. Workaround: Reapply the access group on the interface instead of using a global ACL.
- **CSCtr36240**—With the ACE configured for end-to-end SSL, if the backend server sends its full encrypted payload to the ACE, followed by an SSL close notify and a TCP RST, the ACE forwards the full payload to the client but then forwards the TCP RST to the client without sending an SSL close notify. Workaround: None.

  Note This issue can also occur with nonencrypted servers sending a RST.

- **CSCtr44960**—The HTTP response header for a CRL download fails if the server sets 'Content-length' instead of 'Content-Length' (lower-case “l” instead of an uppercase “L). When this happens, the ACE fails in downloading the CRL file and returns the following error:

  ```
  %ACE-6-253008: CRL My_CRL could not be retrieved, reason: invalid format of data
  ```

  Workaround: None.

- **CSCtr49115**—The ACE reboots when you execute the **vsh -c terminal length 0** command and the core directory creates core files similar to the examples shown below:

  ```
  750330  Jul 11 14:06:45 2011 0x801_vsh_log.16870.tar.gz
  750335  Jul 11 14:06:45 2011 0x801_vsh_log.16871.tar.gz
  750336  Jul 11 14:06:45 2011 0x801_vsh_log.16879.tar.gz
  ```

  This behavior may be due to the ACE running out of memory when executing the **vsh** command. Workaround: None.

- **CSCtr62421**—The ACE may become unresponsive and reboot due to low system memory issues. Workaround: None.
- **CSCtr83034**—In a redundant configuration, after you specify the **no inservice** command followed by the **inservice** command for a real server in a server farm, both ACEs become unresponsive and then reboot. Workaround: None.

- **CSCtr93395**—When UDP Booster is enabled on the ACE to load-balance DNS traffic, the source IP address does not appear in the **show conn** command output.

  ```
  host1/Admin# show conn
  conn-id    np dir proto vlan source               destination           state
  ----------+--+---+-----+----+---------------------+---------------------+-----
  101646    1  in  UDP   302  0.0.38.114:0         80.58.61.250:53       -
  ```

  Workaround: None.
- **CSCtr94589**—In a redundant configuration, where there are contexts active on both the active and standby ACEs along with connection replication and implicit PAT, you may find that TCP port numbers are being reused too quickly. When this issue occurs, the next TCP port number can become corrupted. Workaround: Make all contexts active only the active ACE.
- **CSCts00376**—While you attempt to copy a running-configuration file to the ACE from a remote server using TFTP, the ACE displays a “cmd exec error” on the console. It is expected that the ACE would display the proper error message if there is a failure in applying the running-configuration file. Workaround: None.
- **CSCts08972**—Control Plane (CP) management access stopped working because the Configuration Manager (CFGMGR) became unresponsive while attempting to compile the regex expression contained in the following command:

  ```
  ssl url rewrite location ^gdsp[\].* sslport 443 clearport 80
  ```

  Similar issues can occur because the CFGMGR consumes a large portion of the CP CPU when compiling certain regex expressions. Workaround: Reboot the ACE and use the alternate regex expression:

  ```
  ssl url rewrite location ^gdsp\.* sslport 443 clearport 80
  ```
- **CSCts19247**—When using the ACE appliance Device Manager GUI, if you create a class map condition from the ACE CLI that includes a space in an HTTP URL, that class map will not appear in the DM GUI. Workaround: Use the ACE appliance DM GUI if you need to create a class map condition that includes a space in an HTTP URL match.
- **CSCts24977**—The service name:snmpd(1395) terminates upon receiving signal 8. This issue can occur when polling the ACE CPU utility MIB in a loop; the snmpd process can become unresponsive and cause the ACE to reload. For this particular issue, the OID polled was .1.3.6.1.4.1.9.9.480.1.1.7.1. Workaround: Do not poll the ACE CPU utility MIB continuously in a loop.

Software Version A4(2.2) Open Caveats

The following open caveats apply to software version A4(2.2):

- **CSCsx71993**—You may encounter a discrepancy between the count and the actual connections displayed in the **show conn** command output. Workaround: None.
- **CSCsz71578**—ACL merge error occurs for newly added VLANs and traffic does not pass. This behavior occurs when you attach a traffic policy globally to all VLAN interfaces in the same context and then add the VLAN. Workaround: Remove and then reapply the traffic policy globally to all interfaces using the **service-policy** command.
- **CSCsz71578**—When you apply a service policy globally and then add the VLANs, the ACE displays ACL-merge errors for newly added VLANs and traffic does not flow through them. Workaround: Remove the global service policy and then reconfigure it.

- **CSCtb28070 (CSCtj65690)**—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, that configuration will not be downloaded and dynamic NAT does not work. For example:

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

  Workaround: Remove and add the service policy under the client interface.

- **CSCtb74020**—An access-group download failure may occur when you perform a cut and paste operation at the CLI prompt. For example, while pasting nine configuration lines into the configuration mode CLI prompt, to remove three global service policies and one access-group and reapply them to a single VLAN, the access-group download failure occurs.

  ```
  no service-policy input CLIENT-VIP-LAN-PM
  no service-policy input HOST-VIP-LAN-PM
  no service-policy input PM-ALLOW-REMOTE-MANAGEMENT
  no access-group input ANY

  int vlan 1000
  service-policy input CLIENT-VIP-LAN-PM
  service-policy input HOST-VIP-LAN-PM
  service-policy input PM-ALLOW-REMOTE-MANAGEMENT
  access-group input ANY
  ```

  In this case, the deny counter fails to increment in the **show resource usage** command output as well as the counter in the **show interface** output. In addition, traffic is dropped. Workaround: None.

- **CSCtb79857**—Access-list configuration changes are not downloaded to the data plane in the ACE. This issue is seen when an ACL is removed and then added immediately (approximately with a 5-second interval) with the same line number but with different parameters. Workaround: Wait approximately 10 seconds when removing and then making similar configuration changes to the ACE.

- **CSCtb83022**—An ACL leak occurs in ACE memory. This issue can happen when you configure ACLs using the **copy:disk0: running-config** command, and some of the new created ACLs are deleted while the copy process is in progress. Workaround: None.

- **CSCtc01071**—A server load-balancing policy is not applied to an interface after you specify the **insert-before** command on a Layer 3 class map. This issue typically occurs in cases where a multimatch policy map has a large number of associated class maps. Workaround: Avoid using the **insert-before** command if there are a large number of class maps under a multimatch policy map.

- **CSCtd33226**—The SNMP daemon can be very slow to respond (for example, a delay of approximately 10 to 15 minutes) when the ACE receives a malformed SNMP packet or there is a heavy utilization of SNMP polls. Workaround: None.

- **CSCtd42287**—When the ACE is running with the maximum limit of 8K static entries and you remove a service policy from an interface and quickly readd it, the ACE removes the statements from the NAT policies. Workaround: Provide ample time between removing a service policy from an interface and then readding it.

- **CSCte12130**—When ANM has been polling the ACE for a long time, occasionally ANM does not read all the SNMP responses back from the ACE and reports the Operation status as N/A for many of the virtual servers. This issue occurs on any ACE software version and in ANM 2.0 and 2.2. Workaround: Reboot the ACE to fix this issue.

- **CSCte65621**—With the ACE configured for remote authentication through a TACACS+ server, you find that you are unable to login to the ACE through either a Telnet or SSH session. Workaround: Remove the TACACS+ server from the configuration and reconfigure it again.
- **CSCte76598**—The first packet of a TCP, UDP, or ICMP connection may not be captured; however, the remaining packets are captured for the same flow. This behavior can occur when you have the packet capture function configured for a specific ACL and for Layer 7 load-balanced traffic. Workaround: None.
- **CSCte76618**—When traffic traverses the ACE 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.
- **CSCtf42890**—The primary and backup server farms are in the INACTIVE state due to partial threshold failures. This issue is due to the backup server farm not properly handling the connections when the primary server farm fails over. 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.
- **CSCtg31975**—When using the ACE appliance Device Manager GUI, a system admin account in the ACE software may allow an authenticated user to inject shell commands (hidden DM GUI commands). The system admin account requires authentication. Workaround: None.
- **CSCtg67860**—When you configure multiple track probes in two user contexts and enter the **show cfgmgr internal table track-probe** command, the ACE becomes unresponsive due to a Cfgmgr process failure. Workaround: None.
- **CSCtg68105**—In a redundant configuration, with a large configuration, you may observe "mts_acquire_q_space() failing" errors on both the active and standby ACEs. You may also experience the ACE being nonresponsive to the display of certain **show** commands. This behavior may be due to an MTS buffer leak. Workaround: None.
- **CSCtg87855**—After you change the configuration in a large ACE configuration and enter **show** commands, the CLI becomes unresponsive for a period of time. In this case, the **show processes cpu | include cfgmgr** command displays one of the configuration manager (cfgmgr) processes consuming CPU resources. After you apply the configuration change, the cfgmgr CPU usage goes to zero, and the CLI becomes unresponsive. Workaround: Wait until the cfgmgr completes its previous operation before entering the **show** command.
- **CSCth04993**—When you configure an ACE interface with single NAT IP address in the NAT pool and the ACE receives SIP UDP traffic, it resets subsequent SIP TCP traffic. Workaround: Perform either of the following:
  - Perform a checkpoint rollback to a non-SIP configuration and then to the existing configuration.
  - Increase the number of IP addresses in the NAT pool.
- **CSCth07709**—When performing the **snmpwalk** or **snmpbulkwalk** command for any object on the ACE, occasionally the ACE displays an Unknown user name error. The frequency of this occurrence can increase by having three contexts on the ACE. Workaround: None.
- **CSCth24647**—When the FT interface VLAN number is lower than the other interface numbers and these interfaces require the downloading of large configurations, an API timed out error occurs when applying the startup configuration. Workaround: Enter the **no ft auto-sync running-config** command and then enter the **ft auto-sync running-config** command.

- **CSCth55362**—When the ACE performs a configuration rollback, existing classes in a policy are not reordered according to the new configuration. The running configuration has a policy that contains several classes. The checkpoint contains that policy with some or all the classes in a different order. After performing the rollback, the order of the classes stays as it was in the running configuration. Workaround: Perform either of the following:
  - Remove the policy that was changed during the rollback and then perform the rollback.
  - If there are many similar policies in the configuration, perform a rollback to an empty configuration and then rollback to the desired configuration.
- **CSCth56931**—With FTP inspection enabled in the configuration and the **logging buffered** command enabled for debugging (level 7), the ACE reboots with the syslogd process creating a core file. 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.
- **CSCth87128**— Sticky entries are seen even though the server farm has been disassociated from the sticky group. Workaround: Stop the traffic before removing the server farm from the sticky group.
- **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.
- **CSCti58831**— In a redundant configuration, with a configuration and the Application Networking Manager (ANM) running in the background, the standby ACE goes into the STANDBY_COLD state with command exec errors when performing bulk config synchronization (sync). Workaround: Specify the **no inservice** command followed by the **inservice** command for the affected FT group.
- **CSCtj00826**—If the ACE is running a large number of HTTP or HTTPS probes when probing a file approximately a megabyte in size, the ACE reboots. The following message may precede the reboot:

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

  Workaround: Reduce the size of the file being probed when running a large number of probes on the ACE.
- **CSCtj12692**—When you configure the ACE with 4000 sticky groups and do not allocate a sticky resource class, the resource values of the sticky are the default of a minimum of 0 and a maximum of unlimited. When the sticky database has 800,000 entries and you create a sticky resource class to a minimum value equal to 20 percent and apply it to the context, the ACE becomes unresponsive after a few minutes because it becomes unresponsive in the LB module at the function LbSticky_ReturnOldestEntry. Workaround: Do not change the resource class when you configure a large number of sticky groups and the database is full with active entries.
- **CSCtj65634**—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.
- **CSCtk53923**—When you delete a user with the name “test”, the ACE may unexpectedly reboot. The last boot reason is Service “securityd.” Workaround: None.

- **CSCtk59163**—When you configure multiple contexts and HTTP return code (retcode) checking, after traffic is sent to all the contexts, most of the context real servers are stuck in the RETCODE state no matter what the setting is of the resume-service timer. Workaround: None.
- **CSCtk76503**—The denied counter for bandwidth increases even before the maximum allocation has been reached. When this occurs, the count does not clear when you specify the **clear stats resource-usage** command. Workaround: None.
- **CSCtk98620**—When you make multiple changes to an SSL parameter map and then specify the **show stats crypto client** command, the ACE configuration manager (cfgmgr) receives a signal 11 and the ACE becomes unresponsive. Workaround: None.
- **CSCtl04271**—After you remove a class map from a policy map, an ACL merge does not work. Workaround: Remove the service policy from the assigned interface and reapply the same policy.
- **CSCtn18486**—Performing a backup and restore of the ACE configuration can cause the ACE configuration manager (cfgmgr) to become unresponsive. This issue may be due to a kernel issue. Workaround: None.
- **CSCto46159**—When you configure the maximum number of the VIP statements in a single class map of 254 and then delete one of the VIP statements, the ACE cannot add a match VIP address in a single class map and displays the following message:

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

  Workaround: Remove the class map and the reconfigure it again with all of the VIP addresses.
- **CSCto71443**—When you configure an FT group ID 64 on the ACE, a bulk sync timeout occurs for this group or connections are not replicated in any FT group. Workaround: Do not use group 64. Use a value between 1 to 63, inclusive.
- **CSCto92997**—When the hit counts are populated in the **show service-policy url-summary** command output and you remove one or more of the URL match statements from Layer 7 class maps, the hit counter clears. Some of the subsequent URL match statistics are affected. This issue does not affect the load balancing to the rest of the URL match criteria. Workaround: Use the **clear service-policy** *policy_name* command to clear all of the statistics and the hit counter repopulates according to the incoming traffic.
- **CSCto94653**—With traffic flowing through the ACE, while creating a checkpoint of a running configuration on your ACE, you may find that the console hangs and that the ACE becomes unresponsive. Workaround: None.
- **CSCtq11972**—When you configure an Oscilloquartz NTP server with stratum 2, the ACE cannot synchronize its time with the NTP server. Workaround: None.
- **CSCtq13738**—In a redundant configuration, a user profile will not be removed from the standby ACE even if the username is removed on the active ACE. Workaround: Disable redundancy and then delete the user profile from the standby ACE.
- **CSCtq39383**—Session Initiation Protocol (SIP) traffic may fail after the ACE receives approximately 15 minutes of traffic if you have enabled strict header validation on the ACE to check SIP packet headers. Workaround: Remove and then readd a SIP parameter map to perform SIP inspection.
- **CSCtr62530**—When a NAT pool is applied and then removed from a VLAN interface, these actions corrupt the Route table in the ACE. This issue happens when the same NAT pool is applied to multiple VLAN interfaces, and that NAT pool is removed from the first VLAN interface while it is still applied on the second VLAN interface. Workaround: None.

- **CSCtr79276**— The ACE does not work properly in one-arm mode with SIP and TCP when source NAT is enabled. SIP registrations and calls may fail depending on whether SIP Inspect is enabled. Workaround: None.
- **CSCtr96229**—With the ACE configured with several contexts, and one of the contexts has a resource class that contains sticky limits, the ACE reboots after you remove the resource class association from that context. The issue is related to the number of contexts configured in an ACE. When the load-balancing module in the ACE tries to remove sticky entries from the free list, it needs to check if there is a starving context that is waiting for resources, which can consume CPU time. Workaround: None.
- **CSCts36540**—In a redundant configuration, with multi-context sticky traffic, if you perform an FT switchover while under heavy traffic and the sticky database is full, the ACE will reboot. Workaround: Increase the sticky timeout value.
- **CSCts45803**—Applying, detaching, and then reapplying a traffic policy to a specific VLAN interface or globally to all VLAN interfaces in the same context results in an “Error: Policy does not exist” error message. Workaround: None.
- **CSCts48048**—With 100,000 sticky instances and IXIA traffic running through the ACE, the ACE may reboot when you change the sticky resource allocation value from 15.00 to 00.01. This behavior may occur when the maximum limit is set as equal-to-min for the sticky resource. Workaround: None.
- **CSCts53405**— After forwarding the real server’s first response packet to the client, the ACE waits for the client to send an ACK to the first response packet before forwarding subsequent server response packets. Workaround: To control how the ACE applies TCP optimizations to packets on a connection associated with a Layer 7 policy map using a round-trip time (RTT) value, use the **set tcp wan-optimization rtt** command.
- **CSCts68281**—With a configured HTTPS health probe, the ACE may display the following system error message:

  ```
  %ACE-3-400001: MSS mismatch from 10.0.5.193:443 (1380) to 127.1.2.34:64571 (1460) on
  interface vlan40
  ```

  Workaround: Remove the HTTPS probe from the server farm.
- **CSCts64847**—Only the default Admin user can run the **show environment temperature** command. If another user has an Admin role but is not the default Admin user, that user may not be able to specify this command and the ACE displays the following error:

  ```
  ACE/Admin# show environment temperature
  Could not open device at /dev/ipmidev or /dev/ipmi/0 or /dev/ipmidev/0:
  Not a directory
  Get Device ID command failed
  Unable to open SDR for reading
  ```

  Workaround: Use the default Admin user to run the **show environment temperature** command.
- **CSCts71740**—When you configure a scripted probe and use the HTTPPROXY_PROBE script, the probe may fail and the ACE displays the following error:

  ```
  internal error = invalid command name "debug" while executing "debug"
  ```

  Workaround: None.
- **CSCts73859**—When using the hash content predictor method for load-balancing, connections to a server farm are not hashed to a single real server. Workaround: None.

- **CSCts79939**—The following rewrite configuration does not successfully rewrite any instances of "http" under some scenarios:

  ```
  action-list type modify http REWRITE
    header rewrite response Location header-value "(.*)http(.*)" replace "%1https%2"
  ```

  While parsing the Location header, the ACE stops parsing after encountering any instance of the first letter in the match string ("h"). At that point, the ACE does not complete the match or perform the rewrite. Workaround: None.
- **CSCts98720**—In an application where the ACE is performing firewall load-balancing with two server farms (where one server farm is for user traffic and the one is for BGP traffic sent to the firewalls), when performing failaction reassign and then undoing the failaction, the ACE incorrectly moves a user connection to the BGP dedicated server farm. Workaround: None.
- **CSCtt02508**—The end-to-end SSL TCP connection encounters issues while uploading a large (approximately 4.5 GB) file through an ACE VIP that is configured for end-to-end SSL. Simultaneous front and back-end traces show that the ACE brings the TCP window to zero on the client side but does not send any further data toward the server on the back-end side even though the last TCP window update from the server is 65K. The upload stops and never resumes after that. Workaround: None.
- **CSCtt06395**—The ACE fails to create sticky entries when HTTP content and HTTP request Header insert for load-balancing are configured on the ACE. In this case, sticky entries should be created in the **show sticky database** command output. Workaround: None.
- **CSCtt42497**—When performing Layer 7 server load-balancing with a configuration that includes a combination of sticky, server connection reuse, and persistence-rebalance, bad HTTP requests may occur on the server as Layer 7 HTTP packets are sent out of order. Packets sent out of order cause the server to drop the packets or tag the request as malformed. Workaround: Disable the **server-conn reuse** command.

Software Version A4(2.2) Command Changes

Table 6 lists the command changes in software version A4(2.2).

Note For a summary of new features for software version A4(2.2), including the associated new or modified commands, see the "New Software Features in Version A4(2.2)" section.

Table 6 CLI Command Changes in Version A4(2.2)

Mode	Command and Syntax	Description
Exec	**show running-config**	Per CSCto81777, the **show running-config** command no longer displays the default probe interval, passdetect interval, and open timeout values for a probe configuration. If values other than the default values are configured for probe interval, passdetect interval, or open timeout, those values do appear in the ACE running configuration.

Software Version A4(2.2) System Log Messages

Software version A4(2.2) includes the following new system log (syslog) messages and syslog identifier changes.

106029

Error Message `ACE-6-106029: ACL` *`name`* `configured with invalid netmask`

Explanation Per CSCto02825, the ACE generates this system message when you configure a non-standard netmask for either a source or destination IP address in an ACL configuration.

Recommended Action Configure a valid netmask for the IP address.

251021

Error Message `%ACE-4-251021: Health Monitoring connection info invalid,` *`socket:xxxx`*`,` *`socket_state:yyyy`*`,` *`connection_state:zzzz`*

Explanation Per CSCto94539, the corruption of health monitoring socket connection information is flagged by this Level 4 syslog. The error message variables are as follows:

- *`socket:xxxx`* displays a negative value.
- *`socket_state:yyyy`*, *`connection_state:zzzz`* displays invalid (mostly large) positive or negative values.

For example:

```
%ACE-4-251021: Health Monitor connection info invalid, socket: 44,
socket_state: 1853121902, connection_state: 9
```

```
%ACE-4-251021: Health Monitor connection info invalid, socket: -1428151032,
socket_state: 3, connection_state: 9
```

Recommended Action Check whether health monitoring is functioning properly on the ACE. If there appears to be issues with health monitoring, contact TAC for further troubleshooting.

729004

Error Message `%ACE-6-729004: Regex compilation is currently running for context` *`xxxx`*`.`

Explanation Per CSCts09818, a Level 6 syslog has been added to the ACE to track if regex compilation is occurring and whether the ACE configuration manager is involved in the compilation. The syslog tracking is performed per context, which occurs in a 5-minute interval to inform you that a regex compilation is in process. The error message variable is as follows:

- *`xxxx`* is the context identifier.

Recommended Action The ACE restricts you from modifying the configuration during the regex compilation process.

Identifier Changes in Selected Health Monitoring ACE System Log Messages

Per CSCtr23603, the order of certain Level 3 health monitoring system message log identifiers has changed as part of the A4(2.2) software release (as shown in Table 7) to ensure consistency with the syslogs in software versions prior to A4(2.x) (including A4(1.x)).

Table 7 Changes in Health Monitoring syslog IDs with Software Version A4(2.2)

Existing Syslog Identifier (pre Software Version A4(2.2))	New Syslog Identifier (Software Version A4(2.2))
251014	251018
251015	251019
251016	251016 (same syslog Identifier)
251017	251017 (same syslog Identifier)
251018	251015
251019	251020
251020	251014

For your reference, this section provides a complete listing of the updated Level 3 system message logs, 251014 through 251020:

251014

Error Message `%ACE-3-251014: Could not probe server` *`IP_address`* `on port` *`port_number`* `for` *`number`* `consecutive tries - Internal error.`

Explanation The health probe could not be sent because of an internal error. The probe is skipped.

Recommended Action Remove and then readd the probe to the real server or server farm.

251015

Error Message `%ACE-3-251015: Scripted probe failed for server` *`A.B.C.D, error message`*`.`

Explanation The configured real server *A.B.C.D* failed its health checks because the associated server response is not as expected or there was an internal error. The possible values of the *error message* variable are as follows:

- Probe error: Server did not respond as expected
- Internal error: Fork failed for TCL script
- Internal error: Script probe terminated due to timeout
- Internal error: TCL interpreter PANIC
- Internal error: Script error
- Internal error: Script-file lookup failed or empty buffer
- Internal error: Failed to allocate memory for tcl workerthread qnode

- Internal error: Unknown script error
- Internal error: Out of sockets for the TCL script
- Internal error: Unable to read persistent variable table
- Internal error: PData (probe data) pointer is null

For example :

```
%ACE-3-251015: Scripted probe failed for server 25.25.25.83, Internal error: Script
error
```

Recommended Action Perform one of the following actions:

- Check the service running on the server.
- Check the script used for the probe.
- Check the memory available for TCL scripts.

251016

Error Message `%ACE-3-251016: Web service internal error: `*`string`*`.`

Explanation The configured server farm failed the VM load query because the Web Service Client encountered an error while performing the probe. These errors are internal to the system. The load information of the server is unknown at this point.

Recommended Action This is a rare error. If it occurs more frequently and causes a server outage, report the error message to the Cisco Technical Assistance Center (TAC) for further troubleshooting.

251017

Error Message `%ACE-3-251017: User input url is not a vcenter.`

Explanation Unable to get load information for the server farm because the user input URL does not represent a vCenter Server.

Recommended Action Verify the web-service CLI input of the URL.

251018

Error Message `%ACE-3-251018: Failed to log in to vCenter, reason `*`reason`*`.`

Explanation Unable to get access and log in to the web service server as indicated by the CLI.

Recommended Action Verify the web service server configuration and network connectivity.

251019

Error Message `%ACE-3-251019: Failed to retrieve load value for vm` *`vm_id`*`, reason` *`reason`*

Explanation Unable to get load information for the real server list because the real server encountered an error while getting information from vCenter.

Recommended Action Verify the real server list and VM probe configuration. This issue may also be caused by vCenter errors.

251020

Error Message `%ACE-3-251020: Online diag vlan` *`vlan_id`* `configuration error.`

Explanation (ACE module only). This message is internally generated when the ACE module online diagnostics detect an error during the bootup configuration phase. The *vlan-id* variable is the value on which the supervisor engine is trying to run the online diagnostic test. The possible values are 1006 to 1011.

Recommended Action None required.

Software Version A4(2.1a) Resolved Caveats and Open Caveats

Note ACE appliance software version A4(2.1a) has replaced software version A4(2.1) on www.cisco.com.

This release note includes resolved and open caveats that have a severity level of Sev1, Sev2, and customer-use Sev3. The following sections contain the resolved and open caveats in software version A4(2.1a):

- Software Version A4(2.1a) Resolved Caveats
- Software Version A4(2.1a) Open Caveats

Software Version A4(2.1a) Resolved Caveats

The following resolved caveats apply to software version A4(2.1a):

- **CSCtq68806**—With a server farm configured for a maximum number of active connections, in some cases when one or more real servers reach the connection limit max and fail their health probes the VIP is not taken out of service. Workaround: Remove the health probe from server farm then reapply it.
- **CSCtq93400**—With AAA authentication configured for the ACE and you are using a TACACS+ server for user authentication, authentication can fail for users that include a period (".") in their username. When this behavior occurs debugs are generated and the ACE does not attempt communication with the TACACS+ server. Workaround: None.
- **CSCtr12755**—In some instances the ACE generates the following syslog when the maximum segment size (MSS) between the front end and the back end connections do not match:

  ```
  %ACE-3-400001: MSS mismatch from A.B.C.D:E (M) to W.X.Y.Z:F (N) on interface
  IFVLAN_NAME
  ```

  This syslog should only be generated when the back end MSS size is lower than the front end size. In the case where the front end MSS is lower than the back end, the ACE uses the front end MSS in the back end connection. Workaround: None.

Software Version A4(2.1a) Open Caveats

The open caveats in software version A4(2.1a) are the same as those in software version A4(2.1). For details, see the Software Version A4(2.1) Open Caveats section.

Software Version A4(2.1) Resolved Caveats, Open Caveats, Command Changes, and System Log Messages

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, command changes, and revised system messages in software version A4(2.1):

- Software Version A4(2.1) Resolved Caveats
- Software Version A4(2.1) Open Caveats
- Software Version A4(2.1) Command Changes
- Software Version A4(2.1) System Log Messages

Software Version A4(2.1) Resolved Caveats

The following resolved caveats apply to software version A4(2.1):

- **CSCsr55832**—When you enable logging console 6 or 7 on the ACE and approximately 200 messages per second flood the console, the **show run** command becomes unresponsive. Workaround: Rate limit the console logging message to 40 cps.
- **CSCsz08381**—When a non-typical Layer 4 type packet is fragmented and the ACE reassembles it, the first 4 bytes of the Layer 4 header on the reassembled packet become corrupted. Workaround: To avoid reassembly, do not fragment the packet.
- **CSCtg17350**—When you configure the Acceleration and Optimization features on the ACE, the integrated packet capture utility may not capture traffic from all interfaces, even when you configure the capture to capture from all interfaces. Workaround: None.
- **CSCth07619**—When you apply or modify ACLs or object groups to an ACE that has operated for a long time and undergone many ACL configuration changes, issues in the ACL object group expansion during the configuration download may cause an unexpected traffic drop. The **show interface** command displays a non-zero download failure counter, similar to the following:

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

  Workaround: Remove and readd the object group.
- **CSCth08116**—When you configure the **expect regex** command on HTTP or HTTPS probes with a long regex string and the web page parsed by the probe is longer than 100 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** (**CSCtg37325**)—During normal ACE operating conditions, the configuration manager becomes unresponsive and the ACE generates a core file. Workaround: None.
- **CSCth23304** (**CSCth12446**)—When the ACE is using a 1-Gbps throughput license, the throughput output displayed through the **show resource** command is rounded to the nearest thousand. For example, a value of 134217728 is rounded to 134217000. This issue does not occur with other throughput licenses. Workaround: Install a throughput license that is not 1 Gbps and then uninstall the license.
- **CSCth26795**—When you configure the **mac-address autogenerate** command with the **ip dhcp relay** command on an interface, the ACE appliance fails to relay the DHCP request to the configured server and the counters displayed by the **dhcp relay statistics** command do not increment. Workaround: Remove the **mac-address autogenerate** command from the interfaces and reboot the ACE.

- **CSCth39505** (**CSCth39502**)—The ACE divides the sticky table and cookies between its two IXP network processors (NPs). If a connection on one NP uses a cookie with a hash that resolves to the other NP, the NPs must perform additional inter-IXP messaging to process the cookie. In a default TCP connection configuration, if the server sends 32K or more of data in less than 10 milliseconds (msec), a zero window may result on the backend. Some server TCP stacks may inadvertently introduce a 5-second delay in this situation. The ACE should advertise a non-zero window to the sending server when the buffers are released. Workaround: You can configure the **set tcp wan-optimization rtt 0** command to apply TCP optimizations to packets for the life of a connection. However, this command results in increased resource consumption.
- **CSCth43108**—The following RBAC configuration does not prevent you from entering the **telnet** command:

  ```
  role test
  rule 1 deny create feature exec-commands
  rule 2 permit create feature xxxx username cisco123 password cisco123 role test domain
  default-domain
  ```

  Workaround: None.
- **CSCth45076**—When you configure a static multicast ARP address on the ACE, you cannot ping to the address from the ACE. Workaround: None.
- **CSCth63553** (**CSCth63549**)—The standby ACE may have a higher number of connections than the active ACE. Workaround: Configure a shorter connection inactivity timeout.
- **CSCth64338**—If you configure TCP probes with small intervals and set the termination mode as forced, the TCP probe stops firing if the server sends an RST after the TCP handshake. Workaround: Remove and readd the faulty probe from the real server.
- **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**—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 these workarounds can prevent a large number of reap messages from being produced and queued, which can cause the slow release of system resources.
- **CSCth90592**—When you configure static NAT port redirection, the ACE does not apply the configuration and displays the following error message:

  ```
  Error: A static ip and source port must be provided in ACL for static port redirection
  ```

  Workaround: Configure a source port in the ACL for static port redirection.

- **CSCti11896**—The ACE treats the deny function inside a management policy or class map as a SKIP. The ACE does not deny the traffic. Instead, it skips the class map and tries to match another one. Workaround: None.
- **CSCti25263**—If the same SNMP request identifier is used in previous SNMP GET and GET NEXT requests to the ACE and an SNMP agent is polling the ACE, the ACE may incorrectly respond to the SNMP request. Workaround: Perform the following:
  a. Change the SNMP agent to use unique SNMP Request Identifiers for each SNMP request.
  b. Wait at least 10 seconds between SNMP requests that use the same SNMP request identifier.
- **CSCti34985**—When you enable the **replicate sticky** command on the active ACE and a sticky entry is synchronized to the standby ACE, if you disable this command on the active ACE and perform a switchover, the sticky entry is synchronized back to the new standby ACE. Workaround: None.
- **CSCti40433**—When the client sends a SYN on an existing Layer 7 connection, the ACE responds to a TCP SYN with an ACK, and an incorrect ACK sequence number. Workaround: None.
- **CSCti40456**—The ACE does not reset a SYN on an existing L7 connection. The SYN is for an existing L7 connection and the sequence number is within the receive window. Workaround: None.
- **CSCti52381**—When you configure an FT track host probe without an FT track host, the probe transitions to the INVALID state. Workaround: Configure an FT track host under the FT configuration.
- **CSCti52534**—When you convert 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 the **ssl urlrewrite** command and the SSL proxy configuration does not have certificate and file names. Workaround: Manually add the missing configuration.
- **CSCti66770** (**CSCth37401**)—When the ACE receives a cookie string that contains many cookies and encounters a space character in the cookie value, it stops processing the cookies. Spaces are not permitted in the cookie name or cookie value. Persistence or stickiness fail. Workaround: None.
- **CSCti72204**—After correcting a license mismatch on the standby ACE, the active ACE replicates configuration changes to the standby ACE and the standby ACE displays the following error message:

  ```
  Running cfg sync enabled : Disabled with sh ft group detail command
  ```

  Workaround: Reboot the standby ACE.
- **CSCti74189 (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.
- **CSCti74520**—When sending malformed requests, SSHD may become unresponsive. This issue has occurred when running testcase 4738 of the Codenomicon SSHV2 test tool. Workaround: None.
- **CSCti76422**—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**—If you configure SNMP traps on a VLAN that is missing either the IP address or the peer IP address and redundancy is enabled, the active ACE does not synchronize the SNMP traps to the standby ACE. The **show ft group detail** command displays the following error:

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

  Workaround: Configure both an IP address and a peer IP address on the interface VLAN that you are using as the trap source.
- **CSCti88468**—After you enter a **show** command at the CLI, the ACE may write a VSH core file when you enter an SSL **crypto** command. The VSH core file does not cause the ACE to reboot. Workaround: None.
- **CSCti90240**—In a redundant configuration, after the **show resource usage all** command is executed either by ANM or by using a script at bootup time, command parse errors are seen on the console of the standby and the context enters the STANDBY_COLD state. Workaround: After the bootup is finished, resynchronize the configuration using the **ft auto-sync running-config** command.
- **CSCti96864**—When you perform dynamic configurations of adding and deleting usernames in multiple contexts and simultaneously attempt to run SNMP walk, the ACE unexpectedly reboots and generates an SNMP core file. Workaround: None.
- **CSCtj04935**—When the Layer 7 TCP path is overutilized that causes the Timer Freelist Empty to be hit several times, the ACE reboots because of the Timer Freelist corruption. Workaround: Reduce the work load of the Layer 7 TCP path.
- **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: Remove the offending contexts manually and then perform the restore operation.
- **CSCtj18833**—When you configure the ACE for bridge mode and it has a static ARP entry for the real server, after the ACE reboots, the ARP entry for a real server is in down (dn) state. Workaround: Remove the static entry and readd it.
- **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.
- **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.
- **CSCtj44561**—Under normal operating conditions, the ACE unexpectedly generates an AVS core file and may reboot. Workaround: None.
- **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 when you are using the Command Line Interface (CLI) or XML, the configuration of a sticky server farm may fail. Workaround: Reboot the ACE.
- **CSCtj62369**—When the application acceleration and optimization features of the ACE are configured, the integrated packet capture utility may not capture traffic from all interfaces even when the capture is configured to capture from all interfaces. Workaround: None.
- **CSCtj65408**—When you configure an ECHO TCP or UDP probe with send-data value, the probe always passes if the server sends a regex that does not match the send-data value. Workaround: You can use a TCP or UDP probe with send-data and regex values as required instead of an ECHO TCP or UDP probe.
- **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 the 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 reboot. 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.
- **CSCtj91896**—When you configure a TCP probe and it becomes active a few seconds later, the server sends out of band data to the ACE causing the ACE to reboot and generate an hm_core file. Workaround: None.
- **CSCtk00432**—After a user account has expired on the ACE, the ACE DM still allows the expired user to log in, view, and edit the ACE configuration. Workaround: The ACE appliance administrator must manually remove the expired user from ACE.

- **CSCtk01918**—When the ACE is configured with access control lists, object groups, and DHCP, an ACL merge failure may occur when you apply the configuration to an interface. This issue can cause the configuration to be incomplete and needs to be manually removed. Workaround: None.
- **CSCtk03294**—When you configure the ACE with a port-channel link, the redundancy heart beat is always sent on one interface only because of the load-balancing mechanism. If that interface goes up and down because of port-hashing convergence, the heart beat may be dropped during 2 to 4 seconds. Both ACEs may then become active /active during that time. This issue is a limitation of the current redundancy implementation. Workaround: Ensure that the heart beat interval is no too aggressive and avoid configuring carrier delay on PO interfaces.
- **CSCtk06591**—If the ACE is configured to get the time via the Network Time Protocol (NTP) and the actual time on the ACE is set incorrectly, a demo license can be installed and work correctly until the ACE is rebooted. Workaround: Set the time correctly using the **clock set** command.
- **CSCtk08750**—If you attempt to log in with a username that contains some special characters, the ACE inserts random text in the login prompt. This behavior occurs only with certain special characters that are invalid for a username. Workaround: Do not create or use a username with invalid characters.
- **CSCtk09730**—A Linux kernel file system error log was observed during bootup of the ACE. Workaround: None.
- **CSCtk11720**—When you are troubleshooting the ACE, the data plane (DP) console logs are difficult to obtain. Workaround: None.
- **CSCtk14790**—When you configure TACACS with the **aaa authentication login default group tacacs local** command, the first attempt to SSH to the ACE fails. A second SSH attempt with the same username is successful. If you enter the **no username** *name* command, the original behavior occurs again and you must SSH twice to be successful. Workaround: You must SSH to the ACE twice.
- **CSCtk30688**—When a Layer 7 policy is configured with a sticky server farm, the StickyConns counter in the **show serverfarm detail** command may overflow. Workaround: None.
- **CSCtk52854**—The time that is required to run the **show tech** [**details**] diagnostic command may take hours with a heavily configured ACE. Workaround: None.
- **CSCtk53132**—An ACE appliance running software version A4(1.0) does not boot properly. When the ACE is running an A3(2.x) software image, it does boot properly and run normally. Workaround: Complete an RMA for the appliance. In this case, the new ACE appliance booted properly.
- **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.
- **CSCtk68122**—When you configure the least loaded predictor in a server farm, the ACE does not set the autoadjust average option. Workaround: None.
- **CSCtk69726**—When you configure inband health checking and return code (retcode) checking together under a server farm, a real server may become stuck in the INBAND FAILED or RETCODE FAILED state 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.
- **CSCtk84003**—When you set the window scale to ALLOW by configuring the **tcp-option window-scale allow** command in a parameter map, the window size calculation for the Layer 4 flows does not occur. Since the ACE calculates the window size without taking the window scale

into account for Layer 4 flows, the ACE may drop some packets that are legal. Layer 7 flows are not affected. Workaround: Remove the **tcp-option window-scale allow** command from the parameter map configuration.

- **CSCtk95076**—If you configure AVS configured in one-arm mode (the server and client are configured on one interface), the debug packet capture occurs only on the server side and does not occur on the client side. It should capture both. Workaround: None.
- **CSCtk96341**—The **duplex** command fails when playing the startup-config or when syncing to an ACE running another software release. For example, if a configuration containing the duplex full command was saved while running software version A3(2.x), the startup-config would be incompatible with other releases.
- **CSCtl03706**—When the ACE performs the **snmpwalk** command on the cpmProcessTable, the **show proc cpu** command becomes unresponsive. The output of **show system internal mts buffers** command displays an MTS leak. The output of the **show system internal mts buffers details** command confirms this leak. Also, the MTS sends error messages similar to the following:

  ```
  mts_do_msg_input() failing since no space available in 91 (src_sap = 91, opc = 1376
  PID = 934) 2
  ```

  Workaround: None.
- **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.
- **CSCtl20133**—When you enable the **logging persistent** command, it allows the ACE to save a specified syslog to its flash memory. As expected, the ACE creates a "messages" file on disk0. However, after you delete this file, the **logging persistent** command does not work again until you remove and reconfigure the command. Workaround: Remove and reconfigure the **logging persistent** command.
- **CSCtl45638**—When you configure usernames with the ACE default roles, a user with the Network-Monitor role does not have access to some commands. Workaround: Assign the user with the admin role.
- **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.
- **CSCtl53644**—When you configure access lists on the ACE and an ACL Merge error occurs on VLAN1 which is an internal VLAN, the **show vlan** *number* command cannot display the error counters because user-configured VLANs start at 2. Workaround: You may be able to use the debug function to display the logs.
- **CSCtl56689**—When you are using the Device Manager (DM) with remote authentication, such as TACACS, and a login is remotely authenticated through TACACS on the ACE, the DM may fail. Workaround: Remove the TACACS filter running on the network.
- **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 when sticky is not configured. Workaround: None.

- **CSCtl68891**—When you configure a real server on the ACE, assign it an IP address, place it in service, and then delete it, the ACE generates an unnecessary trap. When the real server state changes from ARP-FAILED to operational, the ACE generates the CesRServerStateUp trap. 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.
- **CSCtl75924**—When you configure a user context on the ACE for KAL-AP, the ACE unexpectedly reboots and generates a gslb_proto_log.943.tar.gz core file. The last boot reason is Service "gslb_proto". Workaround: None.
- **CSCtl76773**—When you create a real server, class map, policy map, KAL-AP tag, server farm, or context name that includes a space in it, an ACE redundant configuration can become out of synchronization. Workaround: Do not use spaces when naming an object on the ACE.
- **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.
- **CSCtl89566**—When the ACE is performing Layer 5 load balancing and receives a non-compliant HTTP request, if the request hits a default class and is Layer 4 load balanced, the ACE drops the connection. 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*.
- **CSCtl97906**—When you change an ACL configuration for an object group, the following error messages occurs:

  ```
  %ACE-1-106028: WARNING: ACL Merge failed to add ACE in context ContextName. Error
  while processing access-group. Incomplete rule is currently applied on interface
  vlan#.  Configuration on this interface needs to be manually reverted
  ```

  Workaround: Avoid using object-group ACL configurations or reboot the ACE with a new ACL configuration that you applied and saved.

- **CSCtn06176**—When the ACE attempts for several hours to establish the Fault Tolerant TL connection (TCP connection between primary and secondary ACE used for FT communications), it stops its attempts and the ACEs fail to achieve the proper fully redundant state of ACTIVE/STANDBY_HOT. Workaround: Use the **show conn** command in the Admin context to determine whether the TCP connection between the addresses on the FT VLAN exists. If the connection exists, this bug is not the cause the problem. If the TCP connection does not exist, perform a shut and no shut on the FT VLAN causing the ACE to attempt to reestablish the TL TCP connection. If this action does not fix the problem, investigate why the TCP connection could not be established and correct the underlying issue (such as an external network interruption that caused the TCP connection to fail). After you resolve the underlying issue, retry a shut and no shut on the FT VLAN. Note that during the period when the TL connection cannot be established, the response from some of the FT **show** commands may be delayed, due to the FT spending resources attempting to bring up the TL connection.
- **CSCtn12227**—When using the following sticky layer4-payload configuration for an SSL session ID, sticky works; however, the **show sticky database layer4-payload** *session_ID* command does not return a value even though there is an entry in the sticky database:

  ```
  sticky layer4-payload SESSID-STICKY
    serverfarm SF1
    response sticky
    layer4-payload offset 43 length 32 begin-pattern
  "(\x20|\x00\xST)"
  ```

  Workaround: None.
- **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.
- **CSCtn25383**—When you configure a server farm with a scripted probe for health monitoring and scripted probes fail, the ACE does not generate level 3 health probe failed error messages. If you configure SNMP traps, the SNMP device logs the probe failures but the ACE does not generate them in the system log. The expected level 3 message is similar to the following:

  ```
  %ACE-3-251018 Scripted probe failed for server ip_address, error message.
  ```

  Workaround: None.
- **CSCtn40037**—The signal handler has been disabled on the network processor cores. As a result, when one core becomes unresponsive, the ACE immediately generates a core file. Ordinarily, an ME dump would detect this and force all other cores to become unresponsive. Because the signal handler is disabled, the other cores do not get stuck and they continue to process their message queues. This behavior may be an issue when debugging customer problems. This situation happens whenever a core becomes unresponsive. Workaround: None.
- **CSCtn41742**—When you associate a context name with 64 characters on the FT group, the FT group state remains in FSM_FT_STATE_STANDBY_CONFIG. Workaround: Configure a context name with 63 characters or less.
- **CSCtn43569**—The CPU utilization counter that the ACE obtains from the VMware vCenter Server provides the CPU utilization of a virtual machine (VM) as a percentage of the total ESX/Hypervisor CPU utilization. This process works fine for the default case where a VM is allocated with any number of cores and no resource limits are applied. The ACE receives the correct CPU load values of the VM and the feature works as expected. However, if there are resource limits provisioned to the VM (for example, limiting it to 50 percent of maximum CPU), then the counter value that the ACE receives from the vCenter does not accurately reflect the results. For example, a VM can use

the entire 50 percent of the allocated max CPU, and so the reported value should be 100 percent as the VM's CPU load. Instead, the reported value is 50 percent, which is the percent of total available ESX CPU utilization.

When you create a VM, the vCenter provides multiple options for CPU and memory allocation for the VM. As an administrator, you can allocate the number of cores to the VM and limit the CPU utilization of the VM to a portion of the max available CPU power (MHz). When you configure this CPU-limiting option on the vCenter, the average CPU usage counter provided by the vCenter is still calculated against the total CPU power for the ESX/ESXi host. The ACE retrieves this counter, but treats it incorrectly as the VM's CPU usage percentage against its own allocated CPU resource limit.

Workaround: When you create a VM with a CPU resource limit that is lower than the maximum limit (MHz), adjust the CPU burst threshold that you configure on the ACE for the DWS feature to compensate for the incorrect value provided by the vCenter. Calculate the new CPU burst threshold to be configured on the ACE by using the following formula:

New burst threshold = expected burst threshold x VM's CPU resource limit (MHz) / VM's maximum resource limit (MHz)

- **CSCtn56511**—When you configure FTP inspect and enable syslog messages on the ACE, and then any FTP command fails, the ACE displays the incorrect FTP command name in the syslog message or the ACE may reboot. Workaround: Turn off syslog messages.
- **CSCtn78101**—When you configure a service on the ACE with HTTP inspection and a file download that contains video or mp4 content occurs through the service (VIP), the video quality is poor. Workaround: Remove the HTTP inspection policy from the Layer 3/Layer 4 server load-balancing policy.
- **CSCtn91946**—When you log in to an ACE user context directly through the Device Manager, the GUI does not display the Backup/Restore option. Workaround: Log in to the Admin context through the Device Manager and choose the user context. Then, access the Backup/Restore option in the GUI.
- **CSCtn93288**—When redundant ACEs generate SIP probes with the same Call-ID and From-Tag options, the SIP registrar servers interpret these probe messages as duplicates and do not reply to them causing SIP health probes to fail. Workaround: None.
- **CSCtn96103**— When the following **banner motd** configurations trigger a config-sync error, the standby ACE transitions to the FSM_FT_STATE_STANDBY_COLD state with an cmd parse error,:
  - h(H)ostname and a space character:

    ```
    switch/Admin(config)# banner motd #
    Enter TEXT message. End with the character '#'.
    > hostname <--------------<SPACE>
    ```

  - h(H)ostname, a space character, and any character:

    ```
    switch/Admin(config)# banner motd #
    Enter TEXT message. End with the character '#'.
    > hostname a
    ```

  Workaround: Add a colon (:) after the h(H)ostname, for example:

  - > hostname: <--------------<SPACE>
  - > hostname: a
- **CSCtn98107**—When you configure the ACE for redundancy with many contexts and some of these contexts have large configurations, and then you reboot the ACE, a context transitions to the STANDBY COLD state. The FT-related output did not display the correct command that failed in

the context. Workaround: Perform the **no inservice** command and then the **inservice** command on the FT group. For the context in the STANDBY COLD state, assign it with a context ID number greater than one.

- **CSCtn99959**—When you configure an FT group ID 64 on the ACE, connection replication does not work in any context. Workaround: Do not configure FT group 64. Use a value from 1 to 63.
- **CSCto45952 (CSCta87584)**—When you configure persistence rebalance in a configuration with two server farms containing the same real server with different port numbers and attached to two different Layer 7 policy maps, the ACE drops connections intermittently after a rebalance occurs to a different Layer 7 policy. Workaround: None.
- **CSCto54476**—When an SSL certificate or key is in use on the ACE, you can delete it. Workaround: Before removing the certificate or key, manually verify whether it is being referenced in the configuration.
- **CSCto57262**—When the ACE has a high rate of SSL client authentications performing CRL checks, the **show np 1 me-stats -u** command displays 100% utilization of Core 0. This causes issues with the CP to DP communication and HA heartbeats may not be sent. Workaround: Disable CRL checking under the SSL proxy.
- **CSCto82759**—When you enter invalid options in the **show np 1 me stats** command, it does not provide usage help. Workaround: Do not enter invalid options with this command.
- **CSCto91249**—When you enter the **show parameter-map** command to list all of the parameter maps in the context and the first parameter map in the list is a connection type, the ACE does not display all of the parameter maps. Workaround: None.
- **CSCto92790**—In a redundant configuration in which one ACE is running software version A4(2.1) and the other ACE is running A4(2.0) or A4(1.1), the parameter map does not synchronize properly across the ACEs. Workaround: Ensure that both ACEs are running A4(2.1).
- **CSCtq36708**—When a VM probe has been running on the ACE for two day and the vCenter responds back with error conditions that the required field is null in the XML message, the ACE reboots. Workaround: None.

Software Version A4(2.1) Open Caveats

The following open caveats apply to software version A4(2.1):

- **CSCsz71578**—When you apply a service policy globally and then add the VLANs, the ACE displays ACL-merge errors for newly added VLANs and traffic does not flow through them. Workaround: Remove the global service policy and then reconfigure it.
- **CSCtb28070 (CSCtj65690)**—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, that configuration will not be downloaded and dynamic NAT does not work. For example:

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

  Workaround: Remove and add the service policy under the client interface.
- **CSCtd42287**—When the ACE is running with the maximum limit of 8K static entries and you remove a service policy from an interface and quickly readd it, the ACE removes the statements from the NAT policies. Workaround: Provide ample time between removing a service policy from an interface and then readding it.

- **CSCte12130**—When ANM has been polling the ACE for a long time, occasionally ANM does not read all the SNMP responses back from the ACE and reports the Operation status as N/A for many of the virtual servers. This issue occurs on any ACE software version and in ANM 2.0 and 2.2. Workaround: Reboot the ACE to fix this issue.
- **CSCte76598** (**CSCsr21689**)—The first packet of a TCP, UDP, or ICMP connection may not be captured; however, the remaining packets are captured for the same flow. This behavior can occur when you have the packet capture function configured for a specific ACL and for Layer 7 load-balanced traffic. Workaround: None.
- **CSCte76618**—When traffic traverses the ACE 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.
- **CSCtg31975**—A system admin account in the ACE software may allow an authenticated user to inject shell commands. This account does require authentication. Workaround: None.
- **CSCtg67860**—When you configure multiple track probes in two user contexts and enter the **show cfgmgr internal table track-probe** command, the ACE becomes unresponsive due to a Cfgmgr process failure. Workaround: None.
- **CSCtg76150**—When you configure an inline match statement that has a special character or space in its name under an Layer 7 policy, the checkpoint rollback fails. Workaround: Do not configure inline match statements with special characters or spaces.
- **CSCtg87855**—After you change the configuration in a large ACE configuration and enter **show** commands, the CLI becomes unresponsive for a period of time. In this case, the **show processes cpu | include cfgmgr** command displays one of the configuration manager (cfgmgr) processes consuming CPU resources. After you apply the configuration change, the cfgmgr CPU usage goes to zero, and the CLI becomes unresponsive. Workaround: Wait until the cfgmgr completes its previous operation before entering the **show** command.

- **CSCth04993**—When you configure an ACE interface with single NAT IP address in the NAT pool and the ACE receives SIP UDP traffic, it resets subsequent SIP TCP traffic. Workaround: Perform either of the following:
  - Perform a checkpoint rollback to a non-SIP configuration and then to the existing configuration.
  - Increase the number of IP addresses in the NAT pool.
- **CSCth07709**—When performing the **snmpwalk** or **snmpbulkwalk** command for any object on the ACE, occasionally the ACE displays an Unknown user name error. The frequency of this occurrence can increase by having three contexts on the ACE. Workaround: None.
- **CSCth23432**—When you delete a certificate from a full image directory on the ACE and reboot the ACE, the ACE is not accessible from the XML interface and the Device Manager GUI does not work. Also, when the image directory is full, the ACE cannot generate a certificate. Workaround: Delete some data from the image directory and reboot the ACE, which will allow the creation of the certificate.
- **CSCth24647**—When the FT interface VLAN number is lower than the other interface numbers and these interfaces require the downloading of large configurations, an API timed out error occurs when applying the startup configuration. Workaround: Enter the **no ft auto-sync running-config** command and then enter the **ft auto-sync running-config** command.
- **CSCth55362**—When the ACE performs a configuration rollback, existing classes in a policy are not reordered according to the new configuration. The running configuration has a policy that contains several classes. The checkpoint contains that policy with some or all the classes in a different order. After performing the rollback, the order of the classes stays as it was in the running configuration. Workaround: Perform either of the following:
  - Remove the policy that was changed during the rollback and then perform the rollback.
  - If there are many similar policies in the configuration, perform a rollback to an empty configuration and then rollback to the desired configuration.
- **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.
- **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.
- **CSCtj00826**—If the ACE is running a large number of HTTP or HTTPS probes when probing a file approximately a megabyte in size, the ACE reboots. The following message may precede the reboot:

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

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

- **CSCtj12692**—When you configure the ACE with 4000 sticky groups and do not allocate a sticky resource class, the resource values of the sticky are the default of a minimum of 0 and a maximum of unlimited. When the sticky database has 800,000 entries and you create a sticky resource class to a minimum value equal to 20 percent and apply it to the context, the ACE becomes unresponsive after a few minutes because it becomes unresponsive in the LB module at the function LbSticky_ReturnOldestEntry. Workaround: Do not change the resource class when you configure a large number of sticky groups and the database is full with active entries.
- **CSCtj24719**—When the ACE has mixed TCP and UDP SIP traffic running at high rate for five to six hours to a combination of Layer 7 and Layer 4 VIPs, the **show serverfarm** *name* command may display some real servers with current connections after the traffic has stopped and the connections have closed. Workaround: None.
- **CSCtj65634**—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.
- **CSCtk57750**—When you configure SNMP to poll the ACE for a configured class map, the correct information is not retrieved. Workaround: None.
- **CSCtn54768**—Probes fail due to out of sockets condition. Workaround: None.
- **CSCtn69269**—When an XML command is sent through an XML agent, it fails with a 500 error. This problem can occur on any software release. However, the failing commands may be different for the different releases. Workaround: Send the command in raw (text) mode.
- **CSCto45906**—Each time that the standby ACE reboots, a context on it transitions to the STANDBY_COLD state and the ACE displays the following error:

  ```
  Error on Standby device when applying configuration file
  ```

  It is a timing issue due to the configuration size and total number of contexts. This issue can lead to a lot of Configuration Manager (CFGMGR) download processing which can lead to a command failure. CSCtn50357 is tracking the issue of the actual failing command that is not properly placed in the error logs. Workaround: Perform either of the following:

  - On the FT group for the context in the STANDBY_COLD state, enter the **no inservice** command followed by the **inservice** command.
  - Change the context FT group ID in the FT group to a higher number so that the context with the largest configuration does the configuration synchronization last.
- **CSCto46159**—When you configure the maximum number of the VIP statements in a single class map of 254 and then delete one of the VIP statements, the ACE cannot add a match VIP address in a single class map and displays the following message:

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

  Workaround: Remove the class map and the reconfigure it again with all of the VIP addresses.
- **CSCto71443**—When you configure an FT group ID 64 on the ACE, a bulk sync timeout occurs for this group or connections are not replicated in any FT group. Workaround: Do not use group 64. Use a value between 1 to 63, inclusive.
- **CSCto81777**—When you use the CLI to configure a probe on the ACE, you cannot remove the **open** statement. You may also find that even if you did not configure values for probe interval, passdetect interval, and open timeout, those values appear in the ACE running configuration. Workaround: None.
- **CSCto92997**—When the hit counts are populated in the **show service-policy url-summary** command output and you remove one or more of the URL match statements from Layer 7 class maps, the hit counter clears. Some of the subsequent URL match statistics are affected. This issue

does not affect the load balancing to the rest of the URL match criteria. Workaround: Use the **clear service-policy** *policy_name* command to clear all of the statistics and the hit counter repopulates according to the incoming traffic.

- **CSCto94539**—When you configure probes on the ACE, they unexpectedly stop working and an out of socket condition is reported. Additional syslog will be provided to further troubleshoot this type of issue. Workaround: Take the probe out of service and place it back in service. If this action does not resolve the issue, remove the probe from the configuration and reconfigure it.
- **CSCtq12770**—When a port-channel interface is configured and you send an SNMP walk on the ifHighSpeed OID, it returns an invalid value. Workaround: None.
- **CSCtq11972**—When you configure an Oscilloquartz NTP server with stratum 2, the ACE cannot synchronize its time with the NTP server. Workaround: None.
- **CSCtq39716**—When the cesServerFarmRserverCurrentConns OID is polled through SNMP, it returns wrong values. For example:

```
ACE/context# show rserver
 rserver              : server1, type: HOST
 state                : OPERATIONAL (verified by arp response)
 ---------------------------------
                                                ----------connections-----------
       real                  weight state        current    total
   ---+---------------------+------+------------+----------+--------------------
   serverfarm: farm1
       172.21.31.3:0         8      OPERATIONAL  3          5809

CISCO-ENHANCED-SLB-MIB::cesServerFarmRserverCurrentConns.1."farm1"."server1".0 =
Counter64: 12884901891
```

  Workaround: Use the CLI to monitor this counter.
- **CSCtq40340**—When the ACE configured with a Layer 7 rule has a half-open connection (ESTAB/CLOSED) and a SYN hits it, the ACE may drop the SYN silently. Workaround: None.

Software Version A4(2.1) Command Changes

Table 8 lists the command changes in software version A4(2.1).

Table 8 CLI Command Changes in Version A4(2.1)

Mode	Command and Syntax	Description
Exec	**show interface vlan** *number*	Per CSCtl53644, this command now accepts the range from 1 to 4095 to display the internal VLAN information. Previously, the range was 2 to 4094.
Exec	**show np** *number* **buffer usage**	Per CSCtn61051, the **buffer threshold** command in configuration mode now handles external buffers in addition to internal buffers. For more information about this command as per software version A4(1.1), see the "Monitoring and Displaying the Network Processor Buffer Usage" section.

Table 8 CLI Command Changes in Version A4(2.1) (continued)

Mode	Command and Syntax	Description
Exec	**show np** *number* **me-stats "-c** *connection_id* **-v"**	Per CSCtl23213, this command displays the buffer usage per connection in the Buffer usage count field. This count includes the number of buffer particles for chains connected through user_data[0|1] and buffer particles used during setting up http-proxy, tcp-proxy, SSL, AI etc. and displaying the total count used for each.
Exec	**show np** *number* **me-stats "-c t** *number*"	Per CSCtn23472, this command provides buffer monitoring and leak detection as part of the ucdump **-c** arguments. The **t** *number* option is the threshold number of buffer particles. Any connections that use buffer particles greater than the threshold number are displayed along their count, and idle time. This option also displays the total number of buffers used by the connections, and the total allocated buffers in the system.
Exec	**show np** *number* **me-stats "-snorm -M1"**	Per CSCtn93913, when an FE/BE MSS mismatch occurs, this command displays the new normalization statistic field, Fastpath MSS mismatch.
Exec	**show probe detail**	Per CSCtj65408, this command displays the following error message in the Last disconnect err field when the server sends a regex that does not match the configured send-data value for an echo TCP or UDP probe: `Server response not matching with user configured send-data`
Exec	**show parameter-map**	Per CSCtl97681, this command displays the globally-applied inactivity and half-closed connection timeouts by appending the (Global) tag appended to the timeout values as configured by the **connection advanced-option default-override** command. Per CSCtn78101, the inspect non-persistence field was added for the **new inspect non-persistence** command in parameter map HTTP configuration mode.
Exec	**show service-policy**	Per CSCtl97681, this command displays the global parameter map applied to Layer 3 rule by appending the (Global) tag to its name as configured by the **connection advanced-option default-override** command. Per CSCtn73488,the **show service-policy** command now includes the conns per second field that displays the connections per second at the virtual server level when you configure more than one VIP under a class map. When you configure one VIP under a class map, the connections per second field is at the VIP level.

Table 8 CLI Command Changes in Version A4(2.1) (continued)

Mode	Command and Syntax	Description
Configuration	**connection advanced-option default-override** *connection_parameter_map*	Per CSCtl97681, this new command allows you to globally apply the inactivity and TCP half-closed connection timeout values of a parameter map in a context. The *connection_parameter_map* argument is the name of connection parameter map name configured with the inactivity or half-closed connection timeout values, or both. For more information about this command, see the "Globally Applying Parameter Map Inactivity and TCP Half-Closed Connection Timeout Values" section.
Configuration	**buffer threshold active** *number1%* **standby** *number2%* **action reload**	Per CSCtn61051, the **buffer threshold** command now handles external buffers in addition to internal buffers. For more information about this command as per software version A4(1.1), see the "Monitoring and Displaying the Network Processor Buffer Usage" section.
Parameter map HTTP	[**no**] **inspect non-persistence**	Per CSCtn78101, this new command allows you to configure the ACE to bypass connection persistence inspection during HTTP transactions for use with smooth streaming deployments. For more information, see the "Bypassing Inspection during HTTP Transactions" section.
Parameter map HTTP	**parsing non-strict**	Per CSCtl89566, when you apply this command, the ACE now accepts non-RFC requests with space and special characters in the HTTP headers, and parses them at Layer 7.
Sticky cookie configuration	**backup sticky**	Per CSCtk08915, this new command enables the backup sticky feature for new connections to maintain persistence by providing backup persistence for the source IP address. For more information, see the "Configuring the Backup Sticky Feature" section.

Software Version A4(2.1) System Log Messages

Software version A4(2.1) includes following new system log (syslog) messages.

251010

Error Message `%ACE-3-251010: Health probe failed for server` *`address`* `on port` *`number`*`, Server response not matching with configured echo probe send-data`

Explanation Per CSCtj65408, when you configure an echo TCP or UDP probe on the ACE and the server sends a regex that does not match the configured send-data value, the probe fails and the ACE generates this syslog message.

251018

Error Message `%ACE-3-251018: Scripted probe failed for server` *`A.B.C.D`*`,` *`error message`*`.`

Explanation Per CSCtl94488, the ACE generates this syslog message for scripted probe failures. The possible values of the error message variable are as follows:

- Probe error: Server did not respond as expected
- Internal error: Fork failed for TCL script
- Internal error: Script probe terminated due to timeout
- Internal error: TCL interpreter PANIC
- Internal error: Script error
- Internal error: Script-file lookup failed or empty buffer
- Internal error: Failed to allocate memory for tcl workerthread qnode
- Internal error: Unknown script error
- Internal error: Out of sockets for the TCL script
- Internal error: Unable to read persistent variable table
- Internal error: PData (probe data) pointer is null

400001

Error Message `%ACE-3-400001: MSS mismatch from` *`A.B.C.D:E`* `(`*`M`*`) to` *`W.X.Y.Z:F`* `(`*`N`*`) on interface` *`IFVLAN_NAME`*

Explanation Per CSCtn93913, when an FE/BE MSS mismatch occurs, the ACE generates this syslog message. The error message variables are as follows:

- *A.B.C.D* is the server IP address.
- *W.X.Y.Z* is the client IP address.
- *E* is the server port.

- *F* is the client port.
- *M* is the server MSS.
- *N* is the client MSS.
- *IFVLAN_NAME* is the interface name.

Software Version A4(2.0) Resolved Caveats and Open Caveats

This release note includes resolved and open defects that have a severity level of Sev1, Sev2, and customer-use Sev3. The following sections contain the resolved and open caveats in software version A4(2.0):

- Software Version A4(2.0) Resolved Caveats
- Software Version A4(2.0) Open Caveats

Note Some caveats may have more than one number. A number in parenthesis is a caveat number that was associated with the previous software release that now has another number for A4(2.0).

Software Version A4(2.0) Resolved Caveats

Software version A4(2.0) has no resolved caveats.

Software Version A4(2.0) Open Caveats

The following open caveats apply to ACE software version A4(2.0).

- **CSCsr55832**—When you enable logging console 6 or 7 on the ACE and approximately 200 messages per second flood the console, the **show run** command becomes unresponsive. Workaround: Do not turn on logging console 6 when traffic through the ACE exceeds 100 cps. The ACE recovers in less than 10 minutes.
- **CSCsu40160**—When the ACE configuration has more than 500 service policies and you can ping all VIP addresses, some VIP addresses are not served at all. Workaround: None.
- **CSCsu55909**—In a redundant configuration, when you configure the ACE with 20 contexts, apply it to the active ACE, and then bring up the standby ACE with the configuration, the active ACE transitions into the Cold state with the following error:

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

  Workaround: First bring up the active and standby ACEs individually and then enable redundancy.
- **CSCsv62417**—In some instances, the virtual MAC address is used for both the client-side VIP addresses and server-side NAT pools. With an FT VLAN configuration, the virtual MAC address is used as the source MAC for both client- and server-side packets. This behavior can cause issues in specific network topologies where the client-side and server-side end up learning the same MAC address over two ports. Without the FT VLAN, the internal MAC address is used. Workaround: Use the **mac address autogenerate** command to enable the autogeneration of a MAC address.
- **CSCsx06085**—When you enable UDP boost on the ACE, the server-initiated traffic fails because the destination port changes to the source port value. Workaround: Disable UDP boost.
- **CSCsz71578**—When you apply a service policy globally and then add the VLANs, the ACE displays ACL-merge errors for newly added VLANs and traffic does not flow through them. Workaround: Remove the global service policy and then reconfigure it.
- **CSCsz88519**—When you configure a TCP-based syslog server and the syslog server application on the remote system is down even though it can be reached from the ACE appliance, the ACE becomes unresponsive and most of its commands either time out or respond slowly. Workaround: Either bring the syslog server application up or remove the configuration for the TCP-based syslog server.

- **CSCta87584**—Connections may get dropped intermittently when you use persistence rebalance in a configuration and a rebalance is performed across traffic policies. This behavior typically occurs in a configuration with two different server farms that both contain the same real server with different ports, and the server farms are attached to two different Layer 7 load-balancing policy maps. Workaround: None.
- **CSCtd42287**—When the ACE is running with the maximum limit of 8K static entries and you remove a service policy from an interface and quickly readd it, the ACE removes the statements from the NAT policies. Workaround: Provide ample time between removing a service policy from an interface and then readding it.
- **CSCte76618**—When traffic traverses the ACE with the same source and destination port and dynamic NAT for that traffic is enabled, the ACE performs an implicit PAT. This behavior interrupts some sessions. This problem does not occur when NAT is not involved. Workaround: If possible, disable dynamic NAT.
- **CSCte76958** (**CSCsr21689**)—The first packet of a TCP, UDP, or ICMP connection may not be captured; however, the remaining packets are captured for the same flow. This behavior can occur when you have the packet capture function configured for a specific ACL and for Layer 7 load-balanced traffic. Workaround: None.
- **CSCte96191**—On a rare occasion, the route manager becomes unresponsive on the standby ACE when you attempt configuration changes similar to the following on the active ACE:
  - Remove a service policy from local to global and global to local.
  - Remove or add VIPs in a Layer 3 class map which traffic is hitting.
  - Perform a checkpoint rollback.

  Workaround: None.
- **CSCtf54230**—When Layer 2 connected real servers are in the arp-failed state and probes are attached to all of them or the ACE is running a high rate traffic that generates many mac-miss IPCP messages, FT may appear to fail after several hours. Workaround: Remove the real servers in the arp_failed state or make sure that most of the real servers are UP.
- **CSCtg17350**—When you configure the Acceleration and Optimization features on the ACE, the integrated packet capture utility may not capture traffic from all interfaces, even when you configure the capture to capture from all interfaces. Workaround: None.
- **CSCtg31975**—A system admin account in the ACE software may allow an authenticated user to inject shell commands. This account does require authentication. Workaround: None.
- **CSCtg67860**—When you configure multiple track probes in two user contexts and enter the **show cfgmgr internal table track-probe** command, the ACE becomes unresponsive due to a Cfgmgr process failure. Workaround: None.
- **CSCtg76150**—When you configure an inline match statement that has a special character or space in its name under an Layer 7 policy, the checkpoint rollback fails. Workaround: Do not configure inline match statements with special characters or spaces.
- **CSCtg87855**—After you change the configuration in a large ACE configuration and enter **show** commands, the CLI becomes unresponsive for a period of time. In this case, the **show processes cpu | include cfgmgr** command displays one of the configuration manager (cfgmgr) processes consuming CPU resources. After you apply the configuration change, the cfgmgr CPU usage goes to zero, and the CLI becomes unresponsive. Workaround: Wait until the cfgmgr completes its previous operation before entering the **show** command.

- **CSCtg92971**—When the ACE uses an archive with the restore feature that has domain add-object configurations, the restore feature fails with the configurations. Workaround: Manually remove the affected configurations from the archive and restore it with a new archive file. After the restore is complete, you can reapply the manually removed configurations.
- **CSCtg96456**—When you configure the maximum number of the VIP statements in a single class map of 254 and then delete one of the VIP statements, the ACE cannot add a match VIP address in a single class map and displays the following message:

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

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

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

  Workaround: Remove and readd the object group.
- **CSCth07709**—When performing the **snmpwalk** or **snmpbulkwalk** command for any object on the ACE, occasionally the ACE displays an Unknown user name error. The frequency of this occurrence can increase by having three contexts on the ACE. Workaround: None.
- **CSCth08116**—When you configure the **expect regex** command on HTTP or HTTPS probes with a long regex string and the web page parsed by the probe is longer than 100 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** (**CSCtg37325**)—During normal ACE operating conditions, the configuration manager becomes unresponsive and the ACE generates a core file. Workaround: None.
- **CSCth16258**—The **snmpwalk** or **bulkwalk** command on the SSL proxy MIB always returns a timeout. Currently, there is no tnrpc call to fetch data. The number of statistics has increased to string parsing and is taking more time. The default timeout is one second and it is not responding within one second. Workaround: Increase the timeout value.
- **CSCth23304** (**CSCth12446**)—When the ACE is using a 1-Gbps throughput license, the throughput output displayed through the **show resource** command is rounded to the nearest thousand. For example, a value of 134217728 is rounded to 134217000. This issue does not occur with other throughput licenses. Workaround: Install a throughput license that is not 1 Gbps and then uninstall the license.

- **CSCth23432**—When you delete a certificate from a full image directory on the ACE and reboot the ACE, the ACE is not accessible from the XML interface and the Device Manager GUI does not work. Also, when the image directory is full, the ACE cannot generate a certificate. Workaround: Delete some data from the image directory and reboot the ACE, which will allow the creation of the certificate.
- **CSCth24647**—When the FT interface VLAN number is lower than the other interface numbers and these interfaces require the downloading of large configurations, an API timed out error occurs when applying the startup configuration. Workaround: Enter the **no ft auto-sync running-config** command and then enter the **ft auto-sync running-config** command.
- **CSCth26795**—When you configure the **mac-address autogenerate** command with the **ip dhcp relay** command on an interface, the ACE appliance fails to relay the DHCP request to the configured server and the counters displayed by the **dhcp relay statistics** command do not increment. Workaround: Remove the **mac-address autogenerate** command from the interfaces and reboot the ACE.
- **CSCth37401**—When the ACE receives HTTP traffic containing special characters in the cookie value, it does not properly parse the cookie. The ACE accepts a space inside the cookie value. However, a quoted string containing the comma (,) character inside the string may cause a parsing error. Based on RFC2068, special characters are not legal in the cookie value and are not allowed inside a quoted string. Refer to the following information from RFC2068:

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

  Workaround: Do not use special characters inside the cookie value.
- **CSCth39505** (**CSCth39502**)—The ACE divides the sticky table and cookies between its two IXP network processors (NPs). If a connection on one NP uses a cookie with a hash that resolves to the other NP, the NPs must perform additional inter-IXP messaging to process the cookie. In a default TCP connection configuration, if the server sends 32K or more of data in less than 10 milliseconds (msec), a zero window may result on the backend. Some server TCP stacks may inadvertently introduce a 5-second delay in this situation. The ACE should advertise a non-zero window to the sending server when the buffers are released. Workaround: You can configure the **set tcp wan-optimization rtt 0** command to apply TCP optimizations to packets for the life of a connection. However, this command results in increased resource consumption.
- **CSCth45076**—When you configure a static multicast ARP address on the ACE, you cannot ping to the address from ACE. Workaround: None.
- **CSCth53131**—When you add a class map to a configuration with a large number of class maps and the ACE fails to add it to the running configuration, the ACE displays an error message that does not describe the actual issue. Workaround: None.
- **CSCth55362**—When the ACE performs a configuration rollback, existing classes in a policy are not reordered according to the new configuration. The running configuration has a policy that contains several classes. The checkpoint contains that policy with some or all the classes in a different order. After performing the rollback, the order of the classes stays as it was in the running configuration. Workaround: Perform either of the following:
  - Remove the policy that was changed during the rollback and then perform the rollback.
  - If there are many similar policies in the configuration, perform a rollback to an empty configuration and then rollback to the desired configuration.

- **CSCth59247**—When you configure long and complex regular expressions in new or existing commands, the ACE does not allow you to make any additional changes and may become unresponsive for a long duration of time. Workaround: Shorten the regular expressions in the commands.
- **CSCth63553** (**CSCth63549**)—The standby ACE may have a higher number of connections than the active ACE. Workaround: Configure a shorter connection inactivity timeout.
- **CSCth64338**—If you configure TCP probes with small intervals and set the termination mode as forced, the TCP probe stops firing if the server sends an RST after the TCP handshake. Workaround: Remove and readd the faulty probe from the real server.
- **CSCth67961** (**CSCsy66327**)—When you enter the **show snmp group** command from any context other than the Admin context, it does not display any output. Workaround: None.
- **CSCth74700**—Connectivity to the real server may be lost when you configure the following:
  - A client and server side VLAN on the ACE
  - A real server and ensure that it is Layer 2 reachable
  - A static route with a /32 mask to reach the real server through another interface

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

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

  Either of the workarounds can prevent a large number of reap messages from being produced and queued, which can cause the slow release of system resources.
- **CSCth90592**—When you configure static NAT port redirection, the ACE does not apply the configuration and displays the following error message:

  ```
  Error: A static ip and source port must be provided in ACL for static port redirection
  ```

  Workaround: Configure a source port in the ACL for static port redirection.

- **CSCti11896**—The ACE treats the deny function inside a management policy or class map as a SKIP. The ACE does not deny the traffic. Instead, it skips the class map and tries to match another one. Workaround: None.
- **CSCti25263**—If the same SNMP request identifier is used in previous SNMP GET and GET NEXT requests to the ACE and an SNMP agent is polling the ACE, the ACE may incorrectly respond to the SNMP request. Workaround: Perform the following:
  - **a.** Change the SNMP agent to use unique SNMP Request Identifiers for each SNMP request.
  - **b.** Wait at least 10 seconds between SNMP requests that use the same SNMP request identifier.
- **CSCti28255**—When a real server state transitions to UP from a probe-failed or ARP-failed state, the ACE generates the CISCO-ENHANCED-SLB-MIB:cesRserverStateUp trap. However, if the real server goes down due to a probe-failed or ARP-failed state, the ACE generates the CISCO-ENHANCED-SLB-MIB:cesRserverStateChange trap. Workaround: None.
- **CSCti40433**—When the client sends a SYN on an existing Layer 7 connection, the ACE responds to a TCP SYN with an ACK, and an incorrect ACK sequence number. Workaround: None.
- **CSCti40456**—The ACE does not reset a SYN on an existing L7 connection. The SYN is for an existing L7 connection and the sequence number is within the receive window. Workaround: None.
- **CSCti64563**—When you configure access control lists (ACLs) in the ACE, using the **access-list** *name* **resequence** command to renumber the line numbers may cause an ACL merge error and the access-list configuration fails to download to an interface. Workaround: Do not use the **access-list** *name* **resequence** command when you are configuring ACLs.
- **CSCti66770**—When the ACE receives a cookie string that contains many cookies and encounters a space character in the cookie value, it stops processing the cookies. Spaces are not permitted in the cookie name or cookie value. Persistence or stickiness fail. Workaround: None.
- **CSCti68347**—When you use the **system internal snapshot** command to force a cfgmgr core, the ACE generates a core dump. However, the backtrace does not provide correct information. Workaround: None.
- **CSCti68421**—If the ACL merge resources are almost exhausted and you add a configuration statement that places the resources over the limit, the ACE may drop traffic on the VLAN interface in which the configuration statement applies. Workaround: To restore service, remove the last configuration change that you made. To determine the current ACL merge resource status, enter the **show np 1 access-list resource** command in the Admin context and the s**how acl-merge merged-list vlan** *number* **in non-redundant** command in the context or VLAN where you will apply the configuration change.
- **CSCti73091**—When you configure access lists to be shared among multiple features, if you remove and readd the same access lists within the same download frame, the ACL line numbers go out of synchronization among the features. The ACE adds the line duplications for the access list to only one of the features. When you enable acl merge debug on the ACE, the ACE displays the following ACL Merge errors:

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

  Workaround: If the error has already occurred:

  - **a.** Remove the access groups from the features.
  - **b.** Remove and readd the access lists
  - **c.** Readd the access groups to the features.

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

- **CSCti74520**—When sending malformed requests, SSHD may become unresponsive. This issue has occurred when running testcase 4738 of the Codenomicon SSHV2 test tool. Workaround: None.
- **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.
- **CSCti90916**—When you configure DNS load balancing and sticky on the ACE, DNS load balancing fails. Workaround: Do not configure sticky for DNS load balancing.
- **CSCti96864**—When you perform dynamic configurations of usernames in multiple contexts and enter the **no username** *name* command in a user context, the ACE unexpectedly reboots and generates an SNMP core file. Workaround: None.
- **CSCtj00826**—If the ACE is running a large number of HTTP or HTTPS probes when probing a file approximately a megabyte in size, the ACE reboots. The following message may precede the reboot:

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

  Workaround: Reduce the size of the file being probed when running a large number of probes on the ACE.
- **CSCtj04935**—When the Layer 7 TCP path is overutilized that causes the Timer Freelist Empty to be hit several times, the ACE reboots because of the Timer Freelist corruption. Workaround: Reduce the work load of the Layer 7 TCP path.
- **CSCtj07489**—When you configure a policy map that references another policy map on the ACE, if the checkpoint rollback or restore operation removes these recursively referenced policy maps during context deletion while the operation loads another context, the cfgmgr process may become unresponsive. This is especially risky when all context policy maps are removed which can occur during a restore operation. Workaround: None.
- **CSCtj12692**—When you configure the ACE with 4000 sticky groups and do not allocate a sticky resource class, the resource values of the sticky are the default of a minimum of 0 and a maximum of unlimited. When the sticky database has 800,000 entries and you create a sticky resource class to a minimum value equal to 20 percent and apply it to the context, the ACE becomes unresponsive after a few minutes because it becomes unresponsive in the LB module at the function LbSticky_ReturnOldestEntry. Workaround: Do not change the resource class when you configure a large number of sticky groups and the database is full with active entries.
- **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.
- **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.
- **CSCtk53132**—An ACE appliance running software version A4(1.0) does not boot properly. When the ACE is running an A3(2.x) software image, it does boot properly and run normally. Workaround: Complete an RMA for the appliance. In this case, the new ACE appliance booted properly.
- **CSCtk65542**—When you perform VIP-related configuration changes on the ACE, the ACE load balancer incorrectly reports a KAL-AP load value of 255 for various VIPs which forces the GSS to mark the resource out of service. Workaround: Reboot the ACE to recover from this issue.

- **CSCtl03706**—When the ACE performs the **snmpwalk** command on the cpmProcessTable, the **show proc cpu** command becomes unresponsive.The output of **show system internal mts buffers** command displays an MTS leak. The output of the **show system internal mts buffers details** command confirms this leak. Also, the MTS sends error messages similar to the following:

  ```
  mts_do_msg_input() failing since no space available in 91 (src_sap = 91, opc = 1376
  PID = 934) 2
  ```

  Workaround: None.
- **CSCtl08525**—When a script continuously adds and deletes real servers under a server farm for more than two or three hours and removes a real server from a DWS-enabled server farm, the ACE continues Nexus 7000 polling for locality information. Workaround: None.
- **CSCtl24373**—When the ACE connection table lists a previous entry in a half-closed state, the ACE can establish a new connection with the same tuple but the final ACK is not NATed as expected. Workaround: Decrease the half-close timeout value through the parameter map.
- **CSCtl45638**—When you configure usernames with the ACE default roles, a user with the Network-Monitor role does not have access to some commands. Workaround: Assign the user with the admin role.
- **CSCtl53644**—When you configure access lists on the ACE and an ACL Merge error occurs on VLAN1 which is an internal VLAN, the **show vlan***number* command cannot display the error counters because user-configured VLANs start at 2. Workaround: You may be able to use the debug function to display the logs.
- **CSCtl56689**—When you are using the Device Manager (DM) with remote authentication, such as TACACS, and a login is remotely authenticated through TACACS on the ACE, the DM may fail. Workaround: Remove the TACACS filter running on the network.
- **CSCtl68891**—When you configure a real server on the ACE, assign it an IP address, place it in service, and then delete it, the ACE generates an unnecessary trap. When the real server state changes from ARP-FAILED to operational, the ACE generates the CesRServerStateUp trap. Workaround: None.
- **CSCtl76773**—When you create a real server, class map, policy map, KAL-AP tag, server farm, or context name that includes a space in it, an ACE redundant configuration can become out of synchronization. Workaround: Do not use spaces when naming an object on the ACE.
- **CSCtl89566**—When the ACE is performing Layer 5 load balancing and receives a non-compliant HTTP request, if the request hits a default class and is Layer 4 load balanced, the ACE drops the connection. Workaround: None.
- **CSCtn40037**—The signal handler has been disabled on the network processor cores. As a result, when one core becomes unresponsive, the ACE immediately generates a core file. Ordinarily, ME dump would detect this and force all other cores to become unresponsive. Because the signal handler is disabled, the other cores do not get stuck and they continue to process their message queues. This behavior may be an issue when debugging customer problems. This situation happens whenever a core becomes unresponsive. Workaround: None.
- **CSCtn43569**—The CPU utilization counter that the ACE obtains from the VMware vCenter Server provides the CPU utilization of a virtual machine (VM) as a percentage of the total ESX/Hypervisor CPU utilization. This process works fine for the default case where a VM is allocated with any number of cores and no resource limits are applied. The ACE receives the correct CPU load values of the VM and the feature works as expected. However, if there are resource limits provisioned to the VM (for example, limiting it to 50 percent of maximum CPU), then the counter value that the ACE receives from the vCenter does not accurately reflect the results. For example, a VM can use

the entire 50 percent of the allocated max CPU, and so the reported value should be 100 percent as the VM's CPU load. Instead, the reported value is 50 percent, which is the percent of total available ESX CPU utilization.

When you create a VM, the vCenter provides multiple options for CPU and memory allocation for the VM. As an administrator, you can allocate the number of cores to the VM and limit the CPU utilization of the VM to a portion of the max available CPU power (MHz). When you configure this CPU-limiting option on the vCenter, the average CPU usage counter provided by the vCenter is still calculated against the total CPU power for the ESX/ESXi host. The ACE retrieves this counter, but treats it incorrectly as the VM's CPU usage percentage against its own allocated CPU resource limit.

Workaround: When you create a VM with a CPU resource limit that is lower than the maximum limit (MHz), adjust the CPU burst threshold that you configure on the ACE for the DWS feature to compensate for the incorrect value provided by the vCenter. Calculate the new CPU burst threshold to be configured on the ACE by using the following formula:

New burst threshold = expected burst threshold x VM's CPU resource limit (MHz) / VM's maximum resource limit (MHz)

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.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.