splunk>

Install Instructions for Sample SCCM App

1. Install pre-requisities
    - Splunk Enterprise
    - DBConnect App
2. Login to Splunk
3. Click on Settings->Access Controls->Users
4. Grant your logged in use the DBX Role to your account
5. Unzip/Untar the file in the the /opt/splunk/etc/apps directory, or the C:\Program Files\Splunk\etc\apps directory if you're on Windows.
6. In the sccm directory it creates, you will find a inputs.conf file in the root of the directory. DBConnect does not recognize dmon-tail inputs from the app, so you will need to add the stanzas to your inputs.conf located in /opt/splunk/etc/apps/dbx/local or C:\Program Files\Splunk\etc\apps\dbx\local directory.
7. After adding, log back into Splunk and you will now notice an SCCM App. Click on the SCCM App.
8. Click on the Reports Tab
9. Click on Lookup Generator – Step1
10. Click on Lookup Generator – Step2
11. Click on Lookup Generator – Step 3
12. Within 15 minutes, you should start to see data populate each of the dashboards.

Notes

This sample app is only partially complete and still has the need for more features, cleanup and optimization- among others. Below, is a list of known issues with the SCCM Demo App.

- Searches call on fields that are not native to the SCCM Database. (Domain, ComputerName, UserName)
    - In order to get those values, the lookup generator creates not only a reference to the real computer name fields in SCCM, it creates an alias column called "ComputerName." This should later be removed and referenced with only proper or renamed columns.
- Post-process
    - There are several post-processing capabilities that could be implemented within these dashboards, but have not been done yet.
- Inconsistent searches
    - In some searches, you will find that the search references either |inputlookup or from a sourcetype=sccm-computer* . While each approach is viable, it's not consistent.
- Dedup statements
    - Some searches are running dedup, to prevent duplicate records from being pulled. The dedup statements were only partially implemented to some searches and they need to be validated.
- Latest Time Event
    - While being indexed in proper time, searches aren't always calling for the latest TimeKey or unique identifier. If a machine has the same name, but installed twice – you would find two records in the SCCM database. You will want to validate you're pulling the latest reference to a server, in addition to many other metrics
- Missing many use-cases
    - This App was focused on very direct use cases and is missing many more features that could be of value.
        - SCCM Logs
        - SCCM Application Health
        - CM Group Information
        - Patch Management Information
        - Windows Update Services status
        - Detailed asset information
        - Network IP history, by user and machine
        - BitLocker
        - ….And many others!