Upgrading Splunk_TA_windows without breakage!

Gregg & Noah Woodcock
President & Sr. Consultant | Splunxter, Inc.

splunk> .conf19

.conf19

splunk>

Gregg Woodcock

President, Splunxter, Inc.
#3 on Splunk Answers!

Noah Woodcock

Sr. Consultant, Splunxter, Inc.
#134969 on Splunk Answers!

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

All of these details are included in the “Upgrade Planner for Splunk Add-on for Windows” app on SplunkBase

https://splunkbase.splunk.com/app/4594/

.conf19
splunk>

Changes to “source” values

It is unlikely that your searches depend on these values, or that you are using xml

version<=4.8.4

- WinEventLog:System
- WinEventLog:Application
- WinEventLog:Security
- WinEventLog:System
- WinEventLog:Application
- WinEventLog:Security

version>=5.0

- WinEventLog:System
- WinEventLog:Application
- WinEventLog:Security
- **Xml**WinEventLog:System
- **Xml**WinEventLog:Application
- **Xml**WinEventLog:Security

Changes to “sourcetype” values

Most searches use “sourcetype=WinEventLog:<something>” which will break

version<=4.8.4

- WinEventLog:**System**
- WinEventLog:**Application**
- WinEventLog:**Security**
- XmlWinEventLog:**System**
- XmlWinEventLog:**Application**
- XmlWinEventLog:**Security**

version>=5.0

- WinEventLog
- WinEventLog
- WinEventLog
- XmlWinEventLog
- XmlWinEventLog
- XmlWinEventLog

Mitigation Options to fix your SPL

IF YOU USE THIS	THEN SWITCH TO THIS	BUT *NOT* THIS!
sourcetype=wineventlog:*	(source="WinEventLog:*" OR source="WMI:WinEventLog:*" OR source="XmlWinEventLog:*")	eventtype="wineventlog_windows“
sourcetype=XMLeventlog:*	(source="WinEventLog:*" OR source="WMI:WinEventLog:*" OR source="XmlWinEventLog:*")	eventtype="wineventlog_windows“
sourcetype=wineventlog:System	(source="WinEventLog:System" OR source="WMI:WinEventLog:System" OR source="XmlWinEventLog:System")	eventtype="wineventlog_system“
sourcetype=XMLeventlog:System	(source="WinEventLog:System" OR source="WMI:WinEventLog:System" OR source="XmlWinEventLog:System")	eventtype="wineventlog_system“
sourcetype=wineventlog:Security	(source="WinEventLog:Security" OR source="WMI:WinEventLog:Security" OR source="XmlWinEventLog:Security")	eventtype=wineventlog_security“
sourcetype=XMLeventlog:Security	(source="WinEventLog:Security" OR source="WMI:WinEventLog:Security" OR source="XmlWinEventLog:Security")	eventtype="wineventlog_security“
sourcetype=wineventlog:Application	(source="WinEventLog:Application" OR source="WMI:WinEventLog:Application" OR source="XmlWinEventLog:Application")	eventtype="wineventlog_application“
sourcetype=XMLeventlog:Application	(source="WinEventLog:Application" OR source="WMI:WinEventLog:Application" OR source="XmlWinEventLog:Application")	eventtype="wineventlog_application"

Changes to apps (3 merged to 1)

Both “Splunk_TA_microsoft_dns” and “Splunk_TA_microsoft_ad” are GONE!

- Create your own app called something like “**MyCompany_TA_windows**”
  - For every file inside the “local” directory of any of these 3 apps, create the same file in your new app.
  - Inside each of those new files, create 3 sections using comments like this: “**#### Splunk_TA_windows ####**”, “**#### Splunk_TA_microsoft_dns ####**”, and “**#### Splunk_TA_microsoft_ad ####**”.
  - For each of the original files, copy the content from the original file to the appropriate section in the new file in your new app.

Dangerous changes to defaults

Get this right or you WILL lose data!

- Add explicit settings to "**MyCompany_TA_windows**"or base config apps:
  - The default "**indexes.conf**" is just gone. Make sure that if you are using the "**windows**", "**wineventlog**", or "**perfmon**" index values, that you copy the contents of "**indexes.conf**" to your "**MyCompany_all_indexes**" app (you do have one of those, right?) and push to your indexers.
  - The default "**authorize.conf**" is just gone. Make sure that if you are using the "**role_windows-admin**" role, that you copy the contents of "**authorize.conf**" to your "**MyCompany_search_base**" app (you do have one of those, right?) and push to your search heads.
  - The default "**inputs.conf**" has been stripped of "**index=**" settings. Make sure that you are following best practices and have (or create) "**index=**" lines for every stanza in the "**inputs.conf**" file in your "**MyCompany_TA_windows**" app (especially if you are using the "**windows**", "**wineventlog**", or "**perfmon**" index values and may be relying on defaults that are now gone) and push to your forwarders.
  - The default "**props.conf**" has been stripped of the built-in **NTSyslog**, **Snare**, **MonitorWare**, and **Enterprise Security 2.0.2** field extractions. Make sure that if you need these that you copy them to your "**MyCompany_TA_windows**" app and push to your search heads.

Arbitrary changes to defaults

Splunk considers these changes improvements but you may disagree

- Add explicit settings to “**MyCompany_TA_windows**”or base config apps:
  - The default “**inputs.conf**” has added “**renderXml = true**“. Unless you’d like your windows events to completely change format this way, make sure that you set “**renderXml = false**” for every stanza in the “**inputs.conf**” file in your “**MyCompany_TA_windows**” app and push to your forwarders.
  - The default “**inputs.conf**” has changed the “**[perfmon://*]**” stanzas to “**mode = multikv**” Unless you’d like your **perfrom** events to completely change format this way, make sure that you set “**mode = single**” for every “[perfmon://*]” stanza in the “inputs.conf” file in your “**MyCompany_TA_windows**” app and push to your forwarders.

There is some good news!

You can reduce the wasteful bloat in windows events and save $$$ on license!

- The full steps are here: https://docs.splunk.com/Documentation/WindowsAddOn/5.0.1/User/Configuration#Configure_props.conf but the gist is:
  - Copy the default "**props.conf**" to the "**local**" directory of your new "**MyCompany_all_indexes"** app
  - Strip out all the lines except the "**SEDCMD-**" lines that are appropriate for your settings (half are for "**renderXml = false**" and the other half for "**renderXml = true**"
  - Uncomment those lines
  - Push out to your indexers

One last thing: are you using Splunk's ES SIEM?

You may not be completely in control of which version you will use and when!

- These 3 apps are bundled with "**Enterprise Security**" and different version of it are packaged with different versions of "**Splunk_TA_windows**". For example:
  - "Enterprise Security" v5.2.2 is bundled with "**Splunk_TA_windows**" v5.0.1.
  - "Enterprise Security" v5.3.1 is bundled with "**Splunk_TA_windows**" v6.0.0.
- The good news is that ALL of the preparatory steps described herein are forwards- and backwards-compatible with ALL versions of both "**Enterprise Security**" and "**Splunk_TA_windows**" so do your prep work NOW while you have time to do it instead of waiting for when you are forced to upgrade "**Enterprise Security**".

Upgrade Planner for Splunk Add-on for Windows

This is a free app intended to be the “easy button” for everyone!

- You’re upgrade-ready if all of the panels show blank or “**You are good-to-go here!**”
- The app only validates enabled Knowledge Objects. For example, if you are using “**Enterprise Security**”, there are probably hundreds of saved searches that exist but have “**disabled = true**”. These will NOT be examined. Therefore, it might make sense to keep this app installed and revisit it periodically.

We have used the “Upgrade Planner for Splunk Add-on for Windows” app to prepare for and execute 3 client upgrades and each went perfectly, with no breakage or service interruption whatsoever.

No, the one and only rating for this app on splunkbase (which happens to be 5-stars) did not come from us.

Live Demo and Q&A

Gregg Woodcock | President, Splunxter, Inc.
Noah Woodcock | Sr Consultant, Splunxter, Inc.

.conf19
splunk>

splunk>

Thank You!

Go to the .conf19 mobile app to

RATE THIS SESSION