DevDays 10th Edition

HL7® FHIR® DevDays

NOV | 2020

One FHIR Facade for Multiple Servers

Grahame Grieve, Health Intersections / HL7

HL7 FHIR DevDays 2020, Virtual Edition, November 17–20, 2020 | @FirelyTeam | #fhirdevdays | www.devdays.com/november-2020

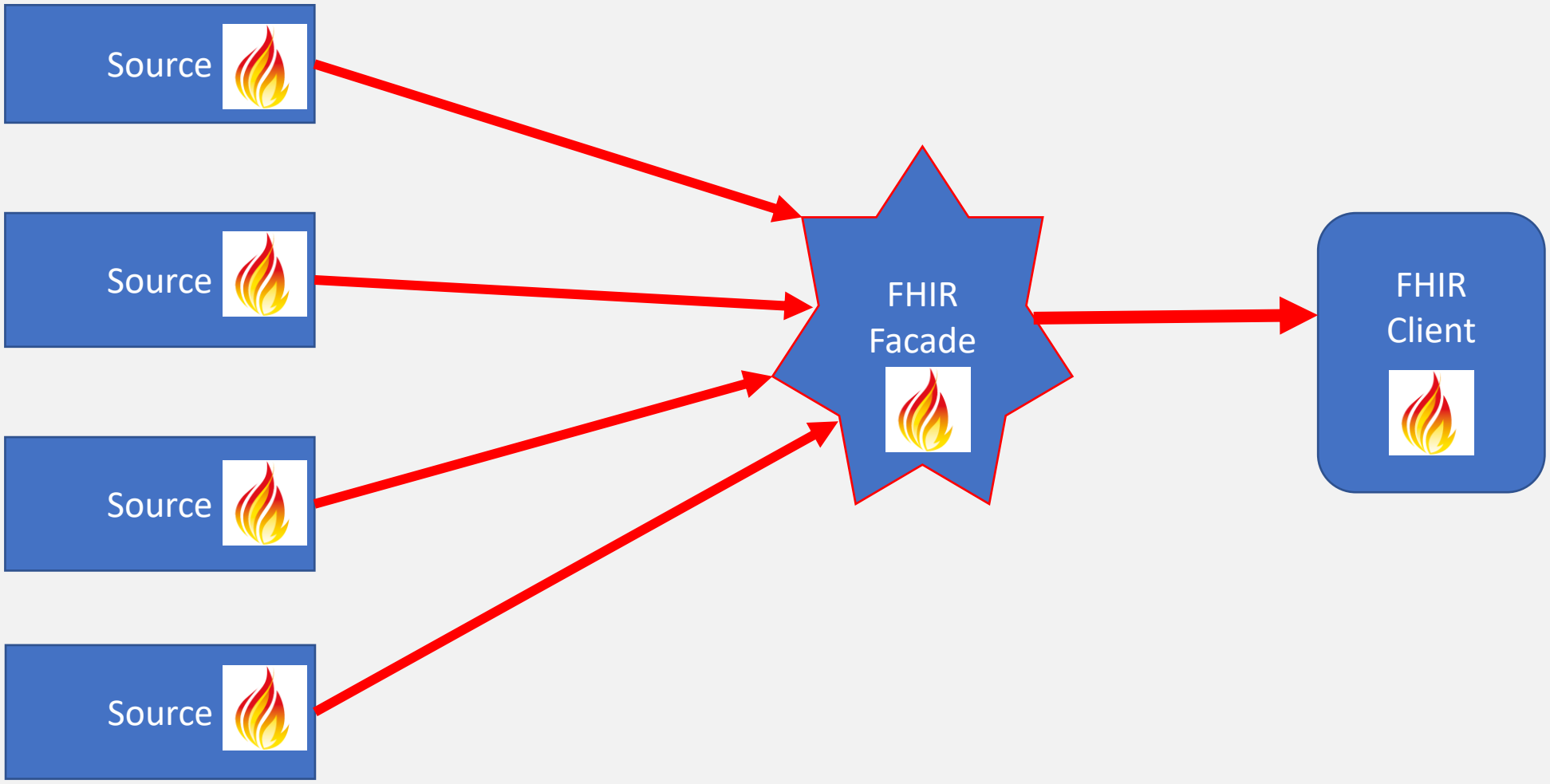
ORGANIZED BY firely

Who am I?

- Grahame Grieve
- FHIR Product Director
- FHIR Community Lead

Learning Objectives

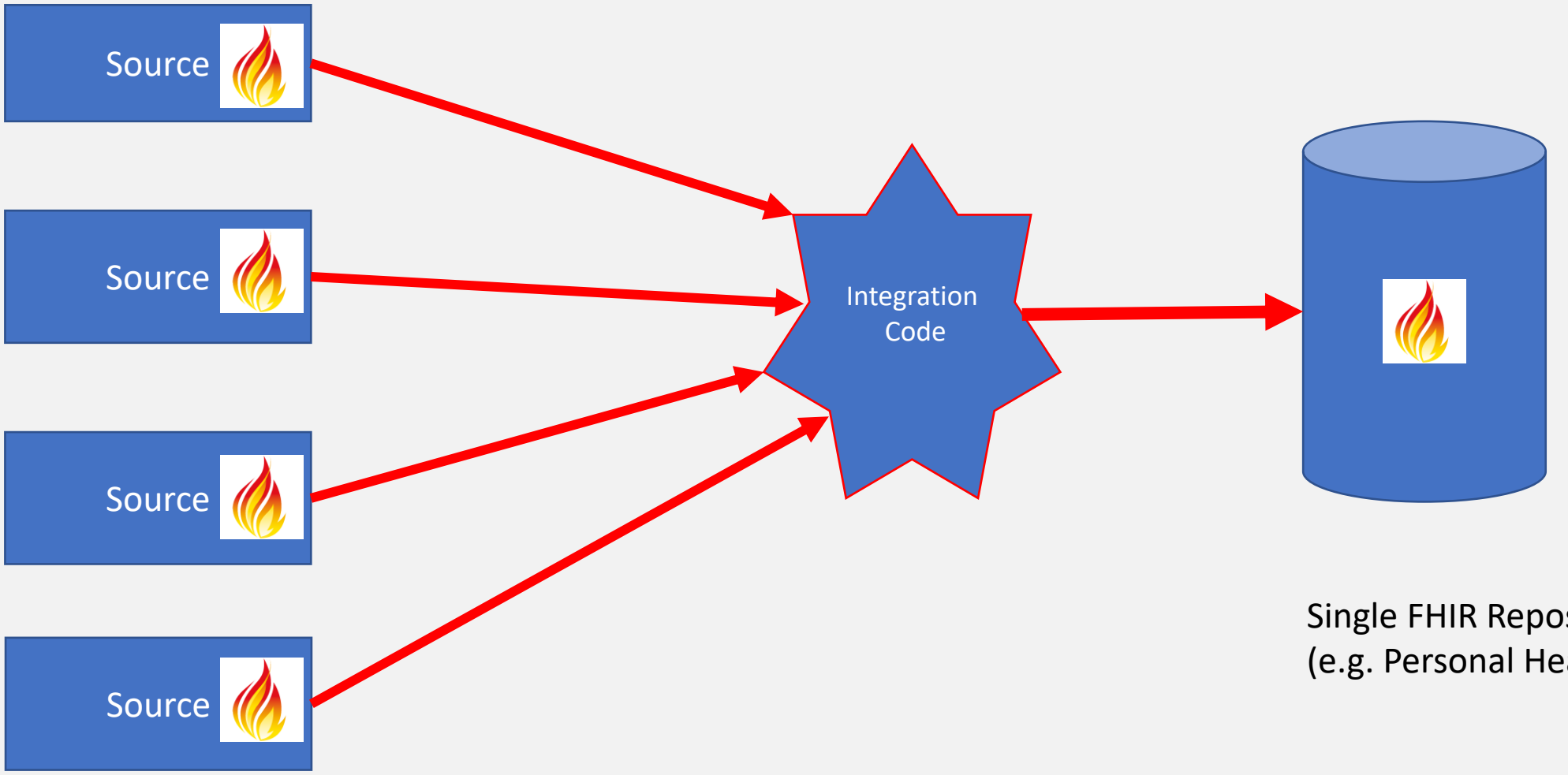
- Know the likely challenges for one facade over multiple servers
- Know some possible choices for solving the problems that arise


Source
Source
Source
Source
FHIR
Facade
FHIR
Client

One Façade Server

Assumptions:

- The client deals only with one server
- It doesn’t (need to) know about the other servers
- The back end servers are implementing a FHIR interface
- Some resources only on one server, with references between servers
- Other resources on both servers
- You have administrative/development control over both



Single FHIR Repository
(e.g. Personal Health Record)

General Challenges

- Managing Access Rights & security
- Identification / references
- Combining Search
- Inconsistent record keeping
- Distributed business logic

Managing Access

- User Authenticates with Façade Server (OAuth?)
- Façade server manages user tokens/sessions
- It's responsible for security
  - General case: API Accelerator
- Who approves requests / responses?
- Cannot just be the Façade

Scenario

- User has rights to see multiple patient records, and to search for patients meeting clinical criteria
  - “e.g. all patients with elevated creatinine today”
- User doesn’t have rights to see
  - VIP patients
  - information pertaining to sexual health clinic (Encounter.location.location = Location/shc)
  - HIV related information

Scenario #1: fetching Patients

- Get Patient/3123123123
  - Patient returned from back end has security label “VIP” → 404 Not Found
  - Patient returned doesn’t have VIP security label → 200 OK

- Get Patient?name=peter
  - Strip patients with VIP label
  - What if request is Patient?name=peter&_count=20 ?

Scenario #2: Fetching Observations

- Get Observation?code=http://loinc.org|25835-0
  - HIV request – don't pass it on; 404 instead (~400 relevant loinc codes)
  - What about Get Observation?code=25835-0 (or Observation?code=45246-6)

- Instead: pass the request on, and strip any responses with security labels

  http://terminology.hl7.org/CodeSystem/v3-ActCode#HIV + others
  - Requires specific agreements with back end systems
  - What about Get Observation?code=25835-0&_summary=count

Scenario #3: Selecting Patients

- GET Observation?encounter.patient=Patient/234
- GET Observation?subject=Patient/234

- The difference tells you if the patient has a sexual health clinic visit
- The façade server has nothing to say about this

Managing Access

- Implementing Security is a joint responsibility of façade and back end
- Recommendation:
  - Add JWT to request from façade to server
  - Server has documented responsibilities
- Other choice:
  - Restrict functionality to only what is easy – not a good choice for users

Identification / References

- Basic problem: multiple servers for one resource type
- General approach:
  - Client — search → façade
  - façade — search → multiple servers (in parallel)
  - Servers — search → façade
  - Assemble final bundle
  - Façade — search response → client

Assembling the bundle

- Identifying resources:
  - Assume client identifiers are unique (GUIDs)?
  - Prefix them with a server id e.g. s1-[id] (64 chars!)
  - Reidentify every resource with random id
    - Maintain look up table?
  - Fix all references, including html references

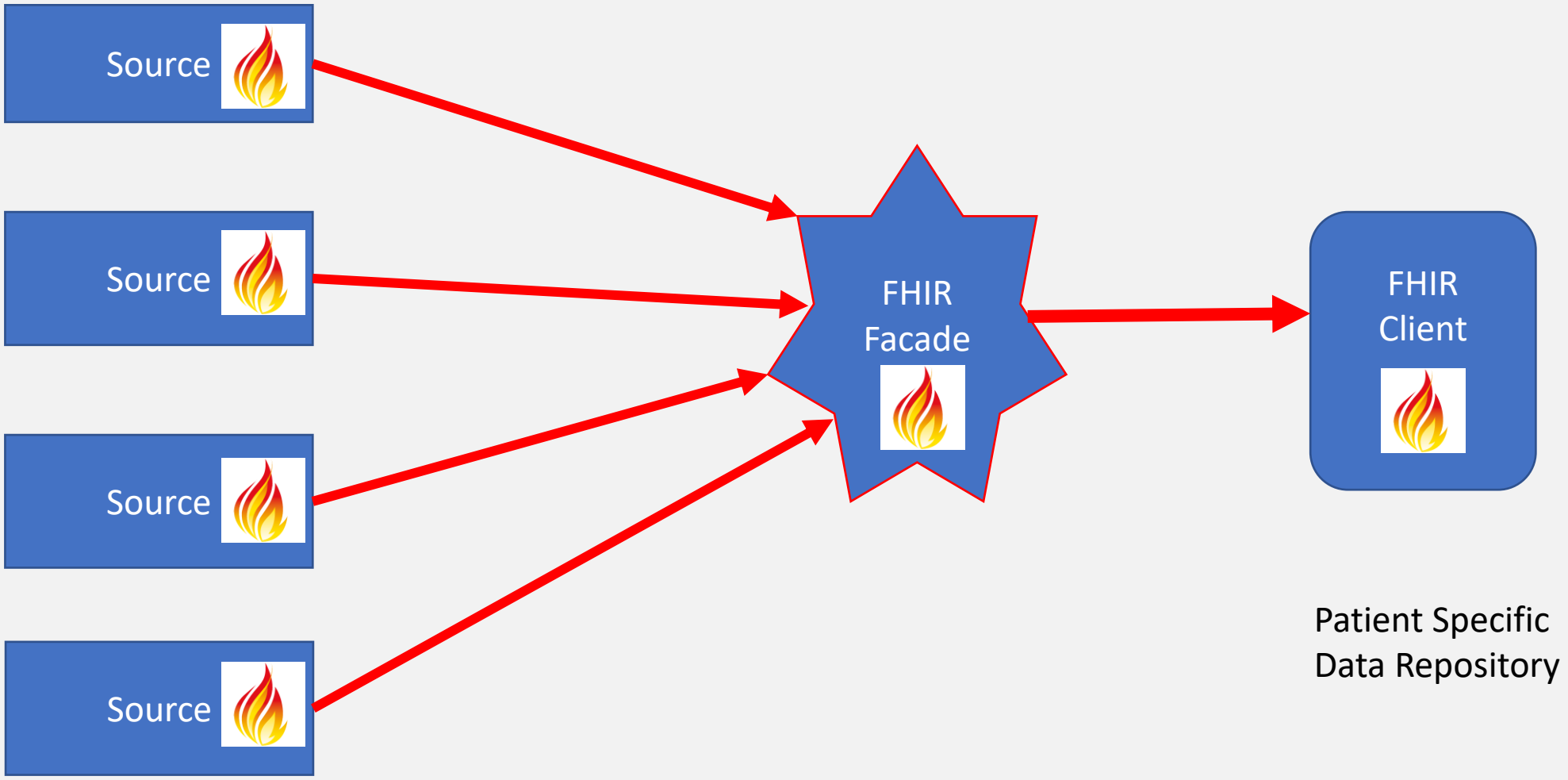
- Must know how to route reads (Get [type]/[id]) to the right server
  - GUIDs – can send to all servers
  - Don’t have to support gets…. But problematic…

Other problems

- If servers accepts POST / PUT (upsert) – which server?
  - Facades are *usually* read only
- Where does the server log?
  - Or, interplay between server & façade logs
- Joins, paging, counts…
  - Page size is implemented on the façade – all solutions inefficient somewhere
  - Join logic depends on underlying compartment logic (business specific)

Record alignment problems

- Matching Patients / Encounters on systems
  - Deep structural problems predate FHIR
- Do different resources on system represent the same concept?
  - How could you tell?
  - What should you do about it?
  - All answers are wrong (not a FHIR problem)


Source
Source
Source
Source
FHIR
Facade
FHIR
Client
Patient Specific
Data Repository

Synchronization…

Need to get records from the source. Options (not exclusive):

- Do Patient/$everything
- Do what $everything does iteratively
- Use _lastUpdated on query
- Use _history operation:
  - GET [url]/[Type]/_history
- Use Subscription
  - Notification of any change to a record for the patient

Synchronization Problem #1

What records belong to the patient?

- Resources in the patient compartment - Yes
- Linked Resources (Provenance, AuditEvent) ?
- Admin resources (Practitioner, Organization, Device…) ?
- Configuration resources (Questionnaire, ValueSet….)

Synchronization Problem #2

What about resources that go missing?

- Temporary unavailability of source (takes too long to respond)
- Too old to send (some servers sunset at 5 years)
- Moved from active list (e.g. server only sends active meds)
- Deleted on source system
- Re-assigned to a different patient
- No longer available due to changes in security / privacy on source

- Many safety problems here! (http://www.healthintersections.com.au/?p=2950)

Patient Merge

- Duplicate records for patients are created
  - Rate varies from 1% -> 20% (link, link)
    - Depends on culture, processes, patient-mix
- Specialist and Clinical staff find and fix duplicates
  - Fixing duplicates itself has an error rate – 5%?
- -> Link Patient Records - Mark duplicate in both records
  - Do you have access to linked patient?
- -> Merge Patient records - Move all information
  - What is impact for destination system? Should it merge? Should you delete anything? (How do you know what happened?)

After a Patient Merge

- What does reading the patient return?

  Get [base]/Patient/B

- 200 + record for Patient B that refers to Patient A
- 304 + redirect to Patient A, then return Patient A

- Both are potentially unsafe. Both are implemented today

After a Patient Merge

- What does referring to the patient mean?

  Get [base]/Observation?subject:Patient=B

- No records (+ OperationOutcome?)
- Records for Patient A

- Both are unsafe. Both are implemented today.
- See http://www.healthintersections.com.au/?p=2950

Learning Objectives

- Know the likely challenges for one facade over multiple servers
  - Many challenges; a facade cannot be independent of the servers
  - Security & identity are key issues
- Know some possible choices for solving the problems that arise
  - None of your choices are great
  - a facade is a special case of the general problem

Contact

- During DevDays, you can find / reach me here:
  - Via Whova App – Speaker's Gallery
  - On chat.fhir.org
  - Email: grahameg@gmail.com
  - Twitter: grahamegrieve