Launch Control System Master Console Event Message Reduction

Uyen Nguyen
Kennedy Space Center
Electrical Engineering
KSC FO Spring Session
09/04/2014

Launch Control System Master Console Event Message Reduction

Uyen Nguyen[1]
University of Central Florida, Orlando, FL, 32816

System monitoring and control (SMC) message browsers receive so many messages daily that operators do not need to see. Important messages are often mixed up among the less important ones. My job is to reduce the messages displayed in the message browser so that warning and emergency messages can be seen easily and therefore, responded promptly. There are multiple methods to achieve this. Firstly, duplicate messages should not appear many times in the message browser. Instead, the message should appear only once but with a number that counts the times that it appears. This method is called duplicate message suppression. Secondly, messages that update the most recent state (e.g. up/down) of a component should replace the old-state messages. This method is called state based message correlation. Thirdly, messages that display "normal" alarm level should be suppressed unless it's a response to an operator action. In addition to message reduction, I also work on correcting the severity level and text formats on messages.

Nomenclature

LCS	=	Launch Control System
LCC	=	Launch Control Center
SMC	=	System Monitoring and Control
COTS	=	Commercial-Off-The-Shelf
DA	=	Development Activity
F1R	=	Launch Control System Firing Room 1 Set
PWS	=	Portal Workstation
SNMP	=	Simple Network Management Protocol
GUI	=	Graphical User Interface
LDA	=	LCS Development Set A
HP	=	Hewlett-Packard Company
OMU	=	HP Operations Manager for UNIX
NNM	=	HP Network Node Manager
OID	=	Object Identifier
NC	=	Non Conformances
CMS	=	Common Services and Framework
ICMP	=	Internet Control Message Protocol

I. Introduction

THE System Monitoring and Control (SMC) is responsible for controlling, configuring, and monitoring various Launch Control System (LCS) hardware and software during launching events. SMC uses HP Commercial-Off-The-Shelf (COTS) software to maintain communication between the SMC components. SMC agents analyze the health and status of numerous machines and summarize it in the form of messages. The SMC agent then forwards this information to the SMC Management Server, where it will be stored, processed, and displayed to the operators via the SMC message browser. Messages can be formatted, correlated, and suppressed by using the HP Operations Manager for UNIX (OMU) and the HP Network Node Manager (NNM).

[1] KSC FO Intern, NE-C2, Kennedy Space Center, University of Central Florida.

II. Training

At first, I was given appropriate trainings for my tasks. On the first few weeks, I needed to familiarize myself with the system and software design documents so that I could fully understand how the whole system worked. I read the LCS Coding Standards to understand the different terminology that defined message severity. I also read the user guide that instructed me on how to use the HP COTS Admin Graphical User Interface (GUI).

III. Development Activity (DA) Assignment

The previous intern was working on a DA halfway. My job is to pick up where he left off. The DA has five parts. The first part addresses the problem with time delays in displaying messages. The second part mentions the incorrect severity and inconsistent verbiage in messages. The third part is about timestamp replacement when messages correlate. The fourth part states that failure messages are not displayed in the message browser. The fifth part talks about too many messages.

A. Time Delay

When a node or a network is turned off, red messages are supposed to appear in the message browser, like those shown in Fig. 1. The operators did receive messages that provided sufficient information about the nonfunctioning node. In case these messages are not received, NNM is configured to send secondary messages. I observed during a validation testing that on average, secondary messages took about 1 or 2 minutes to appear. Even though this shouldn't pose any serious problem, it's still desirable that messages should only take a few seconds to appear.

Severity	Dup.	SUIAONE	Time Last Received	Node	Application	MsgGrp	Message Text
Emergency		--X--X-	19:24:03 03/31/14	ldapws001	HP Operation...	OpC	Node ldapws001 is probably down. Contacting it with ping packages failed. (OpC40-436)
Emergency		--X--X-	19:20:16 03/31/14	ldapws001	HP Operation...	OpC	Failed to contact node ldapws001 with BBC. Probably the node is down or there's a network problem. (OpC40-191
Emergency	1	--X--X-	19:21:47 03/24/14	ldapws009	SNMPTraps	SMC_TRAP	Node or Connection Down
Emergency	1	--X--X-	19:21:27 03/24/14	ldands001	SNMPTraps	SMC_TRAP	Interface Down

Figure 1. Red messages take a few minutes to appear.

To troubleshoot this problem, I changed the Fault Polling Interval in the NNM GUI. The actual polling time should be 1 second. Simple Network Management Protocol (SNMP) Server sends Internet Control Message Protocol (ICMP) requests to each interface every 1 second and receives response from ICMP every 0.8 second. However, for testing purpose, I changed the polling time to 5 seconds for Ethernet and VLAN Interfaces, Routers, Networking Infrastructure Devices, Microsoft Windows Systems, Non-SNMP Devices, and Default Settings.

Then I tested the condition by pulling the utility cable off a Portal Workstation (PWS) in the LCS Development Set A (LDA). The messages still took a few minutes to appear. I did another test by enabling and disabling ICMP on the PWS to generate the message in Fig. 2. Before I changed the polling interval, it took 5 minutes for this particular message to appear. However, after I changed the polling interval, it only took about 1 minute to appear.

Severity	Dup.	SUIAONE	Time Last Received	Node	Application	MsgGrp	Message Text
Emergency	1	--X--X-	12:28:32 04/01/14	ldapws001	SNMPTraps	SMC_TRAP	Non-SNMP Node Unresponsive

Figure 2. Message generated by ICMP.

I talked to a member on the team about the testing results. He looked into the problem and found out that the default configuration for the polling frequency was still more than 1 minute, even though we changed the polling time to a few seconds. Currently, this problem is not solved because I'm working on the other parts of the DA. Now I know the source of the problem and hopefully, I can fix the error from there.

B. Incorrect Severity and Inconsistent Verbiage

The operators want to change the alarm level of the two messages shown in Fig. 3. The network message comes from the switch. Its severity is advisory. The host message comes from the PWS. Its severity is warning. Anytime an interface is down, the message's severity should appear as emergency to capture the attention of the operators.

Severity	Dup.	SUIAONE	Time Last Received	Node	Application	MsgGrp	Message Text
Advisory	1	-----X-	12:29:29 04/01/14	ldands001	smc_netconf...	SMC_AUTO	NETWORK UTIL IF DOWN: switch=ldands001 port=1:1 ifindex=1001
Warning	1	-----X-	12:29:29 04/01/14	ldapws001	smc_netconf...	SMC_AUTO	HOST UTIL IF DOWN: switch=ldands001 port=1:1 ifindex=1001

Figure 3. Messages with incorrect severity.

To change the severity, I modified a script in AccuRev. There are five LCS severities: normal, advisory, caution, warning, and emergency. I changed the severity of the network message from advisory to emergency. Likewise, I changed the severity of the host message from warning to emergency.

Inconsistent and vague verbiage also makes it hard for the operators to keep track of messages. There are several generic messages that are formatted differently but have the same meaning. For an example, "Node or Connection Down" and "Interface Down" generally state that a node is down but they do not provide any valuable information. The messages in Fig. 3 should replace those two messages because they provide more useful information like the switch number, the port number, and the interface index.

Each message has a unique Enterprise Object Identifier (OID). An OID is tied to a policy condition to match an incoming SNMP Trap, which is used by devices to report events to the SNMP Server when certain types of events occur. By knowing the OID, I can locate the policies in the NNM GUI. To stop the messages from being generated, I disabled the following policies in NNM: Duplicate Correlation, Interface Down, Node Down, and Node or Connection Down.

Then I tested the conditions by pulling the cable off a PWS. "Interface Down", "Node Down", and "Node or Connection Down" were successfully removed. However, "Duplicate Correlation…" messages were still generated. I talked about the testing results to a member of the team. He disabled another policy in NNM. This time, the duplicate correlation disappeared from the message browser. We know that this may be the source of the problem. Our next step is to contact the NNM group, telling them to disable the messages from their side. If they cannot do it, we will create a policy that automatically acknowledges the message and sends it to history.

What I have done so far is just for testing purpose. To implement the real changes, my mentor still needs to create a Work Order (WO). After the WO is approved, I can disable the policies permanently.

C. Correlation

To improve readability, I changed the wording of the message in Fig. 4. The first two messages in Fig. 5 are the modified versions of the message in Fig. 4.

Severity	Dup.	SUIAONE	Time Last Received	Node	Application	MsgGrp	Message Text
Advisory		-------	20:18:57 03/31/14	ldasmc001	smc_netconf...	SMC_AUTO	LINK EVENT (PID-541) ABORT: Failed to find ldancs001 9046 in hardware configuration map (/lcs/hwid/lda_hardware.x

Figure 4. Message's wording needs to be revised.

Severity	Dup.	SUIAONE	Time Last Received	Node	Application	MsgGrp	Message Text
Normal	1	-----X-	19:32:01 03/26/14	ldasmc001	smc_netconf...	SMC_AUTO	UNKNOWN HOST IF UP: switch=ldands002 ifindex=1007 failed to be found in set hardware configuration map (/lcs/hwid/lda_hardware.xml)
Emergency	7	-----X-	16:26:05 03/24/14	ldasmc001	smc_netconf...	SMC_AUTO	UNKNOWN HOST IF DOWN: switch=ldands002 ifindex=1005 failed to be found in set hardware configuration map (/lcs/hwid/lda_hardware.xml)
Normal		--XF-X-	14:09:45 03/20/14	ldancs002	SNMPTraps	SMC_TRAP	9026 Interface Up (linkUp Trap)
Emergency	6	--XF-X-	14:09:43 03/20/14	ldancs001	SNMPTraps	SMC_TRAP	9023 Interface Down (linkDown Trap)

Figure 5. Correlated messages.

Correlation is a process in which more informative messages acknowledge less useful ones and send them to history so that operators only see necessary messages in the message browser. My job was to correlate the four messages shown in Fig. 5. The first message and the second message correlate with each other. The first message correlates with the third one. The second message correlates with the fourth one.

I created new matching texts and message keys for two correlations under a SMC policy. I learned that the policy was very specific with certain characters. There should not be any space between the | symbol and the keywords. At first, I put MSG_NODE_NAME in the message keys, which are shown in Fig. 6. After a test failure, I realized that the two messages came from two different nodes; one was from SMC and one was from the switch. Therefore, one of them did not recognize MSG_NODE_NAME.

Figure 6. Wrong correlation, $MSG_NODE_NAME should not be included.

Under the same SMC policy, I also created a new correlation for "UNKNOWN HOST IF DOWN…" The correlation was the last one on the list. I did a test to see if the correlation worked. It failed. I looked into the trace file and found out that the message key did not match the key that I created in the policy. Apparently, the correlation grabbed the message keys from other correlations between "UNKNOW HOST IF UP…" and "UNKNOWN HOST

IF DOWN..." Therefore, I put the "UNKNOWN HOST IF DOWN…" on the top of the list so that it would be the first one to be matched from the list.

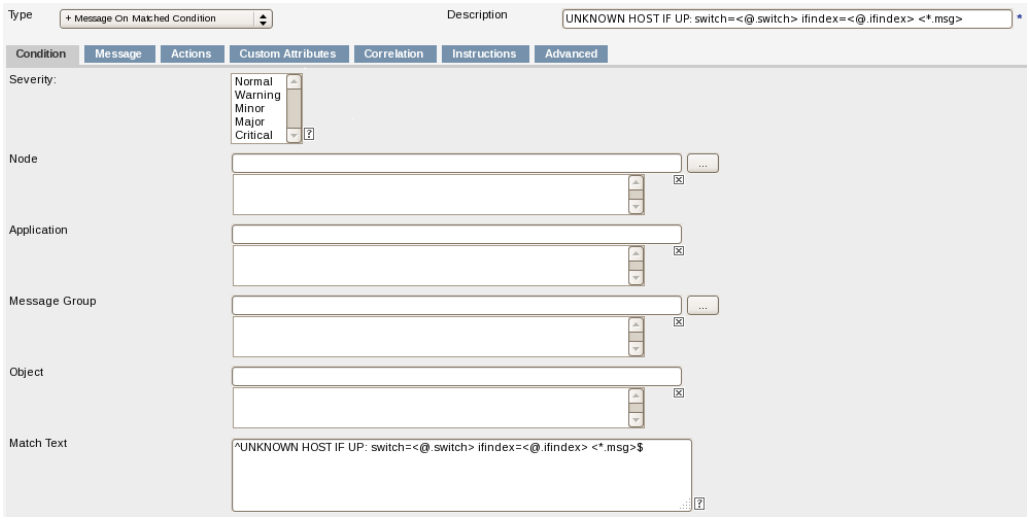

Figure 7. Modified matching text.

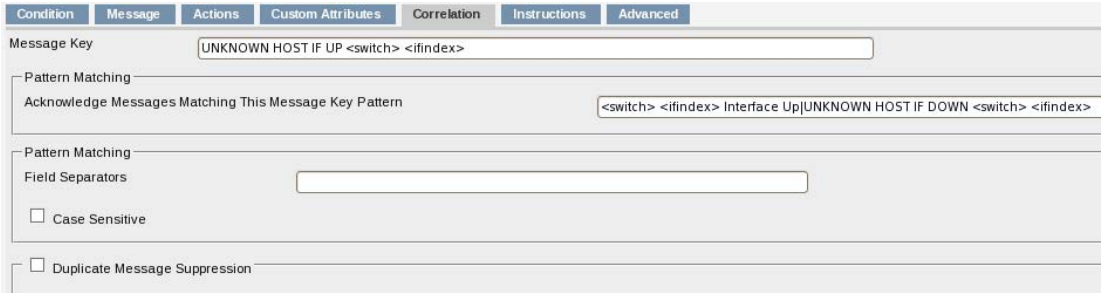

Figure 8. Modified message keys.

D. Timestamp Replacement

The operators complained that message correlation replaced timestamps of older messages, making it unable to determine the exact sequence of events and exact time of failures. This can be solved by clicking on message properties. Under Annotation section, it will list the acknowledged messages, their IDs and timestamps.

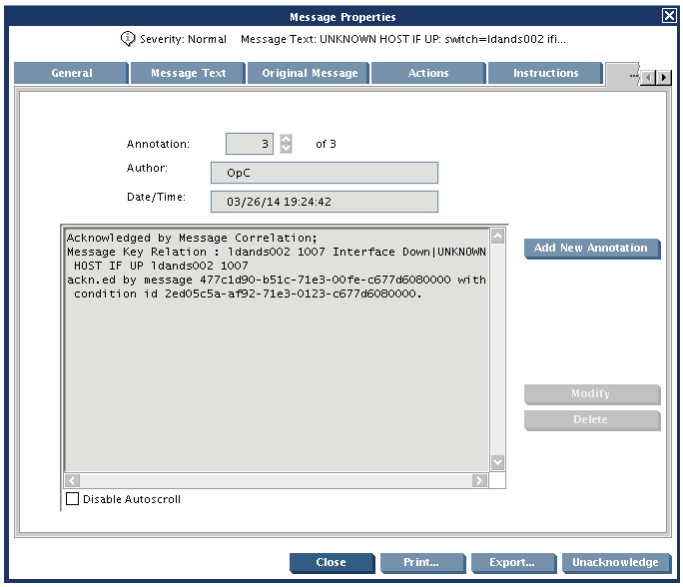

Figure 9. Date/Time box shows the timestamp of the acknowledged message.

E. Failure Messages

The operators also stated that failure messages were marked as normal and sent to history, instead of appearing in the message browser. I compiled a list of normal messages from the archived history of Launch Control System Firing Room 1 Set (F1R). I sent it to the operators so that they could point out the exact messages that they were referring to. They sent back two messages: "…Input voltage to AC power supply in slot 3 is off" and "…AC power supply in slot 3 is powered off".

Normal messages are often automatically acknowledged because they do not indicate an abnormal activity. To solve this problem, I will change the severity of the messages to other severities that are not normal.

F. Message Overload

The final part of the DA talks about message overload. The ultimate goal of my internship is to reduce the number of messages displayed in the message browser. So I asked the operators to give me a list of ten most annoying messages that I could fix during my internship. Some of these messages come from sendmail application. Sendmail is not used by either the operators or the SMC groups. Therefore, it was strange that we found it in the browser. I found out that an application called LogWatch caused sendmail to execute. LogWatch is not configured to run, so it uses its default setting by sending out emails. Sendmail is not configured to run either so it sends out error messages to syslog-ng, another application. SMC picks up messages from syslog-ng and display them on the browser. LogWatch will be removed to solve this problem.

I also needed to resolve one message from Common Services and Framework (CMS) application. After talking to the CMS group, I found out that this advisory message reports a single packet drop. It could not be removed from the message browser because it was necessary. The message is generated when the transmitting end sends more samples than the receiving end can accept. During normal operation, the transferring rate between the transmitter and the receiver should not differ but these messages only appeared during performance testing.

From talking to various people, I obtained the Non Conformances (NC) numbers for the redundant messages. Other groups were working on these problems. The NC numbers will be given to the operators as references.

IV. Conclusion

I've learned a lot from this internship. I learned that messages come from different sources. When an event occurs, several messages are sent to SMC. Sending several messages for a single event may seem redundant. However, it is important that the messages successfully reach the operators. For an example, whenever a PWS is turned off, there should be 3 messages sending to SMC Agent. One is from NNM Server; the other is from OMU; and the third one is from the switch. In case one of the three fails to send the message, we still have the other two.

I also learned that it's better to solve a problem from the source. If the problem is not solved from the source, it may return later and is harder to fix than before. For an example, if a message from the switch is not behaving correctly, I should trace to the root of the problem and ask the network group to fix it. Only if they cannot fix it, then SMC group can mask the message.

Acknowledgments

I would like to thank the following people for helping me during this internship. First, I would like to thank Dave Miller, who I worked most closely with. I'm grateful for his patience, time, and effort as he directed me through the whole process. He took the time to explain every single detail to me. As a result, I learned a lot from him. Secondly, I would like to thank my mentor, Dave Slaiman, for his counsel and guidance. I noticed that he was very organizational and thorough. From him, I learned to be precise and detailed in my observation and documentation. I appreciate that he took the time in his busy schedule to check on me and made sure if everything was alright. Lastly, I would like to thank Jolene Hall for helping me in the set. She readily came to my aid whenever I had any technical issues. She also took the time to escort me in and out the Launch Control Center (LCC).

References

HP Network Node Manager, Software Package, Ver. 9.11.004, Hewlett-Packard Development Company.

HP Operations Manager for Unix, Software Package, Ver. 09.11.040, Hewlett-Packard Development Company.