

DaPlan

Round Two of Data Gathering

Sunday 12-18-2005

OVERVIEW	2
OUTLINE	2
<i>BlueArc</i>	2
<i>Network Counters</i>	2
<i>Packet Traces</i>	2
CAVEATS	2
ASSUMPTIONS.....	2
OUTSTANDING ISSUES	3
SCOPE OF WORK.....	3
<i>In Scope</i>	3
<i>Out of Scope</i>	3
WHO.....	3
OWNER	3
TEAM.....	3
ROLES.....	4
<i>Tidal Monitor</i>	4
<i>Client Operator</i>	5
<i>Float</i>	6
<i>Indigo Sniffer</i>	6
<i>Admains Sniffer</i>	7
<i>Real-Time Watcher</i>	8
<i>Management Support</i>	9
PREPARATION.....	9
TIMELINE.....	9
ARRIVE.....	9
SDS TRAY	10
CAPTURE FIRST ROUND.....	10
CAPTURE SECOND & SUCCEEDING ROUNDS.....	10
CRD TRAY	10
CAPTURE FOURTH ROUND.....	10
CAPTURE FIFTH ROUND.....	11
BACK-OUT	11
FOLD UP THE TENTS.....	11

OVERVIEW

This document itemizes the steps which we will take on Sunday 12-18-2005 to gather data about the “minute of silence” issue.

Outline

We will initiate the pathology using Uncle Stewart’s Tidal jobs and then perform a range of data captures, first when the Tidal jobs are running against the SDS tray, second when the Tidal jobs are running against the CRD tray. I have the following strategies in mind:

BLUEARC

Using the BlueArc tools, we will capture the parameters which Robert has identified as relevant. From the graphs Robert produces, we may acquire additional insights into the cause of the “minute of silence” we have witnessed. Plus, this data may prove useful to BlueArc, as they work on confirming the cause of the “minute of silence”.

NETWORK COUNTERS

Using an in-house tool, we will capture Rx/Tx and error counters on port j4sr-a-esx:6/47 (Indigo’s port) and on all of the live ports on the Fibre Channel switches. I am guessing that this data will rule out the Fibre Channel network as a contributor to the “minute of silence”. Of course, it may not, in which case, we will likely want to dig deeper into analyzing the FC network.

PACKET TRACES

With sniffers inserted in front of Ana, Indigo, and admaims21, we will capture packet traces. The Ana traces will allow us to confirm the behavior we saw during the last big Sunday event, the Indigo traces will allow us to confirm or deny the theory that Indigo is blocking on a DNS/LDAP/NTLM call, and the admaims21 traces will allow us to dig deeper into the “file not found” issues which some SDS jobs experience.

Caveats

- We will likely run into potholes as we go and then deviate from DaPlan. “The Plan is nothing; planning is everything”.
- I recommend using headphones for the conference call -- reduces the background noise. However, speaker phones will work

Assumptions

- bluearc-x-av are disabled
- Running the Tidal jobs against the SDS tray will re-create the problem

Outstanding Issues

- Introduce Admains Sniffer to Ethereal

Scope of Work

IN SCOPE

During set-up, we will disable Indigo's second NIC and insert an in-line sniffer on Indigo's surviving NIC. We will also do this for admains21. We will replicate the problem, using test routines which Uncle Stewart has provided and then capture data on various components using various tools. We will store this data in the project directory tree. At the end, we re-enable the second NIC on Indigo and admains21 and remove both in-line sniffers.

OUT OF SCOPE

We will not change the production environment. We recognize that doing this may be tempting, particularly if we discover what we believe to be the cause of a problem ... but we resolve to resist this temptation and to pass proposed changes through the usual change control process next week instead.

SUMMARY

We will put everything back the way we found it.

WHO

Owner

Stuart Kendrick owns the event.

Team

The on-site team consists of:

<u>Person</u>	<u>Role</u>
Estella McDermott	Admains Sniffer
Jason Burdullis	Client Operator
Stuart Kendrick	Float
Rick Bawaan	Indigo Sniffer
Sonja Outlaw	Management Support
Robert McDermott	Real-Time Watcher
Susan Way	Tidal Monitor

Roles

From a high level, Client Operator leads a three-way dance, calling out the steps, with Indigo Sniffer and Admains Sniffer following. All three capture data from their three perspectives, saving it in a coherent manner. Tidal Monitor keeps the pathology going (i.e. keeps the pipe from SDS servers to Indigo full). Real-Time Watcher dances his/her own dance, aware of the activities of Tidal Monitor, but otherwise decoupled from what everyone else is doing.

I prefer using text files to record comments. However, if you prefer to use Microsoft Word or WordPad or whatever, please feel free.

I would like Client Operator, Indigo Sniffer, and Admains Sniffer to name their data files (traces and text files) using the same naming convention, namely their role name followed by a time stamp which the Client Operator will call out at the end of a dance routine. See the role descriptions for details.

TIDAL MONITOR

Overview

This is the person who manages the SDS procedures which we believe will degrade client/Indigo performance. This person's chief function is to launch Tidal jobs as needed, to remove the resulting files on Indigo as needed, and to report to the Client Operator on the state of Tidal jobs as needed. In addition, this person captures "netstat" output from admains boxes. Also, this person owns the PIR data capture process. Finally, this person is point on any Indigo care & feeding.

Details

The only data which this person captures is the output of "netstat" commands; please save this in the 'Tidal' directory.

I'm imagining that this person will perform other data gathering tasks ... perhaps watching parameters on Indigo using BlueArc-specific tools (watching the event log, perhaps). Perhaps running a 'tail -f grep indigo' on syslog. If Indigo logs a critical error message during this event, this person owns the task of investigating it, freeing up the rest of the team to continue their work.

This person communicates with the Client Operator, ensuring that the Client Operator knows the current state of the Tidal jobs. In general, this person will be 'keeping the pipe full', i.e. if a Tidal job completes, then s/he will likely launch another job. (Or perhaps re-launch a past job, taking care to erase the target file before doing so.)

At various points during the evening, this person captures the output of "netstat -e" and "netstat -s" on each of the admains boxes involved in Tidal jobs, storing the result in <\\sluff22\BlueHeat\Data\2005-12-18\Tidal>. Please name these files in some coherent fashion. e.g. netstat-2115-admains21.txt (i.e. 'netstat' to tell us the contents of the file, '2115' meaning 9:15pm, the time when the netstat output was taken), and 'admains21', the name of the box on which the 'netstat' was performed).

Directory

<\\sluf22\BlueHeat\Data\2005-12-18\Tidal>

Preparation

- Verify that the target directory on Indigo is empty (because robocopy won't overwrite a file if it exists and is complete).
- Practice initiating a Tidal job and verifying that the file lands where you expect it to land.
- Verify that you have Uncle Stewart's home number available, in case you need to consult.
- Record baseline "netstat -e" and "netstat -s" output

CLIENT OPERATOR

Overview

This person guides us through the paces, calling out the steps. This person runs the client (any Windows box) along with a sniffer (a Windows or Unix box with Ethereal installed on it). This person's primary function is to capture client-side packet traces at various points during the evening, coordinating these captures with the traces taken by Admains Sniffer and Indigo Sniffer. This person also determines the timestamp to be used when naming trace files.

Details

The Client plugs into a mini-hub (must be a hub, not a switch, borrow Stuart's NetGear mini-hub if you aren't sure). Sniffer One plugs into the mini-hub. The mini-hub plugs into the wall (and from there to j4-esx). Please verify that you are running the latest version of Ethereal: .10.13 (see <\\sluf22\vdops\utilities\network-analysis\Ethereal>). Also, please make sure that Sniffer One is a *faster* machine than the Client¹. Employ a capture filter on the MAC address of the client. Please simplify the client as much as possible: i.e. close all programs except for the command prompt, unmap all drives except for the one mapping to Indigo, etc. Do the same for Sniffer One. I recommend having a third box around so that you can perform "other tasks", like reading e-mail and working with a browser, etc.

The Client will copy a ten megabyte file to Indigo, using a DOS window and the 'copy' command:

```
c:\temp> timethis copy test-file.jnk h:\
```

Please save Ethereal files in CAP format (aka "Network Associates Sniffer (Windows-based) 2.00x" format), with a ".cap" extension (you have to add the .cap extension yourself; Ethereal won't do it for you, even when you select "Network Associates Snifer (Windows-based) 2.00x" from the drop-down File type menu).

¹ Strictly speaking, this step isn't really necessary ... a slow machine is still capable of capturing packets emanating from a faster machine, up to some limit. But I'd prefer to rule out any doubt about this, ergo my request that the Sniffer be faster than the client.

Trace Naming Convention:

Client-{timestamp}.cap

e.g. client-2015.cap

The trace above was stopped at 20:15, i.e. 8:15pm.

Directory

After each test, this person will save the trace file to <\\sluf22\BlueHeat\Data\2005-12-18\Client>. This person will also maintain a text file describing the traces (see 'Client-Traces.txt' in this directory) and recording the time it took to copy test-file.jnk.

Preparation

- Create a precise ten megabyte test file (use the creatfil.exe command from the Windows resource kit). Perform a 'dir' command and record the precise size of the file in bytes in your 'Client-Traces.txt' file.
- Verify that you have the "timethis.exe" program from the Windows resource kit
- Copy it from Indigo to the client PC five times and record how long it takes each time.
- Copy it from the client PC to Indigo five times and record how long it takes each time.
- Record the results in the 'Client' directory in the 'Client-Traces.txt' file.
- Practice configuring Ethereal to capture only on the client. Verify that this works by emitting Pings from the client to, say, spot, then stopping the capture and looking for the pings. You should see very little other than the Pings in the trace.
- Coordinate with Indigo Sniffer and Admains Sniffer to capture a baseline trace prior to 8:00pm.

FLOAT

Overview

This person floats during the event, available to trouble-shoot data capture issues, answer procedural questions, and to substitute should anyone get distracted by other issues.

INDIGO SNIFFER

Overview

This person will operate the Indigo-oriented sniffer, also called the "THG Notebook System" or the "Finisar pod", which will be placed in-line with Indigo. This person's chief function will be to capture packet traces from Indigo's point of view, at various points throughout the evening as determined by Client Operator.

Details

The Finisar pod is an external PCI expansion bus attached to the laptop "maya" via a high-speed serial cable. The pod contains a pair of specialized Ethernet NICs which are optimized for packet capture.²

² If the Finisar pod becomes unstable, we have a THG System screwed into the Indigo rack and ready to take over. It lacks the 'Capture-Disk' function of the pod, but otherwise is identical. The THG System consists of a PC stuffed

This person starts captures at appropriate times, watches the real-time throughput graphs for expected behavior (they should jump high whenever the Tidal jobs are running ... if they aren't, this person informs the Client Operator of this, as this indicates a problem), and saves traces at the end of each test to the Indigo directory, updating the text file there with comments.

Trace Naming Convention:

Indigo-{timestamp}.cap

e.g. indigo-2015.cap

Directory

<\\sluf22\BlueHeat\Data\2005-12-18\Indigo>

Preparation

- Verify that you know how to start a capture, stop a capture, save a file (to CAP format), copy the file to the 'Indigo' directory, and update the 'Indigo-Traces.txt' file.
- Verify that you know how to enable the 'Capture-Disk' feature.
- Coordinate with Client Operator to capture a baseline prior to 8:00pm.

ADMAIMS SNIFFER

Overview

This person will operate a sniffer capturing packets from the point of view of admaims21 at various points throughout the evening as determined by Client Operator.

Details

This person operates one of the Shuttle PCs ("apeman" or "caveman") remotely (via Remote Desktop Connection), capturing via an in-line tap on admaims21.

Please save Ethereal files in CAP format (aka "Network Associates Sniffer (Windows-based) 2.00x" format), with a ".cap" extension (you have to add the .cap extension yourself; Ethereal won't do it for you, even when you select "Network Associates Sniffer (Windows-based) 2.00x" from the drop-down File type menu).

Data File Naming Convention:

admaims-{timestamp}.cap

e.g. admaims-2015.cap

Directory

<\\sluff22\BlueHeat\Data\2005-12-18\Admaims>

into a rack-mountable form-factor, equipped with the exact same specialized NICs which are installed in the pod. It runs some version of Windows plus Finsiar's Surveyor. It is accessible via Surveyor, Protocol Expert (Fluke's OEMed version of Surveyor), or a Web browser.

Preparation

- Verify that you know how to start a capture, stop a capture, save a file (to CAP format), copy the file to the 'Admains directory, and update the 'Admains-Traces.txt' file.
- Verify that you know how to filter the capture using admains21's MAC address
- Coordinate with Client Operator to capture a baseline prior to 8:00pm.

REAL-TIME WATCHER

Overview

This person will run the in-house BlueArc Tools plus the in-house SNMP grabber tool, watching various parameters on Indigo , j4sr-a-esx, and bluearc-x-fsx in near-real-time. This person's chief function is to capture counter data. Secondly, this person's function is to observe near-real-time graphs, looking for correlations between them and the events occurring around the Client Operator and Indigo, and giving the rest of the team warning when we have entered a "minute of silence". This role is heavily decoupled from the rest of the team – s/he doesn't have to 'do' anything at any particular moment, doesn't have to coordinate any activities with anyone else ... s/he is watching and analyzing.

Details

See <\\sluf22\vdops\Utilities\Network-Analysis\WhatsUp> for the installer and a stack of patches. Alternatively, have a look at <\\sluf22\vdops\Utilities\Network-Analysis\Fluke\OPV-PEb256.zip> ... this package contains something called 'MG Browser' ... I've never used it, but I know that Mike Pennachi does. Same thing as WUG -- it graphs SNMP parameters in near-real-time.

Counters to watch on j4sr-a-esx: ifInOctets, ifOutOctets, ifOutDiscards
Port 6/47 = ifIndex.202

Port 6/47: ifInOctets.202, ifOutOctets.202, ifOutDiscards.202

Counters to watch on bluearc-x-fsx, ports ??? (this is a lot of graphs!)

swFCPortTxWords.1
swFCPortRxWords.1
swFCPortRxWords.2
swFCPortRxWords.3
swFCPortRxWords.4
swFCPortRxWords.5
swFCPortRxWords.6

swFCPortTooManyRdys.1
swFCPortTooManyRdys.2
swFCPortTooManyRdys.3
swFCPortTooManyRdys.4
swFCPortTooManyRdys.5
swFCPortTooManyRdys.6

swFCPortNoTxCredits.1
swFCPortNoTxCredits.2
swFCPortNoTxCredits.3
swFCPortNoTxCredits.4
swFCPortNoTxCredits.5
swFCPortNoTxCredits.6

swFCPortRxEncOutFrs.1

swFCPortRxEncOutFrs.2
swFCPortRxEncOutFrs.3
swFCPortRxEncOutFrs.4
swFCPortRxEncOutFrs.5
swFCPortRxEncOutFrs.6

Directory

<\\sluf22\BlueHeat\Data\2005-12-18\RealTime>

Preparation

- Familiarize yourself with how the BlueArc tool and the in-house SNMP grabber work.
- Set-up tools to capture data
- Practice interpreting the graphs while copying files to and from Indigo
- Record baseline data in the 'Indigo' directory

MANAGEMENT SUPPORT

Overview

This person provides oversight, support, and fills in as needed.

PREPARATION

Analyze the requirements of your role, determine how long you think you need to perform your preparation steps, and arrive at whatever time suits you. Admains Operator and Indigo Sniffer in particular should arrange with Client Operator on when they will take their baseline sniffs.

TIMELINE

Arrive

<u>Time</u>	<u>Task</u>	<u>Who</u>
6:00pm	Add on-site team to 'duty' group	Stuart
6:00pm+	Perform the preparation tasks for your role	All
6:15pm	Insert in-line sniffer on Indigo	Stuart/Susan
6:20pm	Disable Indigo 2 nd NIC	Stuart/Susan
6:25pm	Insert in-line sniffer on admains21	Stuart
6:30pm	Disable admains21 second NIC	Stuart
7:00pm	Capture baseline "netstat" output	Susan
7:00pm	Perform baseline captures	Client /Indigo/Admains
7:35pm	Set-up conference call ³	Client Operator
7:45pm	Initiate PIR capture	Tidal Monitor
7:50pm	Acquire verbal 'ready' from each participant	Client Operator
7:55pm	Announce beginning of event to 'duty'	Client Operator

³ Indigo Sniffer, Admains Sniffer, Tidal Monitor are the key players on the conference call. If possible, add RealTime Watcher and Float.

SDS Tray

<u>Time</u>	<u>Task</u>	<u>Who</u>
8:00pm	Initiate Tidal jobs against SDS Tray	Tidal Monitor

Capture First Round

<u>Time</u>	<u>Task</u>	<u>Who</u>
8:04pm	Acquire verbal 'ready' from each participant	Client Operator
8:05pm	Start Client capture	Client Operator
8:05pm	Start Indigo capture	Indigo Sniffer
8:05pm	Start Admaims capture	Admaims Sniffer
8:07pm	Start Client copy	Client Operator
8:10pm	Announce end of Client Copy	Client Operator
8:11pm	Stop Client capture	Client Operator
8:11pm	Stop Indigo capture	Indigo Sniffer
8:11pm	Stop Admaims capture	Admaims Sniffer
8:15pm	Save data files, update comment files	All

Capture Second & Succeeding Rounds

This is a repeat of Round One ... except that Client Operator tracks how long the file copy takes. If the file copy takes roughly the same amount of time as the baseline copy (within an order of magnitude), then Client Operator announces that the test is a no-go, and the various Sniffer operators cancel their captures and don't save. However, if the Client Operator sees that the file copy took an order of magnitude longer to complete than the baseline, then s/he announces a successful event, declares the timestamp to be used in the file names, and the various Sniffer operators save their traces and update their comment files as in Round One. We are aiming for three successful events.

CRD Tray

At this point, the time estimates are pure guesswork.

<u>Time</u>	<u>Task</u>	<u>Who</u>
9:30pm	Cancel Tidal Jobs	Tidal Monitor
9:45pm	Capture "netstat" output on admaims boxes	Tidal Monitor
9:55pm	Launch Tidal jobs against CRD Tray	Tidal Monitor

Capture Fourth Round

At this point, we are just capturing traces blindly, without regard for how long the file copy takes.

<u>Time</u>	<u>Task</u>	<u>Who</u>
-------------	-------------	------------

10:00pm	Acquire verbal 'ready' from each participant ⁴	Client Operator
10:05pm	Start Client capture	Client Operator
10:05pm	Start Indigo capture	Indigo Sniffer
10:05pm	Start Admains capture	Admains Sniffer
10:07pm	Start Client copy	Client Operator
10:10pm	Announce end of Client Copy	Client Operator
10:11pm	Stop Client capture	Client Operator
10:11pm	Stop Indigo capture	Indigo Sniffer
10:11pm	Stop Admains capture	Admains Sniffer
10:15pm	Save data files, update comment files	All

Capture Fifth Round

<u>Time</u>	<u>Task</u>	<u>Who</u>
10:30pm	Acquire verbal 'ready' from each participant	Client Operator
10:35pm	Start Client capture	Client Operator
10:35pm	Start Indigo capture	Indigo Sniffer
10:35pm	Start Admains capture	Admains Sniffer
10:37pm	Start Client copy	Client Operator
10:40pm	Announce end of Client Copy	Client Operator
10:41pm	Stop Client capture	Client Operator
10:41pm	Stop Indigo capture	Indigo Sniffer
10:41pm	Stop Admains capture	Admains Sniffer
10:45pm	Save data files, update comment files	All
10:45pm	Capture "netstat" output on admains boxes	Tidal Monitor

Back-Out

<u>Time</u>	<u>Task</u>	<u>Who</u>
10:45pm	Announce end of event to 'duty'	Client Operator
11:00pm	Cancel Tidal jobs	Tidal Monitor
11:05pm	Save PIR output	Tidal Monitor
11:05pm	Restore Indigo second NIC	Stuart
11:06pm	Restore admains21 second NIC	Stuart
11:10pm	Remove in-line sniffers	Stuart
11:15pm	Reboot Indigo	Tidal Monitor
11:15pm	Remove participants from 'duty'	Stuart
11:20pm	Send 'outages' notice	Stuart
11:25pm	Move \\sluf22\vdops\BlueHeat directory to Indigo	Stuart

Fold Up the Tents

<u>Time</u>	<u>Task</u>	<u>Who</u>
11:00pm	Record observations and write final notes as you see fit	All
11:30pm+	Go home	All

⁴ Wait for Tidal Monitor to confirm that the jobs have started.