Release Note for the Cisco ACE 4700 Series Application Control Engine Appliance

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 4700 Series Application Control Engine (ACE) appliance.

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

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

This release note contains the following sections:

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

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-PRAM-MAP
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)

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 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 for A5(3.0)-Specific Features in ACE Appliance Device Manager GUI

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 **expect 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**.
- Users 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.

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 statefully 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 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.

Sample Output of Show Serverfarm Detail

Following are the sample output of “show serverfarm detail”. Here, the count under current represents the total active connections associated with the rserver. The count under total represents the total successful connections hit the rserver and this includes the count of current connection. The count under failure represents the total failed connections to hit the rserver.

```
switch/Admin# sh serverfarm SIP-sfarm detail

serverfarm     : SIP-sfarm, type: HOST
total rservers : 1
state          : ACTIVE
DWS state      : DISABLED
active rservers: 1
description    : -
predictor      : ROUNDROBIN
failaction     : -
back-inservice : 0
partial-threshold : 0
num times failover : 0
num times back inservice : 0
total conn-dropcount : 5

----------connections-----------
       real                 weight state        current    total      failures
```

```
---+--------------------+------+-----------+----------+----------+---------
rserver: s1
    46.100.100.10:0       8   OPERATIONAL     1          4          13
      sticky-conns         :                  0          0
      description          : -
      max-conns            : 2         , out-of-rotation count : 3
      min-conns            : 2
      conn-rate-limit      : -         , out-of-rotation count : -
      bandwidth-rate-limit : -         , out-of-rotation count : -
      retcode out-of-rotation count : -
      inband HM out-of-rotation count : -
      buddy_group          : -
```

Support for A5(3.0)-Specific Features in ACE Appliance Device Manager GUI

With the A5(3.0) software release, the ACE appliance Device Manager GUI includes support for:

- Support of Hex data in TCP / UDP Probe Send-data and Expect Regex
- Enhancements in the HTTP Content Rewrite
- Support of TLS1.1 and TLS1.2
- FTP SLB IPV6 Support
- Updates to Resource Parameter Monitoring
- Ability to Configure the Reassembly Timer Interval
- Automatic Capture of Exec Command Mode Output
- Ability to Allow SSL Record Parsing to a Specific Size
- Caching of snmp-get response for L4-L7 Resource Limit MIB

For details, refer to the *Device Manager GUI Guide, Cisco ACE 4700 Series Application Control Engine Appliance.*

Available ACE Licenses

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

- Performance: 1 gigabit per second (Gbps) appliance throughput
- Virtualization: 1 admin context and 20 user contexts
- Compression: 2.0 Gbps compression
- Secure Sockets Layer (SSL): 6500 transactions per second (TPS)
- Hypertext Transfer Protocol (HTTP) compression: 2 Gbps
- Application Acceleration: 105 connections

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

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

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

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

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

Ordering an Upgrade License and Generating a Key

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

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

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

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

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

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

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

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

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

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

For information on installing and managing ACE licenses:

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

Performing ACE Appliance Software Upgrades and Downgrades

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

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

Supported Browsers for ACE Appliance Device Manager

The ACE appliance Device Manager is supported on the following browsers listed in Table 3. All browsers require cookies and DHTML (JavaScript) to be enabled.

Table 3 Supported Browsers

Browser	Version	Client Platform
Microsoft Internet Explorer	IE 7.0	Windows XP Professional with Service Pack 2 or Windows Vista with Service Pack 1
	IE 8.0	Windows XP Professional with Service Pack 2, Windows Vista with Service Pack 1, or Windows 7
	IE 9.0	IE 9.0 Windows Vista with Service Pack 2 and Windows 7.
	IE 10.0	IE 10.0 Windows 8.
Firefox	20	• Windows XP Professional with Service Pack 2, Windows Vista with Service Pack 1, or Windows 7 • Red Hat Enterprise Linux 5

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.
- 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.

- 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 RDP load balancing is designed to only look for the routing token in the first packet of the client request once TCP connection is established. There is no ability like with HTTP cookies to look in subsequent packets for routing token.
- ACE increments the current connection counter when it sends the SYN to the rserver. Depending on the response of that it could also increment the total or failure counter. If the embryonic timer expires then the current connection is adjusted accordingly. This is reflected in the current connection and when the counter is incremented.
- ACE Fails to detect non-encoded special characters in the URL - This bug changes the default behavior to “URLs that contain RFC non-compliance characters will be dropped”. Earlier the ACE would allow these characters in url by default but now its required to enable “parsing non-strict”. Even though this bug is mentioned in the Release Notes, this needs to be documented/highlighted clearly so customers are aware of this change during upgrade to A5(2.2) or later.
- When a AAA server is marked down, the ACE will use the test user to authenticate every dead-time interval. The authentication is not expected to be successful: any response, even a unsuccessful one, is good enough to confirm that the server is backed up.
- Starting with software version A4(1.0), the default connection inactivity timeout settings for the ACE have changed to the following values:
  - ICMP—2 seconds
  - TCP—3600 seconds (1 hour)
  - HTTP/SSL—300 seconds
  - UDP—10 seconds

  The default HTTP and SSL ports (80 and 443) now have a default inactivity timeout of 300 seconds.
- During an upgrade in a redundant configuration, we recommend that you do not run the two ACE appliances 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 appliances are 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.
- 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.
- Starting with software version 4(2.0), the maximum number of concurrent connections for optimization is reduced to 100 connections. If the ACE startup configuration contains the **concurrent-connections** command in optimize configuration mode, consider the following:
  - If you upgrade the ACE from a version earlier than A4(2.0), the ACE software ignores the configured command and sets it to 100 connections.
  - If you downgrade the ACE to a version earlier than A4(2.0), the command is removed from the startup configuration and you must reconfigure it after the downgrade process is completed.
- It is no longer necessary to configure a resource class in the Admin context to allocate resources for stickiness. You can still allocate sticky resources if you wish, but skipping this step will not affect sticky functionality.
- When redundant ACEs lose connectivity, for example due to a network interruption, and they attempt to reestablish their connection, if you enter the **show ft** command during this time, the response for this command may be delayed.
- In a redundant configuration, dynamic incremental sync is a form of config sync that copies configuration changes that you make on the active ACE to the standby ACE when the two ACEs are running the same version of software and when both ACEs are up. When you upgrade from one major release of ACE software to another major release (for example, from A3(2.7) to A5(1.0)) or later, dynamic incremental sync is automatically disabled only while the active ACE is running software version A5(1.0) and the standby ACE is running software version A3(2.7). See Table 4.

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

Table 4 Redundancy Feature Availability Between Major ACE Software Versions

Platform	Active	Standby	Bulk Sync	Incr Sync	Conn Repl	Sticky Repl	Operation	Comments
Appliance	A3(x)	A5(x)	Yes	No	Yes	Yes	Upgrade	—
Appliance	A4(1.x)	A5(x)	Yes	No	Yes	Yes	Upgrade	—
Appliance	A4(2.x)	A5(x)	Yes	No	Yes	Yes	Upgrade	—

Table 4 Redundancy Feature Availability Between Major ACE Software Versions

Platform	Active	Standby	Bulk Sync	Incr Sync	Conn Repl	Sticky Repl	Operation	Comments
Appliance	A5(x)	A3(x)	Yes	No	Yes (IPv4 flows)	Yes (IPv4 flows)	Downgrade	Standby supports only IPv4
Appliance	A5(x)	A4(1.x)	Yes	No	Yes (IPv4 flows)	Yes (IPv4 flows)	Downgrade	Standby supports only IPv4
Appliance	A5(x)	A4(2.x)	Yes	No	Yes (IPv4 flows)	Yes (IPv4 flows)	Downgrade	Standby supports only IPv4

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

  When redundancy peers run on different version images, the SRG compatibility field of the **show ft peer detail** command output displays WARM_COMPATIBLE instead of COMPATIBLE. When the peer is in the WARM_COMPATIBLE state, the FT groups on standby go to the STANDBY_WARM state instead of the STANDBY_HOT state.
- The 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 appliance.
- 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.
- If you are using the Application Networking Manager (ANM) to manage an ACE appliance 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.
- 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 binary from the same location where ACE images are available for download.

  ACE Appliance: ACE4710_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:ACE4710_A5x_bash_security_fix.bin
     ```

     The dplug will install the fix and exit.

     ```
     switch/Admin# load image:ACE4710_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.

ACE Documentation Set

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

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

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

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

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

Document Title	Description
Release Note for the Cisco 4700 Series Application Control Engine Appliance	Provides information about operating considerations and caveats for the ACE.
Getting Started Guide, Cisco ACE 4700 Series Application Control Engine Appliance	Describes how to use the ACE appliance Device Manager GUI and CLI to perform the initial setup and configuration tasks.
Upgrade/Downgrade Guide, Cisco ACE 4700 Series Application Control Engine Appliance	Describes how to perform the following ACE software upgrade/downgrade tasks: • Upgrade scenarios • Effects of upgrading or downgrading • Ordering an upgrade license and generating a key • Upgrading your ACE software in a redundant configuration • Downgrading your ACE software in a redundant configuration

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

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

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

Document Title	Description
Administration Guide, Cisco ACE Appliance 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
Application Acceleration and Optimization Guide, Cisco ACE 4700 Series Application Control Engine Appliance	Describes the configuration of the application acceleration and optimization features of the ACE. It also provides an overview and description of the application acceleration features and operation.
Cisco 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.
Routing and Bridging Guide, Cisco ACE Application Control Engine	Describes how to perform the following routing and bridging tasks on the ACE: • Ethernet interface ports • VLAN interfaces • IPv6, including transitioning IPv4 networks to IPv6, IPv6 header format, IPv6 addressing, and supported protocols • Routing • Bridging • Dynamic Host Configuration Protocol (DHCP)

Document Title	Description
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 tasks on the ACE: • Real servers and server farms • Class maps and policy maps to load balance traffic to real servers in server farms • Server health monitoring (probes) • Stickiness • 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) tasks 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.
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.

For detailed configuration information on 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.

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.

  - In earlier versions, snmpget requests for objects in L4-L7 Resource Limit MIB used to time out intermittently due to more time taken for read operations. To resolve this, caching mechanism has been implemented in A5(3.0). The 15 seconds delay has been introduced for the snmpget bulk requests.
  - In CSCuu39811, disabling the cache option has been provided to get a faster response. By default the cache is enabled and the CLI provides an option to disable the cache.
  - A new CLI "get-request-cache-disable" is added under the token "snmp-server" to disable the cache i.e. the15 secs delay (To know more on the caching mechanism implementation please refer this link http://www.cisco.com/c/en/us/td/docs/app_ntwk_services/data_center_app_services/ace_appliances/VA5_3_x/release/note/ACE_app_rn_A53x.html#pgfId-907398). So once the CLI "snmp-server get-request-cache-disable" is configured and a bulk of snmpget is sent to ACE, the updated information is returned immediately.

- **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 that is affected by the vulnerability identified by the Common Vulnerability and Exposures (CVE) ID:
  - CVE-2015-4595
- **CSCuv36100**—The Logjam Vulnerability has been addressed by disabling the related ciphers. The following are the disabled ciphers:
  a. TLS_DHE_RSA_WITH_AES_128_CBC_SHA
  b. TLS_DHE_RSA_WITH_AES_256_CBC_SHA
  - The Mozilla Firefox will disable the weak ciphers (mentioned above) in the version 39 or above. The DM 5.3.3 will work with the Mozilla Firefox version 39 or above with the fix to disable the ciphers. However in the older versions of Mozilla Firefox, we will be seeing the impact as there is no cipher overlap supporting these ciphers. Hence, login screen may not appear. Additionally, if the below versions of DM (A5.3.2 and below) are used in the Mozilla Firefox version 39 or above, it will result in the weak DHE Key being used for Handshake, and hence the login page may not appear.
  - For new configurations, these will not be valid ciphers to put into the command and an error will be the result due to failed Handshake if the valid ciphers are not used.

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.
- **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.

- **CSCur27691**—CVE-2014-3566 related to Poodle vulnerability has been fixed in DM release 5.3.1.

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 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):

- **CSCuo24300**— DM 5.3.1 Purge Sticky information
- **CSCup39438**— New feature to support TLS_RSA_WITH_AES_128_CBC_SHA256 in DM
- **CSCup11314**— Standby ACE GUI does not reflect SNMP user change.
- **CSCuo34438**—ICMP probe works fine in admin context but it fails in other context. All contexts are having same VLAN as dedicated management VLAN but different IP. "show acl-merge acls vlan 108 in" shows data only for admin context but not for other context. show acl-merge acls vlan 108 in`. 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, workaround should be applied again afterwards.

- **CSCul39399**—Some sylog messages are missing in 'show logging' even though all messages are sent to the syslog server successfully. Workaround: None.
- **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.
- **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.
- **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".
- **CSCup80089**—ACE4710 crashed running A5(3.0) code and created four core files:np1_hw_state, np1_crash.txt.gz, np1_core.bin.tar.gz, and outstanding_syslogs. Workaround: Block multicast fragmented packets thru ace via ACL or other means.
- **CSCuq30645**—Syslog to inform hash collision while adding VIP IP in "icmp-vip" table.
- **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.

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 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(3.0):

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—"Fail-over between active and standby ACE registered. Workaround:None"

CSCty11329—"ACE appliance primary and standby units rebooted and created core files incfgmgr process while configuring class-map Workaround:A4x does not have this issue"

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.

CSCug51467—"ACE intermittently rejects valid SSL certificates as revoked during the difference hours between timezones in CRL ""Next update"" and on the ACE itself.Workaround: As workaround a parameter map with ""cdp-errors ignore"" command can be configured."

CSCug93530—ACE FT behavior with equal priorities. one with highest IP address always elected as ACTIVE.

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).

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

CSCui59155—ACE30 running A5(2.2) crash last boot reason ifmgr with signal 6. 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

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.

CSCui38998—"FT sync does not happen as well as loss of network reachability in some contexts <B>Conditions:</B> If we go past the string limit of the port-channel interface vlan configuration <B>Workaround:</B> Workaround 1:Remove ""extra "" correct vlans and then try sync. Once sync successfully completes readd the vlans.However if device reloads, remove the 'extra, truncated' vlan , give sync and then add the ""extra correct"" vlans Workaround 2: consolidate the vlans. E.g Switchport trunk allowed vlan 1-4095 Workaround 2 is the preferred option."

CSCuj22959—"ACE 4710 running version A5(2.1) rebooted unexpectedly. Conditions: last boot reason: Service ""cfgmgr"""

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"

CSCuf25829—ACE 4710 config is lost. Workaround: Recover config from checkpoint or external archive."

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.

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

CSCuf35487—Unable to CERT in SSL Proxy.

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.

CSCue29552—Service "Tacacs Daemon" crash on Active Appliance.

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.

Software Version A5(3.0) Open Caveats

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

CSCul34480—Using IE 9 browser, user can create Virtual Server by using the existing Server Farm and existing HTTP Header Modify Action List. However, when you try to Create/Edit “Server Farm” and “HTTP Header Modify Action List”, IE 9 will display a Java Script error message “SCRIPT70: Permission Denied”. To overcome this error in IE 9 browser, the following steps needs to be followed:

- Workaround to create new Virtual Server by creating the NEW Server Farm and NEW HTTP Header Modify Action List in IE 9 browser:
  1. Navigate to **Config > Virtual Contexts > Load Balancing > Server Farm >** Add and create the Server Farm.
  2. Navigate to **Config > Virtual Contexts > Expert > HTTP Header Modify Action List >** Add and create the HTTP Header Modify Action List.
  3. Navigate to **Config > Virtual Contexts > Load Balancing > Virtual Servers >** Add and Deploy the Virtual Server by associating already created Server Farm and HTTP Header Modify Action under the Default L7 Load-Balancing Action.
- Workaround to create new Virtual Server by editing the existing Server Farm and existing HTTP Header Modify Action List in IE 9 browser:
  1. Navigate to **Config > Virtual Contexts > Load Balancing > Server Farm >** Select existing Server Farm and Edit it.
  2. Navigate to **Config > Virtual Contexts > Expert > HTTP Header Modify Action List >**Select an existing HTTP Header Modify Action and Edit it.
  3. Navigate to **Config > Virtual Contexts > Load Balancing > Virtual Servers >** Add and Deploy the Virtual Server by associating already edited Server Farm and HTTP Header Modify Action under the Default L7 Load-Balancing Action.
- Workaround to edit the existing Virtual Server by creating the NEW Server Farm and NEW HTTP Header Modify Action List in IE 9 browser:
  1. Navigate to **Config > Virtual Contexts > Load Balancing > Server Farm >** Add and create the Server Farm.
  2. Navigate to **Config > Virtual Contexts > Expert > HTTP Header Modify Action List >** Add and create the HTTP Header Modify Action List.
  3. Navigate to **Config > Virtual Contexts > Load Balancing > Virtual Servers >** Edit and Deploy the Virtual Server by associating already created Server Farm and HTTP Header Modify Action under the Default L7 Load-Balancing Action.
- Workaround to edit the existing Virtual Server by editing the existing Server Farm and existing HTTP Header Modify Action List in IE 9 browser:
  1. Navigate to **Config > Virtual Contexts > Load Balancing > Server Farm >** Select existing Server Farm and Edit it.

2. Navigate to **Config > Virtual Contexts > Expert > HTTP Header Modify Action List** >Select an existing HTTP Header Modify Action and Edit it.
3. Navigate to **Config > Virtual Contexts > Load Balancing > Virtual Servers** > Edit and Deploy the Virtual Server by associating already edited Server Farm and HTTP Header Modify Action under the Default L7 Load-Balancing Action.

CSCul76427—ACE: kernel crash "Unable to handle kernel paging request".

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, it's just a cosmetic issue."

CSCue79554—"TCP connections destined for SSL-Proxy VIP stuck in connection table in CLSRST state well beyond TCP IDLE timeout configured. Workaround: Switching over the the standby context will clear the CLSRST conns that got stuck until that moment, but new ones will continue to pile on on the newly active 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."

CSCui56286—The default configuration of OpenSSH through 6.1 enforces a fixed time limit between establishing a TCP connection and completing a login, which makes it easier for remote attackers to cause a denial of service (connection-slot exhaustion) by periodically making many new TCP connections.CVE-2010-5107 vulnerability seen on ACE4710.

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

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 5 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 "New Software Features in Version A5(3.1)" section.

Table 5 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 "Support of Hex data in TCP / UDP Probe Send-data and Expect Regex" section for more details

Table 5 CLI Command Changes in Version A5(3.0) (continued)

Mode	Command and Syntax	Description
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	**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 }
```

Software Version A5(3.0) System Log Messages

302032

Error Message `ACE-2-302032: POST Debug 2013:10:16 08:37:47:tcp_send_packet:1403, PktCount: 1, BufChLen: 24, Core#4, fp msg_flags: 0x0, proxyId: 43234, SEQ :  1990829414  , ACK: 0, TCP FLG:0x2`

Note Customers should only open TAC case if they notice any functional impact.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.