Intermittent MOSAIQ Disconnects

Thursday April 1st, 2010, 14:06:07 Citrix1

This narrative combines Josh's 'roll-up' (itself a combination of log messages from various devices) with a packet trace analysis plus firewall logs.

I begin analyzing a trace which spans ~11:45am to ~3:45pm, and focuses purely on Sequencer3 <==> Server Subnet traffic. (I filtered on ip.addr=={Sequencer3} and ip.addr=={server subnet/24).

All times, unless noted, reflect the time Sequencer3 reports (i.e. something pretty close to reality), rather than Sniffer Time, which is off from reality.

Sequencer3 enters this period with connections already built to Citrix1 and Citrix2.

[FYI: I have obscured Patient ID numbers as well as IP addresses. The Patient ID number was a critical string, which I used to sync the trace with the application logs. I haven't posted the application screen shots or the actual traces -- too much sensitive information in them. I realize that the loss of these inputs makes analyzing the issue difficult, perhaps impossible. I'm hoping that the basic feel of the issue remains -- the need to sync and then correlate input from multiple logs plus the packet trace, the need for understanding how the application works, its many components -- along with the dawning realization that the application, ClientVMI, was sustaining two simultaneous conversations with two different Citrix sessions: an unlikely configuration for an application controlling a single instrument. I also want to be clear that while I pulled the pieces together, I didn't do the work to gather the pieces: a crack team of domain experts understood where we were going, did the footwork to gather the information, and contributed the understanding I needed to produce this narrative. Kudos to Josh in particular for contributing the lion's share of the work and effort. --sk]

```
2079413      27626         4/01/2010 13:57:51:00  204          7 Field Change Warning
04/01/10 13:57:52:876       Program State
04/01/10 13:57:53:314       Setup targets copied
04/01/10 13:57:53:908       Setup targets copied
04/01/10 13:57:53:908       Entering field 7 for patient ID: UXXXXXXX

2079414      27626         4/01/2010 13:57:54:00  204          7:Verification Entry - Gantry Rx 215


04/01/10 13:58:09:329       Format Ready State
04/01/10 13:58:09:923       Beam enabled
04/01/10 13:58:10:501       Ready state
04/01/10 13:58:14:079       Beam on state
04/01/10 13:58:57:718       Complete state
04/01/10 13:58:57:718       MULog  ID:        UXXXXXXX  Set MU:63.9, Set Wedged MU: 0.0, Tgt MU:63.9
                            Beam on state        13:58:56        Actual MU: 63.0
                            Beam on state        13:58:57        Actual MU: 63.0
                            Complete state       13:58:57        Actual MU: 63.9
                            ID1: 27626  Fld#:     7  Mismatch:        0
                            D1 Sg. end
04/01/10 13:58:57:718       MLC A,B Leaf Values(all)...
                             1: -486, 504   2: -489, 506   3: -487, 500   4: -488, 501   5: -488, 499   6: -488, 501   7: -488, 499   8: -489, 495   9: -490, 500  10: -489, 496
                            11: -488, 500  12: -486, 500  13: -486, 501  14: -484, 502  15: -378, 602  16: -377, 602  17: -449, 602  18: -338, 531  19: -348, 511  20: -317, 432
                            21: -319, 441  22: -319, 441  23: -370, 392  24: -369, 388  25: -371, 390  26: -370, 388  27: -374, 392  28: -374, 390  29: -373, 390  30: -373, 389
                            31: -369, 392  32: -370, 394  33: -372, 393  34: -372, 394  35: -372, 393  36: -371, 392  37: -372, 393  38: -373, 395  39: -373, 395  40: -373, 394
04/01/10 13:58:57:843       Beam disabled
04/01/10 13:58:59:405       Cancelling TX Cycle because of field exit
```

```
2079420      27626         4/01/2010 13:59:02:00  204         7 : PostDHSForm MU:     63.9 FR: 1 OK: 1
2079421      27626         4/01/2010 13:59:02:00  204         7:RECORD TX NORMAL EXIT MU A/L/S    63.9    63.9     0.0
2079422      27626         4/01/2010 13:59:02:00  204         7    :13:58:15:32  2 1 10 639  215 0 2  50   50 2  37   60
2079423      27626         4/01/2010 13:59:03:00  204         100 Field Change Warning
2079425      27626         4/01/2010 13:59:06:00  204         100: No Field Dose TRT - No Continue
2079426      27626         4/01/2010 13:59:09:00  204         All Fields NOT Treated Warning
2079435      19000         4/01/2010 14:01:02:00  204         TxReadyCheck Inbound:OK To Continue
2079436      19000         4/01/2010 14:01:02:00  204         9:Field has changed since the last treatment
2079437      19000         4/01/2010 14:01:02:00  204         8:Field has changed since the last treatment
2079438      19000         4/01/2010 14:01:02:00  204         7:Field has changed since the last treatment
2079439      19000         4/01/2010 14:01:02:00  204         6:Field has changed since the last treatment
2079440      19000         4/01/2010 14:01:02:00  204         5:Field has changed since the last treatment
2079441      19000         4/01/2010 14:01:07:00  204         96 Field Change Warning
2079442      19000         4/01/2010 14:01:10:00  204         96 Yes on Warn:Field Delta display
2079443      19000         4/01/2010 14:01:13:00  204         96: PF Verification Entry

04/01/10 14:01:13:995       Data latch cleared
04/01/10 14:01:15:026       Program State
04/01/10 14:01:15:167       Beam disabled
04/01/10 14:01:16:854       Setup targets copied
04/01/10 14:01:16:854       Entering field 96 for patient ID: UYYYYYYY
```

Frame #174512 contains 'Entering field 96 for patient ID: UYYYYYYY' at Sniffer Time (ST) 13:58:27.688761
Data timestamp: 14:01:16:854 which suggests that this frame is in
fact the frame carrying the log line above, from ClientVMI running on Sequencer3 to MOSAIQ running on Citrix1
==> Sniffer lags Sequencer by 2 minutes 49 seconds

In Frame #184014 at 14:05:26, Citrix2 RSTs TCP Conversation 1888<==>50000 on Sequencer3.
Citrix2 and Sequencer3 then exchange a handful of RPCs on other ports (Synergistic?)

In Frame #184381 at 14:05:28, Cagvip RSTs TCP Conversation 443<==>2115 on Sequencer3
Normal behavior? Or part of the pathology?

In Frame #186499 at 14:05:58, Sequencer3 RSTs TCP Conversation 50000<==>1552 on Citrix1
Here are the corresponding hospital-fw entries:

```
Apr  1 14:05:58 hospital-fw %ASA-6-302014: Teardown TCP connection 385957132
for outside:{Sequencer3}/50000 to inside:{Citrix1}/1552 duration 1:02:28 bytes 2397021 TCP Reset-O
Apr  1 14:05:58 ga-b-fw-inside %ASA-6-302014: Teardown TCP connection 215972730
for outside:{Sequencer3}/50000 to inside:{Citrix1}/1552 duration 1:02:28 bytes 2396975 Failover primary closed
```

In Frame #186531 at 14:05:58, Citrix1 attempts to start a conversation with Sequencer3 3251 <==> 50000
Here is the corresponding hospital-fw entry for the SYN:

```
Apr  1 14:05:59 hospital-fw %ASA-6-302013: Built outbound TCP connection 3862
99512 for outside:{Sequencer3}/50000 ({Sequencer3}/50000) to inside:{Citrix1}/3251 ({Citrix1}/3251)
```

In Frame #186530, Sequencer3 responds with a RST (capture engine mis-ordered these two frames, ergo the 'backwards' frame numbers --sk)
Here is the corresponding hospital-fw entry for the RST

```
Apr  1 14:05:59 hospital-fw %ASA-6-302014: Teardown TCP connection 386299512
for outside:{Sequencer3}/50000 to inside:{Citrix1}/3251 duration 0:00:00 bytes 0 TCP Reset-O
```

04/01/10 14:05:59:122 Socket Connection with ClientVMI is lost

Note that Sniffer Time at this point is 14:03:10, which starts at Frame #208323

04/01/10 14:05:59:122 Socket Connection with ClientVMI is still lost - notifying SEQ
04/01/10 14:05:59:122 Socket Connection with ClientVMI is still lost - notifying SEQ
04/01/10 14:05:59:122 Socket Connection with ClientVMI is still lost - notifying SEQ
04/01/10 14:05:59:122 Socket Connection with ClientVMI is still lost - notifying SEQ

04/01/10 14:06:?? See 2010-04-01-MOSAIQ-Log-Screen-Shot.jpg for the User Audit Log. Notice in particular:
"Multi-Code Capture" at 14:06 (hard to say when this fits into this narrative, since the
timestamp does not include seconds. I'm inserting it here arbitrarily -- keep in mind that this
message may have been logged anytime between 14:06:00 and 14:06:59.)

04/01/10 14:06:02 According to the firewall, Citrix1 sends another SYN to Citrix1 on port 50000, re-using TCP Port 3251.
But this doesn't show up in the packet trace (filter on 'tcp.port==3251'). What box in the middle drops it? How relevant is this? Would Sequencer3 have responded with a SYN or would it have responded with a RST? In any case, this is the last time Citrix1 attempts to talk on this port until ~17:20.
Apr 1 14:06:02 hospital-fw %ASA-6-302013: Built outbound TCP connection 3862
99953 for outside:{Sequencer3}/50000 ({Sequencer3}/50000) to inside:{Citrix1}/3251 ({Citrix1}/3251)

In Frame #187190 at 14:06:09, Citrix1 initiates TCP Conversation 3252<==>135 with Sequencer3,
then negotiates an RPC relationship. Hypothesis: this is Synergistic traffic, which apparently
flows unmolested throughout the entire experience.

In Frame #187277 at 14:06:09, Sequencer3 emits an RPC to Citrix1 containing 'Patient Request'
In Frame #187229 at 14:06:09, Sequencer3 emits an RPC to Citrix1 containing 'Image Acquisition Request'
In Frame #187231 at 14:06:09, Sequencer3 emits an RPC to Citrix1 containing 'Image Acquisition Request'
In Frame #187237 at 14:06:09, Sequencer3 emits an RPC to Citrix1 containing 'Patient Request'
In Frame #187239 at 14:06:09, Sequencer3 emits an RPC to Citrix1 containing 'Image Acquisition Request'
In Frame #187231 at 14:06:09, Sequencer3 emits an RPC to Citrix1 containing 'Image Acquisition Request'

In Frame #181375 at 14:06:09, Sequencer3 ACKs TCP byte 6743 on TCP Conversation 2103<==>3649
[Why did this seem notable to me? --sk]

*04/01/10 14:06:07 *** Screenshot sent here! ****

2079466 19000 4/01/2010 14:06:10:00 204 96: PF Verification Exit
[Josh, per our exchange, I moved this line here. --sk]

04/01/10 14:06:10:169 Socket Connection with ClientVMI is still lost - notifying SEQ
04/01/10 14:06:10:232 Socket Connection with ClientVMI is still lost - notifying SEQ

Matt suggests that the following represents Synergistic traffic.
In Frame #187606 at 14:06:14, Citrix1 asks a question
In Frame #187607 at 14:06:14, Sequencer3 responds with 'Patient Request'
In Frame #187608 at 14:06:14, Citrix1 asks a question
In Frame #187609 at 14:06:14, Sequencer3 responds with 'Image Acquisition Request'
In Frame #187610 at 14:06:14, Citrix1 asks a question
In Frame #187607 at 14:06:14, Sequencer3 responds with 'Patient Request'
In Frame #187611 at 14:06:14, Citrix1 asks a question
In Frame #187613 at 14:06:14, Sequencer3 responds with 'Patient Request'

In Frame #187620 at 14:06:14, Citrix1 asks a question
In Frame #187621 at 14:06:14, Sequencer3 responds with 'Patient Request'
In Frame #187622 at 14:06:14, Citrix1 asks a question
In Frame #187623 at 14:06:14, Sequencer3 responds with 'Image Acquisition Request'
etc.

In Frame #188582 at 14:06:20, Citrix1 attempts to start a conversation (SYN) with Sequencer3 3257 <==> 50000
In Frame #188580, Sequencer3 responds with a RST (again, the capture engine misordered the frames)
Apr 1 14:06:20 hospital-fw %ASA-6-302013: Built outbound TCP connection 386301491 for outside:{Sequencer3}/50000 ({Sequencer3}/50000) to inside:{Citrix1}/3257 ({Citrix1}/3257)
Apr 1 14:06:20 hospital-fw %ASA-6-302014: Teardown TCP connection 386301491 for outside:{Sequencer3}/50000 to inside:{Citrix1}/3257 duration 0:00:00 bytes 0 TCP Reset-O

```
04/01/10 14:06:27:403       Socket Connection with ClientVMI is still lost - notifying SEQ
04/01/10 14:06:27:403       Socket Connection with ClientVMI is still lost - notifying SEQ
```

In Frame #189741 at 14:07:19, Cagvip RSTs TCP Conversation 443<==>2118 with Sequencer3

In Frame #189747, Sequencer3 shuts down TCP Conversation 2103 <==> 4293 with Citrix2
In ensuing frames, Citrix RSTs a range of conversations with Sequencer3

In Frame #189746 at 14:07:39, Sequencer3 ACKs byte 6744 on TCP Conversation 2103<==>3649 with Citrix1
This is a byte which the sniffer has not seen. Suggests that the Sniffer dropped the frame or that Sequencer3's TCP stack is confused.
In Frame #189746 at 14:07:39, Sequencer3 shuts down TCP Conversation 2103<==>3649 with Citrix1

In Frame #190970 at 14:11:00, Citrix1 initiates a TCP conversation (SYN) with Sequencer3 3465<==>50000
In Frame #190971, Sequencer3 accepts ... and thereafter, they build a successful conversation

Looks like things go back to normal.

```
04/01/10 14:11:00:652       Multi-ACCESS with ClientVMI...
04/01/10 14:11:01:870       Downloaded ClientVMI successfully
04/01/10 14:11:06:542       Successfully downloaded machine DLL \\appserver.hospital.org\mosaiq_app\vmi-uw\synergyc\vmi_icom.dll
04/01/10 14:11:06:960       DLL 'C:\IMPAC\vmi_icom.dll' loaded (version 56,0,0,13)
04/01/10 14:11:06:960       Thread priority set to 15
04/01/10 14:11:07:601       Initialized
04/01/10 14:11:08:257       iCOM on-line

2079495      19000         4/01/2010 14:11:39:00  204          TxReadyCheck Inbound:OK To Continue
2079496      19000         4/01/2010 14:11:39:00  204          9:Field has changed since the last treatment
2079497      19000         4/01/2010 14:11:39:00  204          8:Field has changed since the last treatment
2079498      19000         4/01/2010 14:11:39:00  204          7:Field has changed since the last treatment
2079499      19000         4/01/2010 14:11:39:00  204          6:Field has changed since the last treatment
2079500      19000         4/01/2010 14:11:39:00  204          5:Field has changed since the last treatment
2079501      19000         4/01/2010 14:11:42:00  204          96 Field Change Warning
2079502      19000         4/01/2010 14:11:48:00  204          96: PF Verification Entry

04/01/10 14:11:48:615       Data latch cleared
04/01/10 14:11:49:084       Beam disabled
04/01/10 14:11:51:521       Setup targets copied
```

```
04/01/10 14:11:51:521       Entering field 96 for patient ID: UYYYYYYY
```

Frame #195718 contains 'Entering field 96 for patient ID: UYYYYYYY' at Sniffer Time (ST) 14:09:02.323617
Data timestamp: 14:11:51:521

```
04/01/10 14:13:33:440       Beam disabled
04/01/10 14:13:34:002       Cancelling TX Cycle because of field exit

2079508      19000         4/01/2010 14:13:35:00  204          96: PF Verification Exit
2079509      19000         4/01/2010 14:13:38:00  204          CBCT: PF Verification Entry

04/01/10 14:13:38:830       Data latch cleared
04/01/10 14:13:39:299       Beam disabled
04/01/10 14:13:39:737       Setup targets copied
04/01/10 14:13:39:737       Entering field CBCT for patient ID: UYYYYYYY
04/01/10 14:17:22:808       Format Ready State
04/01/10 14:18:51:164       Program State
04/01/10 14:19:01:945       Cancelling TX Cycle because of field exit

2079586      19000         4/01/2010 14:19:04:00  204          CBCT: PF Record  MU =     0.0 Treat
2079587      19000         4/01/2010 14:19:11:00  204          CBCT: PF Verification Exit
2079588      19000         4/01/2010 14:19:11:00  204          96 Field Change Warning
2079590      19000         4/01/2010 14:19:14:00  204          96: No Field Dose TRT - No Continue
2079592      19000         4/01/2010 14:19:16:00  204          96 Field Change Warning
2079594      19000         4/01/2010 14:19:23:00  204          96: PF Verification Entry
04/01/10 14:19:23:038       Data latch cleared
04/01/10 14:19:23:491       Beam disabled
04/01/10 14:19:25:351       Setup targets copied
04/01/10 14:19:25:351       Entering field 96 for patient ID: UYYYYYYY
```

Frame #211492 contains 'Entering field 96 for patient ID: UYYYYYYY' at ST 14:16:36.145010
Data timestamp 14:19:25:351

```
04/01/10 14:19:59:849       Format Ready State
04/01/10 14:20:00:631       Beam enabled
04/01/10 14:20:01:974       Ready state
04/01/10 14:20:02:256       Beam on state
04/01/10 14:20:09:865       Complete state
04/01/10 14:20:09:865       MULog  ID:        UYYYYYYY  Set MU: 3.0, Set Wedged MU: 0.0, Tgt MU: 3.0
                            Beam on state        14:20:07        Actual MU:  3.0
                            Beam on state        14:20:09        Actual MU:  3.0
                            Complete state       14:20:09        Actual MU:  3.0
                            ID1: 19000  Fld#:    96  Mismatch:        1  (Type )
                            D1 Sg. end
04/01/10 14:20:10:068       Beam disabled
04/01/10 14:20:10:177       Data latch cleared
04/01/10 14:20:10:818       Program State

2079604      19000         4/01/2010 14:20:27:00  204          96: PF Record  MU =     3.0 Open
2079605      19000         4/01/2010 14:20:29:00  204          96: PF Verification Exit
2079606      19000         4/01/2010 14:20:34:00  204          97: PF Verification Entry
```