This article describes the ACE system logging facility, how to enable logging, and how to use system messages as troubleshooting tools.

Guide Contents
Main Article
Overview of ACE Troubleshooting
Understanding the ACE Module Architecture and Traffic Flow
Preliminary ACE Troubleshooting
Troubleshooting ACE Boot Issues
Troubleshooting with ACE Logging
Troubleshooting Connectivity
Troubleshooting ACE Appliance Ethernet Ports
Troubleshooting Remote Access
Troubleshooting Access Control Lists
Troubleshooting Network Address Translation
Troubleshooting ACE Health Monitoring
Troubleshooting Layer 4 Load Balancing
Troubleshooting Layer 7 Load Balancing
Troubleshooting Redundancy
Troubleshooting SSL
Troubleshooting Compression
Troubleshooting Performance Issues
ACE Resource Limits
Managing ACE Resources
Show Counter Reference

Contents

- 1 Overview of ACE System Logging
- 2 Enabling ACE Logging
- 3 Logging Severity Levels
- 4 Adding Information to syslogs
- 5 Troubleshooting ACE Logging
  - 5.1 Displaying Logging Statistics
  - 5.2 Displaying the Logging History
  - 5.3 Displaying Logging Messages
  - 5.4 Displaying Logging Persistence
  - 5.5 Displaying the Logging Rate Limit

Overview of ACE System Logging

The ACE provides a system logging (syslog) facility that collects and saves system messages and outputs them to destinations that you specify as follows:

- Buffer
- Console
- Flash memory
- Host (remote syslog server)
- Monitor
- Standby
- Supervisor

Each virtual context generates logs independently from the other virtual contexts. The admin virtual context does not log on behalf of the other contexts in the ACE.

The ACE logs the following connection setup and teardown messages in the CP at the connection speed: 106023, 302022, 302023, 302024, and 302025. These setup and teardown syslogs are directly forwarded to a remote server. Because of the potentially large number of these messages or if you require high-rate system logging of connection setup and teardown messages, use the **logging fastpath** command. This command disables CP syslogs and enables logging of these messages through the DP using a slightly different format and the following syslog IDs: 106028, 302028, 302029, 302030, and 302031, respectively. You can log these messages through the fast path only to an external syslog server. All other enabled logging destinations are disabled by the **logging fastpath** command.

You can limit the rate at which the ACE generates syslog messages by using the **logging rate-limit** command. This command allows you to rate limit syslogs based on one of the following criteria:

- Time interval
- Logging level
- Message ID

Besides logging system messages, the ACE logs access control list (ACL) deny entries.

Note: Remember to enable logging on the standby ACE in a redundant configuration by entering the **logging standby** command. To log failover information on the standby ACE, you need to set the logging level to 4.

For details about ACE system message logging, see the *Cisco Application Control Engine Module System Message Guide (Software Version A2(1.0))*.

Enabling ACE Logging

To enable logging on the ACE module and send syslogs to the monitor, enter the following commands:

```
ACE_module5/Admin(config)# logging enable
ACE_module5/Admin(config)# logging monitor 7
ACE_module5/Admin(config)# logging trap 7
ACE_module5/Admin(config)# no logging message 111008
ACE_module5/Admin(config)# no logging message 111009
ACE_module5/Admin(config)# logging timestamp
ACE_module5/Admin(config)# do terminal monitor
```

Use the **logging monitor** *severity_level* command only when you are troubleshooting problems on the ACE or when there is minimal load on the network. Using this command at other times when the ACE is active may degrade performance.

Note: **logging trap** defines the severity sent to the syslog server.

Note: If you do not see syslog messages on the console after enabling logging with the **logging enable** and **logging monitor 7** commands, log out of the ACE and then log in again.

To enable logging to a syslog server, use the following command syntax:

logging host *ip_address* [**tcp** | **udp** [/*port#*]] | [**default-udp**] | [**format emblem**]

Note: If you specify the **default-udp** option and TCP logging fails, the ACE sends logging messages over UDP.

You can verify that the ACE defaults to UDP by entering the following command:

```
ACE_module5/Admin# show logging

Syslog logging:                 enabled
Facility:                       20
History logging:                disabled
Trap logging:                   enabled (level - debugging)
Timestamp logging:              disabled
Fastpath logging:               disabled
Persist logging:                disabled
Standby logging:                disabled
Rate-limit logging:             disabled (min - 0 max 100000 msgs/sec)
Console logging:                disabled
Monitor logging:                disabled
        Logging to 5.1.0.40 tcp/514    default-udp
        (sending on UDP)
Device ID:                      disabled
Message logging:                none
Buffered logging:               enabled (level - debugging) maximum size 681984
Buffer info: current size - 681984 global pool - 1048576 used pool - 1048576
                min - 0 max - 681984
                cur ptr = 42894 wrapped - yes
```

Use the **logging supervisor** command to allow the aggregation of critical syslogs from multiple virtual devices to the Catalyst 6500 series switch or to the Cisco 7600 series router syslog. For example, enter the following command:

```
ACE_module5/Context(config)# logging supervisor ?
 <0-7>  0-emerg;1-alert;2-crit;3-err;4-warn; 5-notif;6-inform;7-debug

cat6k# show logging
.
.
.
cat6k#17w3d: %TRINITY-7-TRINITY_SYSLOG_DEBUG:  %ACE-7-111009: User 'admin' executed cmd: show runn
```

Logging Severity Levels

The severity_level argument specifies the maximum level for system log messages sent to the console. The severity level that you specify indicates that you want syslog messages at that level and messages less than the level. For example, if the specified level is 3, the syslog displays level 3, 2, 1, and 0 messages. We recommend that you use a lower severity level, such as 3, since logging at a high rate may impact the performance of the ACE.

Allowable entries are as follows:

- 0?emergencies (System unusable messages)
- 1?alerts (Take immediate action)
- 2?critical (Critical condition)
- 3?errors (Error message)
- 4?warnings (Warning message)
- 5?notifications (Normal but significant condition)
- 6?informational (Information message)
- 7?debugging (Debug messages)

Adding Information to syslogs

After you have enabled system message logging and have specified a destination for the system messages, you can add more information to the system messages that may be helpful in troubleshooting issues with your ACE module. For example, you can do the following:

- Add a timestamp
- Identify the messages sent to a syslog server
- Identify the ACE device ID in messages that are sent to a syslog server

To add a timestamp to syslog messages, enter the following command:

```
ACE_module5/Admin(config)# logging timestamp
```

To identify messages that are sent to a syslog server by severity level, enter the following command:

```
ACE_module5/Admin(config)# logging trap severity_level
```

For example, to identify the ACE device ID in messages that are sent to a syslog server, use the following command syntax:

```
ACE_module5/Admin(config)# logging device-id {context-name | hostname | ipaddress interface_name |
```

Troubleshooting ACE Logging

The commands in the following sections are useful for troubleshooting the system message logging facility.

Displaying Logging Statistics

```
ACE_module5/Admin# show logging statistics

       Syslog statistics:  sent 349 discarded 64

               Messages sent:
                               console 0
                               buffer 348
                               persistent 0
                               supervisor 1
                               history 0
                               monitor 0
                               host 0
                               misc 0

               Messages discarded:
                               cfg rate-limit 0
                               hard rate-limit 0
                               server down 5
                               queue full 59
                               errors 0

               SNMP-related counters:
                               notifications sent 0
                               history table flushed 0
                               messages ignored 0

               NP-related counters:
                               to-CP dropped 0
                               fastpath sent 0
                               fastpath dropped  0


ACE_module5/Admin# show logging queue

       Logging Queue length limit : 80 msg(s), 59 msg(s) discarded.
       Current 0 msg on queue, 80 msgs most on queue

       CP messages received: 426       , 59 msg(s) discarded.
       IXP messages received: 82
       Xscale messages received: 0

       System Max Queue size: 20080
       System Free Queue size for allocation: 19920
```

In the above example, the ACE has discarded 59 control plane (CP) messages. By default, the syslog message queue can hold 80 messages. You can increase the size of the syslog message queue by using the **logging queue** command in configuration mode. Set the queue size before you start collecting syslog messages. When traffic is heavy, messages may be discarded if the queue size is too small. The maximum number of messages that the queue can hold is 8192.

Displaying the Logging History

To display the ACE logging history, enter the following command from the console:

```
ACE_module5/Admin# show logging history
syslog_trinity_show_history for context 0:
        1(Mar 24 2009 16:39:36): from "KERN" ACE-5-111008:User 'admin' executed the 'logging histo
        2(Mar 24 2009 16:39:48): from "KERN" ACE-5-111008:User 'admin' executed the 'logging consc
        3(Mar 24 2009 16:39:56): from "KERN" ACE-7-111009:User 'admin' executed cmd: do sho loggir
        4(Mar 24 2009 16:49:50): from "KERN" ACE-7-111009:User 'admin' executed cmd: do show loggi
        5(Mar 24 2009 16:51:35): from "KERN" ACE-4-405001:Received ARP REQUEST collision from 10.1
        6(Mar 24 2009 16:51:36): from "KERN" ACE-4-405001:Received ARP RESPONSE collision from 10.
        7(Mar 24 2009 16:51:40): from "KERN" ACE-4-405001:Received ARP REQUEST collision from 10.1
        8(Mar 24 2009 16:51:41): from "KERN" ACE-4-405001:Received ARP RESPONSE collision from 10.
        9(Mar 24 2009 16:54:46): from "KERN" ACE-7-111009:User 'admin' executed cmd: telnet 10.1.1
```

Displaying Logging Messages

If a particular system message does not appear in the syslog history, check that the message is enabled and that the logging level is correct for that message. To display the default logging level and the current status of a system message, all system messages, or disabled system messages, enter the following command:

```
ACE_module5/Admin# show logging message message_id | all | disabled
```

For example, to display all disabled system messages in the ACE, enter the following command:

```
ACE_module5/Admin# show logging message disabled
Message logging:
                message 111008: default-level 5 (disabled)
                message 111009: default-level 7 (disabled)
```

Displaying Logging Persistence

The **logging persistence** command enables logging to disk0: in Flash memory. The messages are stored in a subdirectory of disk0: called /messages.

To display logging persistence, enter the following command:

```
ACE_module5/Admin# show logging persistent
Persist info: current size - 6626 global pool - 1048576 used pool - 6626
                min - 0 max - 189582
                cur ptr = 6638 wrapped - no

Mar 24 2009 09:51:31 Admin: %ACE-4-405001: Received ARP REQUEST collision from 10.1.1.240 00.0c.29
Mar 24 2009 09:51:32 Admin: %ACE-4-405001: Received ARP RESPONSE collision from 10.1.1.240 00.0b.f
Mar 24 2009 09:51:36 Admin: %ACE-4-405001: Received ARP REQUEST collision from 10.1.1.240 00.0c.29
Mar 24 2009 09:51:37 Admin: %ACE-4-405001: Received ARP RESPONSE collision from 10.1.1.240 00.0b.f
```

Displaying the Logging Rate Limit

To display the logging rate limit, enter the following command:

```
ACE_module5/Admin# show logging rate-limit
Rate-limit logging:             (min - 0 max 100000 msgs/sec)
                100000 messages 1 seconds level 7
```