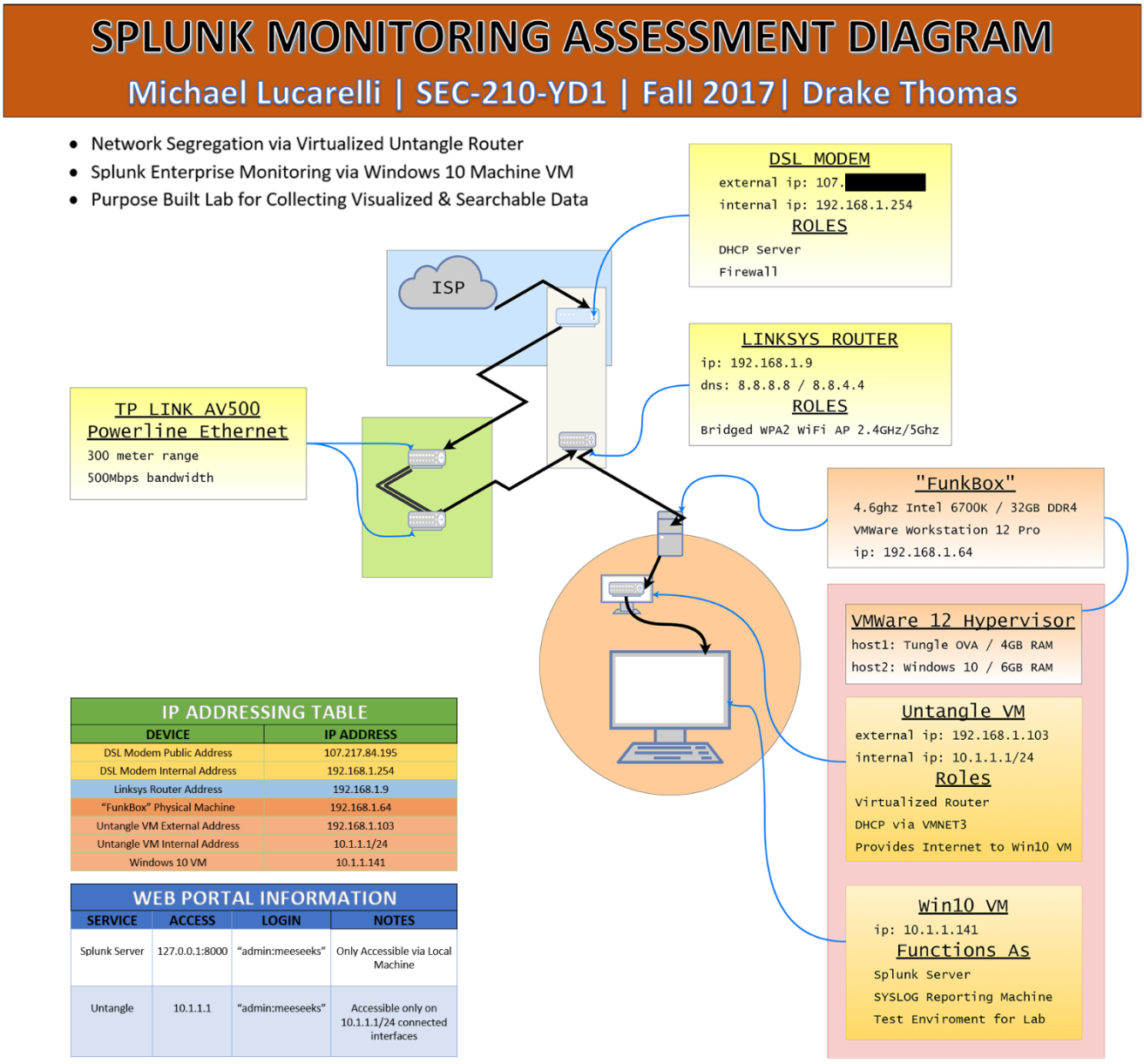
Contents

Network Diagram



Splunk Monitoring Windows 10 Event Logs

1. How to Configure Windows Event Audit Log

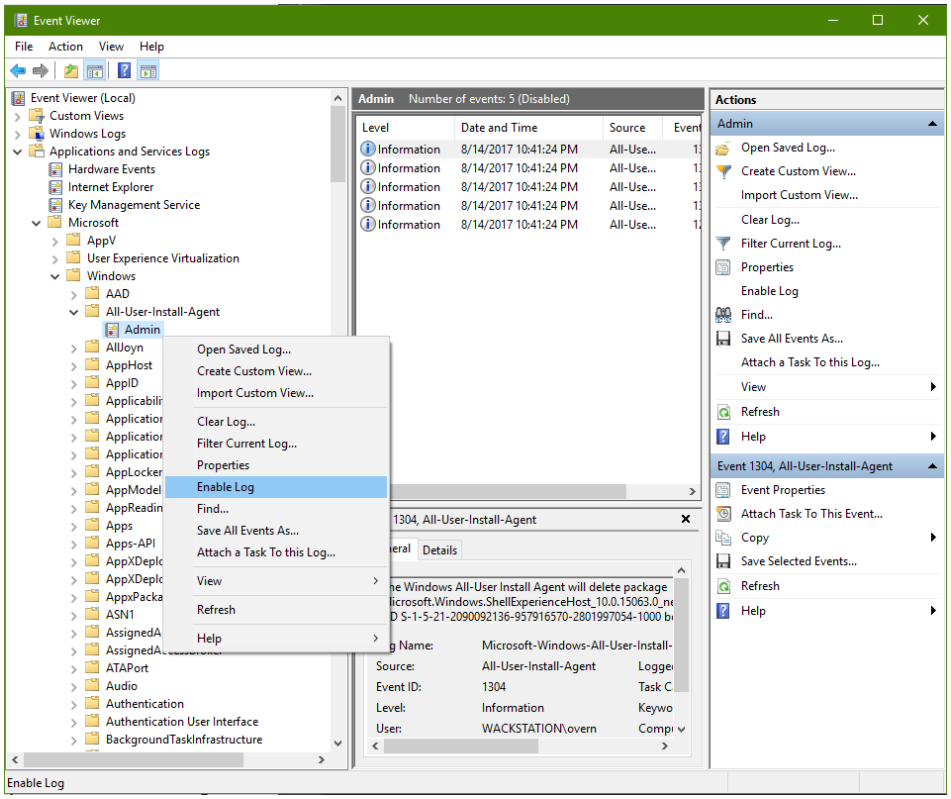
1.1. Open an elevated Command Prompt by running “Cmd.exe” as an Administrator.

1.2. Using the elevated command window run the following command to enable security auditing:

```
Auditpol /set /Category:System /failure:enable
```

1.3. Run “Eventvwr.exe”, after the Event Viewer windows has opened, proceed to expand the following entries to gain granular access to which Windows Logging functions you would like to enable within the Windows Event Log system:
[Applications and Services Logs -> Microsoft -> Windows]

1.4. Expanding each module within this folder, will present options such as Admin and Operational control logging to enable. You can quickly enable logging features one at a time, as needed, by right clicking each entry within the descriptive folders, and clicking “Enable Log” from the list that popups following a right click. The screenshot below shows that functionality:



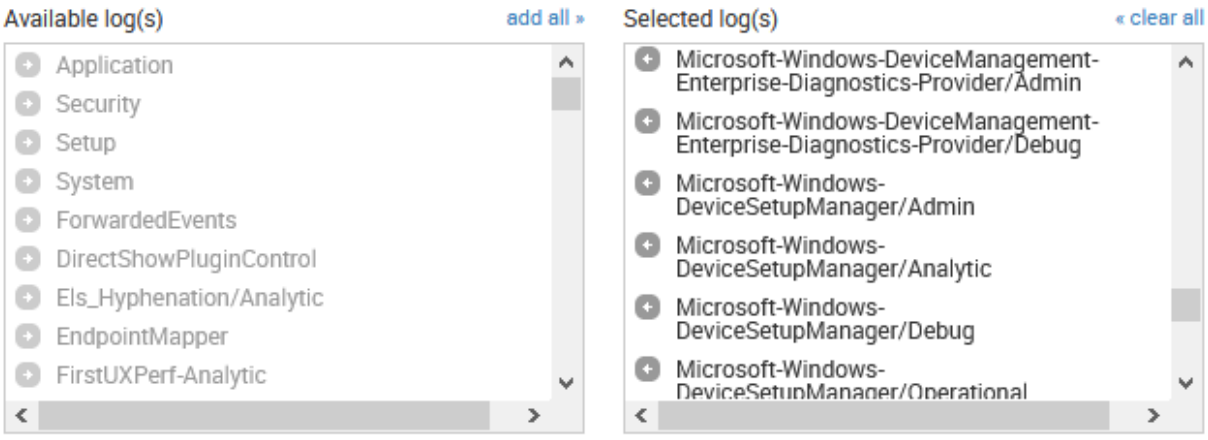
1.5. After you are satisfied with which options you would like to configure logging to be enabled on, the entries will populate in the Splunk options described in the following step.

2. How to Enable Local Event Log Collection for Windows 10 in Splunk

2.1. Access the Splunk server Data inputs page by navigating to in your web browser where your Splunk runs: "**localhost:8000/en-US/manager/launcher/datainputstats**". It is also found by clicking on "Settings" than "Data inputs" at the top of Splunk web panel.

2.2. The page that opens contains the option to enable collection of Windows event logs for both the local and remote machines at the top of the list.

2.3. For our example, we will be configuring the local machine event logs to be populated into the Splunk log database, all event log options that have been enabled on the machine will appear under "Available log(s)" and can be moved either individually or in bulk to the "Selected log(s)" section. Discretion on which logs to enable is recommended due to the large number of logs that the Windows Event Log can generate. For example, by adding all logs available, over 7,000 log entries populated into Splunk from a Windows 10 installation that was running with stock with hardly any activity on the machine. A screenshot is provided below to show what this configuration panel looks like:



Select the Windows Event Logs you want to index from the list.

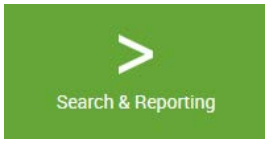
2.4. After selecting which Windows event logs you would like to incorporate into Splunk, you can choose the destination index that you would like this log source to be located in, and should finish by clicking the green "Save" button located on the bottom right.

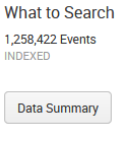
2.5. Completion of this step is vital in enabling Splunk to know which Windows event log information you would like to populate into the Splunk visualized dashboards. Without this step Windows event log will log events, however they will not automatically import into the robust visualization and reporting environment that you benefit from by having Splunk configured properly.

3. Review Evidence that Splunk is Collecting Windows 10 Event Logs

3.1. An installation of Adobe Reader has been conducted by myself at this point to verify that Splunk is configured to capture software installation through the Event Log.

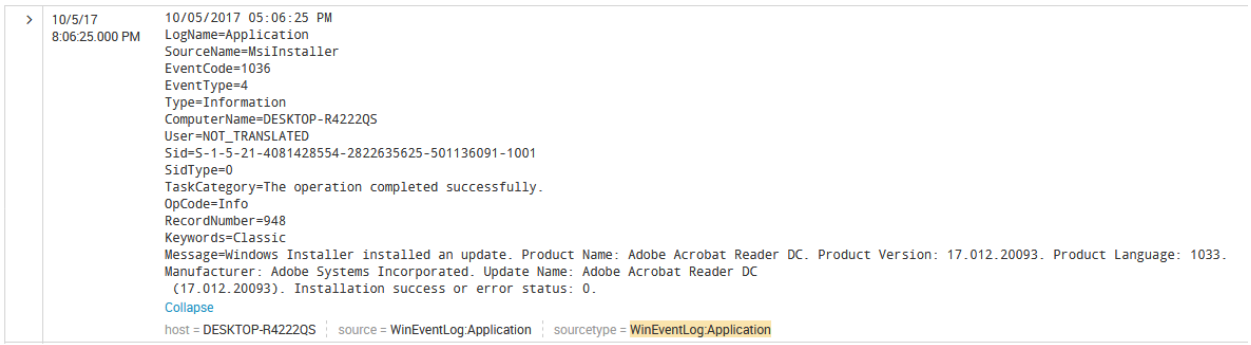
3.2. From the main page of the Splunk dashboard, click on “Search & Reporting”, on the next page click on “Data Summary”, than choose the “Sources” tab, and proceed to click on “WinEventLog:Application” under the source column. Screenshots shown on the next page:

3.2.1. 

-> 

-> 

3.3. Scrolling through the database of Windows event log in Splunk, an entry is found at the time the Adobe Reader installation was conducted. You can see that the entry has a value of “MsiInstaller” as the SourceName value. This entry is shown below:



3.4. This concludes the verification that both Splunk and the Windows event log have been configured to log operating system events such as software installation.

3.5. In conclusion, you can see the value that this information provides as it contains: information such as the time and date of installation, the user account the installation was conducted within, software version information, and manufacturer software id (Sid) information pertaining to the software.

3.6. Further configuration within Splunk can enable certain log triggered events to initiate flags within the dashboard and automatically dispatched alerts to administrators remotely through e-mail settings that can be configured at your discretion.

3.7. Documented information about configuring E-Mail notifications can be found online at: http://docs.splunk.com/Documentation/SplunkCloud/6.6.3/Alert/Emailnotification

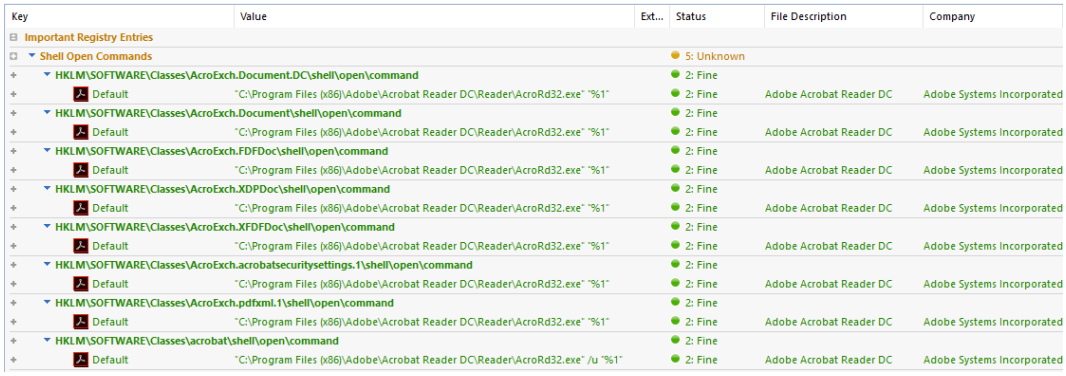
ESET SysInspector

Version 1.3.5.0 of the ESET SysInspector software was used to conduct this assessment. It is portable program that requires no installation that collects system information in the following categories:

- Running Processes
- Network Connections
- Important Registry Entries
- Services
- Drivers
- Critical Files
- System Scheduler Tasks
- System Information
- File Details

Logs were conducted on the machine: “DESKTOP-R4222QA” twice order to do a comparison on the changes made to the system from the installation of Adobe Reader v17.012.20093. The first log was made prior to installation followed by a second log being generated after the installation of the software. SysInspector contains a feature that allows comparison between 2 log files to highlight changes between two snapshots of log data.

1. Registry Changes | Shell Open Commands:



Key	Value	Ext...	Status	File Description	Company
Important Registry Entries					
Shell Open Commands			5: Unknown		
HKLM\SOFTWARE\Classes\AcroExch.Document.DC\shell\open\command			2: Fine		
Default	"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" "%1"		2: Fine	Adobe Acrobat Reader DC	Adobe Systems Incorporated
HKLM\SOFTWARE\Classes\AcroExch.Document\shell\open\command			2: Fine		
Default	"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" "%1"		2: Fine	Adobe Acrobat Reader DC	Adobe Systems Incorporated
HKLM\SOFTWARE\Classes\AcroExch.FDFDoc\shell\open\command			2: Fine		
Default	"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" "%1"		2: Fine	Adobe Acrobat Reader DC	Adobe Systems Incorporated
HKLM\SOFTWARE\Classes\AcroExch.XDPDoc\shell\open\command			2: Fine		
Default	"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" "%1"		2: Fine	Adobe Acrobat Reader DC	Adobe Systems Incorporated
HKLM\SOFTWARE\Classes\AcroExch.XFDFDoc\shell\open\command			2: Fine		
Default	"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" "%1"		2: Fine	Adobe Acrobat Reader DC	Adobe Systems Incorporated
HKLM\SOFTWARE\Classes\AcroExch.acrobatsecuritysettings.1\shell\open\command			2: Fine		
Default	"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" "%1"		2: Fine	Adobe Acrobat Reader DC	Adobe Systems Incorporated
HKLM\SOFTWARE\Classes\AcroExch.pdfxml.1\shell\open\command			2: Fine		
Default	"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" "%1"		2: Fine	Adobe Acrobat Reader DC	Adobe Systems Incorporated
HKLM\SOFTWARE\Classes\acrobat\shell\open\command			2: Fine		
Default	"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" /u "%1"		2: Fine	Adobe Acrobat Reader DC	Adobe Systems Incorporated

2. System Scheduler Tasks:

c:\windows\system32\tasks\Adobe Acrobat Update Task	2: Fine
Command Line c:\program files (x86)\common files\adobe\arm\1.0\adobearm.exe	2: Fine Adobe Reader and Acrobat ManagerAdobe Systems Incorp...
c:\program files (x86)\common files\adobe\arm\1.0\adobearm.exe	
SHA1	3294010C349B3EF1BB462F0C0B1F5C616B9ED125
Last Write Time	2017/07/20 02:50
Creation Time	2017/07/20 02:50
File Size	1165920
File Description	Adobe Reader and Acrobat Manager
Company Name	Adobe Systems Incorporated
File Version	1.824.23.7067
Product Name	Adobe Reader and Acrobat Manager
Internal Name	AdobeARM.exe
Signer	Adobe Systems, Incorporated
(Cloud) Age	a month ago
(Cloud) Volume	10000000
Linked to	Running processes -> adobearm.exe
Linked to	Running processes -> adobearm.exe -> c:\program files (x86)\common files\adobe\arm\1.0\adobearm.exe
Linked to	System Scheduler Tasks -> c:\windows\system32\tasks\Adobe Acrobat Update Task -> c:\program files (x86)\common files\adobe\arm\1.0\adobearm.exe