Cigital, Inc.
21351 Ridgetop Circle
Suite 400
Dulles, VA 20166-6503
Phone: +1.703.404.9293
Fax: +1.703.404.5801
www.cigital.com

Cigital Field Testing Report

Executive Summary

Cigital worked with NRECA and PNNL in order to conduct field testing of the Essence appliance; the entire field test took place over 3 days. The objective of the field testing was to capture Multispeak traffic and exercise the first three layers of the Essence solution. Consequently, the success criterion was defined to be the ability (of Essence) to capture and analyze the Multispeak traffic.

Cigital's overall assessment of the field tests is that it was a success; this is consistent with PNNL's assessment. Despite the overall success, Cigital feels that it is important to reiterate the testing conditions at each CoOp and what caused testing at some CoOps to be more successful than others. Details of these activities are listed in the **Field Tests** section of the report.

Each CoOp network is different and presents its unique challenges pertaining to the Essence deployment. To increase our probability of success as defined above, Essence needs to support a flexible array of deployment options. Given constraints, Cigital has identified three (3) feasible deployment options that will maximize the probability of success when Essence is deployed in the field. Each deployment option has its advantages but no deployment option can be used as a silver bullet approach; these details are listed in the **Deployment Options** section of the report. Additionally, Cigital has identified follow on work that needs to be performed during the current development cycle. The proposed follow on work is aimed at supporting more deployment options and scenarios. These details are listed in the **Next Steps** section of this report.

Field Tests

The primary objective at each CoOp was to exercise the Essence system in a way that would allow us to generate, capture and analyze a specific subset of Multispeak messages at any given time. Once the desired traffic was generated, the field testing team would verify that the Essence appliance properly captured the Multispeak messages via the layer 1 and 2 software and then properly performed analysis via the layer 3 software. Cigital was able to test the Essence appliance on live data at two of the 3 CoOps. A description of the network topology, behaviors observed and lessons learned per CoOp are listed below.

© 2015, Cigital Inc.

Cigital, Inc.
21351 Ridgetop Circle
Suite 400
Dulles, VA 20166-6503
Phone: +1.703.404.9293
Fax: +1.703.404.5801
www.cigital.com

Wake

Issues Encountered

- Most Multispeak traffic was encrypted
    - Essence cannot process encrypted traffic
- Layer 2 software incorrectly identified Multispeak traffic on several occasions

The Wake CoOp had a network setup that allowed us to test the physical appliance with live data, but we were severely limited in our ability to process most of the meaningful Multispeak traffic. Specifically, all Multispeak traffic between the CoOp and AMI was encrypted since the traffic was sent over HTTPS. Fortunately, we were able to capture Multispeak traffic sent to and received from the IVR. It is important to note that it took several hours to discover this problem since we did not initially have a clear understanding of the network topology at Wake. When the team initially tested the network tap to ensure that traffic was being captured, we serendipitously captured it at a moment in time when unencrypted Multispeak traffic was being sent between the endpoints in the CoOp. It took several hours of exploration before we determined we were simply lucky.

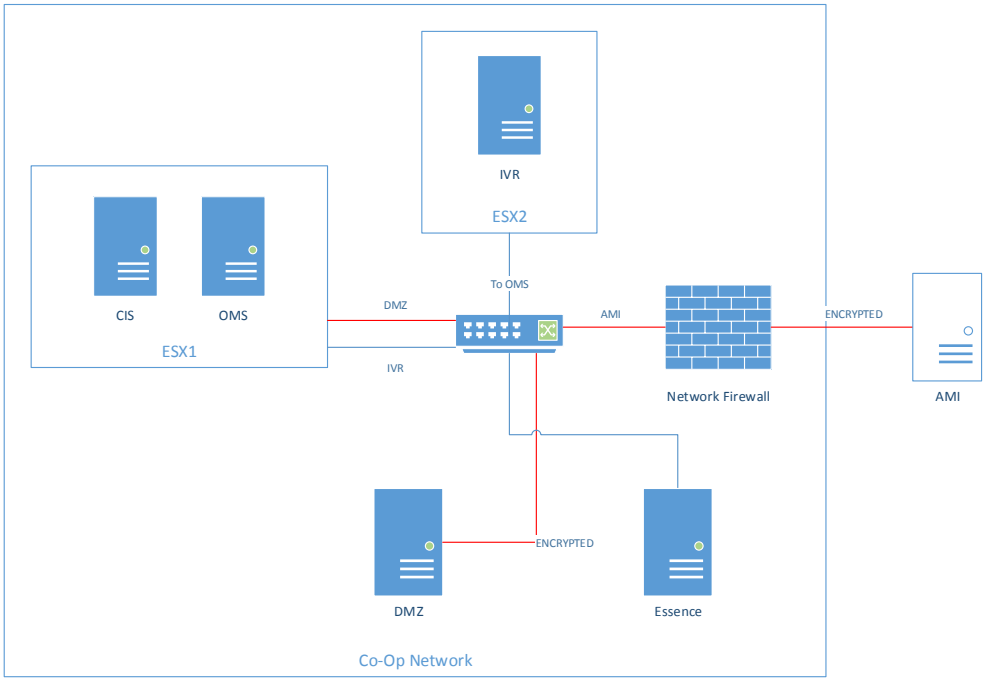

Figure 1: Diagram of Wake Network Topology

Blue lines denote unencrypted traffic

© 2015, Cigital Inc.

Cigital, Inc.
21351 Ridgetop Circle
Suite 400
Dulles, VA 20166-6503
Phone: +1.703.404.9293
Fax: +1.703.404.5801
www.cigital.com

Read lines denote encrypted traffic

The team discovered that this kind of network setup would be a significant challenge to mount in a real world deployment scenario. It still is not clear how many CoOps have a network topology that is similar to that encountered at Wake.

One proposed solution to the encryption problem was to use an Enterprise Service Bus. The ESB would serve as intermediary endpoint between any endpoints that used TLS to protect the transport layer. After additional discussion, Doug and Phil discovered that the ESB would not be a suitable solution due to costs and the degree of difficulty involved to integrate it with Essence given time and budget constraints. Another potential solution was to use a proxy. All HTTP traffic sent into or out of the CoOp would go through the proxy. This may require some CoOps to reconfigure its deployment of Multispeak endpoints to communicate via proxies. Essence would need to be reconfigured to work by capturing data from the proxy.

Central

Issues Encountered

- Unsupported network topology for Essence

The Central CoOp was not setup in a way that allowed the Essence device to be deployed and tested with live data. Specifically, all of the Multispeak endpoints of interest were deployed on the same physical host; this made it impossible for the team to capture live data from outside of the host with the Essence appliance. We had the option of trying to capture all traffic to/from the AMI, but we did not think it was wise to alter the state of the VM manager since the field test was being executed in a production environment.

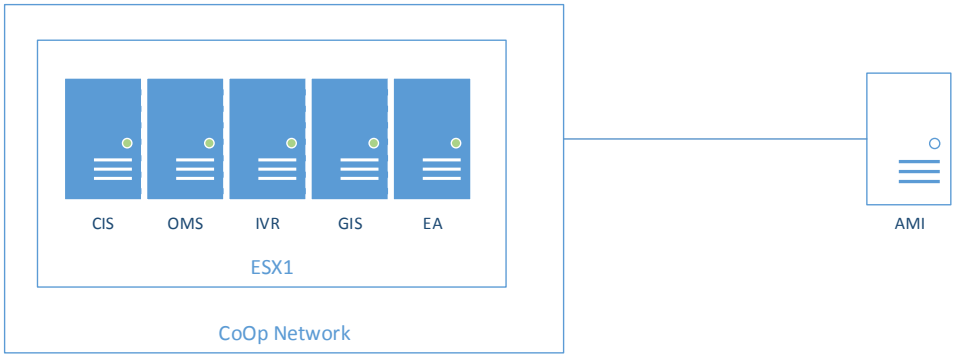

Figure 2: Diagram of Wake Network Topology

© 2015, Cigital Inc.

Cigital, Inc.
21351 Ridgetop Circle
Suite 400
Dulles, VA 20166-6503
Phone: +1.703.404.9293
Fax: +1.703.404.5801
www.cigital.com

The team was able to capture Multispeak traffic by starting Wireshark on each guest virtual machine operating system. The team exercised the system and confirmed that the captured Multispeak traffic had all of the expected data. In that sense, the field test was a success.

The most important lesson learned is that it might not be feasible to deploy Essence as a physical appliance for each CoOp and that a deployment strategy that included the ability to capture traffic from guest operating systems within a virtualized environment would be needed in order to maximize the probability of success for this project.

South River

Issues Encountered

- Essence did not correctly identify the GetAMRSupportedMetersResponse message.

The South River CoOp had a network setup that was allowed us to test the physical appliance with live data. The team deployed the pertinent Multispeak endpoints to different physical VMWware hosts and connected the hosts to a switch; the switch was mirrored to a port that fed directly into the Essence appliance.

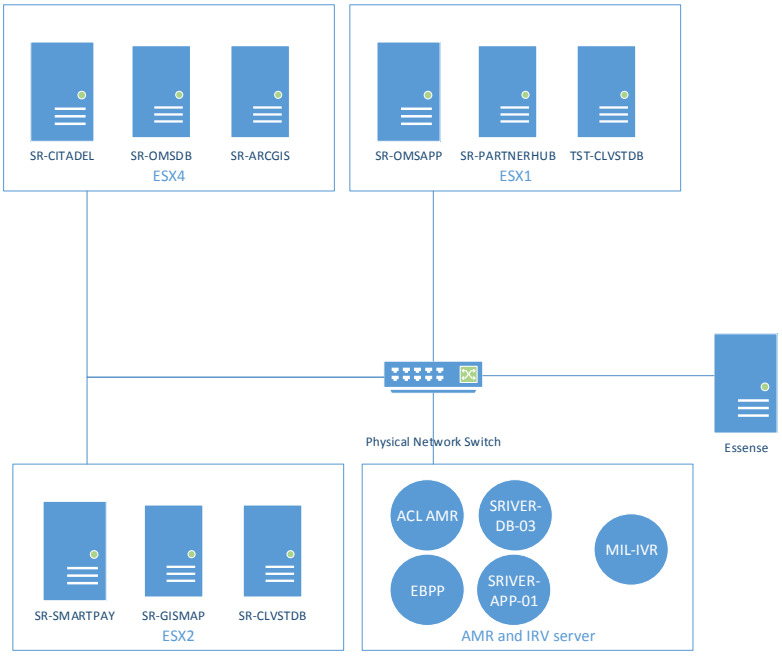

Figure 3: Diagram of South River network topology

© 2015, Cigital Inc.

Cigital, Inc.
21351 Ridgetop Circle
Suite 400
Dulles, VA 20166-6503
Phone: +1.703.404.9293
Fax: +1.703.404.5801
www.cigital.com

With the exception of one kind of message (GetAMRSupportedMetersResponse), we were able to verify that the appliance successfully filtered, stored and analyzed all of the messages it was expected to. The trip was an overwhelming success due to the variety and magnitude of live data captured, processed and analyzed.

Despite the success at south river, it is important to note that the Essence appliance did not have the ability to capture any Multispeak traffic that was sent between the guest operating systems on a host. For example, if Multispeak traffic was sent between the guest operating systems on ESX1, there would be no way for the Essence appliance to capture it since it would never be sent to the physical switch. Cigital's understanding is that almost no traffic of interest would be sent between guest operating systems on the same host.

The most important lesson learned is that Essence appliance can work as intended when the Multispeak endpoints are on different physical hosts. It is also worth noting that the physical server deployment option should work if each guest operating system was bridged to a different physical network interface. This means that we do not need to have a physical appliance per Multispeak endpoint; all we need is to have each Multispeak endpoint communicate from a physical NIC.

Deployment Options

After the field test was complete, Cigital identified 3 deployment options for the Essence project. Note that some of these deployment options were already identified before field testing. Each deployment option has constraints that we will elaborate on.

Physical Appliance

This deployment option would not require any additional effort to implement and it has already been successfully tested in the field under certain conditions. This deployment option requires the Multispeak endpoints to be connected to a physical NIC and the NIC must be connected to a SPAN port. It is also possible to use this deployment option with virtual mirroring, but it requires licensing features that were not present at any of the CoOp's we visited during the field test.

Proxy

This deployment option would require Cigital to redesign the way Essence captures traffic. As currently designed, Essence captures raw Ethernet frames and reassemble them to determine if they are Multispeak messages. In order to work properly, Essence requires the IP packets inside the Ethernet frames to be unencrypted (i.e. cleartext). Recall that the main problem encountered at

© 2015, Cigital Inc.

Cigital, Inc.
21351 Ridgetop Circle
Suite 400
Dulles, VA 20166-6503
Phone: +1.703.404.9293
Fax: +1.703.404.5801
www.cigital.com

Wake was that the Essence appliance could not process data between the OMS and AMI since it was encrypted via HTTPS. One relatively simple and low cost solution that could be implemented immediately is to insert a proxy in the CoOp data center that would decrypt all Multispeak traffic sent over HTTPS. This would allow Essence to capture all currently supported Multispeak traffic, but this option also introduces the most risk since it requires a fundamental redesign of the Essence application. Currently, Essence's layer 1 software extracts raw Ethernet frames from the network. This redesign would require Essence to extract HTTP messages from a proxy; Essence would also need to be integrated into the proxy. The Multispeak endpoints would also need to have the certificate of the proxy installed on them in order for them to trust it when sending HTTPS traffic. A scheme for certificate management would also need to be implemented. These technical challenges made us think that this option should be pursued at the present time.

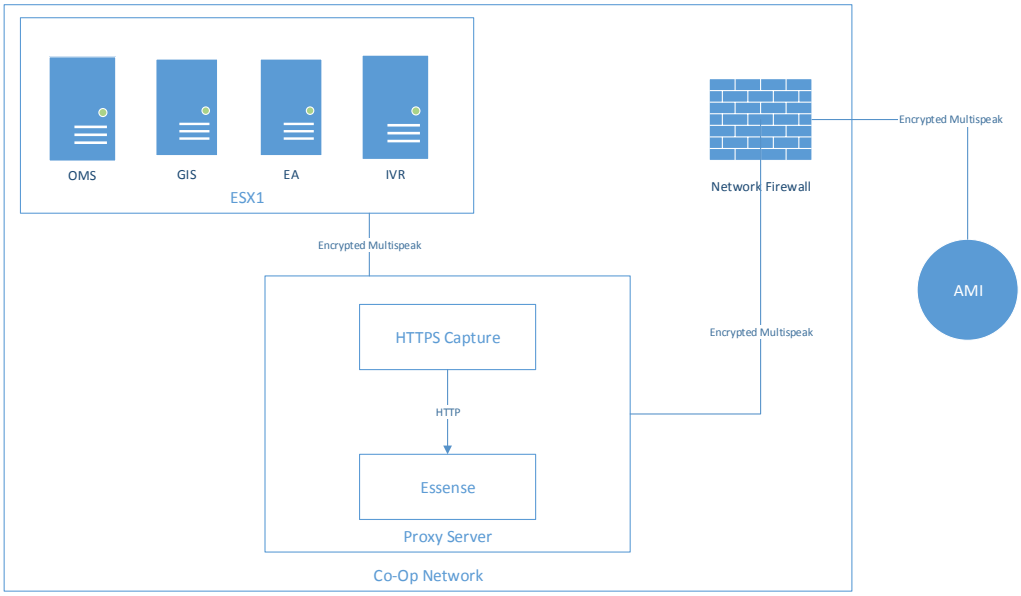

Figure 4: Diagram of Essence running within a proxy

Virtual Appliance

This deployment option would require some additional effort to implement but it appears to be the best option available. The Essence appliance would be virtualized, and each CoOp would it as a guest operating system inside of a VMWare host. Cigital has identified the technical steps that are necessary in order to implement this and partially tested this capability at Central EMC before the field test. It is important to note that no additional licensing features are necessary in order to deploy the virtual appliance. The virtual appliance can be deployed in one of two ways.

© 2015, Cigital Inc.

Cigital, Inc.
21351 Ridgetop Circle
Suite 400
Dulles, VA 20166-6503
Phone: +1.703.404.9293
Fax: +1.703.404.5801
www.cigital.com

The first and most straight forward approach is to create a virtual switch which operates in promiscuous mode on each physical host where Multispeak traffic is being sent/received. Once operating in promiscuous mode, the virtual Essence appliance would be connected to the virtual switch and it would perform just as if it were a physical Essence appliance which runs the full 5 layer stack of essence applications.

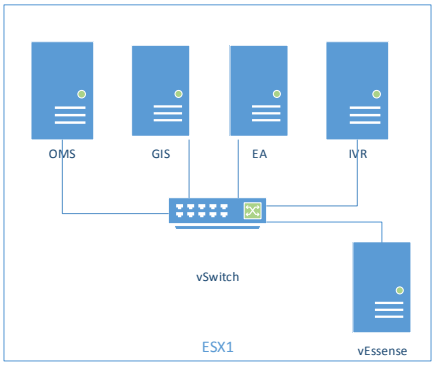

Figure 5: Diagram of Essence running as one virtual appliance

The second way to deploy the virtual appliance is to have an instance of the virtual appliance executing on each physical host where Multispeak traffic is being sent/received. A central Essence data storage would be used in order for the layer 2 software to store Multispeak messages. This change should be transparent to software above layer 2.

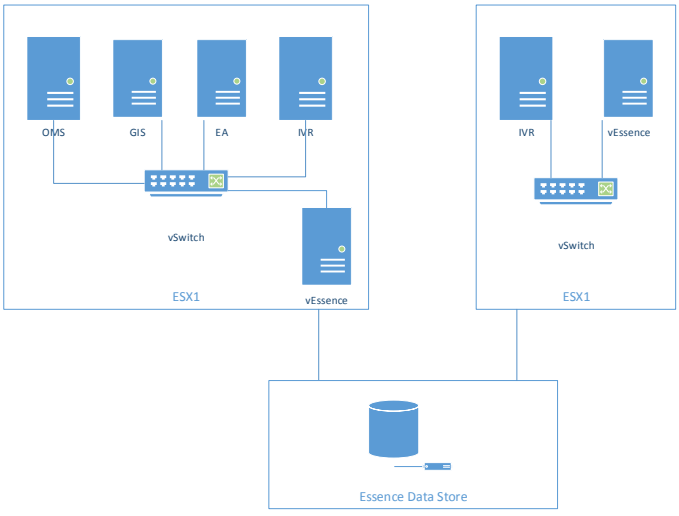

Figure 6: Diagram of Essence running as more than one virtual appliance

© 2015, Cigital Inc.

Cigital, Inc.
21351 Ridgetop Circle
Suite 400
Dulles, VA 20166-6503
Phone: +1.703.404.9293
Fax: +1.703.404.5801
www.cigital.com

Next Steps

This section of the report highlights new tasks that Cigital identified due to the outcome of the field tests.

Multispeak Filter Refinement

One of the most important discoveries during the field test was that the layer 2 software needed additional refinement. Specifically, when field testing was conducted at Wake, the layer 2 software incorrectly flagged some reassembled IP frames as Multispeak data. Also, the layer 2 software did not correctly flag some reassembled IP frames as Multispeak data. This outcome was expected since Multispeak vendors often use different syntax rules when generating Multispeak data. Packet captures from Wake and South River are being analyzed to determine why the layer 2 software did not function as intended.

Virtual Appliance

In practice, it may be very difficult to deploy Essence as a physical appliance due to the problems encountered at Central. It is worth reiterating the fact that South River needed to reconfigure its guest operating systems in a manner that would allow Essence to capture the Multispeak traffic. Cigital is going to test deployment of Essence as a virtual appliance to verify that it would behave as intended. This deployment option requires one change in VMWare. Aside from that change, all other changes to the Essence software stack should be transparent. If successful, Cigital recommends we test this deployment option with one more field test at Central.

Automation

Cigital encountered a hard drive failure on its Essence appliance before it was deployed during field testing. Additional opportunities to quickly build a new Essence appliance were discovered during this event. Cigital will work on methods to automate the build process for a new Essence appliance.

Conclusions

Overall, the Essence field test was successful with the physical deployment option, but lessons learned during the trip lead Cigital to conclude that a virtual appliance would be the best deployment option. The physical deployment option does not appear to be immediately suitable for most CoOps since it

© 2015, Cigital Inc.

Cigital, Inc.
21351 Ridgetop Circle
Suite 400
Dulles, VA 20166-6503
Phone: +1.703.404.9293
Fax: +1.703.404.5801
www.cigital.com

would likely require the staff to make changes to manner in which the guest operating systems are deployed. Also, the proxy deployment option, while best for capturing all kinds of Multispeak traffic introduces the most risk. Therefore, it cannot be recommended as the best way to capture the traffic at the present time.

The pursuit of the virtual appliance should enable us to install Essence in more CoOps, but it would require additional work from Cigital and a new field testing to confirm that it will (at least) perform as well as the physical appliance does. This would require the entire Essence team to coordinate a schedule for us to discover additional problems via discussion and field tests. Also, we need to produce a new installation guide that can be used by the staff at each CoOp. Additional research would be necessary to discuss how we can use Essence when the Multispeak traffic is encrypted by the endpoints, or extend Essence analysis beyond Multispeak traffic.

© 2015, Cigital Inc.