Release Note for the Cisco Application Control Engine Module

October 2016

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 Application Control Engine (ACE) module, model ACE30 (ACE30_MOD_K9).

- A5(3.5)
- A5(3.4)
- A5(3.3)
- A5(3.2)
- A5(3.1b)
- A5(3.1a)
- A5(3.1)
- A5(3.0)

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

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

This release note contains the following sections:

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

Important Considerations for A5(x) Release

Please refer ACE Operating Considerations section for critical considerations for A5(x) Release at the end of the section.

Please refer to the ACE Operating Considerations section for important Notes on A5(3.1b).

New Software Features in Version A5(3.1)

Software version A5(3.1) provides the following new features:

- Enhancements in TLS Feature
- Support of Radius Sticky Information

Enhancements in TLS Feature

In ACE A5(3.1) release following changes are being introduced:

ACE can be provisioned to use the cipher TLS_RSA_WITH_AES_128_CBC_SHA256 for SSL communication under front-end, back-end and end-to-end configuration modes. A new command has been added under the parameter-map type SSL command. In the cipher sub command, support for TLS_RSA_WITH_AES_128_CBC_SHA256 { 0x00,0x3C }has been added.

Configuration

Example:

```
parameter-map type ssl ssl-param
```

```
cipher RSA_WITH_AES_128_CBC_SHA256
```

Note This Cipher is only supported with TLS1.2.

Note This cipher is not supported by HTTPS probes.

Support of Radius Sticky Information

In this Software version support for ‘Deleting Fip Sticky Entries on Acct Stop with Session Stop Indicator’ feature has been added. This features enables to delete the sticky entry based on the Attribute 26 (VSA) 11 called the ‘Session Stop Indicator’ in the Accounting Stop request. In Device Manager 5(3.1) version, under the menu Config >Devices >Load Balancing >Stickiness >Add/Edit screen, when **TYPE** is selected as **RADIUS,** parameters can be added in the form of a check box - ‘Radius Purge Information’ parameter.

New Command

```
sticky radius framed-ip FIP6-STICKY
purge framed-ip session-stop only
```

New Software Features in Version A5(3.0)

This section describes the new features associated with ACE Module software version A5(3.0).

Software version A5(3.0) provides the following new features:

- Support of Hex data in TCP / UDP Probe Send-data and Expect Regex
- Enhancements in HTTP Content Rewrite
- Support of TLS1.1 and TLS1.2
- FTP SLB IPV6 Support
- Updates to Resource Parameter Monitoring
- Ability to Configure Fixed Encap IDs for Active-standby redundancy setup with Virtual MAC configuration
- Ability to Configure Fragment Timeout in Milliseconds
- Ability to Configure the Re-assembly Timer Interval
- Automatic Capture of Exec Command Mode Output
- Ability to Capture the Complete Output of the LbInspect tool
- Caching of snmp-get response for L4-L7 Resource Limit MIB
- Ability to Allow SSL Record Parsing to a Specific Size
- Ability to Allow HTTP to Parse the Non-encoded Characters

Support of Hex data in TCP / UDP Probe Send-data and Expect Regex

ACE software version A5(3.0) supports configuring of **send-data** and **expect regex** CLI commands to accommodate the configuration of Hex data. If Hex data configured is “ae5530”(6 bytes) then the converted value will be Hex ae,55,30 (3 bytes).

The first two bytes of the Hex string are taken and converted to one byte actual Hex value (For example- ‘a’ & ‘e’ from the string would be combined to form hex value ‘ae’). This conversion model is based on the existing hash value config under HTTP/HTTPS probe. The same CLI command modification can be covered under TCP and UDP probes.

New CLI Commands

The following new commands have been added to configure hex data and hex regex under TCP and UDP probes:

```
switch/Admin(config-probe-tcp)# ?
Configure tcp probe params:
connection     Configure probe connection parameters
description    Configure description string for probe
do             EXEC command
end            Exit from configure mode
exit           Exit from this submode
expect         Configure expected probe result code
faildetect     Configure parameters to detect probe failure on servers
interval       Configure interval between probes
ip             Configure probe IP parameters
no             Negate a command or set its defaults
open           Configure maximum time to wait for TCP connection to open
passdetect     Configure params needed to pass the servers in fail state
port           Configure port number for this probe
receive        Configure max time to wait inorder to receive reply from server
send-data      Configure data to be sent for probe
send-hex-data  Configure hex data to be sent for probe

switch/Admin(config-probe-tcp)# send-hex-data
<WORD>  Enter the data in hex format to be sent as part of probe request (Max Size - 254)
```

Note You can use the keyword **send-hex-data** to configure the probe for allowing hex data.

```
switch/Admin(config-probe-tcp)# expect ?
hex-regex Configure Hex data expected as response
regex Configure probe expected   response

switch/Admin(config-probe-tcp)# expect hex-regex ?
<WORD> Enter the expected response data in Hex format (Max Size - 254)
```

Note You can use the keyword **hex-regex** to configure the probe for allowing hex in expect regex CLI commands.

Guidelines and Restrictions

The following conditions should be taken care while configuring hex data:

- Enter Hex data in an even numbered length and a maximum size of 254

- The Hex data entered must be a single string consisting of alphanumeric within the range of 0-9, a-f or A-F.
- The Hex data configured will be stored and shown as ASCII text in the **show probe detail** and **show running-config** CLI commands.
- For **send-hex-data <data>**, the conversion from Hex ASCII to Binary will occur when the probe data is sent out.
- For **expect hex-regex <data>**, the configured regex hex data is converted to binary data at the time of parsing the server response against the configured regex hex data
- If **send-hex-data** is configured then **expect hex-regex** should be configured and if **send-data** is configured then **expect regex** should be configured.
- Data strings should be even-numbered length both in **send-hex-data** and in e**xpect hex-regex**
- Do not include white space
- Only specify hex values
- **expect hex-regex ae5530da offset 2** behavior will be same as **expect regex aedsfte offset 2**.
- User should take care of expect regex configuration For example if **send-hex-data** is configured then **expect hex-regex** should be configured and if **send-data** is configured then **expect regex** should be configured.

Enhancements in HTTP Content Rewrite

The HTTP content rewrite feature provides the capability to rewrite configured regex patterns in the HTTP response data. This feature has been enhanced to introduce the rewrite functionality to support rewrite for HTTP content in server to client direction.

The feature uses a rule-based rewriting engine (based on a regular-expression parser) to rewrite requested patterns on the fly. Content rewrite will provide a flexible and powerful content manipulation mechanism. URL content rewrite feature is effectively a search on the full content for each HTTP response in range and replace a match of regex search pattern with the defined regex replace pattern.

New CLI Commands

The following **content rewrite** command has been added newly as part of HTTP modify action list

```
action-list type modify http <Action list name>
content rewrite response content-string <content_regex_pattern> replace <new_string>
```

Example:

```
action-list type modify http data_rewrite
content rewrite response content-string "text" replace "data"
```

Note Only one rewrite configuration is allowed per action list.

Configuration and Restrictions

The **content-rewrite** happens for the response data based on the amount of data that HTTP module received from TCP. By default, HTTP receives up to 32K bytes (including headers) of response data (Default TCP buffer share is 32K). Hence the **content-rewrite** works fine up to first 32K response data, if the response data is more than 32K then ACE will send out the remaining data without doing any **content-rewrite**.

If you want to send more data from TCP to HTTP then you can increase the tcp buffer-share size to up to 48K, then ACE will do the content-rewrite for the first 48K response data and bypasses the remaining response data without **content-rewrite**.

Example:

```
parameter-map type connection conn-tcp
set tcp buffer-share 49152
```

Note We have observed ACE is taking more time to do content-rewrite for large response files, (For one GET request of 48K byte data with **content-rewrite** is taking approximately 6 seconds.)

The ability to support basic and extended regex will depend on the support of regex parser on DP. Content rewrite rule must have both content regex pattern and replacement pattern.

```
action-list type modify http data_rewrite
  content rewrite response content-string "first" replace "last"

policy-map type loadbalance first-match NM-WEB-PROD
  class WEB-SB17
    serverfarm WEB-SB17
    action data_rewrite
  class WEB-SB16
    serverfarm WEB-SB16
    action data_rewrite
  class class-default
    serverfarm WEB-SB10
    action data_rewrite

policy-map multi-match CLIENT-VIPS
  class NM-WEB-PROD
    loadbalance vip inservice
    loadbalance policy NM-WEB-PROD
    loadbalance vip icmp-reply active
    nat dynamic 10 vlan 112
```

Support of TLS1.1 and TLS1.2

ACE Software A5(3.0) supports the newer versions of TLS (TLS 1.1 and TLS 1.2). This enables ACE to successfully negotiate with TLS1.1 and TLS1.2 clients (in front-end and end-to-end SSL configuration) and to also act as a TLS1.1 or TLS1.2 server (in back-end and end-to-end SSL configuration).

This feature is implemented over existing SSL/TLS software stack. The existing Handshake design or packet flow is re-designed to support application record and handshake record interleave feature, at the same time it does not impact existing features of SSL/TLS.

Note A5(3.0) supports TLS 1.1 and 1.2 end to end however it does not support TLS 1.1 and 1.2 for HTTPS probes.

New CLI Commands

The following new commands have been added to support TLS1.1 and TLS1.2:

```
switch/Admin(config)# parameter-map type ssl test
switch/Admin(config-parammap-ssl)# version ?
  all          All SSL versions upto TLS Version 1
  SSL3         SSL Version 3
  TLS1         TLS Version 1
  TLS1_1       TLS Version 1.1
  TLS1_2       TLS Version 1.2
  Upto_TLS1_1  All SSL versions upto TLS Version 1.1
  Upto_TLS1_2  All SSL versions upto TLS Version 1.2
switch/Admin(config-parammap-ssl)# version TLS1_1
switch/Admin(config-parammap-ssl)# version TLS1_2
switch/Admin(config-parammap-ssl)# version Upto_TLS1_1
switch/Admin(config-parammap-ssl)# version Upto_TLS1_2

== Attach the map in the corresponding ssl-proxy service

Switch/Admin(config)# ssl-proxy service test
switch/Admin(config-ssl-proxy)# ssl advanced-options test
```

Note The configuration **version Upto_TLS1_1** indicates that ACE supports SSL3.0, TLS1.0 and TLS1.1 versions.

Note The configuration **version Upto_TLS1_2** indicates that ACE supports SSL3.0, TLS1.0, TLS1.1 and TLS1.2 versions.

Note Only one version configuration is allowed in one ssl parameter map. The previous version gets overwritten if a new version is configured.

Modified CLI Commands

For TLS1.1:

```
switch/Admin(config-parammap-ssl)# version ?
TLS1_1       TLS Version 1.1
Upto_TLS1_1  All SSL versions upto TLS Version 1.1
Upto_TLS1_2  All SSL versions upto TLS Version 1.2
```

For TLS1.2:

```
switch/Admin(config-parammap-ssl)# version ?
TLS1_2      TLS Version 1.2
Upto_TLS1_2 All SSL versions upto TLS Version 1.2
```

Configuration

For TLS1.1

```
switch/Admin(config-parammap-ssl)# version Upto_TLS1_1
```

For TLS1.2:

```
switch/Admin(config-parammap-ssl)# version Upto_TLS1_2
```

Signature Hash Algorithm

ACE only supports SHA256(0x04)/RSA(0x01) as the signature hash algorithm hash/signature hash algorithm signature in the case of TLS1.2 if client authentication is used. Handshake will fail if the peer doesn't support this combination.

Guidelines and Restrictions

For TLS1.1 and TLS1.2 SSL versions, only certain ciphers are supported as mentioned in the tables below. If you try to configure any unsupported SSL version or unsupported cipher, an error message will be displayed.

Table 1 Cipher suites supported by TLS 1.1

Cipher Suite Name	Cipher Suite Number
RSA_WITH_RC4_128_MD5	{ 0x00,0x04 }
RSA_WITH_RC4_128_SHA	{ 0x00,0x05 }
RSA_WITH_DES_CBC_SHA	{ 0x00,0x09 }
RSA_WITH_3DES_EDE_CBC_SHA	{ 0x00,0x0A }
RSA_WITH_AES_128_CBC_SHA	{ 0x00,0x2F }
RSA_WITH_AES_256_CBC_SHA	{ 0x00,0x35 }

Table 2 Cipher suites supported by TLS 1.2

Cipher Suite Name	Cipher Suite Number
RSA_WITH_RC4_128_MD5	{ 0x00,0x04 }
RSA_WITH_RC4_128_SHA	{ 0x00,0x05 }
RSA_WITH_3DES_EDE_CBC_SHA	{ 0x00,0x0A }
RSA_WITH_AES_128_CBC_SHA	{ 0x00,0x2F }
RSA_WITH_AES_256_CBC_SHA	{ 0x00,0x35 }
RSA_WITH_AES_128_CBC_SHA256	{ 0x00,0x3C }

ACE does not block the configuration of export ciphers even when version **version Upto_TLS1_1** or **version Upto_TLS1_2** is configured. This is because when **version Upto_TLS1_1** or **version Upto_TLS1_2** is configured ACE will still negotiate with SSL3/TLS1 clients and use those export ciphers with those clients. ACE will not select export ciphers for TLS1.1/1.2 even if you have export ciphers configured in the parameter map.

If only export ciphers are configured in the ssl parameter map along with version Upto_TLS1_1/Upto_TLS1_2 (or a combination of Upto_TLS1_2 and only RSA_WITH_DES_CBC_SHA) then:

1. ACE as a server will not be able to accept any TLS1.1/1.2 request and will send an alert (no_shared_cipher)

2. ACE as a client will send a client hello with only TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff), which is not a cipher but only indicates that it supports secure renegotiation. Server will send alert (no_shared_cipher) in this case.

Note TLS1.1 requests will work with the combination of Upto_TLS1_2 and only RSA_WITH_DES_CBC_SHA.

New MIB Objects for TLS1.1 and TLS1.2

Following are the new MIB objects for TLS1.1 and TLS1.2:

- **cspTl1cFullHandShake–-**Displays the number of full handshakes done with TLS1.1
- **cspTl1cResumedHandShake–-**Displays the number of resumed handshakes done with TLS1.1
- **cspTl1cHandShakeFailed–-**Displays the number of handshakes failed for TLS1.1
- **cspTl1cDataFailed–-**Displays the number of data failures for TLS1.1
- **cspTl2cFullHandShake–-**Displays the number of full handshakes done with TLS1.2
- **cspTl2cResumedHandShake–-** Displays the number of resumed handshakes done with TLS1.2
- **cspTl2cHandShakeFailed–-**Displays the number of handshakes failed for TLS1.2
- **cspTl2cDataFailed–-**Displays the number of data failures for TLS1.2

FTP SLB IPV6 Support

The application firewall currently supports a list of applications including HTTP, SIP, FTP. The FTP deep inspection is an application firewall that state-fully monitors the File Transfer Protocol. Earlier version of ACE supports FTP with IPv4. With A5(3.0), the ACE now supports FTP with both IPv4 and IPv6.

This feature does not support the following:

- SSL based FTP for IPv6.
- FTP from IPv4 client to IPv6 server.
- Addition of static Route cannot be done with SLB64.
- 1-Arm mode config is not supported with SLB64 as static route addition is not supported.
- SFTP is not supported.

Sample Configuration

Included below is a summary of the sample configuration to support FTP IPv6 in A5(3.0):

For FTP IPv6:

```
access-list all1 line 8 extended permit ip anyv6 anyv6

class-map match-all ftp-nat
  2 match destination-address 2015::214:5eff:fe84:30
class-map match-any vip-ftpv6
  2 match virtual-address 2015::214:5eff:fe84:30 tcp eq ftp

policy-map multi-match policy
  class vip-ftpv6
```

```
    loadbalance vip inservice
    loadbalance policy lb
    loadbalance vip icmp-reply
    nat dynamic 1 vlan 200
    inspect ftp
class ftp-nat
    nat dynamic 1 vlan 200
```

For Strict IPv6:

```
access-list all1 line 8 extended permit ip anyv6 anyv6

class-map type ftp inspect match-any mkd_ftp
  2 match request-method mkd
class-map type ftp inspect match-any rmd_ftp
  3 match request-method rmd

class-map match-all ftp-nat
  2 match destination-address 2015::214:5eff:fe84:30
class-map match-any vip-ftpv6
  2 match virtual-address 2015::214:5eff:fe84:30 tcp eq ftp

policy-map type inspect ftp first-match ftpInspect
  class mkd_ftp
    deny
  class rmd_ftp
    deny

policy-map multi-match policy
  class vip-ftpv6
    loadbalance vip inservice
    loadbalance policy lb
    loadbalance vip icmp-reply
    nat dynamic 1 vlan 200
    inspect ftp strict policy ftpInspect
class ftp-nat
    nat dynamic 1 vlan 200
```

Updates to Resource Parameter Monitoring

The existing CLI **show resource monitor-params** has been extended for displaying 1 min and 5 min average of the following utilization parameters:

1. **System Level:** Bandwidth, CPU, Memory, CPS, Total connections, Total SSL connections
2. **Per Context:** Bandwidth, CPS, Total connections
3. **Per VIP:** Bandwidth, CPS, Total connections
4. **Per Rserver:** Bandwidth, CPS, Total connections

Note 1 minute average is calculated based on 2 readings at 30 sec interval and 5 min average is calculated based on 5 readings at 1 minute interval.

Sample output of the CLI commands are as follows:

```
switch/Admin# show resource monitor-params
--------------------------------------------------------------------------------
```

```
 Resource                high    low    watermark   current(%)  1m_avg  5m_avg
------------------------------------------------------------------------------

system-level parameters

bandwidth                  5       1         3         31         25         0
conc-connections           4       2         3         80         85         0
connection-rate            3       1         2         52         76         0
active-ssl-conn            3       -         1          0          0         0
cpu-utilization            3       -         2          1          1         2
memory-utilization         2       -         1         43         43        43

Context-level parameters

Context : Admin
bandwidth                  4       1         2         31         25         0
conc-connections           4       1         3         80         85         0
connection-rate            3       1         2         52         76         0

VIP Level Parameter

Context: Admin
VIP address : 108.1.5.141
l3 rule id  : 148
policymap   : pm
classmap    : vip
```

Ability to Configure Fixed Encap IDs for Active-standby redundancy setup with Virtual MAC configuration

The **fixed encap-id** CLI command allows you to configure the fixed encap entries for the configured VMAC, active and standby MACs in an active-standby redundancy setup with Virtual MAC configuration setup. By default the ICM module in ACE searches for learned encap ID for any source mac in Mac lookup table for bridging and route lookup table for routing before creating a new connection. The new **fixed encap-id** command allows you to configure source vlan id, VMAC, active mac and standby mac. After configuring this CLI, ACE CP module creates a fixed encap ID for these MACs and writes this information into DP. After that if any new connection request hitting ICM from this client interface and source mac is matching with any one of the three configured MACs (VMAC, Active and Standby), then the ICM establishes the connection with the encap id created during the fixed encap configuration.

The ICM module currently selects the encap ID by traversing through the mac lookup table for bridge mode and route lookup table for route mode. **Fixed encap-id** feature is implemented to choose fixed-encap id by ICM for configured vlan id and mac addresses. ICM selects the encap id reserved by CP during the fixed encap configuration when the source vlan and mac address matched with the configured values.

New CLI Commands

Included below is a summary of the new CLI commands added to configure Fixed encap entries:

```
fix-encap vlan <vlan id> vmac <6 bytes mac address in hexa decimal> mac1 <6 bytes mac
address in hexa decimal> mac2 <6 bytes mac address in hexa decimal>
```

Note Use the delimiter "." between each byte of the mac address (For Example: 00.14.5e.84.5b.3f)

Example:

```
fix-encap vlan 13 vmac 00.14.5e.84.5b.3f mac1 aa.aa.aa.aa.aa.aa mac2 cc.cc.cc.cc.cc.cc
```

Guidelines and Restrictions

The **fixed-encap** CLI command is configurable at context level; it is dependent on the vlan interface we are passing as a parameter in the command. It means, the vlan interface must be available in the context, before configuring this CLI. In the above example, the vlan 13 is passed as a vlan parameter. Here the fix-encap for vlan 13 can be configured, only after configuring vlan interface 13. The total number of fix-encap entries is limited to 10 in system level.

Ability to Configure Fragment Timeout in Milliseconds

With A5(3.0) release you can configure the fragment timeout in seconds (**fragment timeout** for IPV4 and **ipv6 fragment timeout** for IPV6). In re-assembly module, the shadow table maintains the time-out values of fragments received by ACE re-assembly. The Re-assembly module scans the shadow table entries and cleans the timed out entries. By default the Re-assembly timer interval timeout is 5 seconds for IPV4 and 60 seconds for IPV6. With the A5(3.0) release, the ACE includes the **re-assembly-time-interval** CLI command to provide a command option to configure the timer interval. By default, the re-assembly timeout scan happens once in a 1000 milliseconds (1 second). By using this command the time interval can be configured as per the requirement.

New CLI Commands

The syntax for the fragment timeout are as follows:

For IPV4:

fragment timeout-msec <timeout value in mille seconds>

For IPV6:

ipv6 fragment timeout-msec <timeout in mille seconds >

Example:

```
interface vlan 230
  fragment timeout-msec 150
  ipv6 fragment timeout-msec 150

switch/Admin(config)# int vlan 230
switch/Admin(config-if)# fragment ?
  chain         Max number of fragment chains allowed
  min-mtu       Min MTU value
  timeout       Reassembly timeout value in seconds
  timeout-msec  Reassembly timeout value in milli sec

switch/Admin(config-if)# fragment timeout-msec ?
  <100-999>  Reassembly timeout value in milliseconds

switch/Admin(config-if)# ipv6 fragment ?
  chain         Max number of IPv6 fragment chains allowed
  min-mtu       IPv6 min MTU value
  timeout       IPv6 reassembly timeout value in seconds
  timeout-msec  IPv6 reassembly timeout in milliseconds
```

```
switch/Admin(config-if)# ipv6 fragment timeout-msec ?
  <100-999>  IPv6 reassembly timeout value in milliseconds
```

Ability to Configure the Re-assembly Timer Interval

In re-assembly module, the shadow table maintains the timeout values of fragments received by re-assembly. The re-assembly timer scans the shadow table entries and cleans the timed out entries. By default the re-assembly timer interval is 1 second (1000 msecs). ACE A5(3.0) provides command option to configure the timer interval. By default, the re-assembly timeout scan happens once in a 1000 mille seconds (1 second). By using this CLI command the interval can be configured as per the requirement. This is a system level parameter.

The syntax for the **re-assembly timer interval** command is as follows:

system-defaults reassembly-timer-interval

Example:

```
switch/Admin(config)# system-defaults reassembly-timer-interval ?
  <100-1000>  Reassembly timer interval
switch/Admin(config)# system-defaults reassembly-timer-interval 100
```

Note This is a global level CLI command which is applicable for all the contexts.

Automatic Capture of Exec Command Mode Output

With A5(3.0), the ACE now supports the ability to automatically capture output of any non-interactive Exec mode show command for debugging purposes.

Use the following CLI command to configure the automatic capture of Exec command mode output:

```
ace0101a/Admin# sh ru | i snapshot
Generating configuration....
auto-snapshot interval 5 count 4 command “sh tech”
```

- **Interval – specifies the time difference in minutes between two snapshots. This value can be between 5 and 32767 minutes**
- **Count – specifies the number of periodic snapshots that should be stored.**
- **Command – specifies the non-interactive exec mode/show command that has to be executed at the specified interval**

In the sample configuration shown above, the output of **show tech** CLI command will be captured and stored every 5 minutes and the latest 4 such outputs will get stored in core:AUTO-SNAP directory.

The content will be stored in .gz format, you must download and extract the content to obtain the text file with the required collected output.

Sample Content:

```
ace0101a/ssl# dir core:AUTO-SNAP
173206 Apr 17 2013 00:23:51 snap-command_output.1926.1366150772.gz
173464 Apr 17 2013 00:28:50 snap-command_output.1926.1366151072.gz
173606 Apr 17 2013 00:33:50 snap-command_output.1926.1366151372.gz
173722 Apr 17 2013 00:38:50 snap-command_output.1926.1366151672.gz
1302793 Apr 17 2013 00:41:08 snap-command_output.1926.1366151972
```

Note This command will occupy disk space and hence needs to be used sparingly (only for debugging purpose).

Ability to Capture the Complete Output of the LbInspect tool

With software version A5(3.0), the **show np x lb-stats** command is extended to include a sub-option **all** under following type of stats which would dump lb stats for:

```
sh np x lb-stats rserver all                    : LB-stats of all real_servers
sh np x lb-stats sfarm all                      : LB-stats for all serverfarms
sh np x lb-stats sticky all                     : LB-stats for all sticky groups
sh np x lb-stats cookie-expiry-string sticky all : LB-stats for all cookie expiry string
(all sticky groups)
sh np x lb-stats policy-map all                 : LB-stats for all policy maps
sh np x lb-stats context all                    : LB-stats for all contexts
sh np x lb-stats vserver all                    : LB-stats for all vservers
sh np x lb-stats default-policy all             : LB-stats for all default policy (all
vservers)
sh np x lb-stats retcode all                    : LB-stats for all retcode (all real
servers)
```

New CLI Commands

```
switch/Admin# sh np 1 lb-stats rserver ?
  <WORD>        Specify rserver name (Max Size - 80)
  all           LB-stats of all real_servers
  CDN-MCS-18-0
  rs1
  rs2
  s1
switch/Admin# sh np 1 lb-stats rserver all


switch/Admin# sh np 1 lb-stats sfarm ?
  <WORD>     Specify serverfarm name (Max Size - 80)
  all        LB-stats for all serverfarms
  PROVAFARM
  sf1
  sf2
  sf3
  sf_http
switch/Admin# sh np 1 lb-stats sfarm all


switch/Admin# sh np 1 lb-stats sticky ?
  <WORD>  Specify sticky group name (Max Size - 80)
  all     LB-stats for all sticky groups
  farm1
  farm2
  farm3
switch/Admin# sh np 1 lb-stats sticky all


switch/Admin# sh np 1 lb-stats cookie-expiry-string sticky ?
  <WORD>  Specify sticky group name (Max Size - 80)
  all     LB-stats for all sticky groups for cookie expiry string
```

```
  farm1
  farm2
  farm3
switch/Admin# sh np 1 lb-stats cookie-expiry-string sticky all


switch/Admin# sh np 1 lb-stats policy-map ?
  <WORD>          Specify policy-map name (Max Size - 80)
  all             LB-stats for all policy maps
  client-vips
  http
  lb
  lb-pm
  M
  management
  MANEGGIO
  rm
  SERVIZIANASTRO
switch/Admin# sh np 1 lb-stats policy-map all


switch/Admin# sh np 1 lb-stats context ?
  <WORD>  Specify context name (Max Size - 80)
  Admin
  all     LB-stats for all contexts
  c1
  c2
  c3
  c4
  c5
switch/Admin# sh np 1 lb-stats context all


switch/Admin# sh np 1 lb-stats vserver ?
  all        LB-stats for all vservers
  class-map  Enter Class map
switch/Admin# sh np 1 lb-stats vserver all


switch/Admin# sh np 1 lb-stats default-policy ?
  all       LB-stats for all default policy
  class-map  Enter Class map
switch/Admin# sh np 1 lb-stats default-policy all


switch/Admin# sh np 1 lb-stats retcode ?
  all         LB-stats for all retcodes
  serverfarm  Enter serverfarm
switch/Admin# sh np 1 lb-stats retcode all
```

Example:

If we want LB-stats of 256 contexts, the following will have to be specified:

```
TB1-ACE2/Admin# show np 1 lb-stats context all
```

Caching of snmp-get response for L4-L7 Resource Limit MIB

With software version A5(3.0), caching has been implemented for snmpget query for objects in CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB (1.3.6.1.4.1.9.9.480).

In earlier version of ACE, **snmpget** requests for objects in above MIB was timing out intermittently due to read operations taking longer time. To overcome this, caching has been implemented. Hence, when first **snmpget** query is done, the response is cached and subsequent queries received within 15 secs interval of the 1st query are provided the same response.

Ability to Allow SSL Record Parsing to a Specific Size

ACE allocates predefined number of buffers for each packet that needs to be parsed due to some L7 configuration, this is 17 by default. However, the valid SSL records can potentially occupy more than this default number of buffers depending on the record size. For example, a record of 16400 bytes can occupy as many as 33 buffers. This falsely triggers an error and packet drop. In order to prevent this ACE allocates as many buffers for SSL requests as per the record size that the client legitimately sends. This will override the default buffer size of 17 for SSL packets that get parsed.

New CLI Commands

The syntax to configure the ACE SSL maximum record size is as follows:

system-defaults allow-ssl-max-record-size

Example:

```
system-defaults allow-ssl-max-record-size <number>
Where <number> is an integer in range 1 to 65535.
EG of usage:
switch/Admin# system-defaults allow-ssl-max-record-size 16400
```

Note This will allow ACE to parse SSL records up to the size defined (<number>) without resulting in a rejection such as a slow-loris detection.

Configuration

```
switch/Admin(config)# ?
Configure commands:
  aaa                 Configure aaa functions
  access-group        Activate context global access-list
  access-list         Configure access control list
  action-list         Configure an action list
....
  ssl-proxy           Configure an ssl-proxy service
  sticky              Configure sticky
  switch-mode         Activate switch-mode in the context
  system-defaults     System Default configuration
  tacacs-server       Configure TACACS+ server related parameters
  telnet              Telnet config commands
  timeout             Configure the maximum timeout duration
  username            Configure user information.
  vm-controller       Configure VM controller


switch/Admin(config)# system-defaults ?
  allow-ssl-max-record-size  Configure maximum SSL Record Size allowed


switch/Admin(config)# system-defaults allow-ssl-max-record-size ?
  <1-65535>  Enter maximum SSL Record Size allowed
```

```
switch/Admin# show runn
Generating configuration....

system-defaults allow-ssl-max-record-size 16400
boot system image:c6ace-t1k9-mzg.nigovind.bin
```

Ability to Allow HTTP to Parse the Non-encoded Characters

With A5(3.0) release you can configure ACE HTTP to parse the non-encoded special characters.

By default, ACE follows RFC-2396 compliance and if any unwise characters (non-encoded special characters) comes in the url request then HTTP detects those non-encoded characters and resets the connection.If you configure this CLI command then ACE will allow the non-encoded special characters.

New CLI Commands

The syntax for this are as follows:

system-defaults http-parsing allow-non-encoded-chars

Example:

```
switch/Admin(config)#
switch/Admin(config)# system-defaults http-parsing allow-non-encoded-chars
Warning: Allowing HTTP traffic containing non-encoded characters implicitly means
non-compliance to RFC 2396
switch/Admin(config)#
```

Note This is a global level CLI which is applicable for all the contexts.

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

Table 3 and Table 4 summarize the chassis, supervisor engine model, and Cisco IOS version support for the ACE30 module in the Catalyst 6500E series switch and the Cisco 7600 series router, respectively.

Table 3 Chassis, Supervisor Engine, and Cisco IOS Support for the ACE 30 in a Catalyst 6500 Series Switch with a Multilayer Switch Feature Card (MSFC3 or Later)

Catalyst 6500 Series Switch Chassis	Supervisor Engine Model	Minimum Required Cisco IOS Version
6503-E	VS-S2T-10G [3]	15.0(1)SY (or later)
6504-E	VS-S2T-10G-XL	
6506-E	WS-SUP720-3B	12.2(33)SXI4 or later releases
6509-E[1]	WS-SUP720-3BXL	
6509-V-E	VS-S720-10G-3C(=)	
6513	VS-S720-10G-3CXL(=)	
6513-E[2]		

1. The Catalyst 6509-E chassis supports up to six ACE 30 modules with Supervisor Engine 2T (VS-S2T-10G or VS-S2T-10G-XL), and running Cisco IOS software version 15.0(1)SY1 (or later) with ACE module software version A5(2.0).
2. The Catalyst 6513-E chassis supports up to nine ACE 30 modules with Supervisor Engine 2T (VS-S2T-10G or VS-S2T-10G-XL), and running Cisco IOS software version 15.0(1)SY1 (or later) with ACE module software version A5(2.0).
3. The minimum required ACE30 module software version for Supervisor Engine 2T support is A5(1.1) or later. This software version supports both supervisor engine models: VS-S2T-10G and VS-S2T-10G-XL.

Table 4 Cisco Supervisor Engine, Route Switch Processor (RSP), and Cisco IOS Support for the ACE30 in a Cisco 7600 Series Router with a Multilayer Switch Feature Card (MSFC3 or Later)

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

Virtual Switching System Support

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

ACE Operating Considerations

The ACE operating considerations are as follows:

- In ACE (A53.1b) release, configuring the command “ssl certificate-expiration ignore” under HTTPS probe will cause the HTTPS probes to fail.

  To make probes work, you have to remove this command by using “no ssl certificate-expiration ignore” under HTTPS probe and use valid certificates.

- From A5(3.1b) onwards ACE will no longer support SSLv3 version of SSL. ACE will only support the following SSL versions:

  1. TLS1.0
  2. TLS1.1
  3. TLS1.2

A performance degradation of 9% may be observed while using TLS1.0 compared to SSLv3.

- When preempt enabled, and both ACE have the same priority after reloading the ACE (either Active/Standby), then the ACE which has the highest IP address will be elected as Active.

  When preempt disabled, and both ACE have the same priority after reloading the ACE (either Active/Standby), then the ACE which has the highest uptime will be elected as Active.

- Server initiated L7 protocols do not work with ACE L7 load balancing. You must first initiate communication before the server can respond. Configuring a backup redirect farm makes the ACE perform L7 load balancing, even if you are matching using the default L7 class map.
- If rserver is down, state change config for a particular rserver performed under serverfarm, will not be updated internally. Users can change the config for rserver under serverfarm as “inservice” or “inservice standby” or “no inservice” only when rserver is up. This state change warning is notified using a new syslog.
- ACE resets the connection when we use inservice standby for SSL traffic. When gracefully terminating the sticky connections for SSL traffic, the ACE resets the connection in case of the SSL traffic with “inservice standby”. The ACE terminates the connection by sending an encrypted close notify message.

Note The ACE resets all Secure Sockets Layer (SSL) connections to a particular real server when you enter the no inservice command for that server.

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

  The default HTTP and SSL ports (80 and 443) now have a default inactivity timeout of 300 seconds.
- Starting with software version A4(1.0), it is no longer necessary to configure a resource class in the Admin context to allocate resources for stickiness. You can still allocate sticky resources if you wish, but skipping this step will not affect sticky functionality.
- In a redundant configuration, dynamic incremental sync is a form of config sync that copies configuration changes that you make on the active ACE to the standby ACE when the two ACEs are running the same version of software and when both ACEs are up. When you upgrade from one major release of ACE software to another major release (for example, from A2(3.0) to A5(1.0) or later, bulk sync, dynamic incremental sync, and connection replication are automatically disabled only while the active ACE is running software version A5(1.0) or later and the standby ACE is running software version A2(3.0). See Table 5.

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

Table 5 Redundancy Feature Availability Between Major ACE Software Versions

Platform	Active	Standby	Bulk Sync	Incr Sync	Conn Repl	Sticky Repl	Operation	Comments
Module	A2(x)	A5(x)	Yes	No	Yes	Yes	Upgrade	—
Module	A4(1.x)	A5(x)	Yes	No	Yes	Yes	Upgrade	—
Module	A4(2.x)	A5(x)	Yes	No	Yes	Yes	Upgrade	—
Module	A5(x)	A2(x)	No	No	No	No	Downgrade	Functionality not supported due to architectural differences between the ACE20 and the ACE30 hardware
Module	A5(x)	A4(1.x)	Yes	No	Yes (IPv4 flows)	Yes (IPv4 flows)	Downgrade	Standby supports only IPv4
Module	A5(x)	A4(2.x)	Yes	No	Yes (IPv4 flows)	Yes (IPv4 flows)	Downgrade	Standby supports only IPv4

- After migrating from ACE10/20 to ACE30 or ACE4710 the "ssl-connections rate" ACE reports via "show resource usage" or SNMP is significantly lower than what ACE10/20 reported, if the SSL Session ID Reuse feature is enabled. The reason for this difference, which can easily be a factor of 10, is that ACE30 and ACE4710 do not count a reused/resumed SSL connection towards the "ssl-connections rate", while ACE10/20 does.
- During an upgrade in a redundant configuration, we recommend that you do not run the two ACEs with different versions of software (split mode) for an extended period of time. However, if you must remain in split mode for a period of time to make configuration changes, we strongly recommend that you disable configuration synchronization (config sync) by entering the following command:

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

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

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

  After you re-enable config sync, the ACE automatically synchronizes the configuration changes from the active ACE to the standby ACE.
- We strongly recommend that you do not make any CLI changes when the ACE modules in a redundant configuration are running different software versions. Unexpected results may occur. Remove any new feature commands before performing a downgrade on the ACE.
- In software version A4(1.0) or later, all four of the network processors (NPs) must transition into the retcode or inband failed state before the ACE marks the real server as RETCODE-FAILED or INHAND-HM-FAILED, respectively, and places it on the reactivate list for recovery. This is also

true for the maxconn limit, where the threshold values are divided among all four NPs similar to the retcode and inband failed states. The real servers will move to the MAXCONN state only when all four NPs reach the MAXCONN state.

Note that the following may occur:

– When some NPs are in the retcode failed state and the other NPs are in the inband failed state due to a traffic pattern that hashes connections to specific NPs, the real servers are in the OPERATIONAL state as displayed by the **show serverfarm** *name* command because the NPs are deadlocked waiting until the other NPs reach the retcode or inband failed state, respectively.

– When some NPs are in the retcode or inband failed state due to a traffic pattern that hashes only to some NPs and not to the other NPs, the real servers are left in the OPERATIONAL state until all NPs transition into the retcode or inband failed state, respectively.

When the traffic distribution is uniform across all NPs, these issues do not occur.

- The ACE requires a route back to the client before it can forward a request to a server. If the route back to the client is not present, the ACE cannot establish a flow and drops the client request. Make sure that you configure the appropriate routing to the client network on the ACE VLAN where the client traffic enters the ACE module.
- When you downgrade the ACE software, the features and commands of the higher release are lost because they are not supported by the lower release.
- When redundant ACEs lose connectivity (for example, because of a network interruption) and they attempt to reestablish their connection, if you enter the **show ft peer** or **show ft group** command during this time, the response to this command may be delayed.
- If you are using the Application Networking Manager (ANM) to manage an ACE module and you configure a named object at the ACE CLI, ANM does not support all of the special characters that the ACE CLI supports for a named object. If you use special characters that ANM does not support, you may not be able to import or manage the ACE using ANM.

  When naming ACE objects (such as a real server, virtual server, parameter map, class map, health probe, and so on) for use with ANM, enter an alphanumeric string of 1 to 64 characters, which can include the following special characters: underscore (_), hyphen (-), dot (.), and asterisk (*). Spaces are not allowed.
- When you remove a NAT pool configuration, wait more than five seconds before adding a NAT pool with the same ID.
- The Account Expiry field for the **show user-account** command displays the date, if any, when the user account expires. This date is based on Coordinated Universal Time (UTC/GMT) which the ACE keeps internally. If you use the **clock timezone** command to configure a UTC offset, this field displays the UTC date and does not reflect the date with the offset as displayed by the **show clock** command.
- ACE30 module sometimes translate ftp-data port number from 20 to random number. This symptom maybe observed on ACE30 module with PAT config. When active ftp-data connection is opened, ACE30 module sometimes translates the port number from 20. This doesn't occur on ACE appliance.

  In any connection-pair setup in ACE30 module, ACE will have to establish the outbound connection in the same NP as the inbound. The NP is determined by the hashing of the ports. The inbound is already established on one NP. Now, when the outbound is being established, the source port here (client port) cannot be changed. The destination port which is by default 20, will be changed if the source and dest port are not hashing to the same NP as inbound. This change is done by an implicit PAT on the dest port.

  The following are the sample output for show connection:

- ## ACE30 Case 1

```
113        4  in  TCP   732  192.168.32.1:20       192.168.32.100:1150 ESTAB
84         4  out TCP   731  192.168.31.1:44645    192.168.31.100:20 ESTAB
(192.168.32.1:20 -> 192.168.31.100:20)
```

Above, the inbound connection is already established in NP4 by way of hashing ports 20 and 1150. Now, the client port in the outbound is 44645. The dest port by default is of course 20, and ACE will hash 20 and 44645 to see if it belongs to the same NP (NP4). In this case, it does belong to same NP and hence ACE is able to establish the outbound using the default port.

- ## ACE30 Case 2

```
100        4  in  TCP   732  192.168.32.1:20       192.168.32.100:1153 ESTAB
116        4  out TCP   731  192.168.31.1:43862    192.168.31.100:1048 ESTAB
(192.168.32.1:20 -> 192.168.31.100:1048)
```

Here, the inbound is established in NP4 due to hash of 20 and 1153. Now ACE will do hashing of client port 43862 and default dest port 20 to see if it belongs to NP4. However, ACE determines that hashing of 43862 and 20 results in NP1. So ACE will now do an Implicit PAT for the dest port so that the outbound will be established on the same NP4. That is why in this case, we see the implicitly PATed port.

- ## ACE4710

```
137526     1  in  TCP   778  192.168.78.41:20      192.168.78.100:1031 ESTAB
138143     1  out TCP   777  192.168.77.41:47784   192.168.77.100:20 ESTAB
(192.168.78.41:20 -> 192.168.77.100:20) - always keep port#20 since it is the same
with ACE30 case 1
```

- ACE20 and ACE30 behaves differently with respect to ToS/DSCP marking for outgoing packets ACE20 does not update the ToS/DSCP marking for outgoing packets. The ToS/DSCP marking is changed in the middle of a connection. Workaround: Migrate to ACE30.

  ACE20 only checks the ToS/DSCP marking of the very first packet it receives on a particular connection per direction. If the ToS/DSCP connection is changed in subsequent packets on the same connection, ACE20 keeps forwarding packets pertaining to this connection with the original ToS/DSCP marking. With ACE30 this behavior is different, as ACE30 checks the ToS/DSCP marking in every single packet, not just the first packet per connection and direction. As a result, ACE30 always forwards the packet out with the same ToS/DSCP marking it received it with (unless manually instructed to change the ToS via parameter map).

- If you are using ssl header insert feature, especially in addition to caching be aware of CSCua81138. There is a fixed amount of buffers available in ACE to carry out header insertion and/or caching. The buffers are periodically cleaned up but the frequency of cleanup maybe slow compared to the insertions happening (specifically during high traffic levels) in which case ACE will stop doing header insertions on a intermittent basis. If you are planning to use ssl header insert and/or caching feature combination on ACE be aware that thorough testing needs to be done. This feature can "break" anytime based on traffic levels.

- The following dplug is provided as a hot fix for the security vulnerability identified by CVE-2014-6271 and CVE-2014-7169.

  If you are using A5X trend release, please download below mentioned dplug binaries from the same location where ACE images are available for download.

  ACE Module: ACE30_A5x_bash_security_fix.bin

  The dplug needs to be installed to address the issues mentioned under defect/bug: “CSCur02195”: ACE evaluation for CVE-2014-6271 and CVE-2014-7169

  Please follow the procedure mentioned below to get the security fix installed via the dplug.

Procedure to install the dplug:

1. FTP the dplug to the ACE box
2. Load the dplug to the image directory

```
switch/Admin# load image:ACE30_A5x_bash_security_fix.bin
```

The dplug will install the fix and exit.

```
switch/Admin# load image:ACE30_A5x_bash_security_fix.bin
bash etc isan itasca usr
################################################################
Warning:
- The debug-plugin should ONLY be used upon request from the
Cisco TAC, Advanced Services, or the Business Unit.
- Once the debug-plugin has been loaded, ONLY the exact
commands provided by TAC,AS,BU should be executed.
Please note:
- Running unauthorized commands with the debug-plugin loaded
may result in damage to the ACE blade.
- For security reason, plugin image has been deleted.
################################################################
Successfully loaded debug-plugin!!!
Installing bash security patch...
Installation Done!
switch/Admin#
```

Note This dplug is only applicable for A5(3.1a) and previous releases.

Note The fix installed via dplug is not persistent. So, it needs to be re-installed across reboot of the ACE.

Available ACE Licenses

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

Table 6 ACE30 License Bundles

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

Table 6 ACE30 License Bundles (continued)

License Bundle	Product ID (PID)	License File	Description
4 Gbps to 8 Gbps	ACE30-MOD-UPG2=	ACE30-MOD-UPG2	8 Gbps bandwidth 6 Gbps compression
8 Gbps Bundle	ACE30-MOD-08-K9	ACE30-MOD-08-K9	30,000 SSL TPS 250 virtual contexts
8 Gbps to 16 Gbps	ACE30-MOD-UPG3=	ACE30-MOD-UPG3	16 Gbps bandwidth 6 Gbps compression
16 Gbps Bundle	ACE30-MOD-16-K9	ACE30-MOD-16-K9	30,000 SSL TPS 250 virtual contexts

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

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

Ordering an Upgrade License and Generating a License Key

This section describes the process to order an upgrade license and to generate a license key for your ACE. To order an upgrade license, perform the following steps:

Step 1 Order one of the licenses from the list in the "Obtaining Documentation and Submitting a Service Request" section using any of the available Cisco ordering tools on Cisco.com.

Step 2 When you receive the Software License Claim Certificate from Cisco, follow the instructions that direct you to the cisco.com website. As a registered user of cisco.com, go to this URL:

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

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

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

Step 5 After the system generates the license key, you will receive a license key e-mail with an attached license file and installation instructions. Save the license key e-mail in a safe place in case you need it in the future (for example, to transfer the license to another ACE).

For information about installing and managing ACE licenses, refer to Chapter 3, Managing ACE Software Licenses, in the *Administration Guide, Cisco ACE Application Control Engine*.

Upgrading Your ACE Module Software in a Redundant Configuration

To upgrade your ACE software to version A5(3.x), the procedure in the following section assumes that your ACEs are configured as redundant peers to ensure that there is no disruption to existing connections during the upgrade process. In the following procedure, the active ACE is referred to as ACE-1 and the standby ACE is referred to as ACE-2.

Note To upgrade your ACE software from version A2(3.x) or A2(1.6a) or later to version A5(3.x), you must also migrate your ACE10 or ACE20 module to a new ACE30 module. For details about migrating to an ACE30 and upgrading your software to A4(1.0) or later, see the procedure in the *Installation Note, Cisco ACE Application Control Engine ACE30 Module*.

This section includes the following topics:

Before You Begin

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

Note If you are upgrading a redundant ACE configuration from an earlier version of ACE software (A4(1.x) or greater) to version A5(3.x) while the two ACEs are in split mode with the earlier software version running on the active ACE, and software version A5(3.x) is running on the standby, config sync is disabled. 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. We recommend that you do not make any configuration changes while the two ACEs are in split mode.

Changing the Admin Password

Before you upgrade your ACE software, you **must** change the default Admin password if you have not already done so. Otherwise, after you upgrade the ACE software, you will only be able to log in to the ACE through the console port or through the supervisor engine of the Catalyst 6500 series switch or the Cisco 7600 series router.

For details on changing the default Admin password, see Chapter 1, Setting Up the ACE, in the *Administration Guide, Cisco ACE Application Control Engine*.

Changing the www User Password

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

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

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

Creating a Checkpoint

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

Copying the Startup Configuration of Each Context

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

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

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

Checking Your Configuration for FT Priority and Preempt

If you want the currently active ACE to remain active after the software upgrade, be sure that the active ACE has a higher priority than the standby (peer) ACE and that the **preempt** command is configured. To check the redundant configuration of your ACEs, use the **show running-config ft** command. The **preempt** command is enabled by default and does not appear in the running-config.

Upgrade Procedure

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

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

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

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

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

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

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

Step 4 Copy the new software image to the image directory of each ACE (active and standby) by entering the **copy ftp**, **copy sftp**, or the **copy tftp** command in Exec mode. For example, to copy the image with the name c6ace-t1k9-mz.A5_3_0.bin through FTP, enter:

```
ACE-1/C1# changeto Admin
ACE-1/Admin# copy ftp://server1/images//c6ace-t1k9-mz.A5_1_0.bin image:
Enter source filename[/images/c6ace-t1k9-mz.A5_3_0.bin]?
Enter the destination filename[]? [c6ace-t1k9-mz.A5_3_0.bin] File already exists, do you
want to overwrite?[y/n]: [y]
Enter hostname for the ftp server[server1]?
Enter username[]? user1
Enter the file transfer mode[bin/ascii]: [bin] Enable Passive mode[Yes/No]: [Yes] no
Password:
```

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

```
ACE-1/Admin# dir image:c6ace-t1k9-mz.A5_3_0.bin
35913728  Oct 1 2013 01:17:01 c6ace-t1k9-mz.A5_3_0.bin

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

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

```
ACE-1/Admin# show bootvar
BOOT variable = “image:c6ace-t1k9-mz.A5_3_0.bin”
Configuration register is 1
```

Step 7 Remove the existing image from the boot variable on ACE-1 by entering the **no boot system image:***ACE_image* command in configuration mode. For example, to remove the A4(2.0) image, enter:

```
ACE-1/Admin# configure
Enter configuration commands, one per line. End with CNTL/Z.
ACE-1/Admin(config)# no boot system image:c6ace-t1k9-mz.A4_2_0.bin
```

Step 8 Configure ACE-1 to autoboot from the latest ACE image. To set the boot variable and configuration register to1 (perform auto boot and use startup-config file), use the **boot system image:** and **config-register** commands in configuration mode. For example, enter:

```
ACE-1/Admin(config)# boot system image:c6ace-t1k9-mz.A5_3_0.bin
ACE-1/Admin(config)# config-register 1
ACE-1/Admin(config)# exit
ACE-1/Admin# show bootvar
BOOT variable = “image:c6ace-t1k9-mz.A5_3_0.bin”
Configuration register is 1
```

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

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

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

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

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

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

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

- Enter the **show version** command in Exec mode to verify that the module has properly rebooted with the latest ACE software image.
- Enter the **show ft group detail** command in Exec mode to verify that the standby ACE has recovered to a STANDBY_WARM state.

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

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

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

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

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

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

Downgrading Your ACE Module Software in a Redundant Configuration

If you need to downgrade your ACE software from version A5(3.x) to an earlier version of ACE software, use the procedure that follows. This procedure assumes that your ACEs are configured as redundant peers to ensure that there is no disruption to existing connections during the downgrade process. In the following procedure, the active ACE is referred to as ACE-1 and the standby ACE is referred to as ACE-2.

Note If you need to downgrade your ACE software from version A5(3.x) to an earlier supported ACE software version (version A2(3.x) or A2(1.6a) or later), use the procedure in the *Installation Note, Cisco ACE Application Control Engine ACE30 Module*.

Before You Begin

Before you downgrade your ACE software, ensure that the following conditions exist:

- Identical versions of the previous software image resides in the image: directory of both ACEs.
- The active ACE has a higher priority than the standby ACE and **preempt** is enabled on the FT group if you want the active ACE to remain active after the downgrade procedure.

Downgrade Procedure

To downgrade your A5(3.x) software in a redundant configuration, perform these steps:

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

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

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

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

```
ACE-1/Admin# config
ACE-1/Admin(config)# boot system image:c6ace-t1k9-mz.A5_2_1.bin
ACE-1/Admin(config)# config-register 1
ACE-1/Admin(config)# exit
ACE-1/Admin#
```

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

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

```
ACE-2/Admin# show bootvar
BOOT variable = “disk0:c6ace-c6ace-t1k9-mz.A5_2_1.bin”
Configuration register is 1
```

```
host1/Admin#
```

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

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

When ACE-2 loads the startup-configuration file, you may observe a few errors if you did not roll back the configuration to a checkpoint. These errors are harmless and occur because the ACE software does not recognize the A5(3.x) commands in the startup-configuration file.

Note Dynamic incremental sync is automatically disabled while the active ACE is running software version A5(3.x) and the standby ACE is running an earlier software version.

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

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

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

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

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

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

ACE Documentation Set

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

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

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

Document Title	Description
Installation Note, Cisco ACE Application Control Engine ACE30 Module	Provides information for installing the ACE module into the Catalyst 6500 series switch or a Cisco 7600 series router.

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

Document Title	Description
Release Note for the Cisco Application Control Engine Module	Provides information about operating considerations and caveats for the ACE.
Getting Started Guide, Cisco ACE Application Control Engine Module	Describes how to perform the initial setup and configuration tasks for the ACE module.

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

Document Title	Description
Administration Guide, Cisco ACE Application Control Engine	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 Application Control Engine (ACE) Configuration Examples Wiki	Provides examples of common configurations for load balancing, security, SSL, routing and bridging, virtualization, and so on.
Cisco Application Control Engine (ACE) Troubleshooting Wiki	Describes the procedures and methodology in wiki format to troubleshoot the most common problems that you may encounter during the operation of your ACE.
Command Reference, Cisco ACE Application Control Engine	Provides an alphabetical list and descriptions of all CLI commands by mode, including syntax, options, and related commands.
Cisco CSM-to-ACE Conversion Tool User Guide	Describes how to use the CSM-to-ACE module conversion tool to migrate Cisco Content Switching Module (CSM) running- or startup-configuration files to the ACE.
Cisco CSS-to-ACE Conversion Tool User Guide	Describes how to use the CSS-to-ACE conversion tool to migrate Cisco Content Services Switches (CSS) running-configuration or startup-configuration files to the ACE.

Document Title	Description
Routing and Bridging Guide, Cisco ACE Application Control Engine	Describes how to perform the following routing and bridging tasks on the ACE: • VLAN interfaces • IPv6, including transitioning IPv4 networks to IPv6, IPv6 header format, IPv6 addressing, and supported protocols • Routing • Bridging • Dynamic Host Configuration Protocol (DHCP)
Security Guide, Cisco ACE Application Control Engine	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)
Server Load-Balancing Guide, Cisco ACE Application Control Engine	Describes how to configure the following server load-balancing features 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 • Dynamic workload scaling (DWS) • Firewall load balancing • TCL scripts
SSL Guide, Cisco ACE Application Control Engine	Describes how to configure the following Secure Sockets Layer (SSL) features on the ACE: • SSL certificates and keys • SSL initiation • SSL termination • End-to-end SSL
System Message Guide, Cisco ACE Application Control Engine	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.
Virtualization Guide, Cisco ACE Application Control Engine	Describes how to operate your ACE in a single context or in multiple contexts.

For detailed configuration information on the Cisco Application Networking Manager (ANM), see the following software document on Cisco.com:

User Guide, Cisco Application Networking Manager	Describes how to use Cisco Application Networking Manager (ANM), a networking management application for monitoring and configuring network devices, including the ACE.

ACE Troubleshooting Wiki

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

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

http://docwiki.cisco.com/wiki/Cisco_Application_Control_Engine_%28ACE%29_Troubleshooting_Guide

Software Version A5(3.5) Resolved Caveats and Open Caveats

This release note includes resolved and open caveats that have a severity level of Sev1, Sev2, and customer-use Sev 3. The following sections contain the resolved caveats in software version A5(3.5):

Software Version A5(3.5) Resolved Caveats

The following resolved caveats apply to software version A5(3.5):

- CSCvb16317—Cisco ACE Denial of Service Vulnerability. When processing some SSL packets, the ACEs reloads with back trace. This issue was able to repro in lab by using script from the cipherscan from the Redhat Website.
- CSCux95091—Evaluation of ace for NTP_January_2016. This bug has been filed against Cisco Application Control Engine (ACE30/ ACE 4710) to address the vulnerability known as NTP_January_2016 and identified by the Common Vulnerability and Exposures (CVE) IDs:
  1. CVE-2015-7973
  2. CVE-2015-7974
  3. CVE-2015-7975
  4. CVE-2015-7976
  5. CVE-2015-7977
  6. CVE-2015-7978
  7. CVE-2015-7979

8. CVE-2015-8138
9. CVE-2015-8139
10. CVE-2015-8140
11. CVE-2015-8158

- CSCuz92646—Evaluation of ace for NTP_June_2016. This bug has been filed against Cisco Application Control Engine (ACE30/ ACE 4710) to address the vulnerability known as NTP_June_2016 and identified by the Common Vulnerability and Exposures (CVE) IDs:
  1. CVE-2016-4957
  2. CVE-2016-4953
  3. CVE-2016-4954
  4. CVE-2016-4955
  5. CVE-2016-4956

Software Version A5(3.4) Resolved Caveats and Open Caveats

This release note includes resolved and open caveats that have a severity level of Sev1, Sev2, and customer-use Sev 3. The following sections contain the resolved caveats in software version A5(3.4):

Software Version A5(3.4) Resolved Caveats

The following resolved caveats apply to software version A5(3.4):

- CSCuw09152—VLAN 4095 was not downloaded properly. It may cause encap table to get full
- CSCuw14044—FT synch takes too long to complete with TACACS enabled - When TACACS is being used for authentication, the FT sync takes a longer time to complete with the A5(3.x).
  - **New CLI Commands**: The following new command has been added to disable crypto chaingroup update feature:

```
switch/Admin(config)# crypto ?
 authgroup                       Configure an authgroup
 chaingroup                      Configure a chaingroup
 chaingroup-order-update-disable  Disable cache for crypto chaingroup order update
 crl                             Configure a crl
 crlparams                       Configure CRL params
 csr-params                      Configure CSR parameters
 ocspserver                      Configure an OCSP Server
 rehandshake                     Enable SSL rehandshake
switch/Admin(config)#
```

  - **Functionality**: The CLI is restricted to Admin and it is a global CLI. When we configure this CLI it will disable the "crypto chaingroup update function"(CSCue49212) to reduce the HA sync time after reload.
  - **Configuration**:

```
switch/Admin(config)#
switch/Admin(config)# crypto chaingroup-order-update-disable
switch/Admin(config)#
```

```
switch/Admin(config)# do sh running-config | include
chaingroup-order-update-disable
Generating configuration....
crypto chaingroup-order-update-disable
switch/Admin(config)#
```

  - **Guidelines and Restrictions**: The following conditions should be taken care while configuring CLI:
    1. When we configure CLI we should not remove any certificate under "crypto chaingroup <NAME>
    2. If we remove the certificates under "crypto chaingroup <NAME>" when CLI is configured, we need to add particular chaingroup again under ssl-proxy once again.

- CSCuw36845— IPV6 VIP gets stuck in DAD TENTATIVE state and not passing traffic - IPV6 VIP stuck in TENTATIVE state and not passing traffic. Were able to reproduce the issue by replying the service policy for the VIP. In customer case it occurred on its own.
- CSCuw84697—Evaluation of ace for NTP_October_2015 - This bug has been filed against Cisco Application Control Engine (ACE30/ ACE 4710) to address the vulnerabilities known as NTP_October_2015 and identified by the Common Vulnerability and Exposures (CVE) IDs:
  1. CVE-2015-7691
  2. CVE-2015-7692
  3. CVE-2015-7701
  4. CVE-2015-7702
  5. CVE-2015-7703
  6. CVE-2015-7704
  7. CVE-2015-7705
  8. CVE-2015-7848
  9. CVE-2015-7849
  10. CVE-2015-7850
  11. CVE-2015-7851
  12. CVE-2015-7852
  13. CVE-2015-7853
  14. CVE-2015-7854
  15. CVE-2015-7855
  16. CVE-2015-7871

Software Version A5(3.3) Resolved Caveats and Open Caveats

This release note includes resolved and open caveats that have a severity level of Sev1, Sev2, and customer-use Sev 3. The following sections contain the resolved and open caveats in software version A5(3.3):

Software Version A5(3.3) Resolved Caveats

The following resolved caveats apply to software version A5(3.3):

- **CSCut83796**—April 2015 NTPd vulnerabilities - This product includes a version of NTPd that is affected by the vulnerability identified by the Common Vulnerability and Exposures (CVE) IDs:
  1. CVE-2015-1798
  2. CVE-2015-1799
- **CSCuu39811**—Make the SNMP fix for CSCuf30894 configuration to provide faster resp
- **CSCuu82343**—Evaluation of ace for OpenSSL June 2015 - This product includes a version of OpenSSL that is affected by the vulnerability identified by the Common Vulnerability and Exposures (CVE) IDs:
  1. CVE-2015-4000
  2. CVE-2015-1788
  3. CVE-2015-1789
  4. CVE-2015-1790
  5. CVE-2015-1792
  6. CVE-2015-1791
  7. CVE-2014-8176
- **CSCuv33150**—Cisco ACE30/4710 TLS Poodle variant vulnerability

Software Version A5(3.3) Open Caveats

The following open caveats apply to software version A5(3.3):

- **CSCul90247**—ACE:ACE resets both sides after sending false encap alert type_21
- **CSCuo74623**—ACE 30: device crashed with "last boot reason: CP Kernel Crash"
- **CSCus40778**—ACE: dst cache overflow

Software Version A5(3.2) Resolved Caveats and Open Caveats

This release note includes resolved and open caveats that have a severity level of Sev1, Sev2, and customer-use Sev 3. The following sections contain the resolved and open caveats in software version A5(3.2):

Software Version A5(3.2) Resolved Caveats

The following resolved caveats apply to software version A5(3.2):

- **CSCuj91023**—ACE A5(2.x) Https probes unable to handle split SSL with Server 2012.

- **CSCug88070**—ACE HTTPS probe (version A522) does not send traffic on wire. Yet ACE thinks it is firing -gives probe fail reason and counters as if probe really fired.
- **CSCup84117**—ACE 30A5(3.0) - Memory Leak
- **CSCuq60062**—Revert CSCug93530 fix
- **CSCuq66230**—A5(3.1) ACE30 Health Monitoring (HM) crash
- **CSCuq92623**—IPV6 address starts pinging even though VIP is out of service.
- **CSCur02195**—ACE evaluation for CVE-2014-6271 and CVE-2014-7169.
- **CSCur16238**—ACE: MIB definition is incorrect.
- **CSCur18171**—Ace X-Forwarded-For rewrite breaks for the subsequent flows.
- **CSCur23304**—/bin/bash user exists in ACE30 that authenticates using external AAA
- **CSCur23683**—ACE4710 content rewrite does not work when compression is enabled.
- **CSCur31344**—Avg 'idle CPU' in "show system resources" is much lower in A5(3.0).
- **CSCur41610**—Failed routed probes shows 0.0.0.0 ip address in syslogs.
- **CSCur42025**—ACE: dir image output not showing byte counts.
- **CSCur57515**—ACE: dir image output not showing byte counts.
- **CSCur77792**—ACE reports incorrect values for buffer usage oids.
- **CSCur92238**—HTTPS probe failing with "ssl certificate-expiration ignore**”**
- **CSCus42709**—JANUARY 2015 OpenSSL Vulnerabilities.
- **CSCus43274**—CVE-2010-4755 - OpenSSH - Memory Corruption Issue with SFTP.
- **CSCus69159**—ACE 30: SSL probe script needs to be fixed for poodle vulnerability
- **CSCus72091**—Telnet failure.
- **CSCur73173**—Web pages do not display when using client authentication and crl.

Software Version A5(3.2) Open Caveats

None.

Software Version A5(3.1b) Resolved Caveats and Open Caveats

This release note includes resolved and open caveats that have a severity level of Sev1, Sev2, and customer-use Sev 3. The following sections contain the resolved and open caveats in software version A5(3.1b):

Software Version A5(3.1b) Resolved Caveats

The following resolved caveats apply to software version A5(3.1b):

- **CSCur02195**—The ACE 4710 and ACE30 include a version of bash that is affected by the vulnerabilities identified by the Common Vulnerability and Exposures (CVE) IDs:
  1. CVE-2014-6271
  2. CVE-2014-6277
  3. CVE-2014-6278
  4. CVE-2014-7169
  5. CVE-2014-7186
  6. CVE-2014-7187
- **CSCur23683**—ACE30: Evaluation of SSLv3 POODLE vulnerability.

Note ACE will no longer support SSLv3 version of SSL. ACE will support the following SSL versions TLS1.0, TLS1.1, and TLS1.2. A performance degradation of 9% may be observed while using TLS1.0 compared to SSLv3.

Software Version A5(3.1b) Open Caveats

The following open caveats apply to software version A5(3.1b):

- **CSCur92238**—HTTPS probe failing with “ssl certificate-expiration ignore.

  Configuring the command “ssl certificate-expiration ignore” under HTTPS probe will cause the HTTPS probes to fail.

  Workaround: To make probes work, you have to remove this command by using “no ssl certificate-expiration ignore” under HTTPS probe and use valid certificates.
- **CSCuj91023**—ACE A5(2.x) Https probes unable to handle split SSL with Server 2012.
- **CSCuo30577**—ACE/A5(3.0): silent reboot with no core dump.
- **CSCup61227**—ACE 30 A5(3.0) - Warning:- MTS queue is full opcode 4062sap%d pid %d.
- **CSCup84117**—ACE 30A5(3.0) - Memory Leak.
- **CSCuq53270**—ACE 30: device crashed with "last boot reason: CP Kernel Crash”.
- **CSCuq60062**—Revert CSCug93530 fix.
- **CSCuq92452**—LMS 4.2.5 ssh sessions getting stuck on ACE.
- **CSCuq92623**—IPV6 address starts pinging even though VIP is out of service.
- **CSCur16238**—ACE: MIB definition is incorrect.
- **CSCur18171**—Ace X-Forwarded-For rewrite breaks for the subsequent flows.
- **CSCur23304**—/bin/bash user exists in ACE30 that authenticates using external AAA.
- **CSCur31344**—ACE4710 content rewrite does not work when compression is enabled.
- **CSCur41610**—Avg 'idle CPU' in "show system resources" is much lower in A5(3.0).
- **CSCur42025**—Failed routed probes shows 0.0.0.0 ip address in syslogs.
- **CSCur57515**—ACE: dir image output not showing byte counts.
- **CSCur63959**—Sticky entries with time-to-expire higher than timeout.
- **CSCur75687**—ACE in bridge mode causes L2 loop during ft switchover.

Software Version A5(3.1a) Resolved Caveats and Open Caveats

This release note includes resolved and open caveats that have a severity level of Sev1, Sev2, and customer-use Sev 3. The following sections contain the resolved and open caveats in software version A5(3.1a):

Software Version A5(3.1a) Resolved Caveats

The following resolved caveats apply to software version A5(3.1a):

- **CSCuq66230**—ACE crashed after upgrading to A5(3.1) from A5(3.0).

Software Version A5(3.1a) Open Caveats

The following open caveats apply to software version A5(3.1a):

- **CSCug27629**—As the Access Control List (ACL) configuration is modified it is sometimes seen that an ACL merge error will be reported on one or more of the interfaces where the ACL list is applied. This leaves the interface in an inconsistent state. The dynamic configuration of ACLs lists within a context. Workaround:
  1. Remove the offending lines one at a time until the ACL can be applied successfully.
  2. Remove the offending lines and try a different line number

Reload the ACE.

- **CSCuj91023**—ACE A5(2.x) is unable to handle Split SSL Records when using HTTPS Probes on Windows Server 2012 (IIS Server). Only happens with Windows Server 2012, the security update seems to be present in every server OS since 2003. Workaround: Change the https probe to SSL v3.

  Or

Follow the instructions here: http://support.microsoft.com/kb/2643584.

Software Version A5(3.1) Resolved Caveats, Open Caveats, 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 A5(3.1):

Software Version A5(3.1) Resolved Caveats

The following resolved caveats apply to software version A5(3.1):

- **CSCul55184**—Client Cert Authentication Failure. Seeing following types of failures in the packet captures:

```
SSL alert CERTIFICATE_REVOKED sent
SSL alert CERTIFICATE_UNKNOWN sent
```

  Seeing the following in the logs:

```
ACE-6-253006  Error peer sent invalid or nonexistent certificate none, reason: unknow
ACE-6-253004  Certificate /C=/O=/CN=/emailAddress= revoked, ssl-proxy: , reason: crl
download/ocsp status check failure
```

- **CSCum86024**—Standby ACE sends IPv6 probes on both client and server vlans. With Bridge configurations, Primary ACE forwards probes received from client vlan to server vlan which may cause MAC flaps. Standby ACE must only send IPv6 Probes on Server Vlan. Workaround: None
- **CSCuo24303**—After upgrading from A5(1.1) to A5(3.0) particular action-lists with regex in them do no longer rewrite location response headers if more than two statements are added to the "action-list".

  Example:

```
action-list type modify http rewrite-location-all
    header rewrite response Location header-value "http://(.+):[0-9]{4}/(.*)" replace
    "https://%1/%2"
    header rewrite response Location header-value "https://(.+):[0-9]{4}/(.*)" replace
    "https://%1/%2"
    header rewrite response Location header-value "http://(.+)/(.*)" replace
    "https://%1/%2"
```

  OR

```
action-list type modify http rewrite-location-all
    header rewrite response Location header-value "http://(.+):[0-9]{4}/(.*)" replace
    "https://%1/%2"
    header rewrite response Location header-value "https://(.+):[0-9]{4}/(.*)" replace
    "https://%1/%2"
    header rewrite response Location header-value "http://([a-zA-Z0-9\.\-]+)/(.*)"
    replace "https://%1/%2"
```

  Workaround: None.

- **CSCue55049**—C4MA2B: SPAN session leak traffic from one session to other session.
- **CSCug01673**—Unexplained buffer leak on NPs for external buffers. Workaround: None.
- **CSCul15825**—ACE with NTPv3 with authentication configured shows one of those symptoms:
  1. show ntp peer-status does not show NTP server
  2. ACE cannot sync clock with NTPv3 server with authentication configured
  3. "Could not find the relevant data" when trying to delete ntp server configured with authentication

  Workaround:

  1. Make sure that NTP key is entered before NTP server where this key is referenced:

```
ntp authenticate
ntp authentication-key 1 md5 <key>
ntp trusted-key 1
```

```
ntp server 10.48.68.81 key 1 prefer
```

2. This workaround will work until the box is rebooted - afterwards workaround should be applied again.

- **CSCul39399**—some sylog messages are missing in 'show logging' even though all messages are sent to the syslog server successfully. Workaround: None.
- **CSCul44877**—ACE30 running A5(2.1) crashed with last boot reason: Unhandled kernel unaligned access. There was no changes whatsoever on the active ACE and ANM is not used to manage the device.
- **CSCum24735**—"no logging message 199008" is added twice to ACE running/startup configuration that can cause ACE import to ANM to fail. Workaround: Enabled logging of this specific message: "logging message 199008"
- **CSCum65701**—Unable to reach outside ip addresses, by using the ldap://57.250.237.230/cn=CRL52,o=EQUANT certificateRevocationList;binary ldap request, Unable to see the ACE sending the ?binary? part of the attribute. Workaround: None.
- **CSCun02703**—ACE30 sends HTTP request using cookie insert to backup rserver instead of primary rserver that is active. Workaround: In the serverfarm do "no inservice standby" followed by "inservice standby" for the backup rserver, when the primary rserver comes back online, in order to update the sticky entry, so that it points to the primary rserver again.
- **CSCun33762**—ACE is removing the threshold line from snmp probe. When we try configuring the threshold and absolute max for snmp probe and do a show run the threshold will be removed.
- **CSCun39570**—Customer rserver was taken down for maintenance. After it was reloaded and the probes passed, new requests were not sent to it. Customer is using a L3/L4 rule with least conn algorithm on a ACE30 load balancer running A5(2.2b). Workaround: change the state again once rserver is up.
- **CSCuo52444**—URL rewrite feature isn't including the entire query string in the new url. Instead, the regex match stops at first ampersand (&) in query string resulting in an incomplete rewrite. Workaround: None.
- **CSCup77796**—SIP client has an established flow and is sending keepalive traffic. After around 15 minutes of this keep-alive traffic, the SIP client sends an UPDATE packet that does not get forwarded to the rserver. Workaround: None.
- **CSCud71628**—HTTP performance across ACE is very bad. Packet captures show, that ACE drops the TCP Window Size it advertises to the client to a very low value early in the connection and never recovers from this.Workaround: Disable the "tcp-options window-scale allow"..
- **CSCuq30645**—Syslog to inform hash collision while adding VIP IP in "icmp-vip" table.
- **CSCum12568**—Standby crash with cfgmgr on lb_fabric.c
- **CSCum24308**—"show IPv6 neighbors"output is showing wrong VLAN in Bridge mode.Workaround: Configuring static entry of the IPv6 neighbor solves the issue.
- **CSCui30210**—ACE unknown Silent reboot without Core Dump.
- **CSCul64560**—ACE 30 crash with last boot reason NP ME Hung

Software Version A5(3.1) Open Caveats

The following open caveats apply to software version A5(3.1):

- **CSCug27629**—As the Access Control List (ACL) configuration is modified it is sometimes seen that an ACL merge error will be reported on one or more of the interfaces where the ACL list is applied. This leaves the interface in an inconsistent state. The dynamic configuration of ACLs lists within a context. Workaround:
  1. Remove the offending lines one at a time until the ACL can be applied successfully.
  2. Remove the offending lines and try a different line number
  3. Reload the ACE.

Software Version A5(3.1) System Log Messages

442008

Error Message `ACE-4-442008: Real Server test1 is down, config change is not updated internally.`

442009

Error Message `ACE-4-442009: Context:0 Hash collision occurred while creating entry in icmp-vip table for VIP ip: 80.0.0.100 ifid: 3`

Note If we add/modify VIP address into class-map, ACE internally adds the new VIP address into icmp-vip table. During this, icmp-vip table update if there is any collision, the above sys log is generated.

Software Version A5(3.0) Resolved Caveats, Open Caveats, Command Changes, and Related SNMP Changes

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 A5(3.0):

Software Version A5(3.0) Resolved Caveats

The following resolved caveats apply to software version A5(3.0):

CSCud71628—The bad performance is due to the way TCP tries to recover from the low Window Size ACE reports: When the client receives a Window Size lower than a certain threshold, it will wait for 5 seconds to allow the peer devices (the ACE in this case) to process the data in its buffers after which it should update the Window Size again. As ACE never sends an updated Window Size, the client waits for the full 5 seconds before attempting to send further data. As ACE still responds to this additional data with the same low (or an even lower) Window Size, the same procedure starts over again. Workaround : Disable the "tcp-options window-scale allow".

CSCue38032—"ACE appliance giving ""write error: No space left on device"" when issuing various commands. Condition : ACE appliance with heavy use of the DM. Workaround : Log to debuguser and issue the following commands from the shell:

```
cd /isan/httpd/logs/
cat /dev/null > ssl_scache.dir
cat /dev/null > ssl_scache.pag
/etc/rc.d/rc3.d/S80apachectl restart"
```

CSCue38310—ACE with IPV6 Enabled attempt to give same IPV6 address to different non shared interfaces fails. Workaround: None.

CSCue49212—The order of issuer certs in the SSL/TLS cert chain sent by the ACE in Server Hello, may be different than their order in the configured chaingroup.Workaround : Remove/re-apply chaingroup or configure a new chaingroup with the certs in the chaingroup in order, from lowest sub at the top, to root CA at the bottom.

CSCue73311—Cisco ACE includes a version of OpenSSL that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:CVE-2011-1473. Wokaround: The SSL/TLS renegotiation can be disabled by disabling the "rehandshake'.

CSCue78766—Arp entry may be incorrect for an interface on a context. The output for that interface via ""show arp"" and ""show int"" do not match Workaround: Do a ""shut"" followed by ""no shut"" on the interface in the context."

CSCue75913—"ACE30 module crashes and generates core file snmpd_log.xxxx.tar.gz Workaround: Stop SNMP polling of ACE30 module."

CSCue88110—"ACE30 module crashes and generates core file snmpd_log.1033.xxxx.tar.gz. Last boot reason: Service ""snmpd"". Death reason: SYSMGR_DEATH_REASON_FAILURE_SIGNAL malloc_printerr () from /lib/tls/libc.so.6 in backtrace. Workaround:Stop SNMP polling of ACE30 module."

CSCue93409—ACE crashed due to service NTP Workaround: none, the box recovers after the crash.

CSCue97543—"TCP connections across ACE are extremely slow (delays of several minutes are possible) or fail completely. In packet captures you will see a jump of the TCP timestamp (TSval) sent from ACE to the backend server at some point (more precisely: when the connection is unproxied on ACE). Workaround:a. Either remove the ""tcp-options timestamp allow"" b. Or, if the timestamp option is required, force the connection to remain proxied on ACE throughout its lifetime by adding ""set tcp wan-optimization rtt 0"" to the parameter map of type connection."

CSCuf16964—"If you add up current ""regexp"" for all contexts in an ACE, that can exceed Max. Workaround: none"

CSCuf90272—SNMPD on both Active and Standby crashed and core dumped Workaround: None.

CSCuf93815—"Failover between active and standby ACE registered. Workaround: none"

CSCub87352—"In A5(2.0), the ACE reloads/crashes with a cfgmgr crash continuously.Workaround:</B>Downgrade to A5(1.2)"

CSCug27144—"ACE30 crash with last boot reason: Service ""cfgmgr"" and cfgmgr_log core dump produced."

CSCub18452—SNMPD on both Active and Standby crashed and core dumped Workaround:None.

CSCuh47599—ACE inserts "internal error" as Session-Verify-Result when using an action-lists with "ssl header-insert session Verify-Result" and OCSP to validate the certificate. Workaround: None.

CSCui06230—'time-to-expire' value of sticky http-cookie database on standby ACE may not be decreased. This symptom maybe observed when ACE only receives 'Set-cookie' from server.It doesn't occur and recover when ACE receives http request with cookie from client. It only occur on standby ACE. Workaround: Send http request with cookie from client.

CSCui27005—"During config changes to HTTPS probes on ACE, the following error occurs %ACE-3-440003: Deletion failed for Probe Sfarm Table and no further probe config changes can be made. Workaround:Reload the device."

CSCui40439—ACE show rserver xml output has changed in A5(2.2).

CSCuj31362—Output of debug hm-scripted all does not show the received bind response code sent by Ldap server if ldap scripted probe is configured.

Workaround:

1. Take packet capture to verify the response code sent by server
2. Upgrade to A530 or higher to see the complete message in debug output

CSCty36868—Cookie expiry string is wrongly set to Jan 1970.If the cookie timeout is recently configured it takes one full cycle to update the time string to correct value. Wokaround : None

CSCuc98599—The ACE running the A52x code train is getting random TCP resets for certain connections and the counter "Exceed max buffer errors" is incrementing.Workaround:Increase the max parselen parameter to 65K.

CSCud43266—In the sticky database some entries have a time-to-expire higher than the configured timeout. Workaround: The entries will be removed from the table eventually, it will just take longer and in case of sticky table full they might not get recycled due to the artificially high time-to-expire leading to legitimate entries to be recycled more quickly. As a workaround is possible to clear the sticky database for the specific group.

CSCue31894—ACE30 crashed with last reboot reason. Workaround : NA

CSCue55944—ACE 30 crash with last boot reason: CP Kernel Crash. Workaround : A defensive fix has been provided after detailed analysis of crash . The fix has been tested and changes have been committed.

CSCue80813—"Symptom:ACE not responding for short time when polled for snmp mibl ""get-request

1.3.6.1.4.1.9.9.480.1.1.7.1.1.2 1.3.6.1.2.1.1.3.0"" Workaround:stop polling mib ""get-request 1.3.6.1.4.1.9.9.480.1.1.7.1.1.2 1.3.6.1.2.1.1.3.0"""

CSCue07477—"Core was generated by hm (health monitor) process Conditions:when there's a change in the probe's connection status with large amount of HTTP/HTTPS probes applied across multiple context. For Example: When the probe connection is in closing/opening/resetting/receiving data state. Workaround: unknown"

CSCuf93726—ACE reloading with last boot reason: Service **"**cfgmgr**"**Workaround:None so far

CSCug57800—ACE crashed with last boot reason as snmp Workaround:ACE recovers with a reboot.

CSCuh34988—"Certain IP sticky entries are not synced to standby ACE (show ip sticky database are different for primary and standby ACE)"

CSCug82161—ACE reloading with last boot reason: Service **"**cfgmgr**"**

CSCue56293—ACE is vulnerable to CVE-2013-0169 "Lucky Thirteen" TLS/DTLS attack. Workaround :None.

CSCua81138—ACE30 not inserting SSL session ID. Workaround : Remove the session cache timeout.

CSCui59155—ACE30 running A5(2.2) crash last boot reason ifmgr with signal 6. Workaround: None.

CSCui56373—The ACE may crash on several control plane processes, like arp_mgr, cgmgr, snmpd. This defect tracks the upgrade of ACE30 toolchain needed in order to address these crashes. Workaround: None.

CSCuh30270—"Cisco Application Control Module (ACE) may accept a non-CA certificate under certain configurations". Configuring a line using a CA certificate and afterwards changing the "respsigncert" for the same OCSP server will cause ACE to accept the non-CA certificate. Workaround: None.

CSCui59183—Changes done in A5x kernel and MTS driver to address crash issues.

CSCuh31912—ACE 30 module crashed and reloaded. Last boot reason: Service "arp_mgr".

Files generated:

```
debug_history.tar.gz
arp_mgr_log.1057.tar.gz
```

CSCuj24550—SSH to ACE (A5.x) fails from IOS switch/Router. Conditions:User trying to connect to ACE module using SSH from IOS switch/router. Workaround: Use Putty/Secure CRT as a SSH client.

CSCum24308—"show IPv6 neighbors" output is showing wrong VLAN in Bridge mode.

CSCtu20125—”ACE reloads after SUP switchover. Conditions: When active SUP2T is removed from the chassis, then standby SUP2T becomes active. This causes diagnostic failures and ACE reloads. Workaround: Use Soft switchover command for carrying out switchover between active and standby SUP2T.”

CSCua85445—When multiple snmpwalk request is made along with LB traffic for extended hours ACE seems to crash with the reason NP 4 Failed: NP ME Hung

CSCuf87619— snmpd crashed two times in A520 renumbered build, please find back trace of both core files.

CSCug24208—cfgmgr crash with certain configs in A5(2.0).

CSCuh42954—While sending TLS1.2 ipv6 EE in context request i am seeing NP ME Hung Crash.

CSCug78717—Seeing ME Dumper Process Crashed? in A530 #42 with SSl v3 configs while running the codenomicon script. Please find the core pcap and config in enclosures.

CSCtz96319—ACE crashes while doing checkpoint rollback on a config having user 'Admin' in non-default domain.

CSCui49546—ACE crashes while doing checkpoint rollback on a config having user 'Admin' in non-default domain. FT GOING TO COLD STATE AFTER KILL THE SYSINFO SIGNAL 11

CSCug44749—"conc-conn" traps are not generated for Per Rserver and per VIP

CSCuh14830—ACE is sending malformed packet as a part of handshake message instead of certificate request when configured with TLS version 1.2 FE with authgroup.

CSCuh54020—When ACE is configiured in BE with highest version as TLS1.2 and server is running on TLS1.1, ACE is sending CSS message with TLS1.2.

CSCug10938—Seeing CfgMgr Crash when configuring basic lb in both ipv4 and ipv6 in multiplcontext with ft setup

CSCui12087—Regex check for hex-data with offset is not working correctly.

CSCud87906—Service "snmpd" crash is seen in Active Module.

CSCud89210—”http probe getting failed with “”unrecognized response”" when hm-strict- parsing is set as 1 and if hash value is configured under the probe config. But the same probe is getting passed when hm-strict-parsing is set as 0. Logs are attached as logs-issue-hash.same behavior is also seen in https probe.”

Software Version A5(3.0) Open Caveats

The following open caveats apply to software version A5(3.0):

CSCtr62421—last boot reason: System low memory detected workaround: None

CSCue30486—"An incorrect regex built-in variable pattern for header insert causes a crash in A521 Workaround:Correct the pattern. If a ""%"" character is to be inserted as a regex string, it should be inserted as ""\%"""

CSCug27629—"As the Access Control List (ACL) configuration is modified it is sometimes seen that an ACL merge error will be reported on one or more of the interfaces where the ACL list is applied. This leaves the interface in an inconsistent state.Workaround:

1. Remove the offending lines one at a time until the ACL can be applied successfully.
2. Remove the offending lines and try a different line number
3. Reload the ACE.

CSCui56373—Upgrade of ACE30 toolchains.

CSCul64560—"ACE 30 running A5(2.1f) crash with NP ME hung, Ace crashed for it is reading a bogus value for the reassembly timer. Conditions: A bogus value is read for the reassembly timer. Workaround: None".

CSCuj43444—"SSL termination connection breaks when uploading a file via HTTP POST When the client sends POST to upload a file, Front and Backend simultaneous traces show that the back-end connection has much less bytes transferred to the back-end server. Server responses with HTTP bad request before POST completes and sends a reset".

CSCul44877—ACE30 crash with last boot reason: Unhandled kernel unaligned access.

CSCul99139—startup-config is not synced during bulk-sync. Conditions: This symptom may be observed when ACE boots up.

CSCum36871—ACE-30 crash A5(2.2b) / ME Dumper Process Crashed last boot reason: ME Dumper Process Crashed.

CSCum41871—ACE-3-251014 message output wrong port#. Conditions: This symptom maybe observed when rserver is configured with port# in serverfarm. Workaround: None.

CSCug01673—High NP Buffer usage on all the NPs on ACE30 for A4.x and A5.x code trains.

CSCug27629—"As the Access Control List (ACL) configuration is modified it is sometimes seen that an ACL merge error will be reported on one or more of the interfaces where the ACL list is applied. This leaves the interface in an inconsistent state. Conditions: The dynamic configuration of ACLs lists within a context

Workaround:

1. Remove the offending lines one at a time until the ACL can be applied successfully.

2. Remove the offending lines and try a different line number

3. Reload the ACE.

CSCui02937—"Bandwidth resource denies occur prior to hitting maximum when the global pool is in use. Conditions: Modifying resource classes multiple times. Workaround: Reboot to allow resource pools to re-carve."

CSCuj91023—ACE A5(2.x) is unable to handle Split SSL Records when using HTTPS Probes on Windows Server 2012 (IIS Server).

CSCul26857—"ACE30 with software version A5(2.1e) got rebooted with log entry""Unhandled kernel unaligned access"" and also crash file has been generated , after the reboot , device comes up it works fine without any issues."

CSCul39399—"Some messages are missing in 'show logging' output even though all messages are sent to the syslog server successfully."

CSCul55184—Client Cert Authentication Failure.

Seeing following types of failures in the packet captures:

SSL alert CERTIFICATE_REVOKED sent

SSL alert CERTIFICATE_UNKNOWN sent

Workaround: Add the following in the SSL Parameter-map ""authentication-failure ignore""

CSCul90247—"SSL termination configured on ACE. ACE sending RESET after sending encrypt alert even after decrypting the packet"

Software Version A5(3.0) Command Changes

Table 7 lists the command changes in software version A5(3.0).

Note For a summary of new features for software version A5(3.0), including the associated new or modified commands, see the "Important Considerations for A5(x) Release" section.

Table 7 CLI Command Changes in Version A5(3.0)

Mode	Command and Syntax	Description
Configuration	**send-data and expect regex**	The **send-data** and **expect regex** CLI commands are configured to accommodate the configuration of Hex data. If Hex data configured is "ae5530"(6 bytes) then the converted value will be Hex ae,55,30 (3 bytes). See the "Chassis, Supervisor Engine, and Cisco IOS Support for the ACE30 Module" section for more details
Configuration	**modify http**	The **modify http** command is used to rewrite configured regex patterns in the HTTP response data.See the "Enhancements in HTTP Content Rewrite" section for more details.
Configuration	**show resource monitor-params**	The **show resource monitor-params** CLI command is used for displaying 1 min and 5 min average of the utilization parameters See the "Updates to Resource Parameter Monitoring" section for more details.
Configuration	**fixed encap-id**	The **fixed encap-id** CLI command allows you to configure the fixed encap entries for the configured VMAC, active and standby MACs in an active-standby redundancy setup with Virtual MAC configuration setup. See "Ability to Configure Fixed Encap IDs for Active-standby redundancy setup with Virtual MAC configuration" section for more details.
Configuration	**fragment timeout**	The **fragment timeout** CLI command is used to configure the fragment timeout in seconds. See Ability to Configure Fragment Timeout in Milliseconds"for more information.
Configuration	**show tech**	The **show tech** CLI command is used to configure the automatic capture of Exec command mode output. See "Automatic Capture of Exec Command Mode Output" section for more details.
Configuration	**show np x lb-stats**	The **show np x lb-stats** command is used to capture complete output of the LbInspect tool. See "Ability to Capture the Complete Output of the LbInspect tool" section for more details.

Related SNMP Changes for A5(3.0)

Per bug CSCtt13316, the following MIB objects have been added to the CISCO-SSL-PROXY-MIB:

- cspTl1cFullHandShake OBJECT-TYPE

  SYNTAX Counter32

  MAX-ACCESS read-only

  STATUS current

  DESCRIPTION

  "This object indicates the total number of full TLS 1.1 handshakes completed.”

  ::= { cspTls11Counters 1 }

- cspTl1cResumedHandShake OBJECT-TYPE

  SYNTAX Counter32

  MAX-ACCESS read-only

  STATUS current

  DESCRIPTION

  "This object indicates the total number of resumed TLS 1.1

  handshakes completed."

  ::= { cspTls11Counters 2 }

- cspTl1cHandShakeFailed OBJECT-TYPE

  SYNTAX Counter32

  UNITS "number of connections"

  MAX-ACCESS read-only

  STATUS current

  DESCRIPTION

  "This object indicates the total number of TLS 1.1 connections failed in handshake phase."

  ::= { cspTls11Counters 3 }

- cspTl1cDataFailed OBJECT-TYPE

  SYNTAX Counter32

  UNITS "number of connections"

  MAX-ACCESS read-only

  STATUS current

  DESCRIPTION

  "This object indicates the total number of TLS 1.1 connections failed in data phase."

  ::= { cspTls11Counters 4 }

- cspTl2cFullHandShake OBJECT-TYPE

  SYNTAX Counter32

  MAX-ACCESS read-only

STATUS current

DESCRIPTION

"This object indicates the total number of full TLS 1.2 handshakes completed."

::= { cspTls12Counters 1 }

- cspTl2cResumedHandShake OBJECT-TYPE

  SYNTAX Counter32

  MAX-ACCESS read-only

  STATUS current

  DESCRIPTION

  "This object indicates the total number of resumed TLS 1.2 handshakes completed."

  ::= { cspTls12Counters 2 }

- cspTl2cHandShakeFailed OBJECT-TYPE

  SYNTAX Counter32

  UNITS "number of connections"

  MAX-ACCESS read-only

  STATUS current

  DESCRIPTION

  "This object indicates the total number of TLS 1.2 connections failed in handshake phase."

  ::= { cspTls12Counters 3 }

- cspTl2cDataFailed OBJECT-TYPE

  SYNTAX Counter32

  UNITS "number of connections"

  MAX-ACCESS read-only

  STATUS current

  DESCRIPTION

  “This object indicates the total number of TLS 1.2 connections failed in data phase.”

  ::= { cspTls12Counters 4 }

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.