Beyond CSVs: Visualization using PowerShell, Excel and Grafana

ISACA North Texas

Friday, November 13, 2020

RCI

Downloads

- Get all of today's demos and PDFs of the slide decks from:

https://github.com/AuditClay/AuditScripts

GitHub

Agenda

- Tactical visualization using:
  - Out-GridView
  - CSVs into Excel
  - Direct-to-Excel with ImportExcel module
  - Pivot tables/charts with ImportExcel
- Strategic/long-term visualization using
  - Time-series databases (Graphite)
  - Dashboards (Grafana)

Tactical Visualization

- Short-term value, immediate results
- Use this
  - During a status meeting
  - To assist operations
  - In initial data gathering
- Tools
  - PowerShell Out-GridView
  - CSV -> Excel
  - Direct to Excel with ImportExcel module

Strategic Visualization

- Long-term tracking of compliance
- Trend/KPI reporting to management
- Dashboards
- Tools
  - Excel with pivot tables/charts
  - Time-series databases with dashboards

Import-Excel Module for PowerShell

- Written by Doug Finke
  - He has some good tutorial videos on YouTube
- Read/write Excel spreadsheets from PowerShell **without Excel installed**
- Available from PSGallery
- Install with:

```
Install-Module ImportExcel
```

Dashboard Software

- Probably already used by your operations teams (especially if you're doing DevOps)
- We'll use Grafana as a dashboard and Graphite as the time-series database

Graphite Database

- Time-series database (TSDB)
- Stores data with:
  - Name
  - Value
  - Date (in Unix epoch format - seconds since 1 January 1970)
- Input format:

```
patchage.Server0 0 1576281600
patchage.Server1 7 1576281600
patchage.Server2 29 1576281600
patchage.Server3 21 1576281600
```

Graphite Architecture (1)

- Carbon
  - Receives data via TCP/UDP input using the format in the last slide
  - Caches in memory and then sends to Whisper database files on disk
- Graphite-web
  - API to query data and build dashboard images

Graphite Architecture (2)

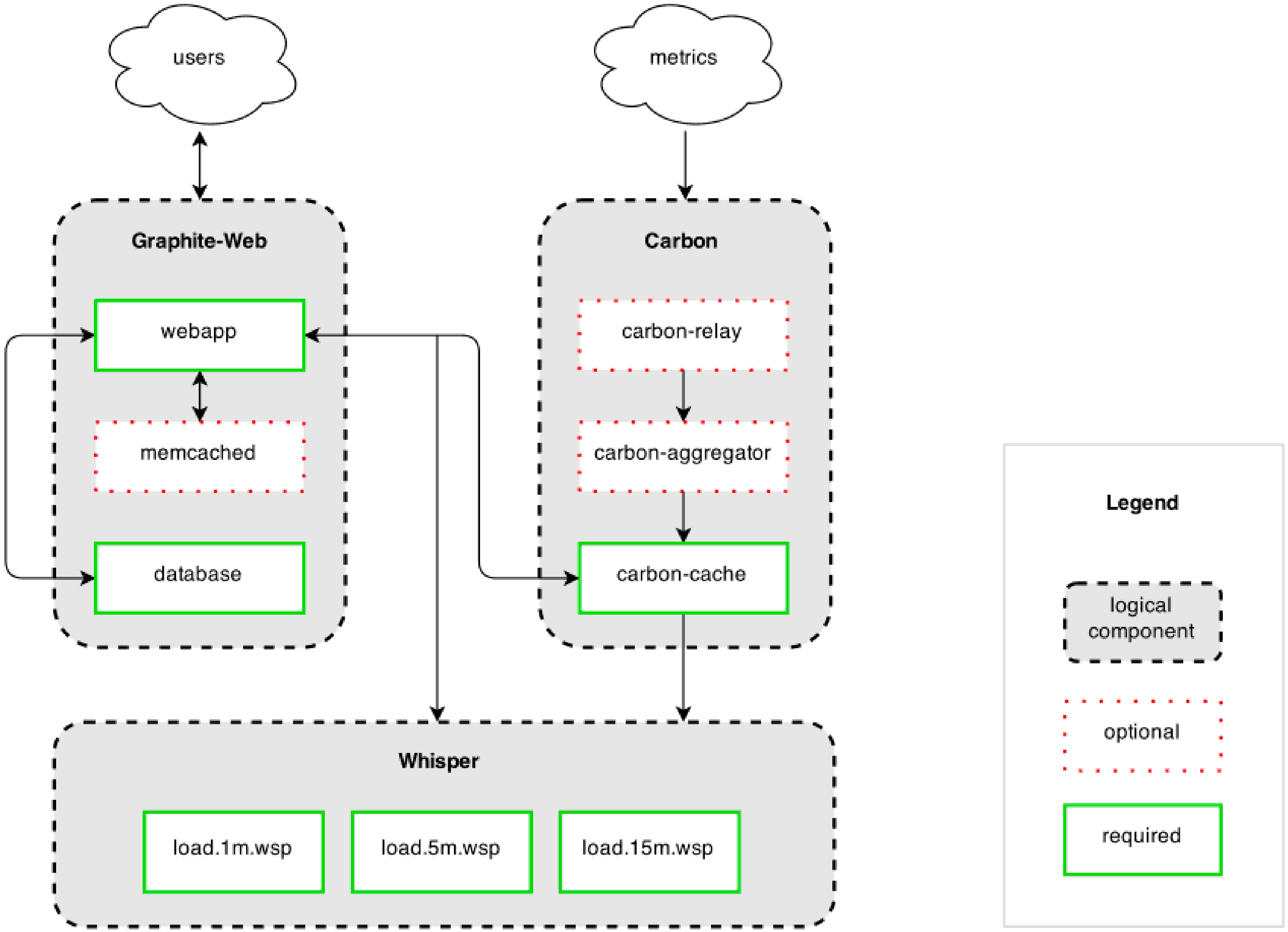
- Whisper
  - File-based database
  - Files are pre-allocated with space for required metrics

```
pattern = ^patch*
retentions = 1d:1y
```

- Metrics are stored in dot-separated form:

```
Serverstats.Server1.CPU
```

Graphite Architecture (3)



Grafana Dashboard Software

- Integrates with multiple databases
  - TSDB
  - Relational
  - AWS CloudWatch
  - Azure Montior
  - Etc.
- Allows multiple visualization types
  - Single-stat
  - Graph
  - Table
  - Etc

On Visualization

- Can't I just use my SIEM for this?
- It depends…
- TSDB works VERY well for measurement/metrics -- anything that can have a number tied to it
- Most SIEMs work well for document-based data like logs
- You may need to combine both to meet all your needs
- We often recommend a dual-SIEM setup with on for forensics/incident handling and one for compliance

Examples for This Session

- Vulnerability scanning results
- OS patching data from Windows servers

- How the data was obtained
- How we can use it strategically and tactically

The Data - Vulnerability Scans - Set 1

- Enterprise provided 80 CSV files of current Nessus scans of all servers for business unit
  - 1,000+ servers scanned
  - 29,000+ results
- Questions from IT operations:
  - How bad is it?
  - Can we batch remediation by host or by solution?
- Visualizations using Excel

The Data - Vulnerability Scans - Set 2

- Enterprise provided one year of aggregated Nessus scan results formatted for import into Graphite TSDB
  - 100 servers
  - Daily scans for one year
- Questions from management:
  - How bad is it?
  - Have we reduced risk in the last year?

The Data - Server OS Patching Data

- Enterprise provided:
  - CSV of all patches from 100 servers (taken with Get-Hotfix)
  - Text file with count of patches installed per server, per day -- suitable for input into Graphite
- Questions from management
  - Is patching happening regularly?
  - Are any servers out of compliance?
  - How many & how far out?
- Good example of measuring in the "worst possible way"
  - *Can we reduce uncertainty with minimal work?*

Demos

1. Vulnerability scans - tactical
2. Vulnerability scans - strategic
3. OS patching - strategic

Shameless Plugs!

- Interested in the 3-day version of this material? I'll have a beta run of the SANS class early in 2021.
- Sign up for more info at:

https://www.sans.org/new-sans-courses

- Check the box for SEC557

Shameless Plugs!

- Can't get enough of hearing Clay talking through your computer speakers?
- I'm teaching a 40-hour CISSP review course for the chapter next month.
- Sign up at:

https://engage.isaca.org/northtexaschapter