

Fragment - Vol: 8-09

Positive guidance for IT managers, staff, and executives

120 Front St E
Suite 202
Toronto ON
(416) 203-1223

www.esubnet.com

September, 2008

Welcome to our September issue of the eSubnet Fragment.

With Fragment, eSubnet provides IT managers, their staff and executives with current information on IT problems, solutions and best practices. We hope this information provides guidance in the daily IT struggle which challenge us all.

In this issue:

- Closing the Loop: Improving your delivery
- Device Logging: Getting a better picture
- Helping IT Help You: A handout for your users

For more information on these topics please contact eSubnet at (416) 203-1223, online at <http://www.esubnet.com>, or by email info@esubnet.com.

We're always looking for interesting topics to write about so please email us any topic that interests or concerns you.

eSubnet
Providing Network Intelligence

Closing the Loop

Understanding the IT requirements of your clients' business, is one of the most important, and underrated, abilities of an IT consultant. To be successful, IT knowledge must be applied with a clear understanding of how it needs to function for the client. Even armed with an understanding of software, hardware, networking, end user behaviors, and being prepared with extensive technical knowledge, you may still have bad IT. So, removing the gaps in your IT or what I call 'Closing the Loop' is one step to moving beyond the simple title of 'geek' and becoming a true IT professional.

Everything in IT is ultimately driven by business goals. If the business leaders involved haven't set or specified your goal, you have a playground - enjoy it while you can. Having a business goal is the starting point for closing the loop. At the end of the project, you will ask whether you achieved the business goal. And, if so, how do you know?

Most IT projects involve deployment of a service, such as a website, email, or improved network connectivity, to meet a business goal, such as marketing a product, enabling customer communication, or providing better internet access for staff. The functionality of this service is your next marker point, forming a check list for success. Before claiming the project has been successfully completed, check that these services are up and available, and whether they come back online after the device is restarted. While sometimes it isn't possible to restart the server, you can set the service to start when the server powers up again. Your check list: is the primary service available, does it work, and if so, how do you know?

To establish functionality of a service, often secondary services are required. For example, the status of remote connectivity is your third marker for success. When contemplating the project, required secondary services should be listed to ensure that nothing is missed. Then you can check: Do these services come back online after the device is restarted? As with the primary service, are they available, do they work, and if so, how do you know?

Finally, we have the end users. Did they get what they needed, and if so, how do you know?

How do you know?

So far I have been asking "How do you know?". How do you know? You test. Testing should be performed throughout the process. At the end of the project you should test again to ensure completeness. The list of primary and secondary services comes in handy at this point. Tests only need to be as complicated as the services which they provide; for instance, testing an email server is pretty simple compared to testing a disaster recovery plan.

I mentioned remote connectivity as an example of a secondary service. Always test remote connectivity before final implementation, otherwise you may end up having to make a trip to the device location whenever an emergency occurs. This will extend the necessary service repair time.

"If you can't measure it, you can't manage it."

Peter
Drucker,
Management
consultant

Closing the Loop, continued

Planning your tests

Let's return to the business goal, the services, and the end users. To ensure your services are working as required, test for expected results. Keep one thing in mind when testing, while many servers and devices appear to be radically different, when testing, they are remarkably similar.

A simple test template can, and should, be drawn up and reused with only minor tweaks.

The test template should have the following items at minimum.

Project _____			Date _____
- Networking			
- TCP/IP addressing	Y		N
- Routing	Y		N
- DNS (Local)	Y		N
- Reachable			
- Remote access	Y		N
- DNS (Network Internal)	Y		N
- DNS (Network External)	Y		N
- Services			
- Primary service _____		Y	N
- Secondary Service #1 _____		Y	N
- Secondary Service #2 _____		Y	N
- Secondary Service #3 _____		Y	N
- Secondary Service #4 _____		Y	N
- Documentation			
- Updated	Y		N

Use this to start from, and add test requirements as needed. Just as no two organizations are the same, no two projects are the same, and so no two test templates will be the same. Customize the test templates to meet the primary and secondary service requirements.

Many of these tasks do become habitual. Though I caution against relying on habit alone as specific or unique tasks can be forgotten.

Closing the Loop

Selling a closed loop process to upper management often may be difficult as it adds time and money to every project. In many cases management's attitude is to see the project completed ASAP and then move on to the next one. This line of thinking often isn't in their best interests. Projects scheduled to follow are pushed back when there is a problem with the earlier project which needs your attention, also end users are impacted when the services they expect are not available as expected or worst yet, are denied. Upper management may have difficulty in enforcing the closed loop process as their IT staff's ego may come into play. Knowing that everything works, not just accepting that everything should work is important to management, and should be of primary importance to all IT professionals; both in house and outsourced alike.

Device logging

Every device running in an IT environment produces log files, an important tool in IT management. Log files provide insight into past events within an organization's daily struggle for information availability, confidentiality, and integrity. And, to maintain compliance with the ever growing list of legal and association based regulations, often log files must be created and retained.

The PCI-DSS requires the following.

10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.

10.2 Implement automated audit trails for all system components to reconstruct the following events:

10.2.1 All individual user accesses to cardholder data

10.2.2 All actions taken by any individual with root or administrative privileges

10.2.3 Access to all audit trails

10.2.4 Invalid logical access attempts

10.2.5 Use of identification and authentication mechanisms

10.2.6 Initialization of the audit logs

10.2.7 Creation and deletion of system-level objects.

10.3 Record at least the following audit trail entries for all system components for each event:

10.3.1 User identification

10.3.2 Type of event

10.3.3 Date and time

10.3.4 Success or failure indication

10.3.5 Origination of event

10.3.6 Identity or name of affected data, system component, or resource.

10.7 Retain audit trail history for at least one year, with a minimum of three months online availability

What to log?

Beyond the needs set by regulatory and legal requirements there are a number of networking and server device logs that every network administrator should include in their arsenal. Though each technology environment is unique, here are some log files which I consider a must to create and retain:

- Firewall activity

- Email activity

- Web server activity

- VPN or remote access

Since the beginning, life has relied upon the transmission of messages. For the self-aware organic unit, these messages can relay many different things

RFC 3164

Device logging Continued

Why bother?

In a perfect world there would be no reason for retaining log files. There would be no SQL injection attacks, all emails would be delivered, and no one would attempt any security breach of any kind. Until we create a workable IT Utopia, we will continue to suffer from security attacks, things break, and there is the rare situation where end-users insist that they are entering their credentials properly when they aren't. Log files are the primary source for trouble shooting, the security camera of the network, and should be used after an incident to obtain a better understanding of what has transpired.

How to log

Every system deployed generates log files they only vary in detail. The premiere log file collection device is the syslog daemon. The syslog daemon or `syslogd`, was born in the UNIX world but has since been ported to Linux, Microsoft Windows, and other platforms. The syslog daemon provides useful plain text information which clearly describes what has occurred. The syslog daemon, the philosophy behind it, how it operates, and its parameters are described in RFC 3164.

Microsoft has two types of logging, one is very much like those found in syslog; these typically are text files though not as informative as syslog and are generated when the system interacts with other computers, for example, web traffic and email activity. The other log type provided by Microsoft resides in "Event Viewer"; for events where the system is interacting with itself or with users. Microsoft Event Viewer is often cryptic, uninformative and generally not very helpful.

OK, I'm logging. Now what?

Log files provide information only on what has happened. So, when email isn't flowing properly or a web page is not providing the information that it should be, looking into the log files can assist you in finding out more about the problem, when it started, and how the service's behaviour differed from normal. These in turn may assist in solving the problem. Log files are the first and most important stop on your way to problem resolution.

View Your Logs

Viewing logs on POSIX machines On LINUX or UNIX boxes, there are tools which can help you to review the logs files. The primary tools I use are `'tail'` and `'grep'`.

Commands:

tail – this command displays the last ten lines of a file by default. The command is entered at the command prompt as shown below:

```
tail <file>
```

Device logging Continued

The functionality of tail can be expanded with various switches as shown below:

`-n <#>`

This displays the last 'n' lines.

`-f`

This displays the last 10 lines and follows the file as more lines are added.

grep – this command displays lines in a file which matches a specific pattern. The command is entered at the command prompt as shown below:

```
grep [pattern] <file>
```

The functionality of grep can be expanded with various switches, as shown below:

`-i`

Perform case insensitive matching. By default, grep is case sensitive.

`-v`

Selected lines are those not matching any of the specified patterns.

For more information on tail or grep, look for their manual pages by typing "linux man grep" or "linux man tail" in your favorite search engine. These two commands can be combined. This is the real power of using these commands. For example if you wish to track down a problem about email (for example, email being sent by me) you would enter the following command at the command prompt:

```
tail -f /var/log/maillog | grep rdanielli
```

Then you'd ask me to send an email. Or, you could use the following line to view the history of related events stored in the log files: `grep rdanielli /var/log/maillog` Note: The log files of a system may contain sensitive information so typically you don't want everyone having access. This is reserved for 'root' level privileges, and few people should have the rights to access them.

Viewing logs on Windows machines

Windows Event Viewer allows filtering of event logs. To filter events, right click on the event log you wish to filter and look under properties. More information on this can be found at this URL:

<http://support.microsoft.com/kb/308427>

Using logs You are now well armed to view log histories and real time logging, and can better troubleshoot problems as they show up on your servers and devices.

Helping IT to help you

No matter how well designed and implemented the system, someone eventually calls upon their IT helpdesk for assistance. These requests are typically entered into helpdesk software, made over the phone, or sent by email.

The IT helpdesk staff is there to assist, to ensure that end users are not hindered by technology. It is not just part of their job, many of these unsung heroes enjoy assisting. Everyone understands that things break. It is the task of IT helpdesk staff to get the broken things fixed so end users can get back to work quickly.

To speed up the repair process, helpdesk staff benefit from receiving detailed problem descriptions. The better the description the end user sends, the quicker every problem is resolved.

Here are some examples:

Bad:	"The internet is down."
Good:	"I get an error every time I open my browser. The error says, "Error in memory location 23F6x0"."
Bad:	"I can't open the attachment."
Good:	"A client sent me an MS Word document and my computer says that I can't open this version."
Bad:	"Email doesn't work."
Worse*:	"I can't send emails. Something pops up that says I am above quota and need to delete some of my emails."

* This last example is labeled worse because the error message explains the problem and the end user hasn't taken the time to help themselves by following the stated instructions.

By being clear and detailed with descriptions of their problems, the end user assists the helpdesk staff to resolve the problem in a much more timely fashion; thereby the end user can get back to work rapidly. Remember, the more detailed the information, the quicker the helpdesk staff can resolve the issue.

Regards,

Richard Danielli
President, eSubnet

eSubnet
Providing Network Intelligence

There are no stupid questions, but they are the easiest to answer

Anonymous

About eSubnet

Based in Toronto Canada, privately held eSubnet Enterprises, Inc. offers tactical advice and implementation services in Internet security, connectivity, and data networking. eSubnet staff assist companies to develop and maintain secure, resilient, and available network services.

eSubnet customers include many medium and large businesses including many of Canada's most respected Law firms, and one of the most recognized Canadian theatre production companies.

For information on how eSubnet can help, visit us online <http://www.esubnet.com>.

To reprint one of our articles, please contact Richard Danielli at (416) 203-1223.

ESUBNET PROVIDES THIS PUBLICATION AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR PARTICULAR PURPOSE.

QUICK FACTS

McAfee, Inc. Agrees to Acquire Secure Computing

McAfee expects to be able to deliver the industry's most complete network security portfolio (covering intrusion prevention, firewall, Web security, email security and data protection, network access control), from small and mid to the world's largest organizations. All this for just under \$500 Million

Hackers Busted

Eleven people were indicted Tuesday for allegedly stealing more than 40 million credit and debit card numbers, federal authorities said. The indictments, which alleged that at least nine major U.S. retailers were hacked, were unsealed Tuesday in Boston, Massachusetts, and San Diego, California, prosecutors said. It is believed to be the largest hacking case that the Justice Department has ever tried to prosecute. Three of the defendants are from the United States; three are from Estonia; three are from Ukraine, two are from China and one is from Belarus.

Read our back issues and subscribe at: <http://www.esubnet.com/fragment.html>.

Copyright 2008, eSubnet Enterprises, Inc. All rights reserved.