WinWatch App for Splunk

Document Name	WinWatch App for Splunk - Installation and Configuration Guide
Document Version	1.0
Document Location	Github
Date Released	2-Jun-2016
Last Revised on	2-Jun-2016
Document Owner	Anjaneyulu Bollimuntha

Table of Contents

Contents

Purpose

This document has been developed to provide clear and detailed instructions for installation,configuration and usage of the WinWatch App for Splunk.

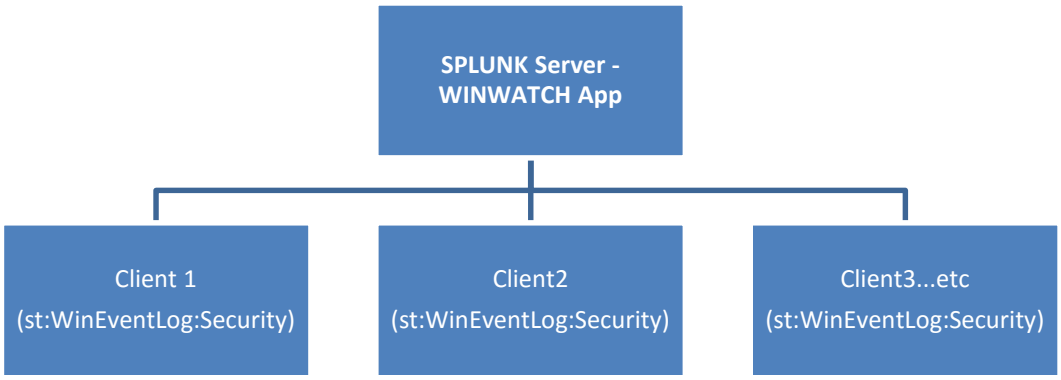
Description of the App

The WinWatch App for Splunk provides an Executive and Operational view of key metrics and trends derived using windows security event log.

App Download Location

This app is available as an approved app on the Splunkbase.
https://github.com/anjirhl/winwatch/blob/master/winwatch.tar.gz

Data Sources and Flow



Prerequisites

The following components must be installed and configured on your Splunk infrastructure for the WinWatch App to function correctly.

- Splunk Enterprise / light / cloud server.
- Log data with source type : WinEventLog:Security

```
6/1/16          06/01/2016 05:57:08 PM
5:57:08.000 PM  LogName=Security
                SourceName=Microsoft Windows security auditing.
                EventCode=4797
                EventType=0
                Type=Information
                ComputerName=anjipc
                TaskCategory=User Account Management
                OpCode=Info
                RecordNumber=24908
                Keywords=Audit Success
                Message=An attempt was made to query the existence

                Subject:
                        Security ID:            S-1-5-19
                        Account Name:           LOCAL SERVICE
                        Account Domain:         NT AUTHORITY
                        Logon ID:               0x3E5
```

Tested Splunk versions

This version of the WinWatch App has been tested on all 6.x versions.

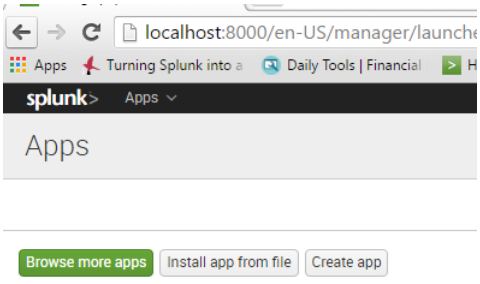
Installation Instructions

The steps to install and use the WinWatch app are provided in the sections below.

Install the WinWatch App

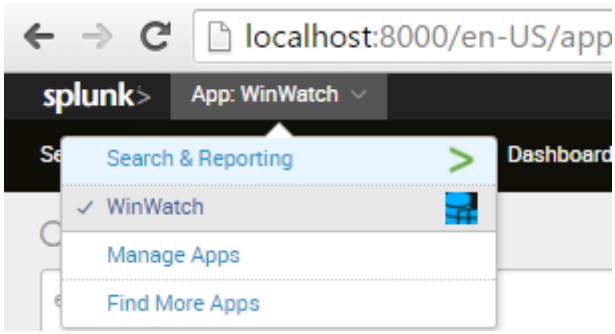
The WinWatch app has been provided as a ".tar.gz" file. Please follow the standard app import process in Splunk through the "Manage Apps" menu to install the WinWatch App.

>> Click on the "Manage Apps" from Apps drop down and Choose "Install app from file" option.

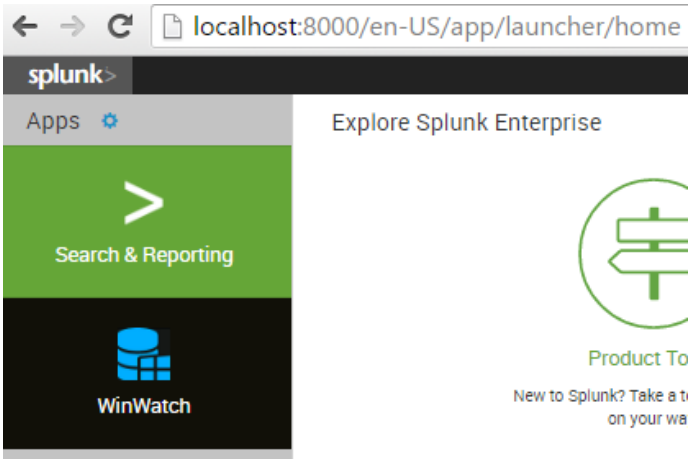


Launching WinWatch App & Dashboards

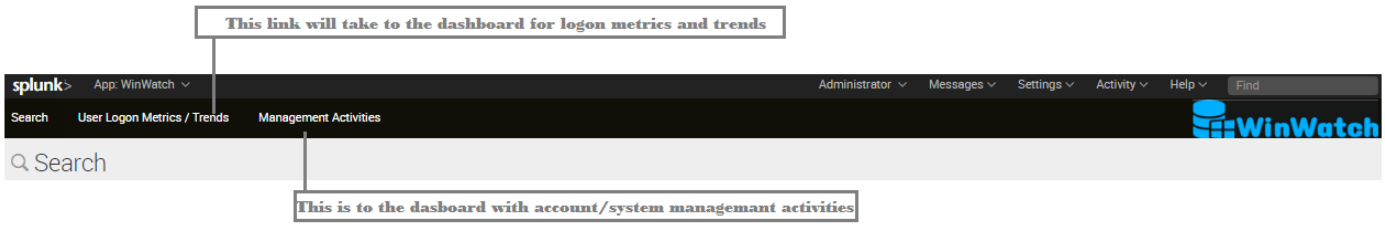
Once installed WinWatch App can be accessed from the Splunk Apps menu or from the Splunk launcher home page.



http://SplunkHost:8000/en-US/app/launcher/home



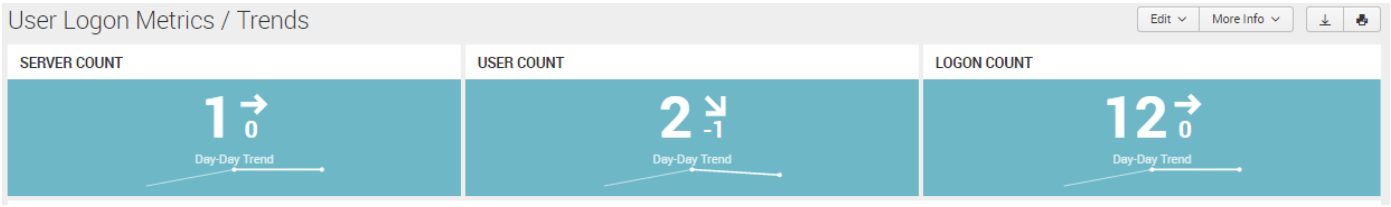
The snapshot below is that of the WinWatch App menu bar and some detail.



User Logon Metrics / Trends

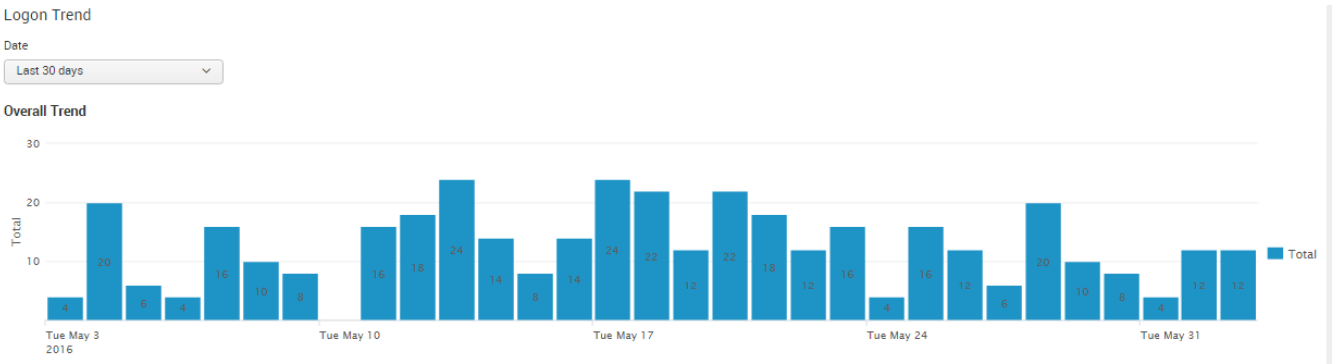
The initial three panels provide day-day comparison of below items (last 48hrs).

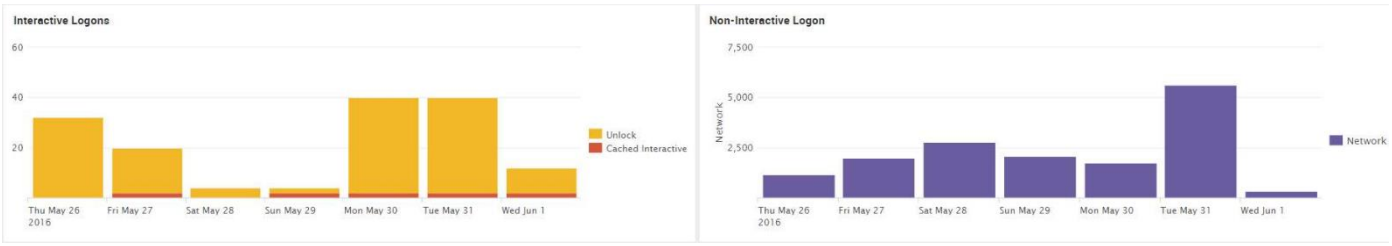
- ✓ No of servers people accessed.
- ✓ No of unique accounts used.
- ✓ Total logon count.



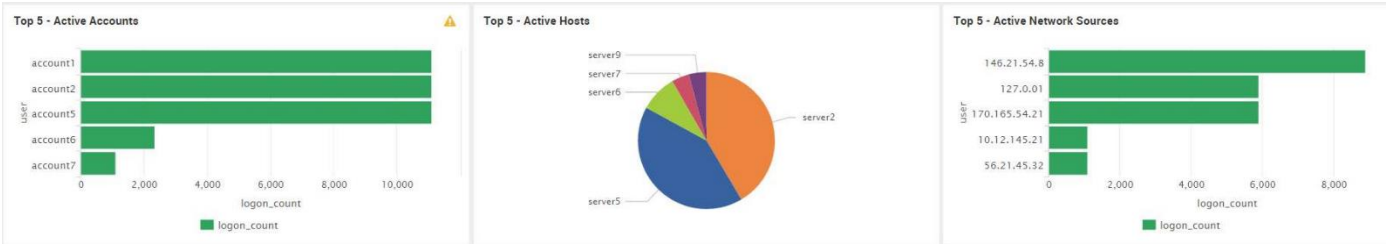
The next three charts provides logon trend over the time frame we selected.

- ✓ Total logon trend.
- ✓ Interactive logon trend
- ✓ Non-Interactive logon trend (network,batch ..etc).





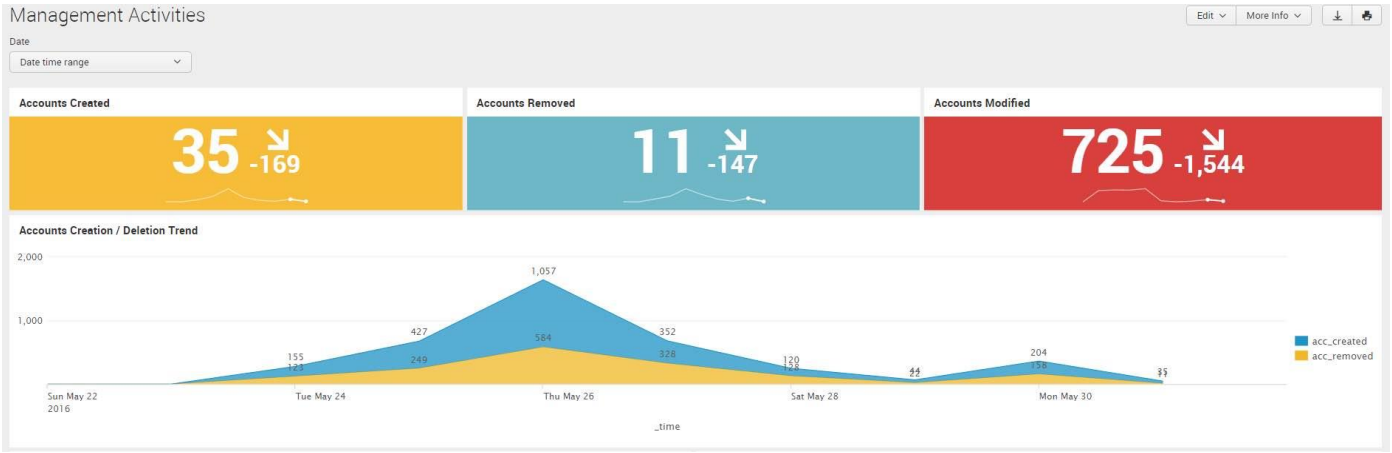
The final three charts provide the view about most active Account/Server/ Network Source details (Top - 5).



Management Activities

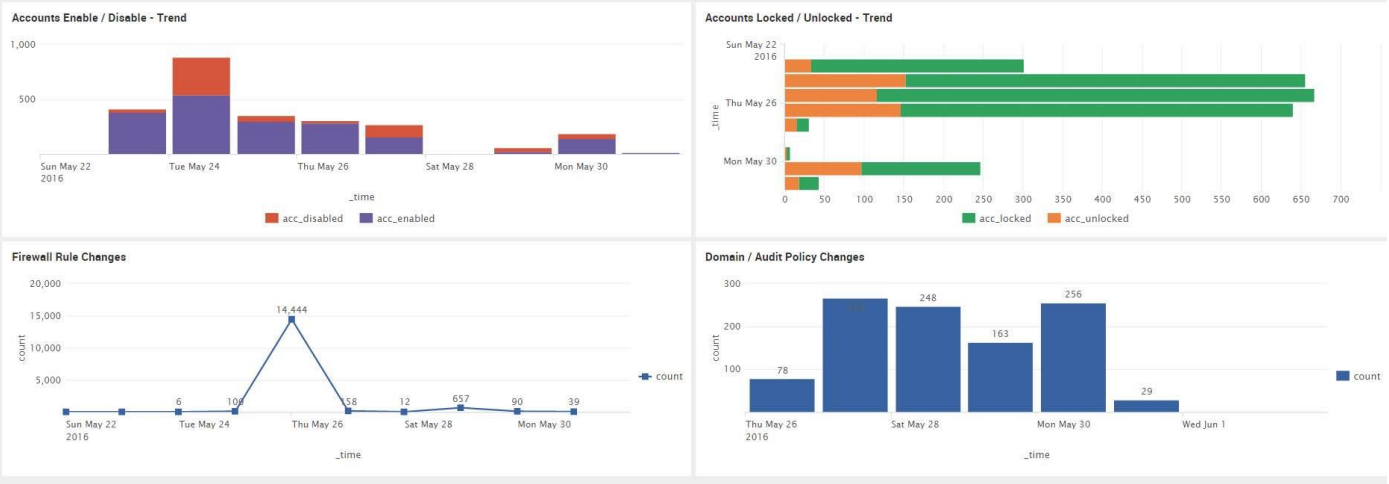
The first four panels in the dashboard provides the below details.

- Count of accounts created count (Day-Day comparison)
- Count of accounts Removed count (Day-Day comparison)
- Count of accounts Modified (Day-Day comparison)
- Trend over time (Account created / removed) for the selected timeframe.



The last four charts of dashboard provides the below details.

- Activity trend of accounts being enabled and disabled.
- Activity trend of accounts being locked and unlocked.
- Activity trend of firewall rule changes.
- Activity trend of domain and audit policy changes.



Customization for your environment

Based on what attributes are used in your environment, you can add/remove attributes in the Splunk query that is used to populate the dashboards. All of the code mentioned in the dashboard is customizable.

Support Process and Contacts

For any issues or questions related to the WinWatch App for Splunk, You can contact “anjirhl@gmail.com”

Response time SLA: **3 Days**

Resolution Time: Depends on the nature of the problem