GRR Meetup: 3.1.0 Release

Apr 2016

Greg Castle @mrgcastle

What we're releasing

Server 3.1.0rc1

Client 3.1.0.0

PyPi today. deb, docker, install scripts etc. coming soon

Release notes: goo.gl/a7Z8Hv

What's new

Components: easier client customization

Rekall: faster acquisition, more linux profiles

Approval ACLs: require different approvals based on client labels

What’s new: continued

Powerful API: automatic collection and export

Bigquery output plugin: fast analysis at scale

Build system: pip install grr-{server|client}

What’s new: continued

Lots of bugfixes and perf improvements

Hunt UI: OR conditionals

Tons more forensic artifacts

Components

Components

Bundles of python code

Download/update separately from GRR client

Delivering Rekall and Chipsec

Add your own: blogpost coming soon

Rekall

Updateable independently of GRR

Good profile coverage of Ubuntu kernels (others coming)

AFF4acquire: faster mem acquisition (snappy)

Build system

Pip support!*

pip install --pre grr-response-server

pip install --pre grr-response-client

*For now: still some deps required and manual config to use client and server on the same machine

Approval ACLs

Approval ACLs

Powerful ACLs to enforce complex approvals

E.g. “Machines labelled ‘sensitive’ requires approval from legal and security before access is granted”

Blogpost with examples: coming soon

API

Covered in previous meetup: goo.gl/8ix5YV

Continued to migrate UI functionality to API

Enabling externally triggered collection

Bigquery

Bigquery Output Plugin

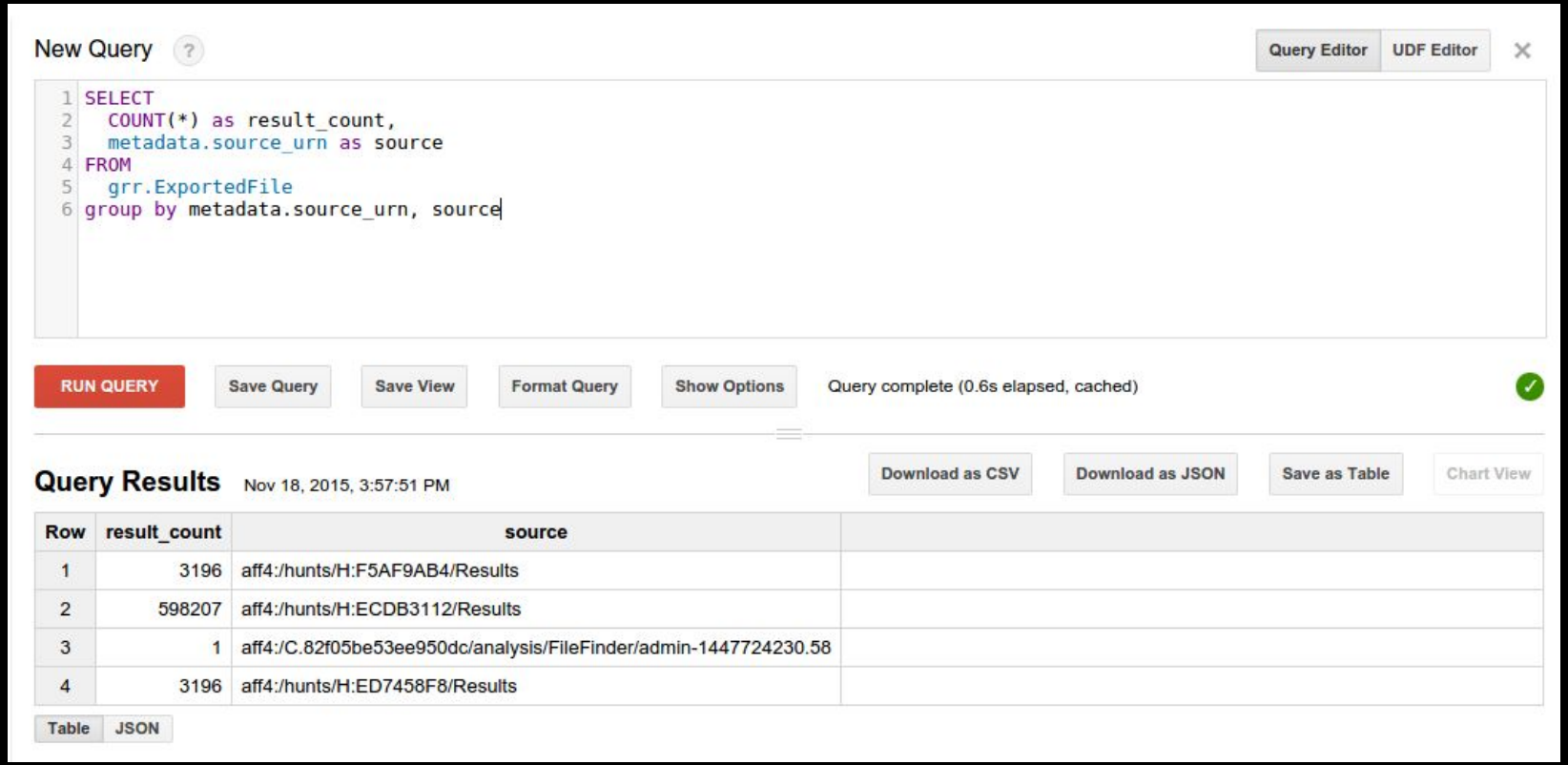
Select Bigquery output for hunts/flows

Results streamed as they arrive

Fast queries over large result sets

See blogpost: goo.gl/vRTxPW

Bigquery Output Plugin



New Query

Query Editor | UDF Editor

```
SELECT
  COUNT(*) as result_count,
  metadata.source_urn as source
FROM
  grr.ExportedFile
group by metadata.source_urn, source
```

RUN QUERY | Save Query | Save View | Format Query | Show Options | Query complete (0.6s elapsed, cached)

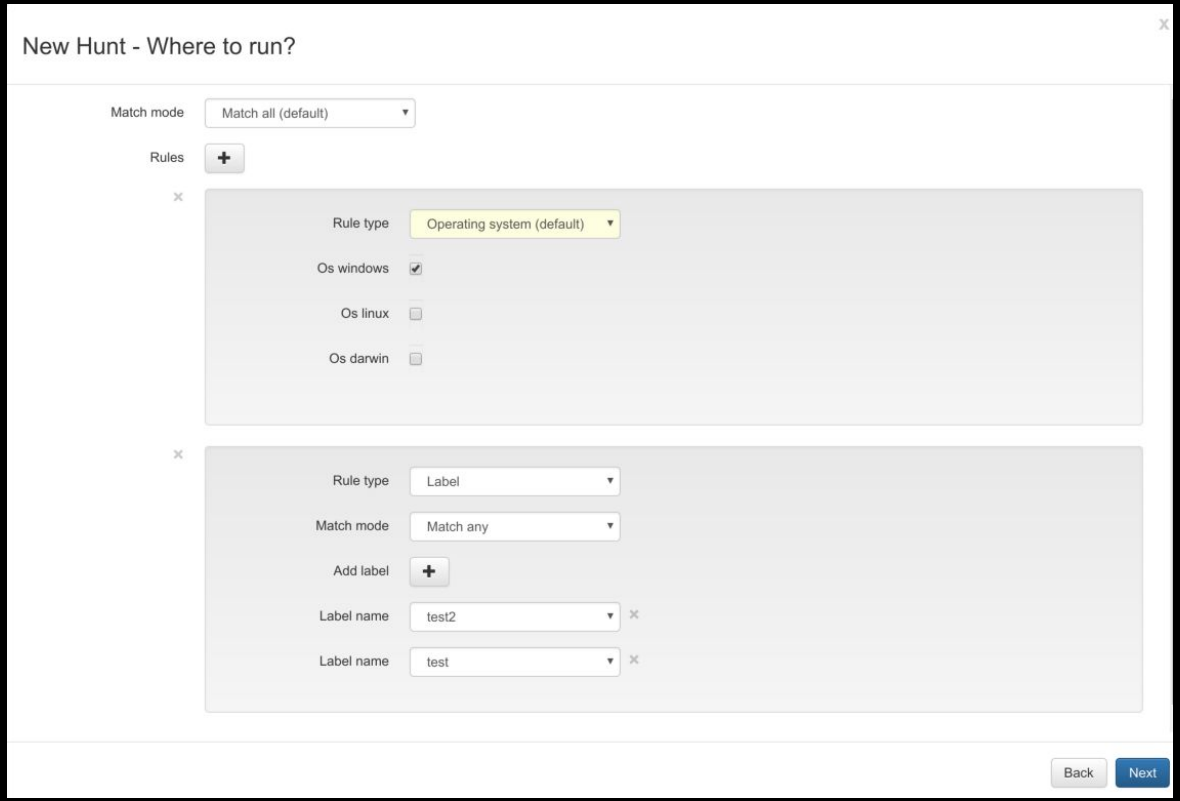
Query Results Nov 18, 2015, 3:57:51 PM

Download as CSV | Download as JSON | Save as Table | Chart View

Row	result_count	source
1	3196	aff4:/hunts/H:F5AF9AB4/Results
2	598207	aff4:/hunts/H:ECDB3112/Results
3	1	aff4:/C.82f05be53ee950dc/analysis/FileFinder/admin-1447724230.58
4	3196	aff4:/hunts/H:ED7458F8/Results

Table | JSON

UI: Hunt OR conditionals



Q2 2016

Cloud deployment: gcloud deployment mgr

Self-upgrade used at scale

Perf: hunt processing, notification Q's

UI: rekall results, hunt UI

Links

Release notes: https://github.com/google/grr-doc/blob/master/releasenotes.adoc

Bigquery blogpost: http://grr-response.blogspot.com/2015/11/using-bigquery-to-analyze-data.html

API meetup slides: https://drive.google.com/a/google.com/file/d/0B1wsLqFoT7i2MEltRFp1Zzk1Rkk/view

PyPi packages:

https://pypi.python.org/pypi/grr-response-server

https://pypi.python.org/pypi/grr-response-client

Artifact repo:

https://github.com/ForensicArtifacts/artifacts