Fighting viruses with Alfviral

2013

Fernando González

fernando.gonzalez@ricoh.es
@fegorama

Why?

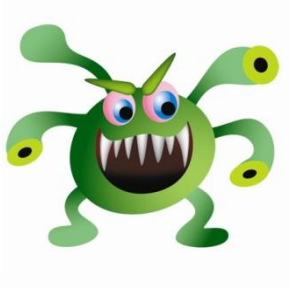
Virus today... inside of:

- Word and Writer documents
- PowerPoint and Impress documents
- PDF (Portable Document Format)
- …more

fernando.gonzalez@ricoh.es
@fegorama

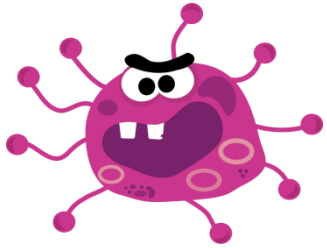
What is it?

Alfviral is a module installable in Alfresco (Repository and Share) that uses an antivirus software (currently ClamAV and VirusTotal.com) to scan both new uploaded documents and those already present in the repository.



fernando.gonzalez@ricoh.es
@fegorama

How it works



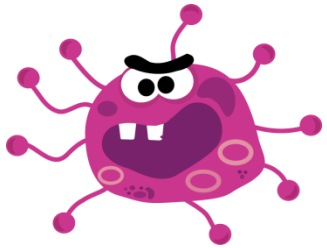
Three different modes:

- Running virus scan program with defined parameters
- Sending document data flow to an antivirus port
- Using JSON/HTTP protocol to send files to www.totalantivirus.com

fernando.gonzalez@ricoh.es
@fegorama

Features

- Detection through 3 modes
- Use of "policies" to scan uploaded and/or read content
- Use of "scheduler" to scan spaces programmatically
- Use of action "Scan" in user interfaces (Alfresco and Share)
- File exceptions
- Assignment of "aspects" to classify infections

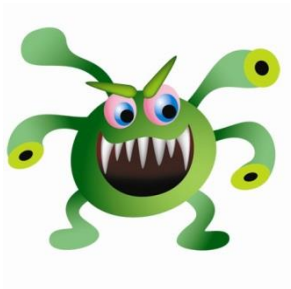


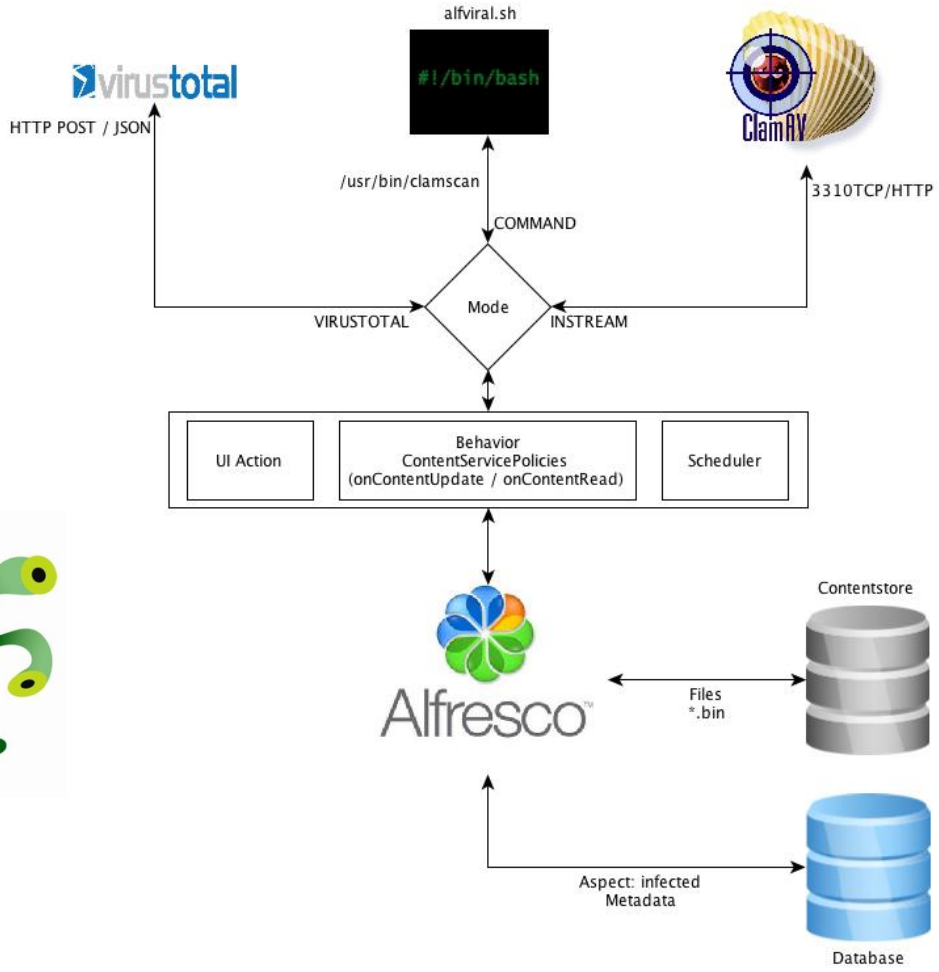
fernando.gonzalez@ricoh.es
@fegorama

Architecture

Modes

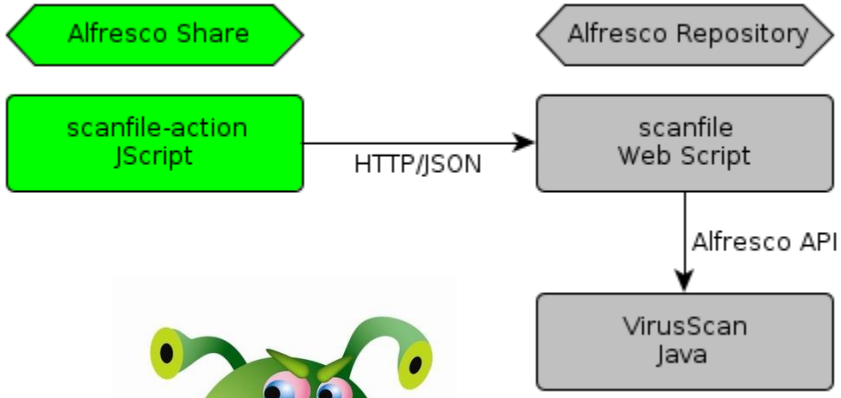
- Command
- Instream
- Virustotal





Action Share to Repository

- Java Class
  - VirusScan
- Repository action (Javascript)
  - Scanfile
- Share ui-action (Web Script)
  - Scanfile-action

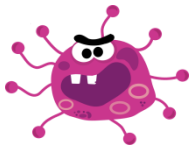


Configuration

Use of alfviral.properties file for configuration

- Modes
- Events
- Schedules
- Exceptions

```
# Command to exec, i.e. clamscan, alfviral.sh, etc.
alfviral.command=C\:\\Users\\fegor\\Documents\\alfviral.bat

# Config for ClamAV in stream data
alfviral.timeout=30000
alfviral.host=127.0.0.1
alfviral.port=3310

#Config for VIRUSTOTAL
vt.key=246df658bca5e2968956c01b2eb3a00b0cb506bda774b7148802020302
vt.url=https://www.virustotal.com/vtapi/v2/file/scan

# Modes: COMMAND, INSTREAM, VIRUSTOTAL
alfviral.mode=VIRUSTOTAL

# Events
alfviral.on_update=TRUE
alfviral.on_read=FALSE

# Scheduled action
alfviral.scheduled.pathQuery=/app:company_home/st:sites
alfviral.scheduled.cronExpression=* * 3 * * ? 2099

# List of file exceptions
alfviral.file.exceptions=text/html|text/xml|application/pdf|image/jpeg|text/plain
```



Aspects for detection control

Properties personalized based on type of infection, for example:

- Date of detection
- Code of response
- ID Scan
- SHA256
- Positives
- Etc.

Fecha de detección:

10/10/2013

DD/MM/AAAA

¿Desinfectado?

Código de respuesta: *

1

Mensaje: *

Scan finished, scan information embedded in this object

Recurso: *

275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538a

ID Scan: *

275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538a

Link: *

https://www.virustotal.com/file/275a021bbfb6489e54d471899f7

SHA256: *

275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538a

Positivos:

46

More ways to scan

- **Automation**
  - Upload/Create and Load documents
  - Actions/Rules
- **Scanning Planification**
  - Scheduled Actions
- **Interactive Scanning**
  - Actions Run
  - UI Actions

fernando.gonzalez@ricoh.es
@fegorama

To Do…

List of Mime-Types inclusions

Dashlets for monitorization

Reports of activity

Refactoring, refactoring and refactoring…

Advanced To Do… ☺

Connectors and interfaces for scanning and virus detection for:

- Symantec
- Trend Micro
- McAfee
- Avast!
- …and more!

Where is the project?

http://code.google.com/p/alfviral

fernando.gonzalez@ricoh.es
@fegorama

PUT YOUR CONTENT TO WORK

Alfresco Summit 2013