Update on the Filtered Alert Hub

Presented 21 September, 2017
by Eliot Christian
at the 2017 CAP Implementation Workshop
(Rome, Italy)
http://preparecenter.org/resources/cap-workshop-2017-filtered-alert-hub

We see many countries have already implemented CAP-enabled alerting, and it looks like all countries will do so eventually. Soon there will be thousands of CAP alert sources worldwide, together delivering hundreds of alerts per second.

And so, the time is ripe for the next step: technology to select from this rich trove of emergency alerting just those alerts needed for a particular use.

This presentation is an update on the Filtered Alert Hub project--one example of such technology.
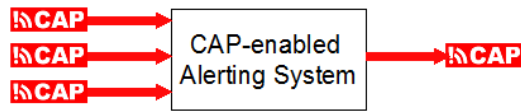
Presentation Outline

➡️ **Overview**

➤ Current Status

➤ Technology

➤ From Prototype to Operations

Filtered Alert Hub

2

I will start with an overview of the Filtered Alert Hub.

CAP-enabled Alerting

➢ CAP-enabled systems gather from selected sources, then process alerts as needed for the particular purpose (e.g., disaster management, news, public safety...)

➢ Internet news feeds and the CAP standard enable alerting to focus on any topic and at any scale (community, city, nation, region, worldwide)

➢ CAP alert feeds from many sources: only some are official, not all are public, not all are without charge

Filtered Alert Hub   3

As we know, CAP-enabled systems gather from selected sources, then process alerts as needed for the particular purpose (e.g., disaster management, news, public safety, and so on). Today, you can get CAP alert feeds focused on many different types of hazard, at any scale.

The smallest scale CAP-enabled systems are "Neighborhood Watch". At the city scale, CAP-based systems are available in products and services such as "Microsoft CityNext" and IBM's "Smarter Cities".

Most commercial weather companies offer CAP-based systems, including The Weather Company, Accuweather, and MeteoFrance International. The International Federation of Red Cross and Red Crescent Societies is actively pushing CAP-based alerting, especially in its "Hazards App".

We recognize that many CAP-enabled sources are not official from a government perspective.

We also note that most CAP-enabled alerting is not published to the public--alerts are exchanged privately.

Not all CAP-enabled alerting is free, either. For instance, Pinkerton's charges for its CAP-based alerting services, used by 80 of the world's largest 100 businesses.

Alert Hubs

➢ Online publish/subscribe service aggregates CAP alerts for easy access, and pushes new alerts to subscribers

➢ Filtered Alert Hub like a search engine, for CAP alerts

➢ Copies of cap alerts from alerting authorities are then disseminated broadly, at no extra cost to the authority

➢ Major Benefits, as a "cloud-based service":
- Speed
- Scale (performance, reliability, availability)
- Redundancy
- Security and Authenticity
- Analytics

Filtered Alert Hub   4

Many CAP-enabled alerting systems gather CAP alerts from multiple online sources, typically Internet news feeds operated in "publish/subscribe" mode. A CAP Alert Hub aggregates alerts from CAP news feeds to simplify discovery and access, just as a search engine aggregates Web pages.

Alert publishers can decide to have a copy of their posted CAP alerts on any available Alert Hub. This extra copy is in addition to, and does not interfere with, any other ways that the authority publishes alerts.

The advantage of an Alert Hub is that popular network publishers can then easily disseminate alerts to everyone who needs them. In addition to Google, these publishers include companies such as The Weather Company, Accuweather, news organizations, telecomm services, and NGO's such as the IFRC, among others. This dissemination help is at no cost to the alerting authority.

When implemented on the cloud, a CAP Alert Hub has other benefits:
Speed - Dissemination time is crucial for sudden-onset events such as earthquakes, tsunami, flash floods, and tornadoes
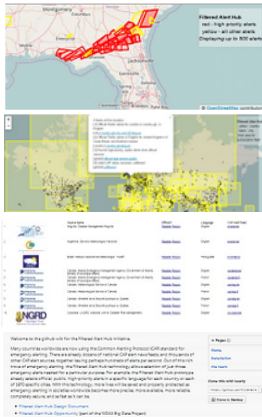**Scale** - The global scale dissemination infrastructure has high performance, high reliability, and high availability
Redundancy - An additional copy of alert messages is kept elsewhere from the originator
Security and Authenticity
**Analytics** - An aggregator simplifies analysis for optimizing alert dissemination

It should be understood that emergency alerting is accomplished through the efforts of many actors, from family through community, to cities, states, and nations, and to various international institutions, spanning government, commercial, and other sectors.

The Filtered Alert Hub will be one among the many services in societies worldwide that support emergency alerting.

Here is a screen shot of the Filtered Alert Hub web site. This page includes links to:
    the current CAP alerts,
    the available subscription feeds,
    the CAP sources, and
    the wiki page about our project.
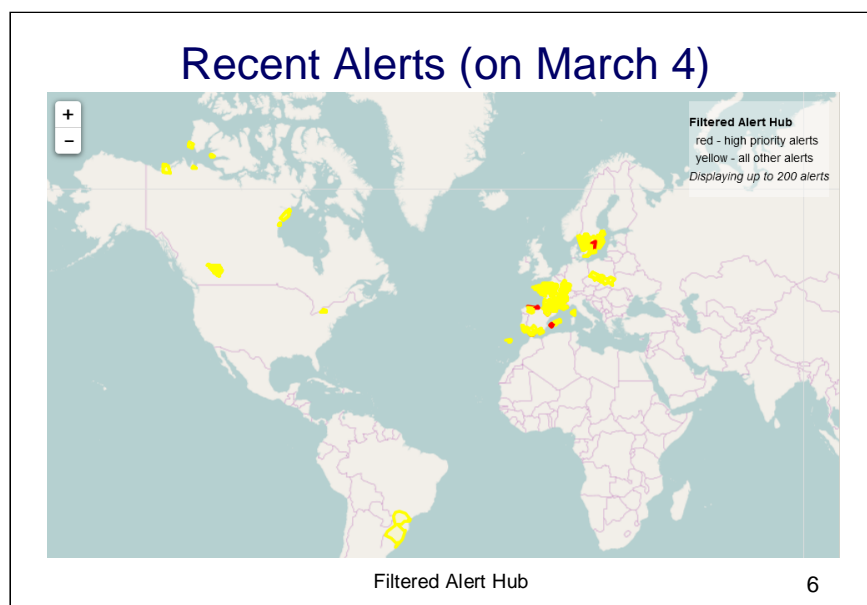
This screen shot, taken on March 4, shows what were then-recent alerts.
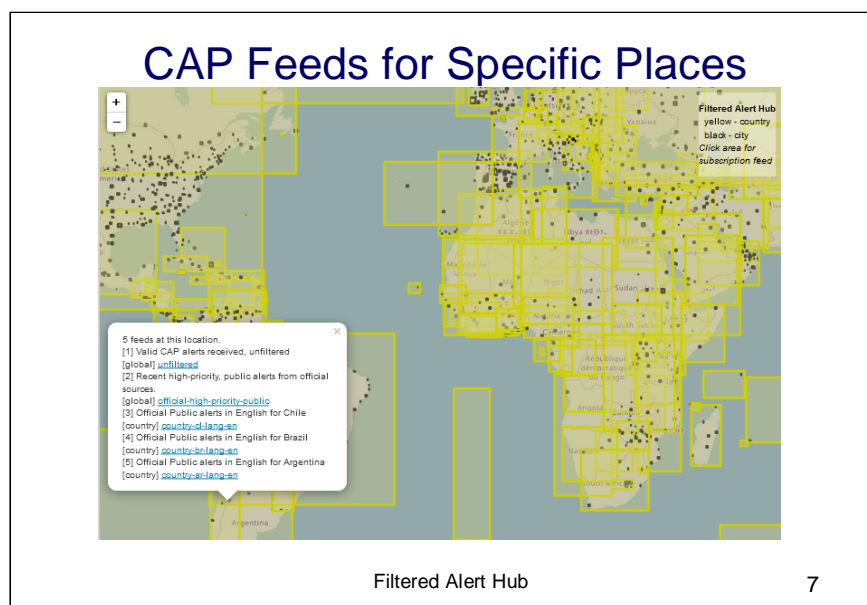
This screen shot shows the areas covered by feeds specific to a place. The Filtered Alert Hub generates about 2100 feeds now--one per country and one for each of 1870 cities.

At the clicked point, we see there are 5 Alert Hub feeds available--three at national scale (Argentina, Brazil, and Chile) plus two at global scale.

Filtered Alert Hub Sources

Global Disaster Alert and Coordination System (GDACS)
International Federation of Red Cross and Red Crescent Societies (IFRC)

Anguilla	Estonia	Macedonia	Romania
Argentina	Finland	Maldives	Samoa
Austria	France	Malta	Serbia
Belgium	Germany	Mexico	Slovakia
Bosnia and	Greece	Moldova	Slovenia
Herzegovina	Guyana	Montenegro	Solomon Islands
Brazil	Hungary	Myanmar	Spain
Bulgaria	Iceland	Netherlands	Sweden
Canada (3)	Indonesia	New Zealand (2)	Switzerland
China (2)	Ireland	Norway	Taiwan
Colombia	Italy	Papua New	Thailand
Croatia	Kuwait	Guinea	Tonga
Cyprus	Latvia	Poland	United Kingdom of Great
Czech Republic	Lithuania	Portugal	Britain and Northern Ireland
Denmark	Luxembourg		United States (6)

Filtered Alert Hub   8

Here are the CAP alert sources now defined at the Filtered Alert Hub. The first two sources are international, the rest are at a national level. In parentheses we see where a nation has multiple CAP news feeds.

Please note that any of these sources may be an aggregator itself. For instance, one of the United States sources aggregates CAP alerts from more than 1,000 sources within the U.S.

Also, some official, national CAP feeds are not included merely because the CAP alerts provide only a geocode for the alerting area. The Filtered Alert Hub does not include a gazetteer of geocodes, so it needs the CAP alert source to provide circle or polygon coordinates .

Filtered Alert Hub is Part of the *NOAA Big Data Project*

➢ NOAA Collaborators: Amazon Web Services, Google Cloud Platform, IBM, Microsoft, Open Commons Consortium

➢ Each Collaborator has a signed CRADA (Cooperative Research and Development Agreement) with NOAA

➢ Each Collaborator also anchors a "Data Alliance", allowing other companies/organizations to join in

Filtered Alert Hub

9

The effort to develop and deploy the Filtered Alert Hub technology is part of the "NOAA Big Data Project". That project involves five NOAA Collaborators: Amazon Web Services, Google Cloud Platform, IBM, Microsoft and the Open Commons Consortium.

Each Collaborator was invited to help develop this technology under its existing CRADA (Cooperative Research and Development Agreement) with NOAA.

Under the Big Data Project, each of these five Collaborators is also an anchor for a "Data Alliance". This allows other companies and organizations to be included, subject to mutual agreement with NOAA.

Presentation Outline

➢ Overview

➡ **Current Status**

➢ Technology

➢ From Prototype to Operations

Filtered Alert Hub

10

Now, let me report on the Current Status of the Filtered Alert Hub.

Filtered Alert Hub Project

➢ Collaborative project with working prototype now
➢ Several partners at present (others are welcome):
Amazon Web Services, Open Commons
Consortium, IBM and The Weather Company,
Hong Kong Observatory, Honeycomb Networks
➢ Core components are *Free Open Source Software*
➢ Contact me about getting involved in this

Filtered Alert Hub   11

At the wiki page, you can see the collaborators on the Filtered Alert Hub technology: Amazon Web Services, the Open Commons Consortium, IBM and The Weather Company, WMO's Hong Kong Observatory, and Honeycomb Networks.

Core functions of the Alert Hub are Free Open Source Software in the public domain.

I am leading this initiative and we welcome additional collaborators.

Current Status

➢ Prototype running on the Amazon Cloud, 3 copies

    Original in Europe, AWS account: Eliot Christian account

    Clone-1 in USA, AWS account: Hong Kong Observatory

    Clone-2 in USA, AWS account: Honeycomb Networks

➢ AWS is helping to optimize the implementation for speed

➢ Separate implementation developed by Ian Ibbottson,
running on the Open Commons Consortium (OCC) cloud

➢ Ian's version uses "Rabbit Message Queue"

    RabbitMQ implementation not dependent on any specific cloud;
appears to be faster, and simpler to document and maintain

Filtered Alert Hub

12

A Filtered Alert Hub prototype is running now. It is implemented on the Amazon Cloud, and there are two clones of the original. The original is running on the Amazon Cloud in the Europe region, specifically in Ireland. It runs under my personal account.

One of the clones is running on the Amazon Cloud in the USA, under an account belonging to Hong Kong Observatory (HKO). This was mentioned in the GMAS presentation by Miriam Andioli in her presentation yesterday.

The other clone is also coming up on the Amazon Cloud in the USA, under an account belonging to Honeycomb Networks.

AWS experts are helping us to optimize the Amazon Cloud implementation to make it as fast as possible.

There is a separate implementation of the Filtered Alert Hub which does not use the Amazon Cloud. That was developed by Ian Ibbottson and It is running on the cloud facilities of the Open Commons Consortium. It uses a technology called "Rabbit Message Queue".

This RabbitMQ implementation appears to be substantially faster than the Amazon Cloud implementations, although testing and optimization are ongoing. In any case, we expect theRabbitMQ implementation to be simpler to implement, document, and maintain. Also, the RabbitMQ implementation will not have a strong dependency on any one cloud provider.

Presentation Outline

➢ Overview

➢ Current Status

➡ **Technology**

➢ From Prototype to Operations

Filtered Alert Hub   13

Next, I want to do a brief Technology Overview of the Filtered Alert Hub.

The Filtered Alert Hub handles only alerts that comply with the CAP standard and only CAP alert messages published with Internet news feeds. The Filtered Alert Hub technology supports both of the Internet news feed standards: RSS and Atom.

Design of the Filtered Alert Hub

➤ Free technology for CAP alerts filtered by location, language, and other criteria (e.g., "official−only")

➤ Cloud-based: Highly Available, Reliable, Secure

➤ To minimize delay, sources push a stream of alerts to the Hub, the Hub immediately pushes to subscribers

Filtered Alert Hub   14

The "Filtered Alert Hub" prototype aggregates CAP alerts from selected sources and offers those alerts as more specific CAP news feeds. The output feeds are filtered by location, language, or other alert content.

For example, there is a filtered feed for "official−only" and "high-priority only". This feed selects high-priority CAP messages from official sources, making it easy to quickly warn everyone in the alerting area to take immediate action.

The Filtered Alert Hub is cloud-based. As noted before, this imparts high levels of availability, reliability, authenticity, and security.

For updating, CAP alert feeds are normally polled periodically, typically once per minute. But, for sudden-onset events, the Filtered Alert Hub offers CAP alert sources the option to "push" an alert immediately and it offers CAP alert subscribers the option to receive a pushed alert immediately. Used this way, warnings can be delivered in a second or two.

Prototype Architecture

Alert Hub

CAP alerts by news feed (RSS, ATOM) — alerts → pull → input feed subscriber

output feed publisher → pull → CAP alerts by news feed (RSS, ATOM) → Alert Hub news feed subscribers

CAP alerts by direct push (HTTPS POST) — alert → push → input push receiver

output push sender → push → CAP alerts by direct push (HTTPS POST) → Alert Hub direct push receivers

Filtered Alert Hub 15

The architecture of the existing Filtered Alert Hub prototype focuses on the real-time challenge to get a copy of every newly published CAP alert and disseminate it quickly to each subscription that has specified filters matching that alert.

The heart of the system is a Near Real-Time Event Processing pattern. This event-driven architecture is implemented with Amazon Web Services (AWS) Lambda.

The prototype uses four additional AWS Services primarily: Simple Storage Service (S3), Simple Notification Service (SNS), ElasticSearch, and DynamoDB. It also uses the AWS Simple Email Service and the AWS API Gateway service.

Other CAP Alert
Publishing Methods

- Publish an alert by e-mail to *sourceID*@alert-hub.net

- Upload a single CAP alert file already prepared

- Use this online form to create a new CAP alert

Filtered Alert Hub

16

The Filtered Alert Hub includes other ways to publish a CAP alert in addition to a direct push to the Hub or an updating of an Internet news feed.

For example, the Botswana Department of Meteorological Services disseminates its CAP alerts by e-mail. The Filtered Alert Hub lets DMS publish to the world as well. They just send alerts in English to "bw-dms-**en**@alert-hub.net"; and alerts in the Tswana language to "bw-dms-**tn**@alert-hub.net".

As part of the ability for the Filtered Alert Hub prototype to accept a "pushed" alert immediately, the prototype also provides a web form for direct entry of a CAP alert via the AWS Simple Storage Service "hosted Web site option".

This web form (example shown here) uses simple HTML and client-side Javascript. The form can accept immediate upload of an already prepared CAP alert as well as direct editing from an empty form. The form also links to templates for text CAP elements such as headline, description, and instruction. As you can see, the form includes a mapping tool as well.

This form is open for any alerting authority to create and publish CAP alerts. That would be much easier and cheaper than installing freeware or buying a CAP publishing tool.

WMO Alert Hub Prototype

The WMO Alert Hub prototype aggregates alerts across feeds published by sources in the International Register of Alerting Authorities

Filtered Alert Hub

17

The WMO Alert Hub was proposed by the United States several years ago, and has been widely endorsed in WMO and associated commercial companies. The Filtered Alert Hub technology now running is designed to be a prototype of the WMO Alert Hub.

A key feature of the prototype is that it aggregates CAP alerts from CAP news feeds published by official alerting authorities listed in the international Register of Alerting Authorities.

International Register of Alerting Authorities

Filtered Alert Hub

18

WMO established the international Register of Alerting Authorities in 2009. Today there are about 500 registered authorities, including at least one from each of the WMO Members, plus one from each of the National Red Cross/Red Crescent Societies.

Technology can be Customized

> ➢ **Scale can be from Local to Global**

> ➢ Alerting can be Private and/or Public

> ➢ Alerts can be Official Sources or Not

> ➢ Filters can Distinguish Priority Alerts

Filtered Alert Hub

19

The Filtered Alert Hub technology can be customized to suite different purposes.

For instance, the vast majority of emergency alerting occurs at the scale of a neighborhood or city. Such local alerting sources could be served by a community-scale Filtered Alert Hub instance that aggregates among police, fire, NGO's and other actors.

Yet, the same Filtered Alert Hub technology can support aggregation at much broader levels: county, state, nation, region, or global. For example, the national alerting system of the United States currently aggregates only about 1,000 CAP sources, although many thousands of CAP sources can be expected when CAP feeds are published by the nation's 3,000 counties and 300 large cities.

Technology can be Customized

➢ Scale can be from Local to Global

➢ **Alerting can be Private and/or Public**

➢ Alerts can be Official Sources or Not

➢ Filters can Distinguish Priority Alerts

Filtered Alert Hub   20

The Filtered Alert Hub technology can support private as well as public messaging about hazard threats. For instance:
- the initial report of an emergency situation is often a private message to the local emergency call center;
- private messaging is common as experts or security personnel communicate with emergency managers about a given hazard among themselves as a threat is being evaluated;
- alerting authorities in different jurisdictions may send alerts privately so that the appropriate local authority can send public alerts if they so decide.

Because each valid CAP alert message is identified as "Public", "Private", or "Restricted" in its mandatory "scope" element, the Filtered Alert Hub easily makes that distinction by simply adjusting filter expressions as needed.

Technology can be Customized

➢ Scale can be from Local to Global

➢ Alerting can be Private and/or Public

➢ **Alerts can be Official Sources or Not**

➢ Filters can Distinguish Priority Alerts

Filtered Alert Hub

21

The Filtered Alert Hub technology can ingest any CAP alert feed, whether the source is considered official or not. As mentioned before, the WMO Alert Hub prototype distinguishes official sources of public alerts through reference to the international Register of Alerting Authorities. That distinction can be customized.

Technology can be Customized

> ➢ Scale can be from Local to Global

> ➢ Alerting can be Private and/or Public

> ➢ Alerts can be Official Sources or Not

> ➢ **Filters can Distinguish Priority Alerts**

Filtered Alert Hub   22

The Filtered Alert Hub technology can distinguish "high priority" alerts. These are alerts issued when people need to be alerted in a "broadcast intrusive" manner, such as sounding a siren, inserting a television "crawl text", sending a cell broadcast message, etc.

These alerts are usually reserved for situations in which people need to act: immediately or within the next hour,

in response to an extraordinary or significant threat,

that is already observed or is likely to occur.

Although high priority alerts are less than one percent of the alert messages accessible to the public, such messages are especially crucial to enabling people to preserve life and protect property.

In a CAP message, this "high-priority" distinction is indicated by the "urgency", "severity", and "certainty" elements each having one of the top two values.

Again, the Filtered Alert Hub can easily make the "high-priority" distinction by simply adjusting filter expressions as needed.

Filtered Alert Hub Seminars

Seminar Topic	Powerpoint (PPT)	Notes (PDF)
Sources Display	Hub-Seminar-01	Hub-Seminar-01-Notes
Implementing a Source of CAP Alerts	Hub-Seminar-02	Hub-Seminar-02-Notes
Publishing a CAP Alert News Feed	Hub-Seminar-03	Hub-Seminar-03-Notes
XML for CAP Implementors	Hub-Seminar-04	Hub-Seminar-04-Notes
Alerts Display	Hub-Seminar-05	Hub-Seminar-05-Notes
Alert Ingest Methods	Hub-Seminar-06	Hub-Seminar-06-Notes
New Alert Processing	Hub-Seminar-07	Hub-Seminar-07-Notes
Geospatial Searching	Hub-Seminar-08	Hub-Seminar-08-Notes
Finish Alert Processing	Hub-Seminar-09	Hub-Seminar-09-Notes
A Tool for Creating and Publishing CAP Alerts	Hub-Seminar-10	Hub-Seminar-10-Notes

Filtered Alert Hub

23

We do not have time today to delve further into the Filtered Alert Hub technology. However, I developed a free online Seminar Series for programmers who want to understand the Filtered Alert Hub technology at a program coding level.

The series is geared to the original prototype running on the Amazon Cloud.

The seminars are available for download at the links given. The explanation page, including recommended pre-requisites, is at the slide title hyperlink.

For each Seminar, the Powerpoint has the narrative in the Notes pages; the PDF has the narrative as document pages.

Presentation Outline

➢ Overview

➢ Current Status

➢ Technology

➡ **From Prototype to Operations**

Filtered Alert Hub   24

Now I want to make some general remarks for how an organization might proceed from this prototype to an operational system.

From Prototype to Operations

➢ Functions Already Prototyped

➢ Security and Authentication Needs

➢ Exception Reporting Needs

➢ Organizational Resources

Filtered Alert Hub   25

The Filtered Alert Hub prototype offers proof-of-concept, open source, running code.

In keeping with the architecture as described, the code includes several functions that are particular to handling CAP alerts and these are linked with well-defined interfaces as described in the Filtered Alert Hub design document.

Each of the functions is fairly simple. The total amount of application code across all functions is estimated to be about 3,000 lines.

An operational Filtered Alert Hub needs a robust set of facilities to assure that the system is secure and that alerts are authentic as received and as delivered. These functions would not be highly customized to this application. Rather, these functions should leverage industry best-practice facilities, especially those already available in cloud-based services that support other life-critical systems.

An operational Filtered Alert Hub needs a fuller suite of functions for operational exception reporting to address input, processing, and output conditions such as data errors and performance issues. These functions also should leverage industry best-practices, especially any already available in cloud-based systems for similar Near Real-Time Event Processing.

From Prototype to Operations

➤ Functions Already Prototyped

➤ Security and Authentication Needs

➤ Exception Reporting Needs

➤ Organizational Resources

Filtered Alert Hub   26

Staff time will be needed to support the Filtered Alert Hub as an operational system. The people involved would typically receive automatic notifications by e-mail, such as the notices generated by the exception reporting and security functions discussed above.

In the vast majority of cases, the follow-up would require minimal expertise. For instance, a common notice would be that a particular CAP alert feed is experiencing problems or has begin emitting a high percentage of invalid CAP alerts.

On rare occasions, a notice may be generated that indicates a possible problem with the Filtered Alert Hub software. Those notices would have to be directed to more technical staff.

Also, as the operational Filtered Alert Hub gains broad acceptance and recognition, a stream of enhancement suggestions can be expected. Such suggestions would have to be addressed through management as well as technical channels.

References

- ➤ Filtered Alert Hub Opportunity Document
- ➤ Filtered Alert Hub Design Document
- ➤ Filtered Alert Hub Seminars
- ➤ Project Lead:
  Eliot Christian <eliot.j.christian@gmail.com>

Filtered Alert Hub

27

This concludes my presentation.

Here are links to some key documents on which my presentation is based.