



Embedded Linux
Conference

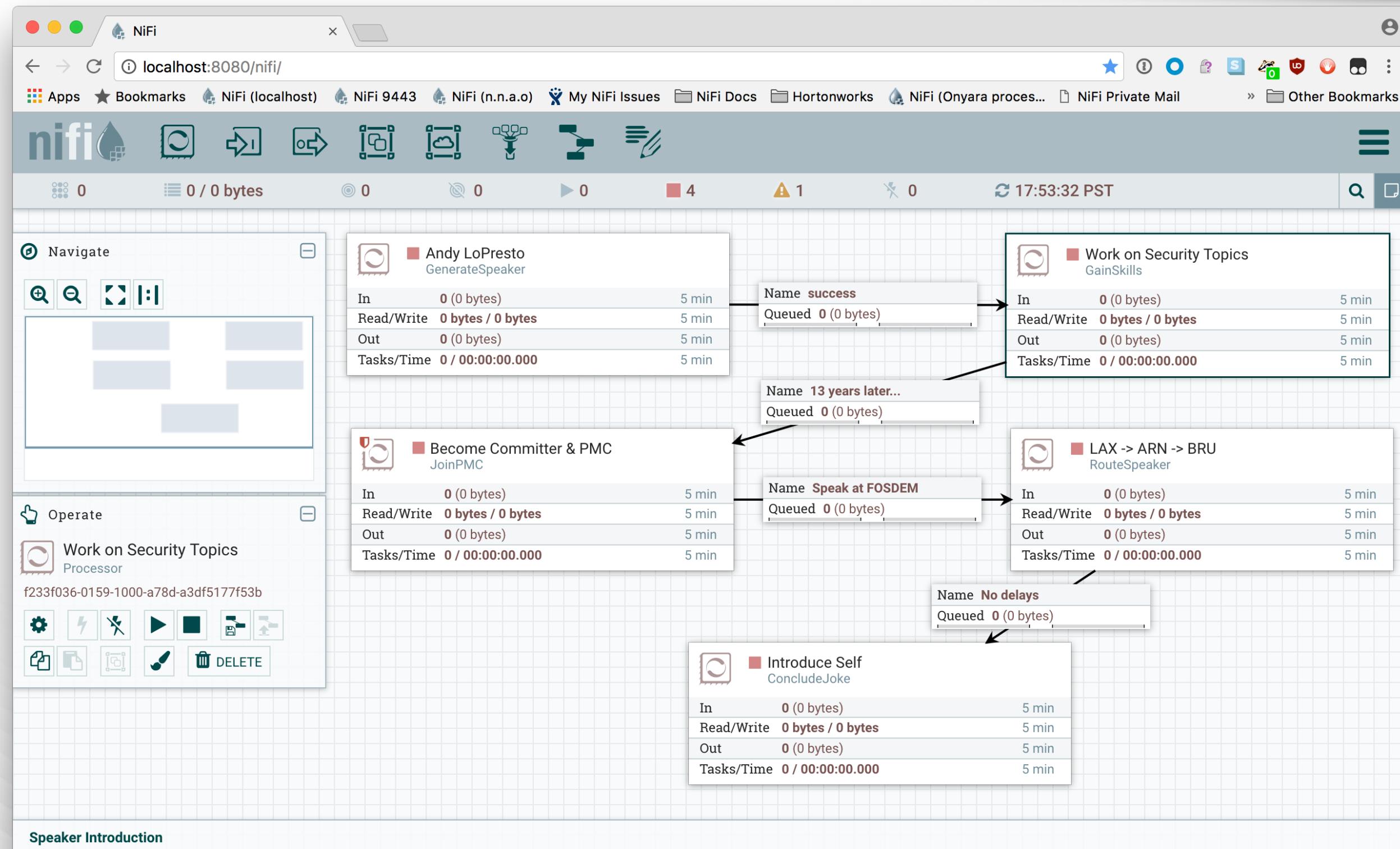


OpenIoTSummit

— FEBRUARY 21-23 — PORTLAND, OR —

Secure IoT Command, Control, and Exfil with Apache MiNiFi

Andy LoPresto, Sr. Member of Technical Staff, *Hortonworks*



Agenda

What is dataflow and what are the challenges?

Apache NiFi

IoT Challenges

Apache MiNiFi

Exploration

Community

Agenda



What is dataflow and what are the challenges?

Apache NiFi

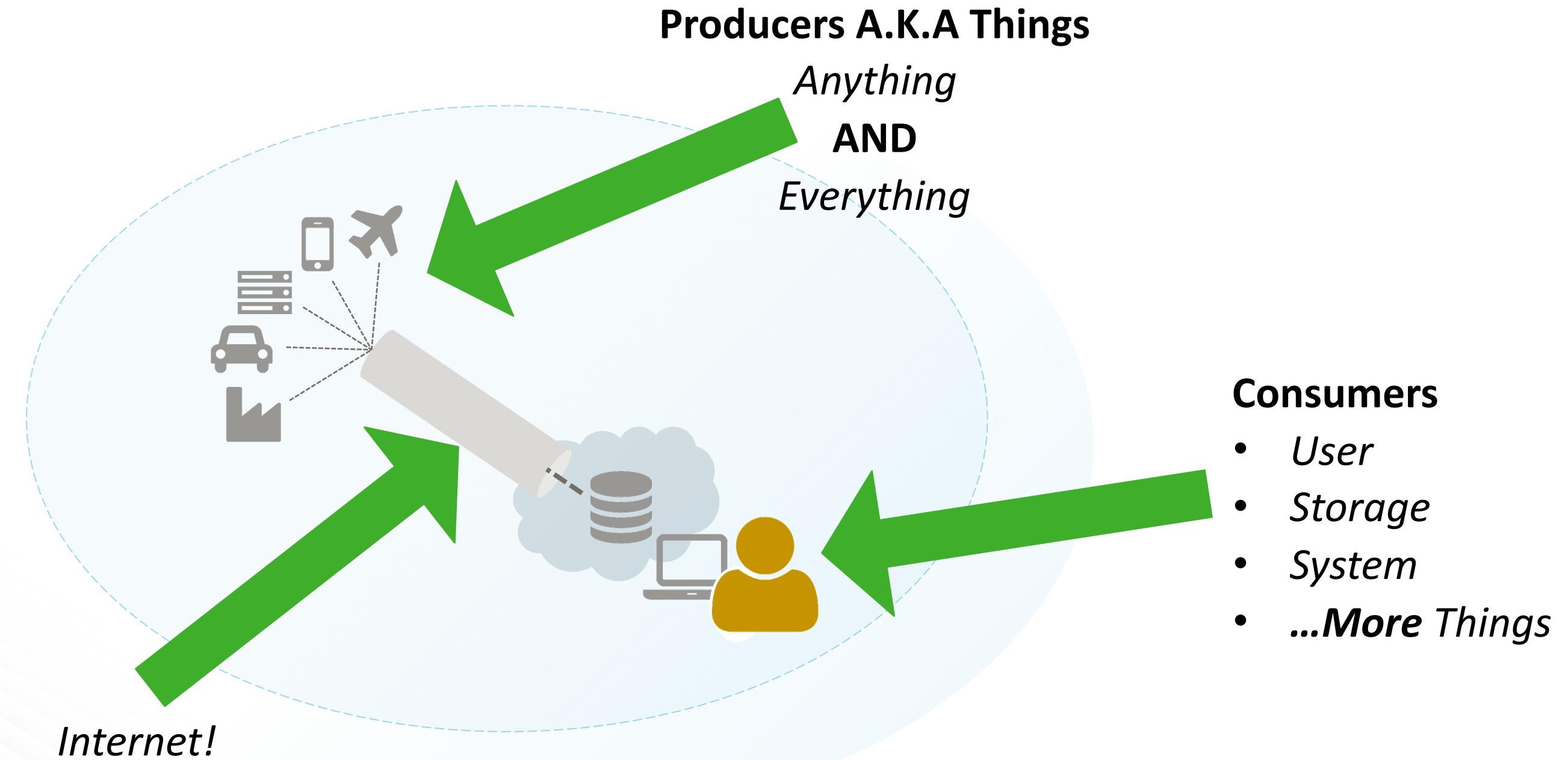
IoT Challenges

Apache MiNiFi

Exploration

Community

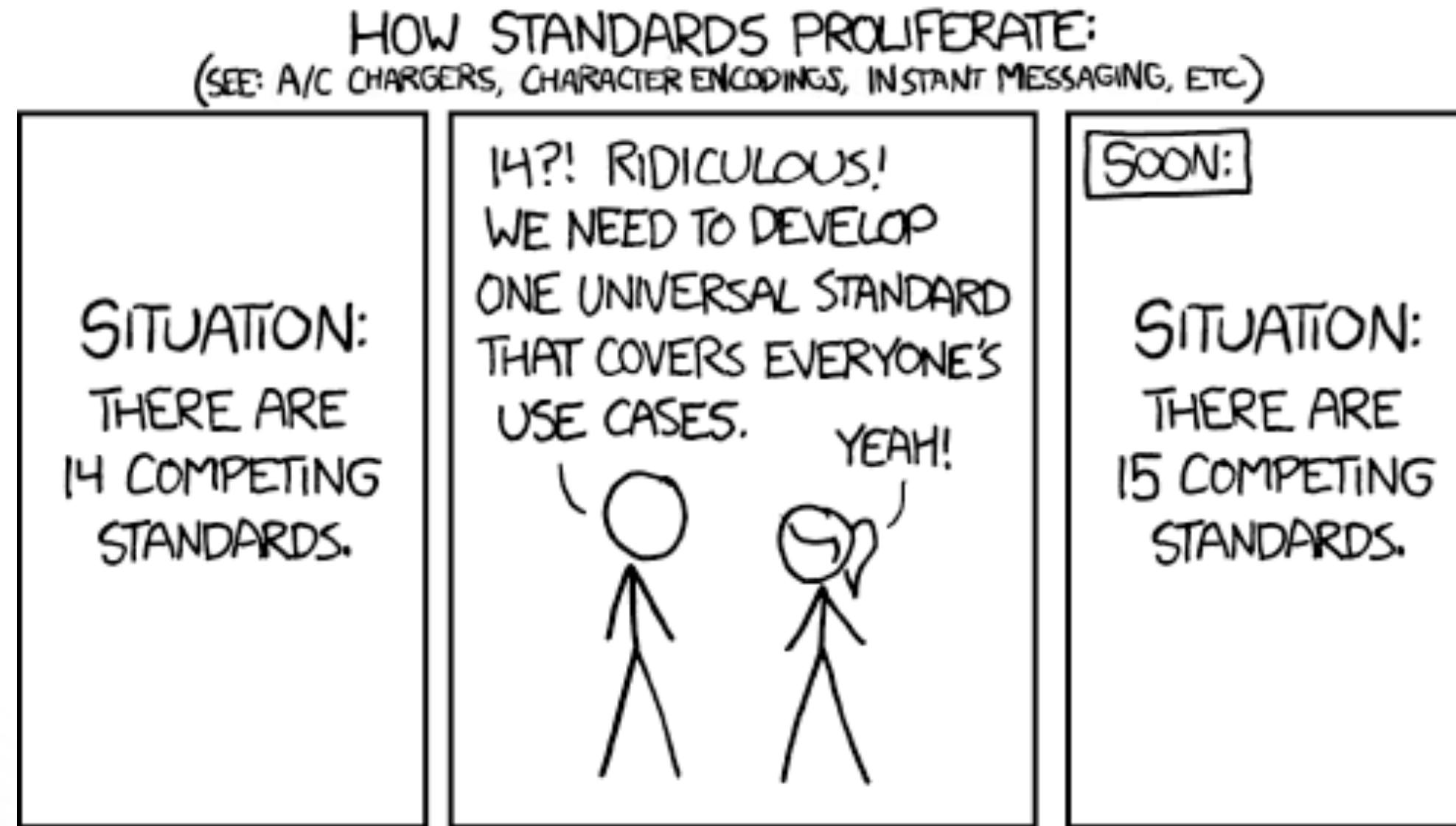
Let's Connect A to B



All Week I've Seen



Moving data *effectively* is hard



Standards: <http://xkcd.com/927/>

Why is moving data *effectively* hard?

- ◆ Standards
- ◆ Formats
- ◆ “Exactly Once” Delivery
- ◆ Protocols
- ◆ Veracity of Information
- ◆ Validity of Information
- ◆ Ensuring Security
- ◆ Overcoming Security
- ◆ Compliance
- ◆ Schemas
- ◆ Consumers Change
- ◆ Credential Management
- ◆ “*That* [person|team|group]”
- ◆ Network*
- ◆ “Exactly Once” Delivery

Agenda



What is dataflow and what are the challenges?

Apache NiFi

IoT Challenges

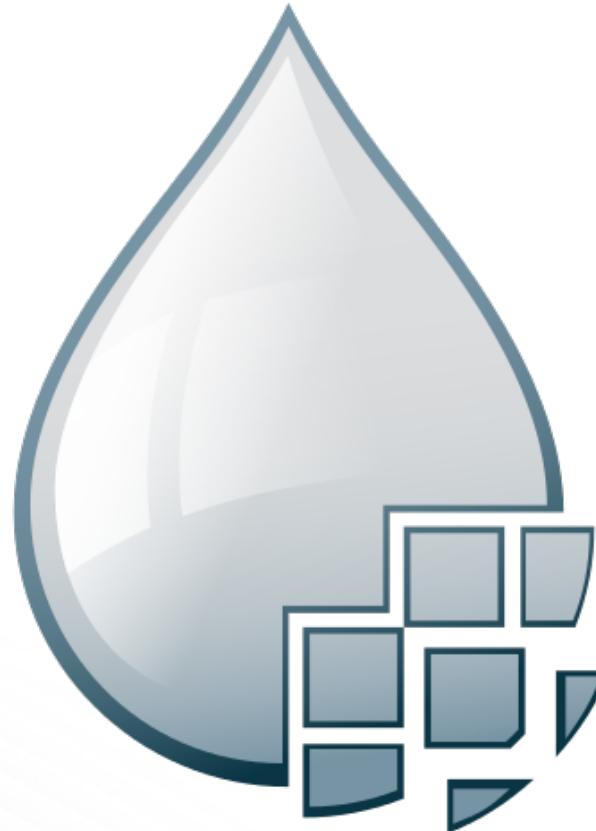
Apache MiNiFi

Exploration

Community

Apache NiFi

Key Features



- Guaranteed delivery
- Data buffering
 - Backpressure
 - Pressure release
- Prioritized queuing
- Flow specific QoS
 - Latency vs. throughput
 - Loss tolerance
- Data provenance
- Supports push and pull models
- Recovery/recording a rolling log of fine-grained history
- Visual command and control
- Flow templates
- Pluggable, multi-tenant security
- Designed for extension
- Clustering

NiFi is based on Flow Based Programming (FBP)

FBP Term	NiFi Term	Description
Information Packet	FlowFile	Each object moving through the system.
Black Box	FlowFile Processor	Performs the work, doing some combination of data routing, transformation, or mediation between systems.
Bounded Buffer	Connection	The linkage between processors, acting as queues and allowing various processes to interact at differing rates.
Scheduler	Flow Controller	Maintains the knowledge of how processes are connected, and manages the threads and allocations thereof which all processes use.
Subnet	Process Group	A set of processes and their connections, which can receive and send data via ports. A process group allows creation of entirely new component simply by composition of its components.

FlowFiles & Data Agnosticism

- ◆ NiFi is data agnostic!
- ◆ But, NiFi was designed understanding that users can care about specifics and provides tooling to interact with specific formats, protocols, etc.

Robustness principle

“ Be conservative in what you do,
be liberal in what you accept from others

PUBLIC SERVICE ANNOUNCEMENT:

OUR DIFFERENT WAYS OF WRITING DATES AS NUMBERS CAN LEAD TO ONLINE CONFUSION. THAT'S WHY IN 1988 ISO SET A GLOBAL STANDARD NUMERIC DATE FORMAT.

THIS IS **THE** CORRECT WAY TO WRITE NUMERIC DATES:

2013-02-27

THE FOLLOWING FORMATS ARE THEREFORE DISCOURAGED:

02/27/2013 02/27/13 27/02/2013 27/02/13

20130227 2013.02.27 27.02.13 27-02-13

27.2.13 2013. II. 27. 27/2-13 2013.158904109

MMXIII-II-XXVII MMXIII ^{LVII}_{CCCLXV} 1330300800

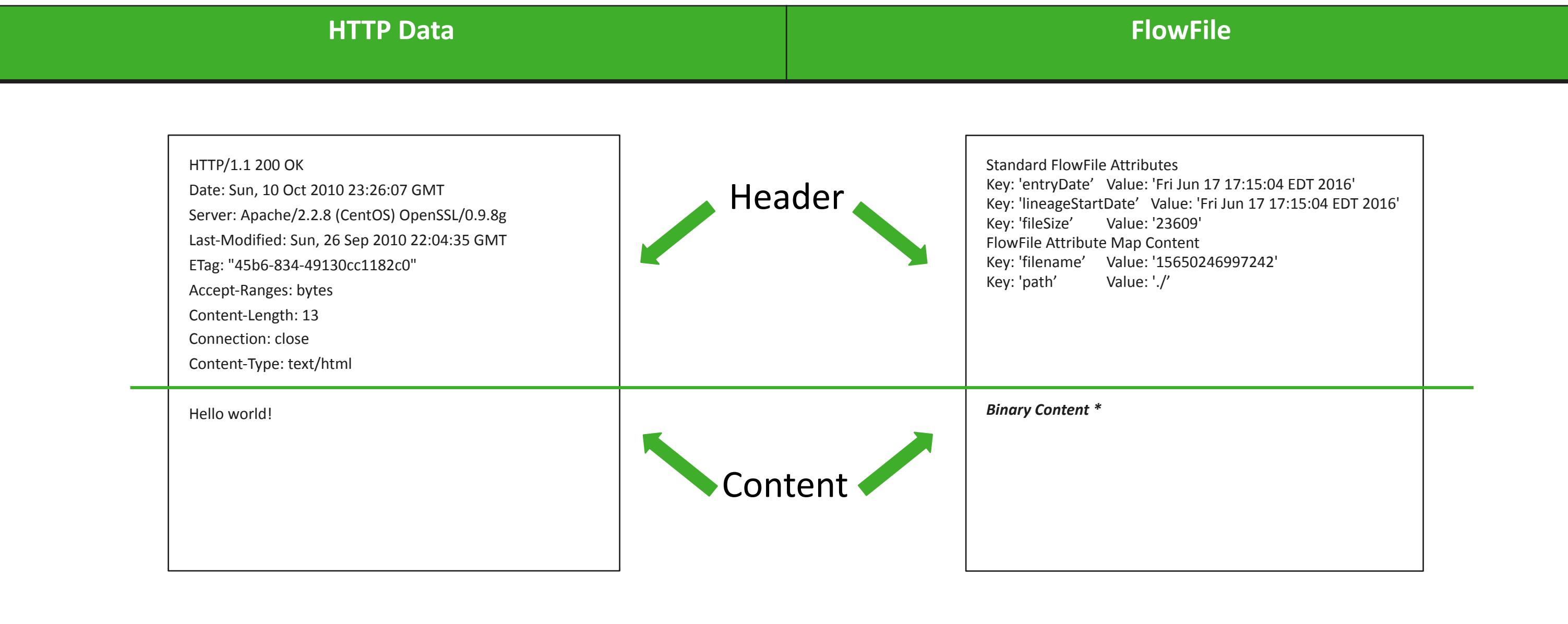
$((3+3)\times(111+1)-1)\times3/3-1/3^3$ 2013 ²⁰¹³₂₀₁₃ HISSSS

10/11011/1101 02/27/20/13 $\frac{2}{5} \frac{3}{6} \frac{1}{7} \frac{4}{8}$ 01237 ²⁻²⁻²₂₋₂₋₂

ISO 8601 - <http://xkcd.com/1179/>



FlowFiles are like HTTP data



User Interface

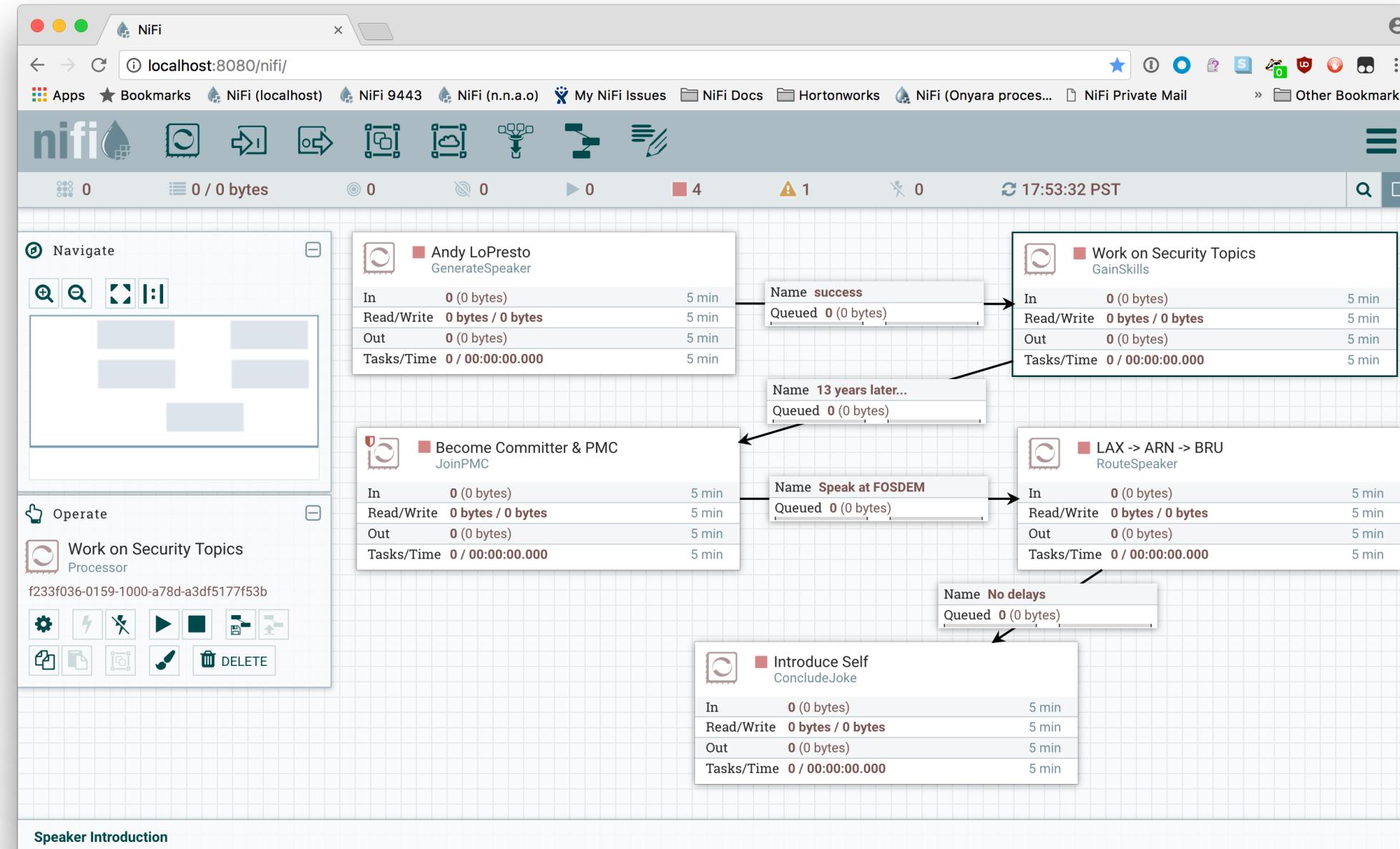
Less of this...

```
1. scratch/release_verification (bash)
hw12203:/Users/alopresto/Workspace/scratch/release_verification (master) alopresto
 3s @ 17:25:51 $ ls
hw12203:/Users/alopresto/Workspace/scratch/release_verification (master) alopresto
 8s @ 17:26:00 $ hunt users.xml
./nifi-1.1.0-RC1-failed/nifi-1.1.0/nifi-assembly/target/nifi-1.1.0-bin/nifi-1.1.0/conf/users.xml
hw12203:/Users/alopresto/Workspace/scratch/release_verification (master) alopresto
 2s @ 17:26:21 $ ll nifi-1.1.0-RC1-failed/nifi-1.1.0/nifi-assembly/target/nifi-1.1.0-bin/nifi-1.1.0/conf/
total 144
drwxr-xr-x 16 alopresto staff 544B Nov 24 19:20 .
drwxr-xr-x 17 alopresto staff 578B Nov 24 14:25 ..
drwxr-xr-x 38 alopresto staff 1.3K Nov 24 14:33 archive/
drwxr-xr-x 1 alopresto staff 2.5K Nov 24 19:20 authorizations.xml
drwxr-xr-x 1 alopresto staff 3.7K Nov 24 19:19 authorizers.xml
drwxr-xr-x 1 alopresto staff 2.1K Nov 23 23:36 bootstrap-notification-services.xml
drwxr-xr-x 1 alopresto staff 3.1K Nov 24 19:29 bootstrap.conf
drwxr-xr-x 1 alopresto staff 2.5K Nov 24 14:33 flow.xml.gz
drwxr-xr-x 1 alopresto staff 3.0K Nov 24 19:16 keystore.jks
drwxr-xr-x 1 alopresto staff 8.0K Nov 23 23:36 logback.xml
drwxr-xr-x 1 alopresto staff 6.2K Nov 23 23:36 login-identity-providers.xml
drwxr-xr-x 1 alopresto staff 9.0K Nov 24 19:17 nifi.properties
drwxr-xr-x 1 alopresto staff 3.6K Nov 23 23:36 state-management.xml
drwxr-xr-x 1 alopresto staff 911B Nov 24 19:16 truststore.jks
drwxr-xr-x 1 alopresto staff 226B Nov 24 19:20 users.xml
drwxr-xr-x 1 alopresto staff 1.4K Nov 23 23:36 zookeeper.properties
hw12203:/Users/alopresto/Workspace/scratch/release_verification (master) alopresto
 21s @ 17:26:43 $ more nifi-1.1.0-RC1-failed/nifi-1.1.0/nifi-assembly/target/nifi-1.1.0-bin/nifi-1.1.0/conf/authorizations.xml
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<authorizations>
  <policies>
    <policy identifier="b2c0320b-0384-38d2-8ff7-58a26dd63897" resource="/flow" action="R">
      <user identifier="9860132a-283e-370b-ba63-b023393be562"/>
    </policy>
    <policy identifier="7e67308c-a837-3ba1-8b37-4a40ff8d43fe" resource="/data/process-groups/9871f1da-0158-1000-c0b2-42aaca57d800" action="R">
      <user identifier="9860132a-283e-370b-ba63-b023393be562"/>
    </policy>
    <policy identifier="b762618f-3636-3b45-943e-6d38605e276e" resource="/data/process-groups/9871f1da-0158-1000-c0b2-42aaca57d800" action="W">
      <user identifier="9860132a-283e-370b-ba63-b023393be562"/>
    </policy>
    <policy identifier="61df3e5b-837f-37f4-b36-b2e7bc4989c3" resource="/process-groups/9871f1da-0158-1000-c0b2-42aaca57d800" action="R">
      <user identifier="9860132a-283e-370b-ba63-b023393be562"/>
    </policy>
    <policy identifier="ff9f93ce-1fd4-3b08-9309-088ba6abc5a9" resource="/process-groups/9871f1da-0158-1000-c0b2-42aaca57d800" action="W">
      <user identifier="9860132a-283e-370b-ba63-b023393be562"/>
    </policy>
    <policy identifier="bc5512df-2a78-33ba-959e-3bc1ba5f781d" resource="/restricted-components" action="W">
      <user identifier="9860132a-283e-370b-ba63-b023393be562"/>
    </policy>
    <policy identifier="70197f52-a4fd-3938-3d46-498626032fa" resource="/tenants" action="R">
      <user identifier="9860132a-283e-370b-ba63-b023393be562"/>
    </policy>
    <policy identifier="30f46aab-baa8-3b50-8b9d-d768a83e719f" resource="/tenants" action="W">
      <user identifier="9860132a-283e-370b-ba63-b023393be562"/>
    </policy>
    <policy identifier="6c25353b-fca4-3813-baa8-f87949853e7e" resource="/policies" action="R">
      <user identifier="9860132a-283e-370b-ba63-b023393be562"/>
    </policy>
    <policy identifier="3906378a-8fb9-3a71-aa0b-44325b1723cf" resource="/policies" action="W">
      <user identifier="9860132a-283e-370b-ba63-b023393be562"/>
    </policy>
    <policy identifier="26c66358-8548-31c8-a38c-e0ebbc3ddb4" resource="/controller" action="R">
      <user identifier="9860132a-283e-370b-ba63-b023393be562"/>
    </policy>
    <policy identifier="4470abbe-3b1e-31cd-9daa-598eae5c59ef" resource="/controller" action="W">
      <user identifier="9860132a-283e-370b-ba63-b023393be562"/>
    </policy>
  </policies>
</authorizations>
hw12203:/Users/alopresto/Workspace/scratch/release_verification (master) alopresto
 9s @ 17:26:53 $ ls
nifi.flowfile.repository.always.sync=false
nifi.swap.manager.implementation=org.apache.nifi.controller.FileSystemSwapManager
nifi.queue.swap.threshold=2000
nifi.swap.in.period=5 sec
nifi.swap.in.threads=1
nifi.swap.out.period=5 sec
nifi.swap.out.threads=4
# Content Repository
nifi.content.repository.implementation=org.apache.nifi.controller.repository.FileSystemRepository
hw12203:...space/nifi/nifi-assembly/target/nifi-1.2.0-SNAPSHOT-bin/nifi-1.2.0-SNAPSHOT (NIFI-3313) alopresto
 157s @ 17:40:39 $ nfkl
Java home: /Users/alopresto/.jenv/versions/1.8
NiFi home: /Users/alopresto/Workspace/nifi/nifi-assembly/target/nifi-1.2.0-SNAPSHOT-bin/nifi-1.2.0-SNAPSHOT
Bootstrap Config File: /Users/alopresto/Workspace/nifi/nifi-assembly/target/nifi-1.2.0-SNAPSHOT-bin/nifi-1.2.0-SNAPSHOT/conf/bootstrap.conf
2017-01-30 17:40:43,812 INFO [main] org.apache.nifi.bootstrap.Command Apache NiFi has accepted the Shutdown Command and is shutting down now
2017-01-30 17:40:43,854 INFO [main] org.apache.nifi.bootstrap.Command Waiting for Apache NiFi to finish shutting down...
2017-01-30 17:40:45,867 INFO [main] org.apache.nifi.bootstrap.Command NiFi has finished shutting down.
hw12203:...space/nifi/nifi-assembly/target/nifi-1.2.0-SNAPSHOT-bin/nifi-1.2.0-SNAPSHOT (NIFI-3313) alopresto
 9s @ 17:40:49 $ sub conf/nifi.properties
hw12203:...space/nifi/nifi-assembly/target/nifi-1.2.0-SNAPSHOT-bin/nifi-1.2.0-SNAPSHOT (NIFI-3313) alopresto
 5s @ 17:40:55 $ nfgo
Java home: /Users/alopresto/.jenv/versions/1.8
NiFi home: /Users/alopresto/Workspace/nifi/nifi-assembly/target/nifi-1.2.0-SNAPSHOT-bin/nifi-1.2.0-SNAPSHOT
Bootstrap Config File: /Users/alopresto/Workspace/nifi/nifi-assembly/target/nifi-1.2.0-SNAPSHOT-bin/nifi-1.2.0-SNAPSHOT/conf/bootstrap.conf
2017-01-30 17:41:13,874 INFO [main] org.apache.nifi.bootstrap.Command Starting Apache NiFi...
2017-01-30 17:41:13,874 INFO [main] org.apache.nifi.bootstrap.Command Working Directory: /Users/alopresto/Workspace/nifi/nifi-assembly/target/nifi-1.2.0-SNAPSHOT-bin/nifi-1.2.0-SNAPSHOT
2017-01-30 17:41:13,874 INFO [main] org.apache.nifi.bootstrap.Command: /Users/alopresto/.jenv/versions/1.8/bin/java -classpath /Users/alopresto/Workspace/nifi/nifi-assembly/target/nifi-1.2.0-SNAPSHOT-bin/nifi-1.2.0-SNAPSHOT:/conf:/Users/alopresto/Workspace/nifi/nifi-assembly/target/nifi-1.2.0-SNAPSHOT-bin/nifi-1.2.0-SNAPSHOT:/lib/jcl-over-slf4j-1.7.12.jar:/Users/alopresto/Workspace/nifi/nifi-assembly/target/nifi-1.2.0-SNAPSHOT-bin/nifi-1.2.0-SNAPSHOT:/lib/jcl-over-slf4j-1.7.12.jar:/Users/alopresto/Workspace/nifi/nifi-assembly/target/nifi-1.2.0-SNAPSHOT-bin/nifi-1.2.0-SNAPSHOT:/lib/logback-classic-1.1.3.jar:/Users/alopresto/Workspace/nifi/nifi-assembly/target/nifi-1.2.0-SNAPSHOT-bin/nifi-1.2.0-SNAPSHOT:/lib/logback-core-1.1.3.jar:/Users/alopresto/Workspace/nifi/nifi-assembly/target/nifi-1.2.0-SNAPSHOT-bin/nifi-1.2.0-SNAPSHOT:/lib/nifi-api-1.2.0-SNAPSHOT.jar:/Users/alopresto/Workspace/nifi/nifi-assembly/target/nifi-1.2.0-SNAPSHOT-bin/nifi-1.2.0-SNAPSHOT:/lib/nifi-documentation-1.2.0-SNAPSHOT.jar:/Users/alopresto/Workspace/nifi/nifi-assembly/target/nifi-1.2.0-SNAPSHOT-bin/nifi-1.2.0-SNAPSHOT:/lib/nifi-framework-api-1.2.0-SNAPSHOT.jar:/Users/alopresto/Workspace/nifi/nifi-assembly/target/nifi-1.2.0-SNAPSHOT-bin/nifi-1.2.0-SNAPSHOT:/lib/nifi-nar-utils-1.2.0-SNAPSHOT.jar:/Users/alopresto/Workspace/nifi/nifi-assembly/target/nifi-1.2.0-SNAPSHOT-bin/nifi-1.2.0-SNAPSHOT:/lib/nifi-properties-1.2.0-SNAPSHOT.jar:/Users/alopresto/Workspace/nifi/nifi-assembly/target/nifi-1.2.0-SNAPSHOT-bin/nifi-1.2.0-SNAPSHOT:/lib/nifi-runtime-1.2.0-SNAPSHOT.jar:/Users/alopresto/Workspace/nifi/nifi-assembly/target/nifi-1.2.0-SNAPSHOT-bin/nifi-1.2.0-SNAPSHOT:/lib/nifi-slf4j-1.7.12.jar:/Users/alopresto/Workspace/nifi/nifi-assembly/target/nifi-1.2.0-SNAPSHOT-bin/nifi-1.2.0-SNAPSHOT:/lib/nifi-slf4j-api-1.7.12.jar:/Users/alopresto/Workspace/nifi/nifi-assembly/target/nifi-1.2.0-SNAPSHOT-bin/nifi-1.2.0-SNAPSHOT:/lib/nifi-avt-headless=true-Djava.net.http.allowRestrictedHeaders=true-Djava.net.preferIPv4Stack=true-Djava.awt.headless=true-Xms12m-Xmx12m-DSun.net.http.AllowRestrictedHeaders=true-Djava.net.preferIPv4Stack=true-Djava.awt.headless=true-Xms12m-Xmx12m-Dndlpr.pkgs=sun.net.www.protocol.Dnifi.properties.filePath=/Users/alopresto/Workspace/nifi/nifi-assembly/target/nifi-1.2.0-SNAPSHOT-bin/nifi-1.2.0-SNAPSHOT:/conf/nifi.properties-Dnifi.bootstrap.listen.port=59772-Dapp=Nifi-Dorg.apache.nifi.bootstrap.config.log.dir=/Users/alopresto/Workspace/nifi/nifi-assembly/target/nifi-1.2.0-SNAPSHOT-bin/nifi-1.2.0-SNAPSHOT/logs org.apache.nifi.NiFi
hw12203:...space/nifi/nifi-assembly/target/nifi-1.2.0-SNAPSHOT-bin/nifi-1.2.0-SNAPSHOT (NIFI-3313) alopresto
 21s @ 17:41:17 $ nfkl
Java home: /Users/alopresto/.jenv/versions/1.8
NiFi home: /Users/alopresto/Workspace/nifi/nifi-assembly/target/nifi-1.2.0-SNAPSHOT-bin/nifi-1.2.0-SNAPSHOT
Bootstrap Config File: /Users/alopresto/Workspace/nifi/nifi-assembly/target/nifi-1.2.0-SNAPSHOT-bin/nifi-1.2.0-SNAPSHOT/conf/bootstrap.conf
2017-01-30 20:54:26,971 INFO [main] org.apache.nifi.bootstrap.Command Apache NiFi has accepted the Shutdown Command and is shutting down now
2017-01-30 20:54:27,075 INFO [main] org.apache.nifi.bootstrap.Command Waiting for Apache NiFi to finish shutting down...
2017-01-30 20:54:29,085 INFO [main] org.apache.nifi.bootstrap.Command NiFi has finished shutting down.
hw12203:...space/nifi/nifi-assembly/target/nifi-1.2.0-SNAPSHOT-bin/nifi-1.2.0-SNAPSHOT (NIFI-3313) alopresto
 11595s @ 20:54:33 $
```

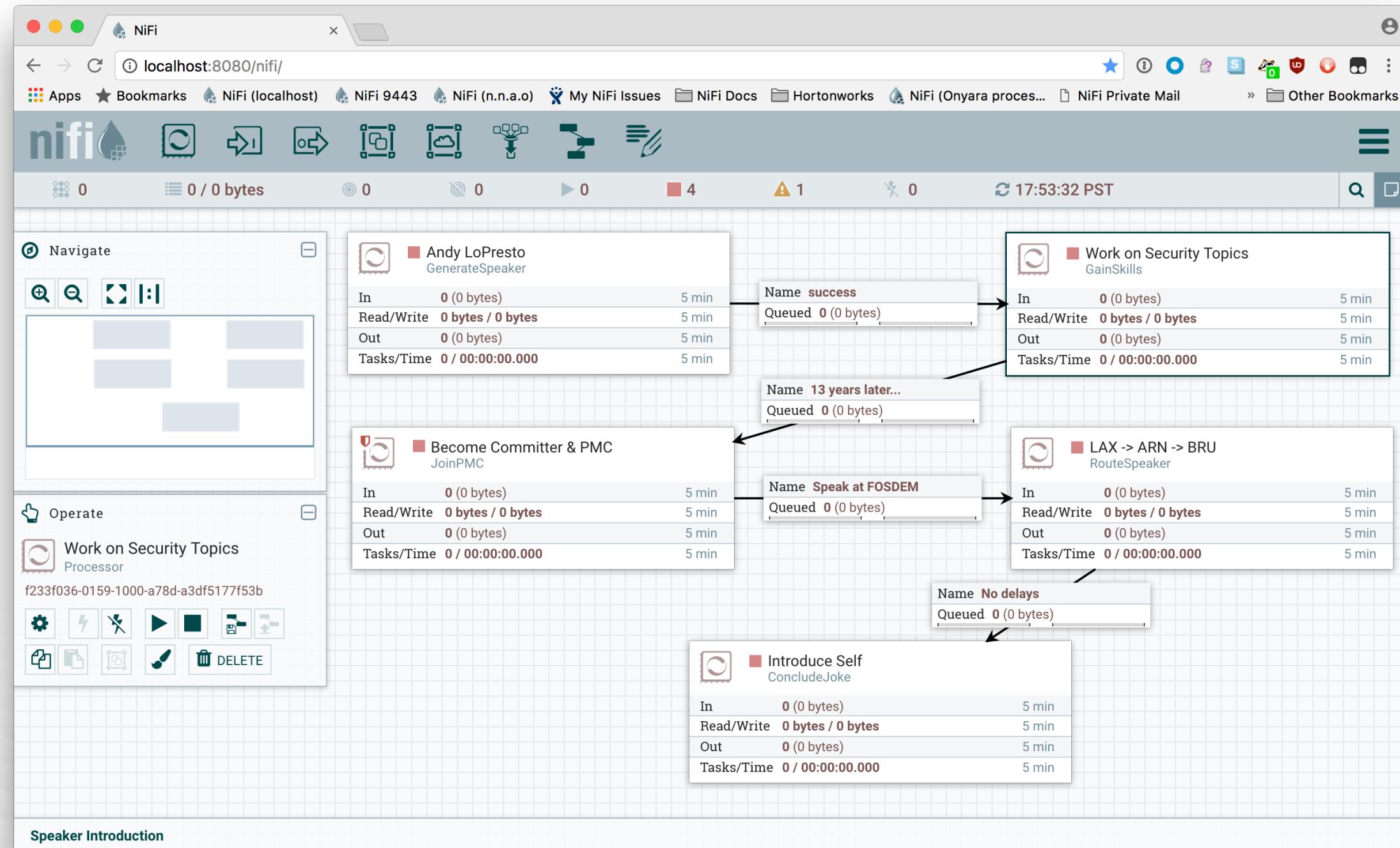


User Interface

Less of this... ... more of this



User Interface



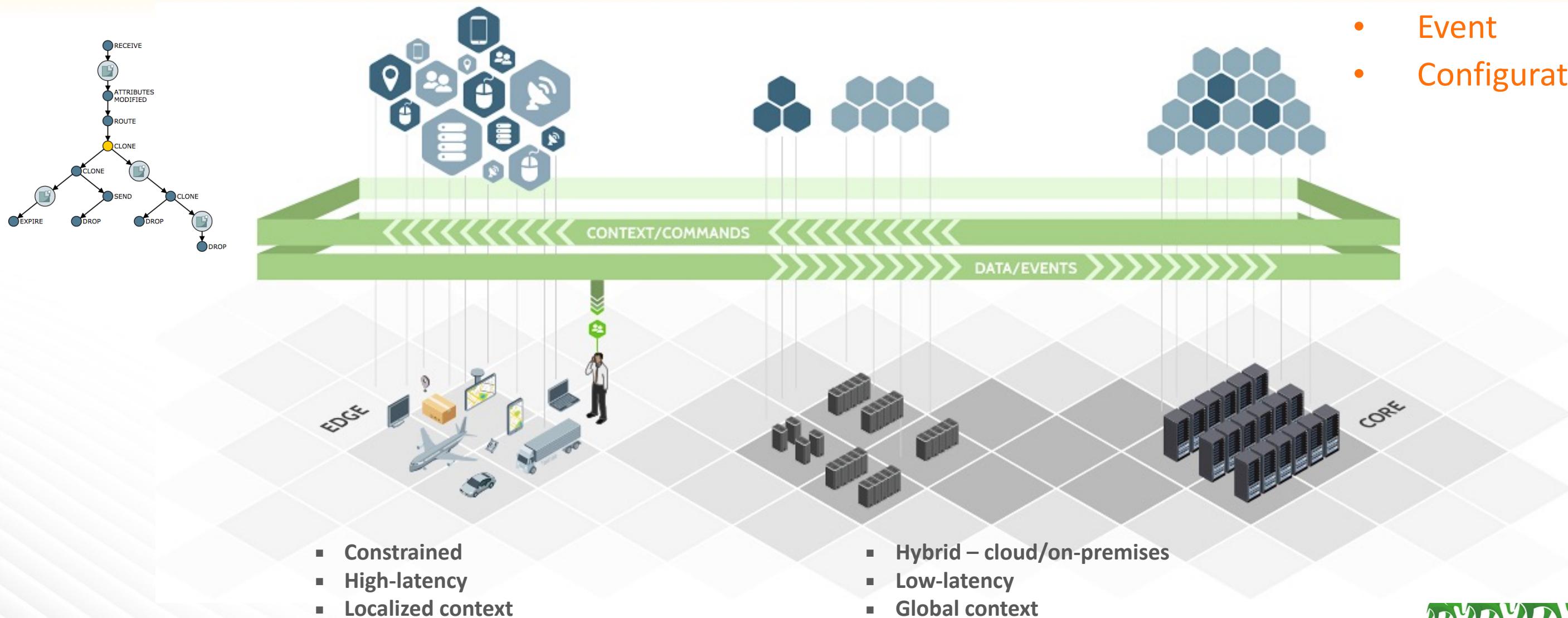
Data Provenance

Origin – attribution
Replay – recovery

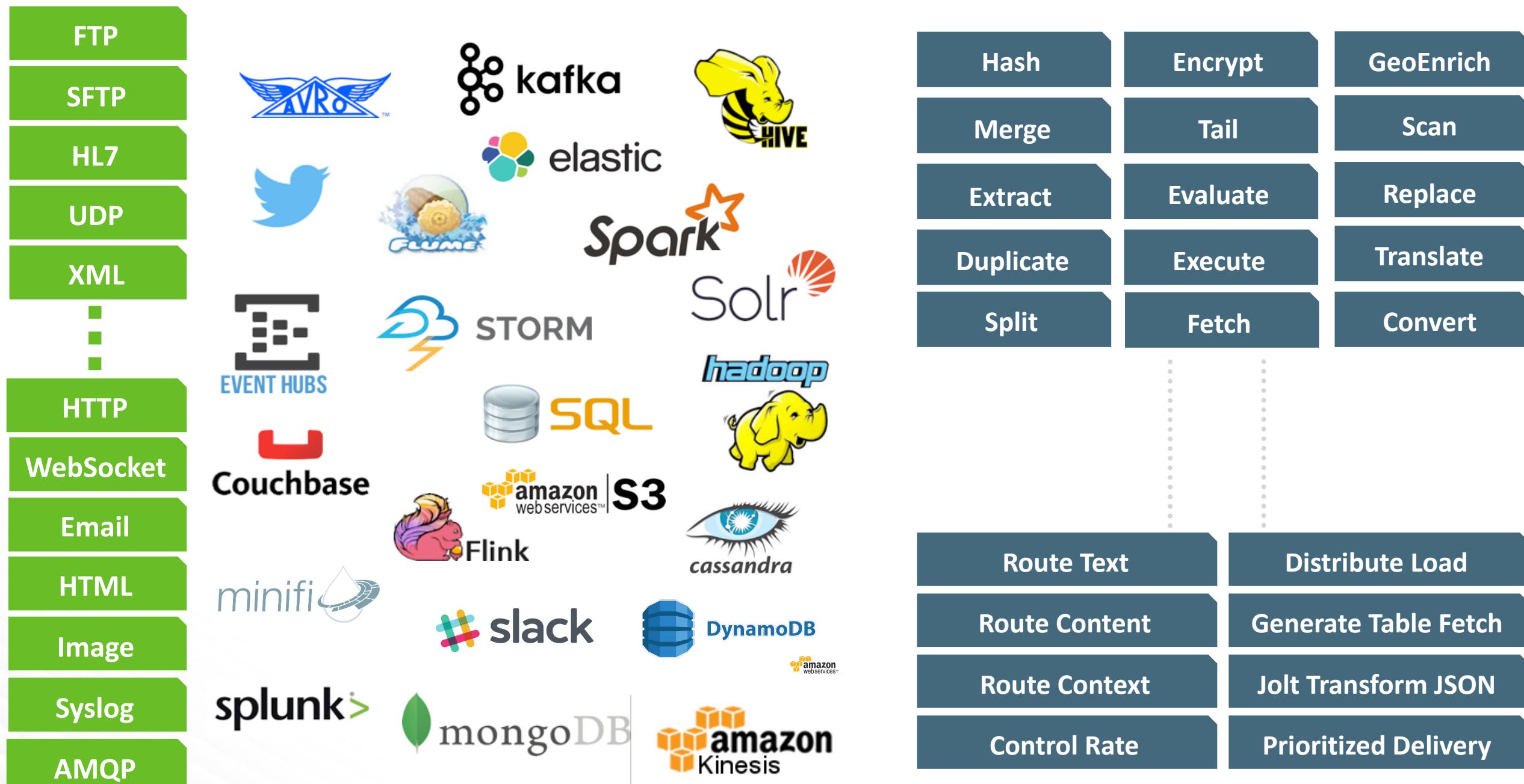
Evolution of topologies
Long retention

Types of Lineage

- Event
- Configuration



Deeper Ecosystem Integration: 180+ Processors



All Apache project logos are trademarks of the ASF and the respective projects.

Agenda



What is dataflow and what are the challenges?

Apache NiFi

IoT Challenges

Apache MiNiFi

Exploration

Community

IoT Challenges

- ◆ Limited computing capability
- ◆ Limited power/network
- ◆ Restricted software library/platform availability
- ◆ No UI
- ◆ Physically inaccessible
- ◆ Not frequently updated
- ◆ Competing standards/protocols
- ◆ Scalability
- ◆ Privacy & Security

Recent Examples

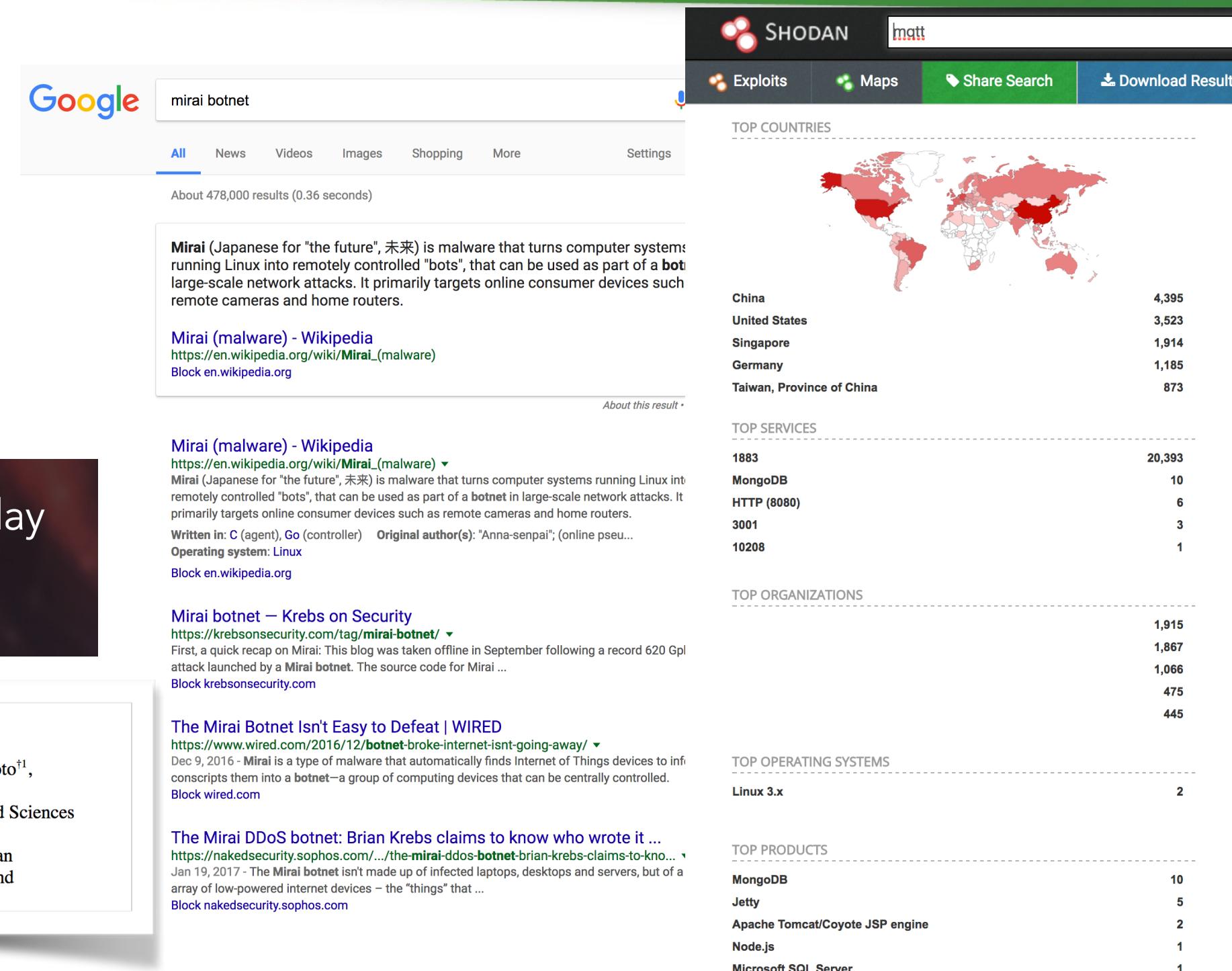
- When the Mirai attack has its own Wikipedia page, that's not good



IoTPOT: Analysing the Rise of IoT Compromises

Yin Minn Pa Pa^{†1}, Shogo Suzuki^{†1}, Katsunari Yoshioka^{†1}, Tsutomu Matsumoto^{†1},
Takahiro Kasama^{†2}, Christian Rossow^{†3}

^{†1}Graduate School of Environment and Information Sciences/Institute of Advanced Sciences
^{†1}Yokohama National University, Japan
^{†2}National Institute of Information and Communications Technology, Japan
^{†3}Institute of Advanced Sciences, Yokohama National University, Japan and
^{†3}Cluster of Excellence, MMCI, Saarland University, Germany



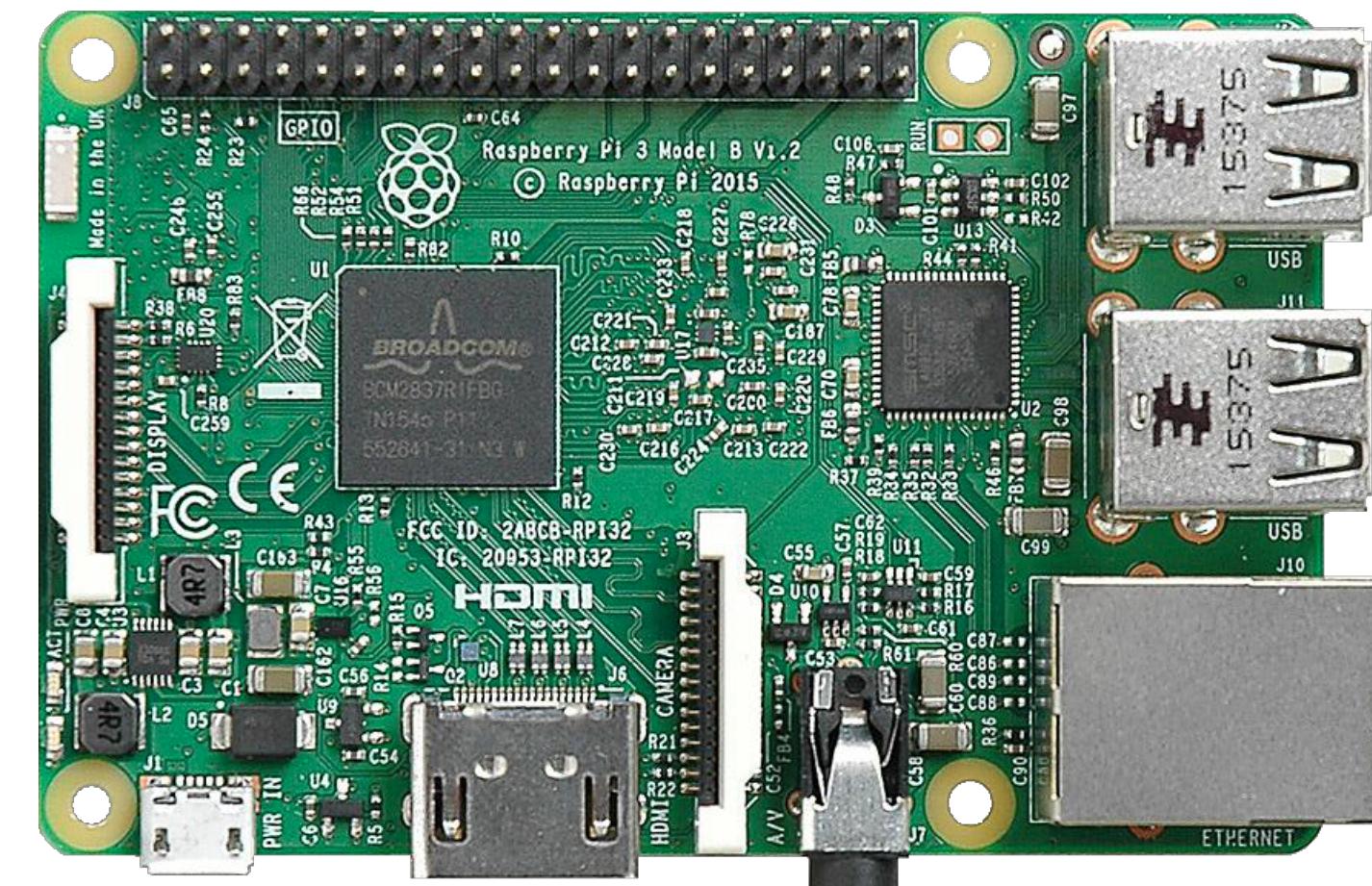
NiFi Solves Everything*

- ◆ Runs on JVM
- ◆ Provides UI for flow design & monitoring
- ◆ Security built-in
 - ◆ TLS, authn/authz, encrypted data
- ◆ Handles practically any format/protocol

NiFi for IoT

- NiFi supports AMQP, MQTT, UDP, TCP, HTTP(S), CEF, JMS, (S)FTP, *AWSIoT*
 - With a little pruning, NiFi can run on a Raspberry Pi

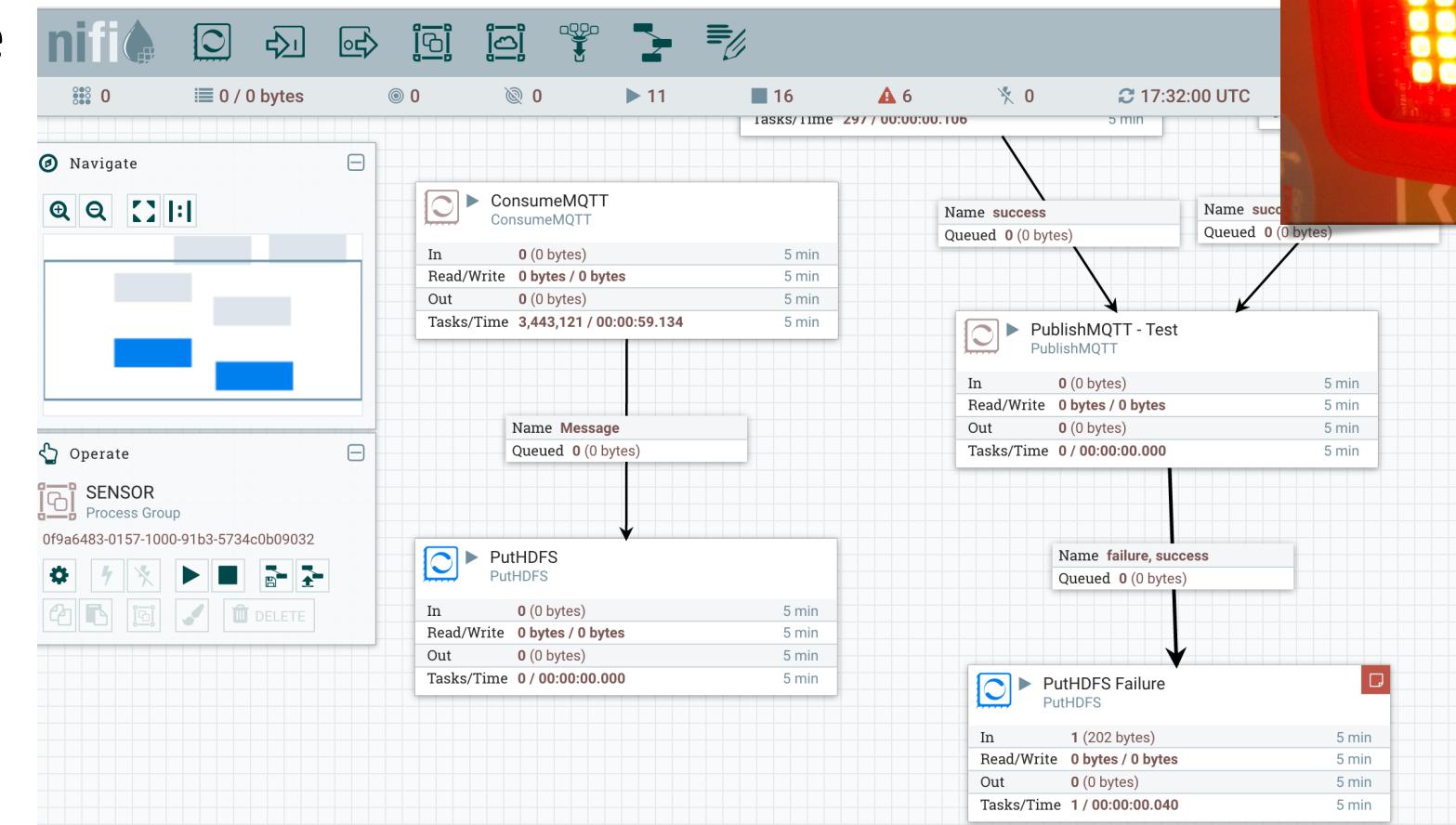
```
└── bootstrap
    ├── jcl-over-slf4j-1.7.12.jar
    ├── jul-to-slf4j-1.7.12.jar
    ├── log4j-over-slf4j-1.7.12.jar
    ├── logback-classic-1.1.3.jar
    ├── logback-core-1.1.3.jar
    ├── nifi-api-0.6.1.jar
    ├── nifi-documentation-0.6.1.jar
    ├── nifi-framework-nar-0.6.1.nar
    ├── nifi-html-nar-0.6.1.nar
    ├── nifi-http-context-map-nar-0.6.1.nar
    ├── nifi-jetty-bundle-0.6.1.nar
    ├── nifi-kerberos-iaa-providers-nar-0.6.1.nar
    ├── nifi-ldap-iaa-providers-nar-0.6.1.nar
    ├── nifi-nar-utils-0.6.1.jar
    ├── nifi-properties-0.6.1.jar
    ├── nifi-provenance-repository-nar-0.6.1.nar
    ├── nifi-runtime-0.6.1.jar
    ├── nifi-scripting-nar-0.6.1.nar
    ├── nifi-ssl-context-service-nar-0.6.1.nar
    ├── nifi-standard-nar-0.6.1.nar
    ├── nifi-standard-services-api-nar-0.6.1.nar
    ├── nifi-update-attribute-nar-0.6.1.nar
    └── slf4j-api-1.7.12.jar
```



Example – Sensor Readings via RP3B



- Tim Spann
 - Sense Hat sensor attachment
 - Temp, humidity, pressure
 - 8x8 LED display
 - Python Flask server reading sensor and pushing to MQTT
 - NiFi consuming MQTT



Building Command & Control

- ◆ Can expand Flask server to listen for incoming requests
- ◆ NiFi performs logic/routing/analysis
 - ◆ Can offload to Spark, Kafka, HDFS, etc.
- ◆ Decisions push new information back to Flask
- ◆ Writes to config for sensor
- ◆ Displays message/levels

So Why Do We Need A Different Solution?

- ◆ NiFi is designed to “own the box”
- ◆ NiFi 0.7.x started up in about 10-15 minutes on RP3 (593 MB)
- ◆ NiFi 1.x started up in about 30 minutes on RP3 (760 MB)
 - ◆ 33 new processors
 - ◆ Rewrite for multi tenant authorization
 - ◆ Complete UI overhaul

```
▶hw12203:/Users/alopresto/Workspace/scratch/rp3b-demo (master) alopresto
└─ 113s @ 17:09:05 $ ssh pi@my-raspberry-pi
^C
▶hw12203:/Users/alopresto/Workspace/scratch/rp3b-demo (master) alopresto
└─ 145s @ 17:09:37 $
```

Agenda



- What is dataflow and what are the challenges?*
- Apache NiFi*
- IoT Challenges
- Apache MiNiFi
- Exploration
- Community

Apache NiFi Subproject: MiNiFi

- ◆ Get the key parts of NiFi close to where data begins and provide bidirectional communication
- ◆ NiFi lives in the data center — give it an enterprise server or a cluster of them
- ◆ MiNiFi lives as close to where data is born and is a guest on that device or system
 - ◆ IoT
 - ◆ Connected car
 - ◆ Legacy hardware

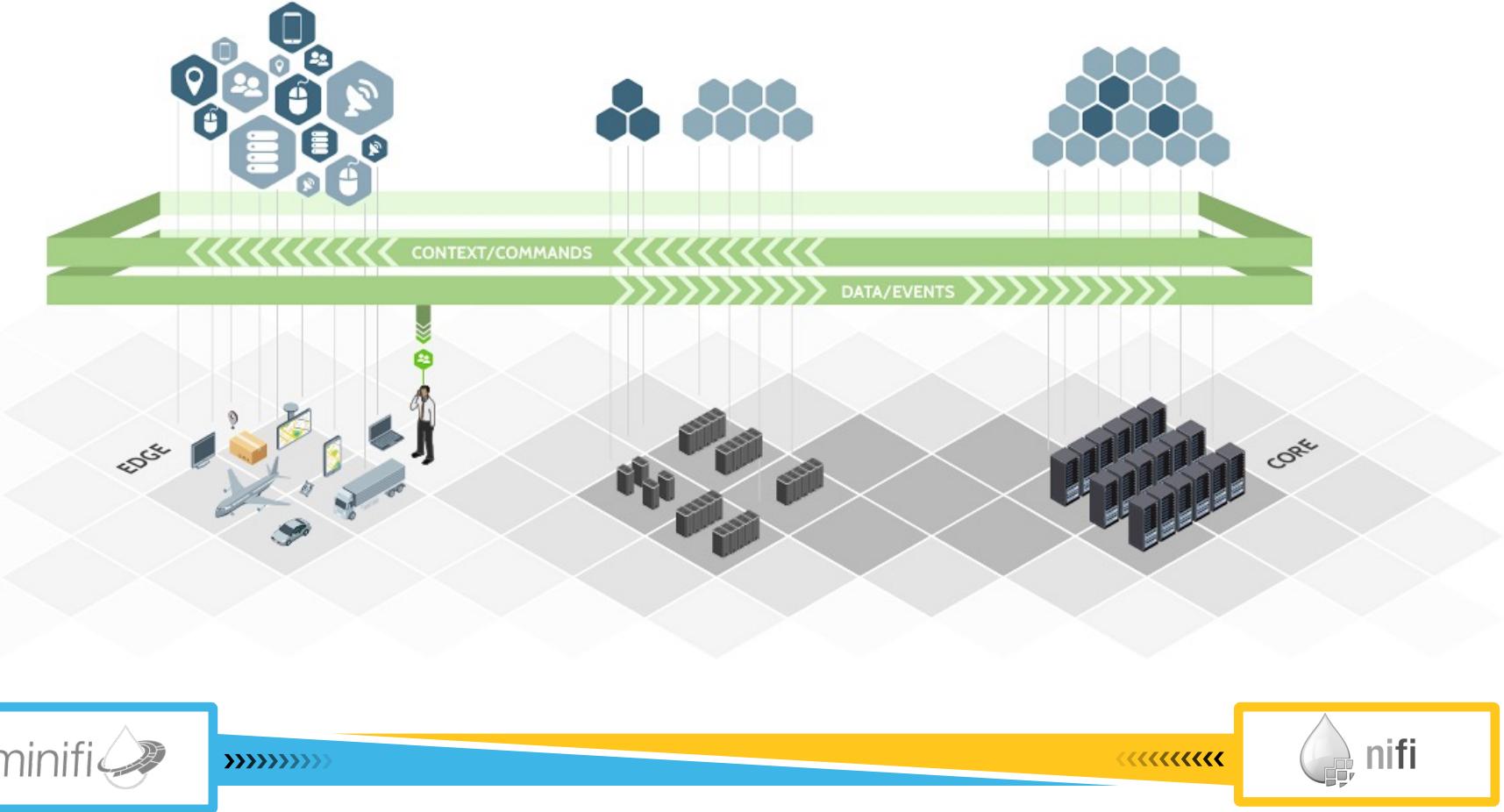


Why build MiNiFi?

- ◆ NiFi is big
 - ◆ 1.1.2 release is 760 MB compressed
 - ◆ Can be modified to run in restricted environments, but requires manual surgery
 - ◆ Provides UI, provenance query, etc.
 - ◆ Runs on dedicated machines/clusters — “owns the box”
- ◆ MiNiFi lives at the edge
 - ◆ No UI
 - ◆ 0.1.0 Java binary is 45 MB, C++ binary is 746 KB
 - ◆ “Good guest”

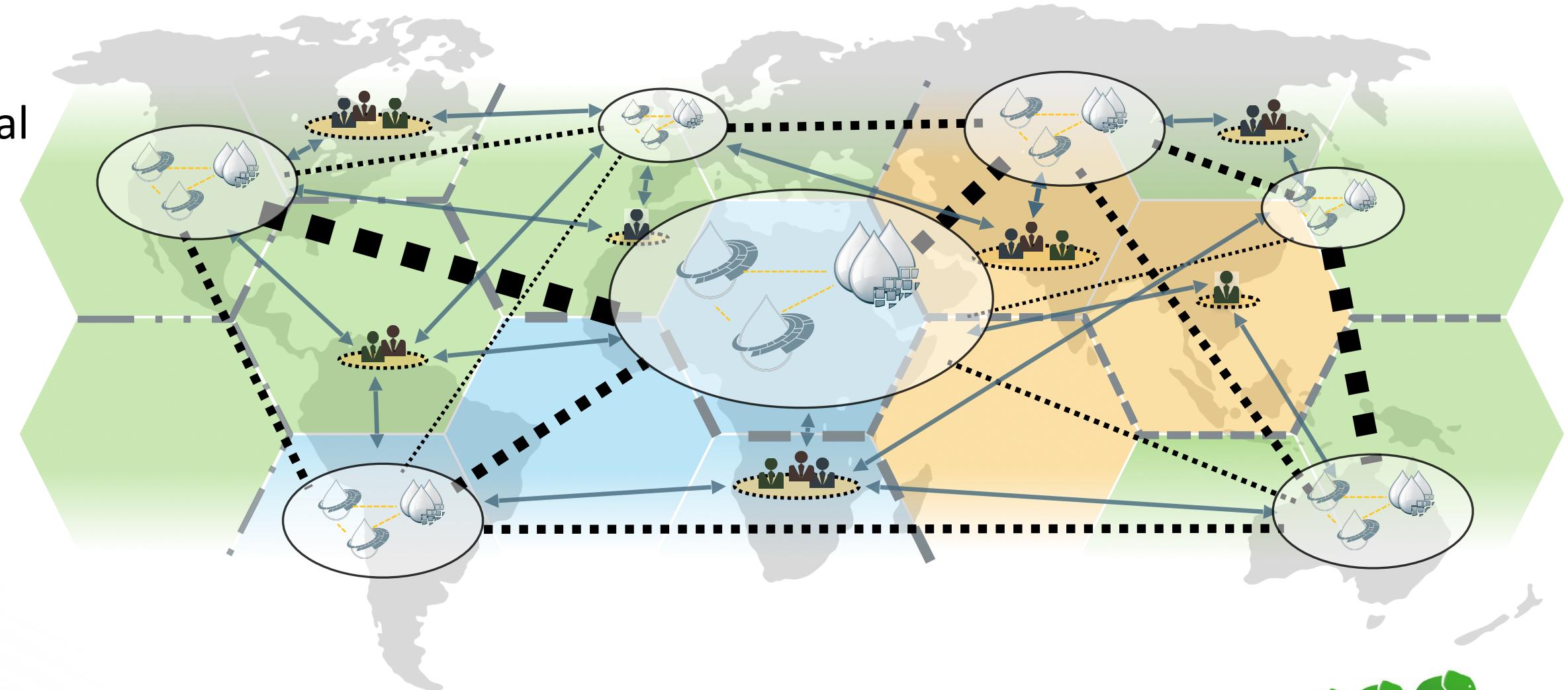
How Does MiNiFi Interact With NiFi?

- ◆ NiFi
 - ◆ Design flows
 - ◆ Aggregate data from many sources
 - ◆ Perform routing/analysis/SEP
- ◆ MiNiFi
 - ◆ Receive flows
 - ◆ Collect data
 - ◆ Send for processing



Let's Add Dimensionality

- ◆ We've been imagining EDGE to CORE as a bi-directional linear system
- ◆ Let's expand that to the real world



Flavors of MiNiFi

◆ MiNiFi Java (v0.1.0)

- ◆ Modified version of NiFi

- ◆ No UI

- ◆ YAML configuration

- ◆ Reduced processor count

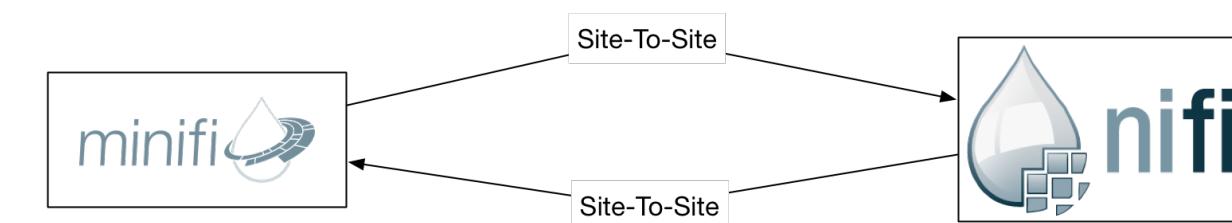
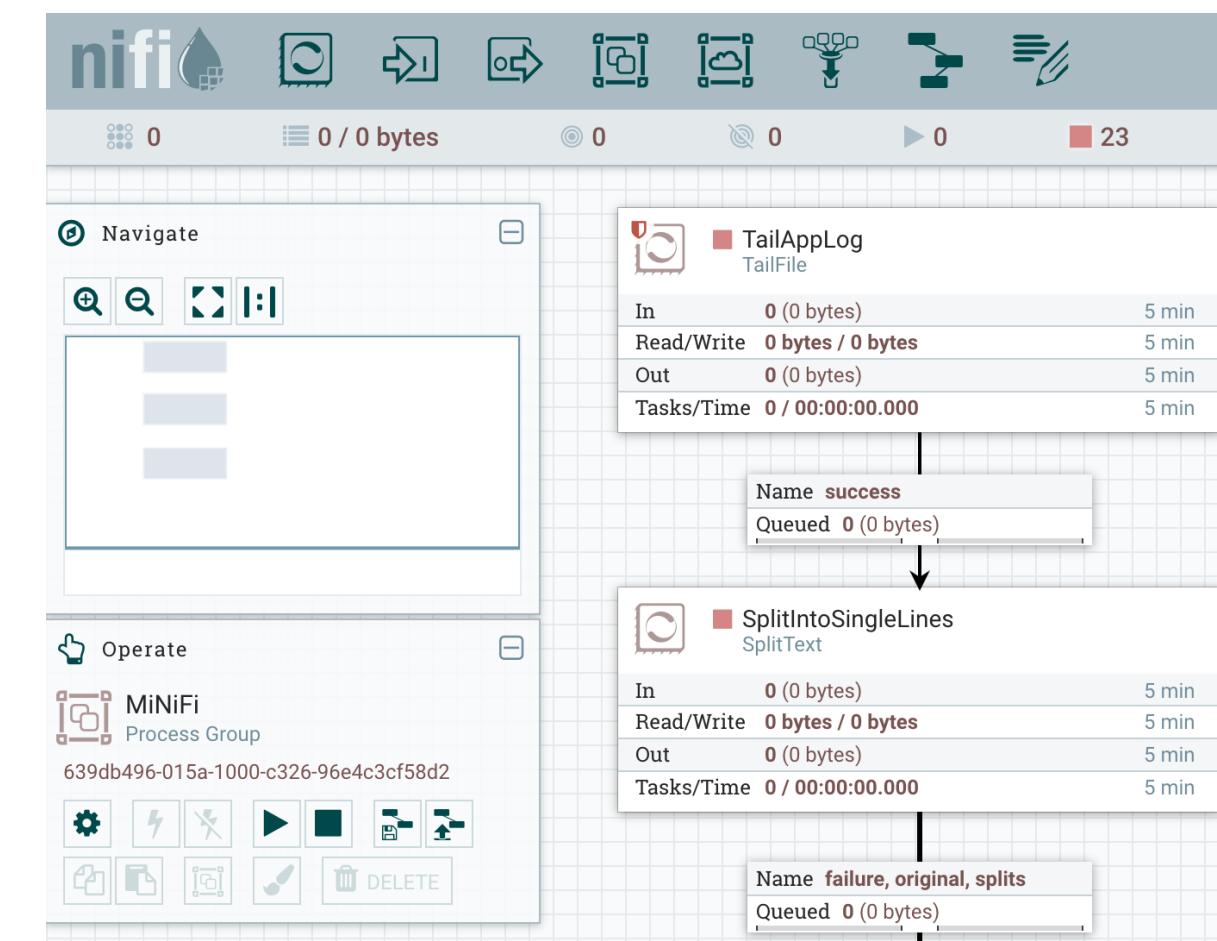
- ◆ 63 by default, more available with additional NARs

◆ MiNiFi C++ (v0.1.0)

- ◆ Written from scratch

- ◆ 7 processors by default

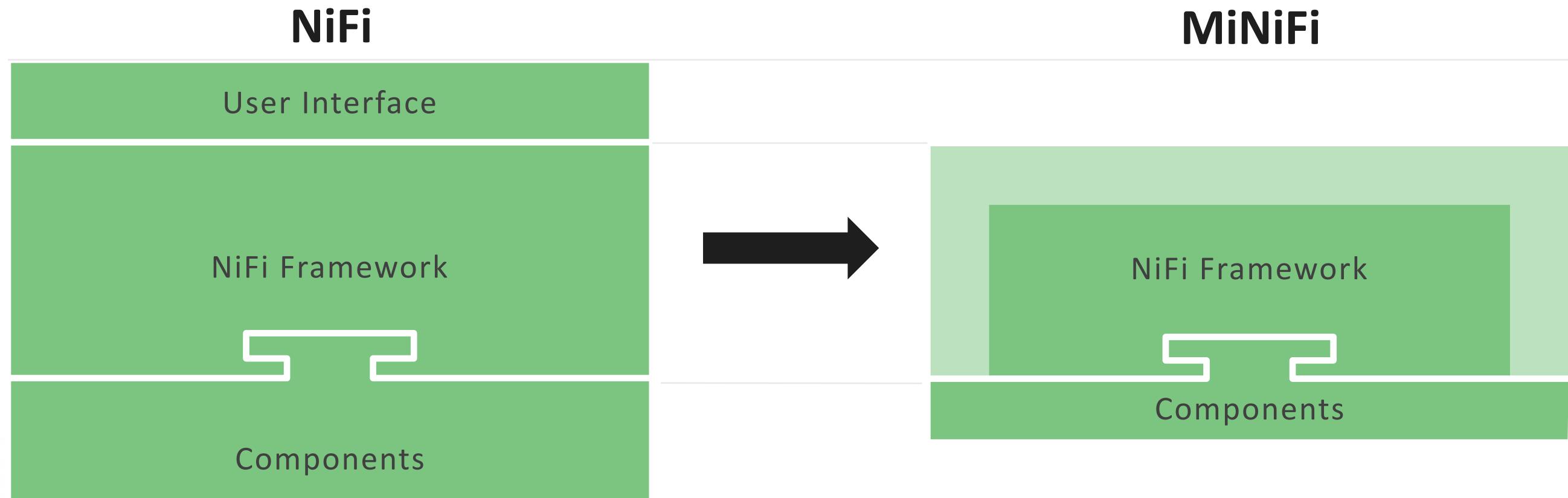
- ◆ Bi-directional site-to-site & provenance data



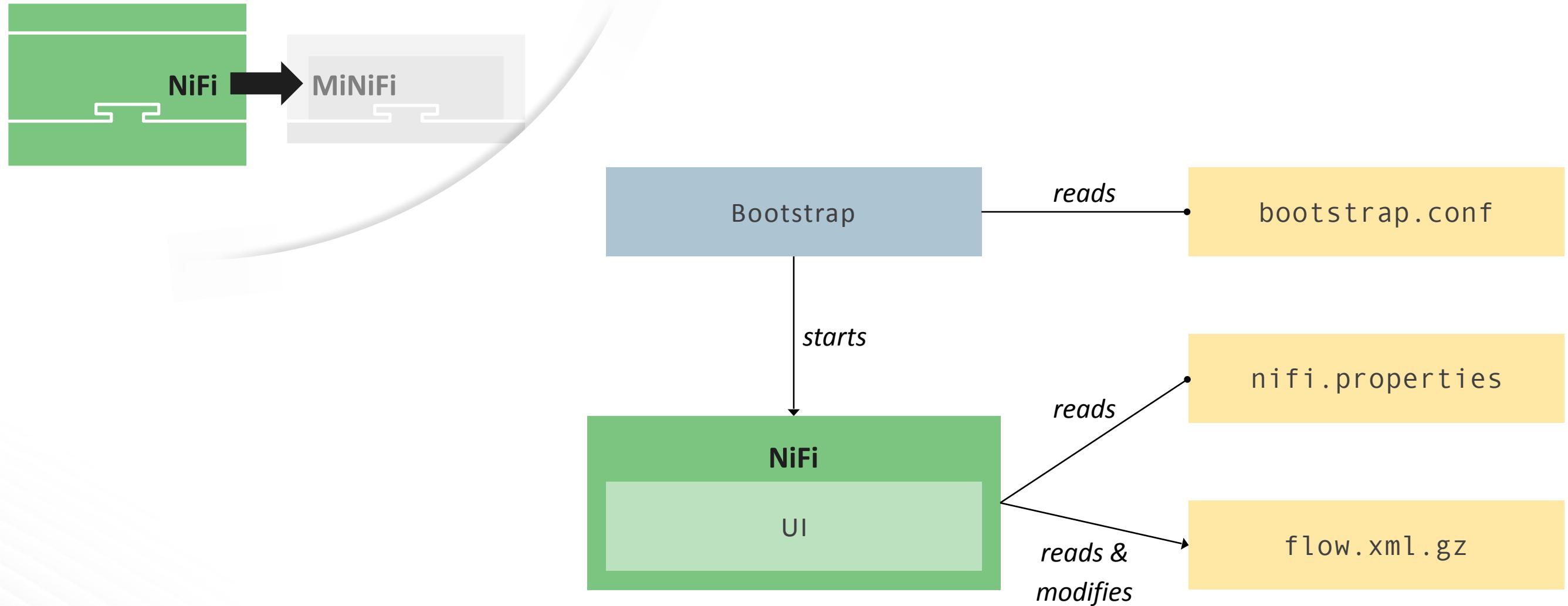
```
Security Properties:
  keystore: /tmp/ssl/localhost-ks.jks
  keystore type: JKS
  keystore password: localtest
  key password: localtest
  truststore: /tmp/ssl/localhost-ts.jks
  truststore type: JKS
  truststore password: localtest
  ssl protocol: TLS
  Sensitive Props:
    key:
      algorithm: PBWEWITHMD5AND256BITAES-CBC-OPENSSL
      provider: BC

Processors:
  - name: TailAppLog
    class: org.apache.nifi.processors.standard.TailFile
    max concurrent tasks: 1
    scheduling strategy: TIMER_DRIVEN
    scheduling period: 10 sec
    penalization period: 30 sec
    yield period: 1 sec
    run duration nanos: 0
    auto-terminated relationships list:
      Properties:
        File to Tail: logs/minifi-app.log
        Rolling Filename Pattern: minifi-app*
        Initial Start Position: Beginning of File
  - name: SplitIntoSingleLines
    class: org.apache.nifi.processors.standard.SplitText
    max concurrent tasks: 1
    scheduling strategy: TIMER_DRIVEN
    scheduling period: 0 sec
    penalization period: 30 sec
    yield period: 1 sec
    run duration nanos: 0
    auto-terminated relationships list:
      - failure
      - original
    Properties:
      Line Split Count: 1
      Header Line Count: 0
      Remove Trailing Newlines: true
```

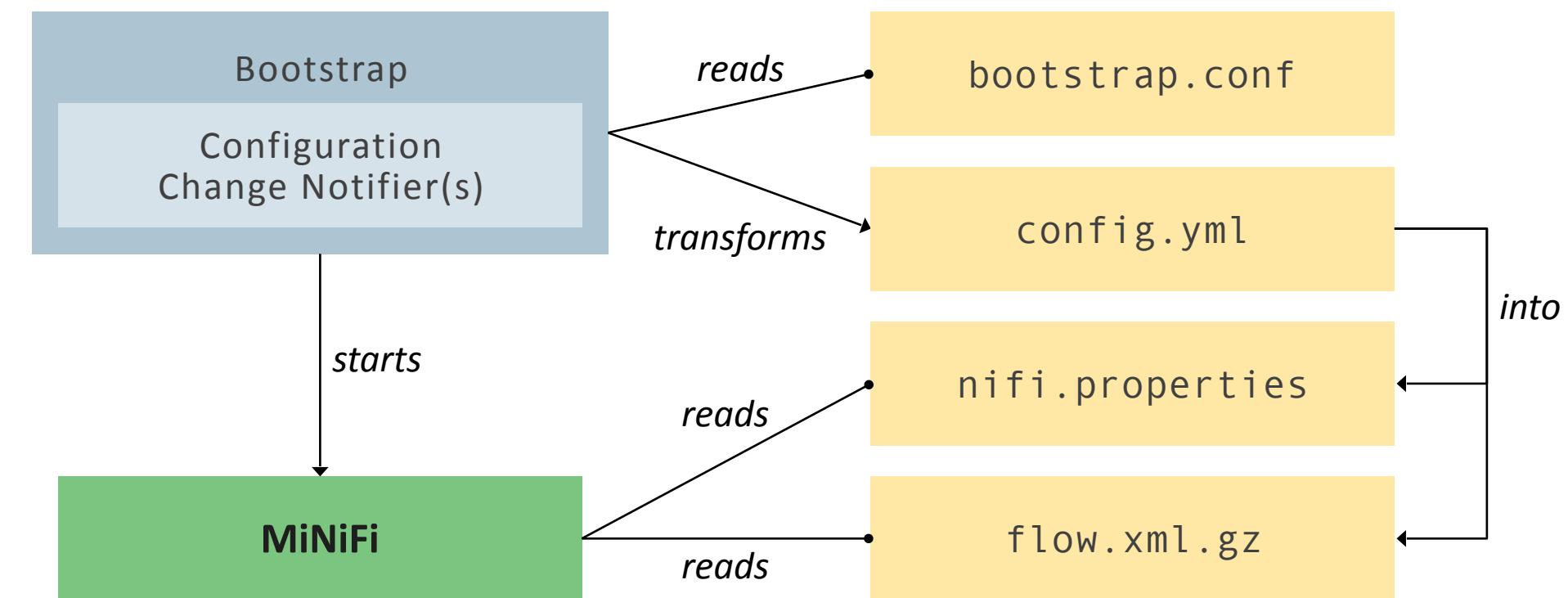
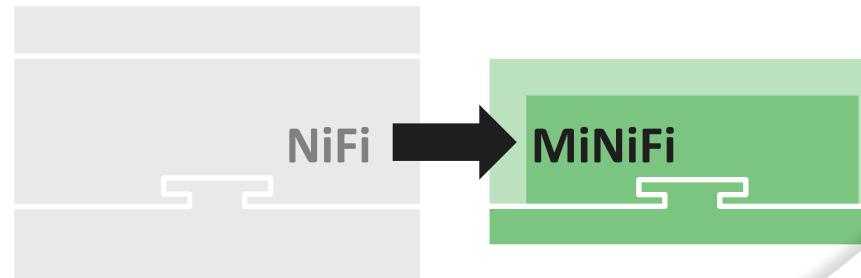
NiFi vs MiNiFi Java Processes



NiFi Java Processes



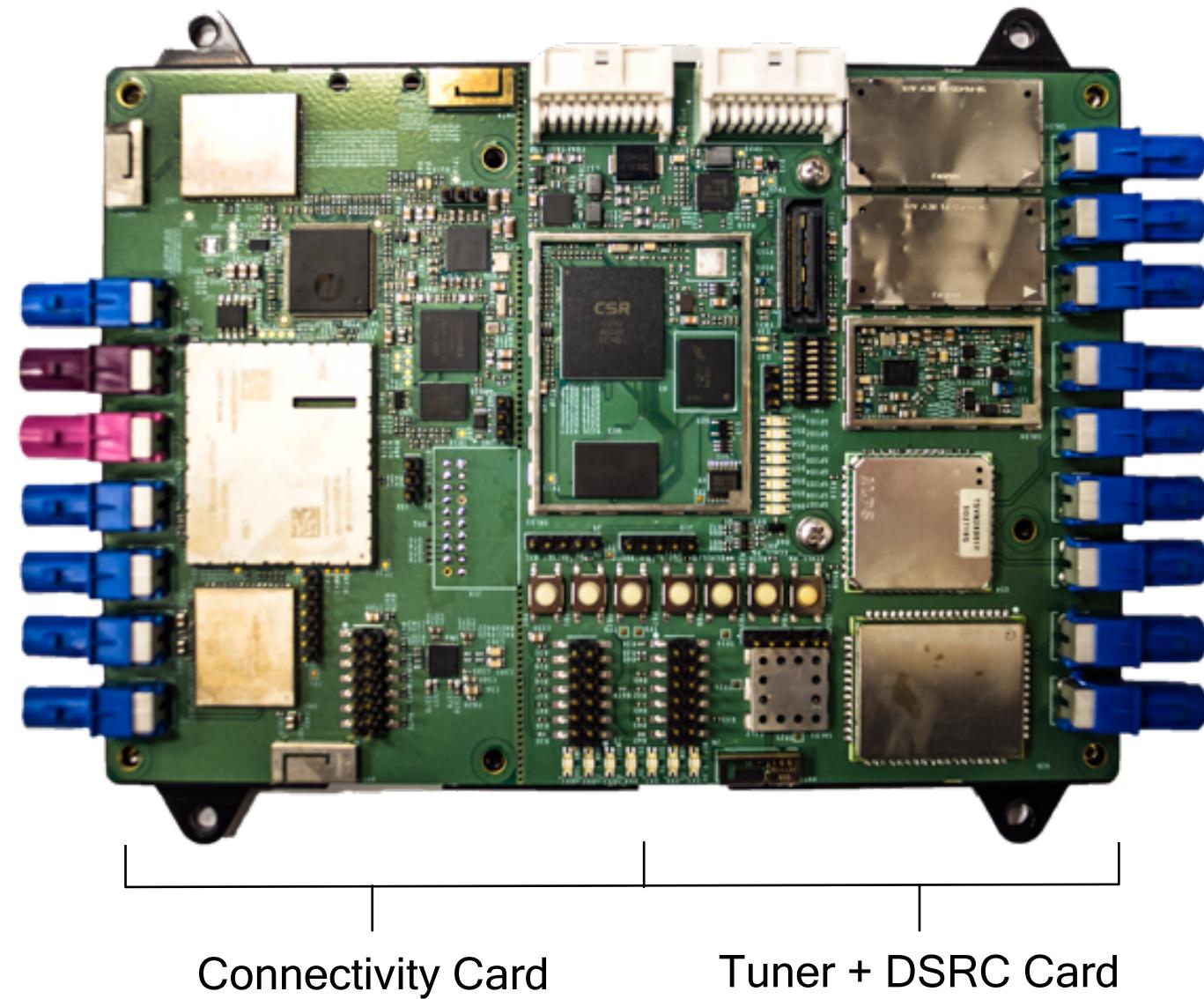
MiNiFi Java Processes



What does MiNiFi provide?

- ◆ Data tagging/provenance
- ◆ Governance from edge (geopolitical restrictions)
- ◆ Security (encryption, certificate-based authentication)
- ◆ Low latency (immediate reactions & decision-making)

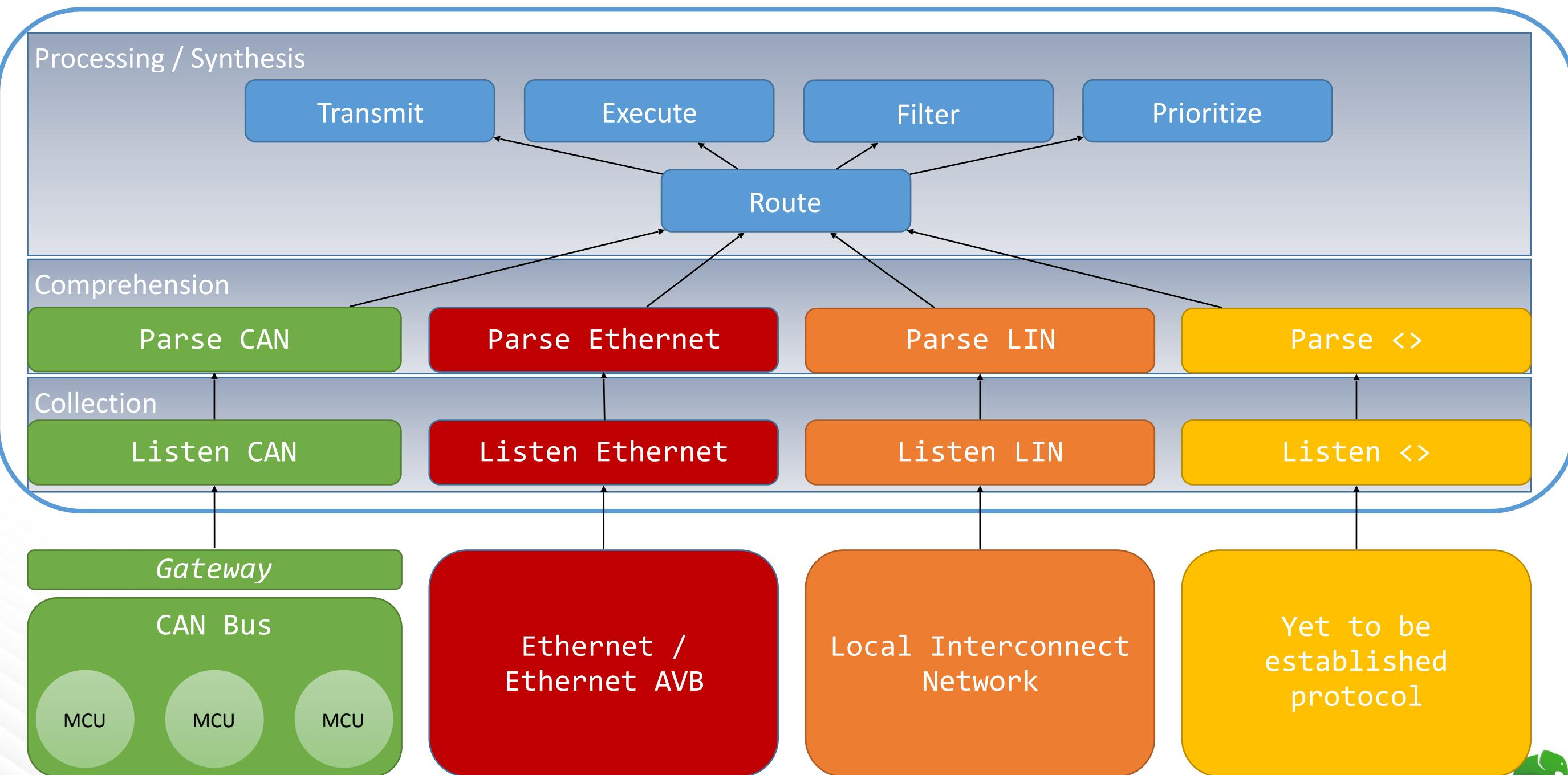
Connected Car Reference Platform Box



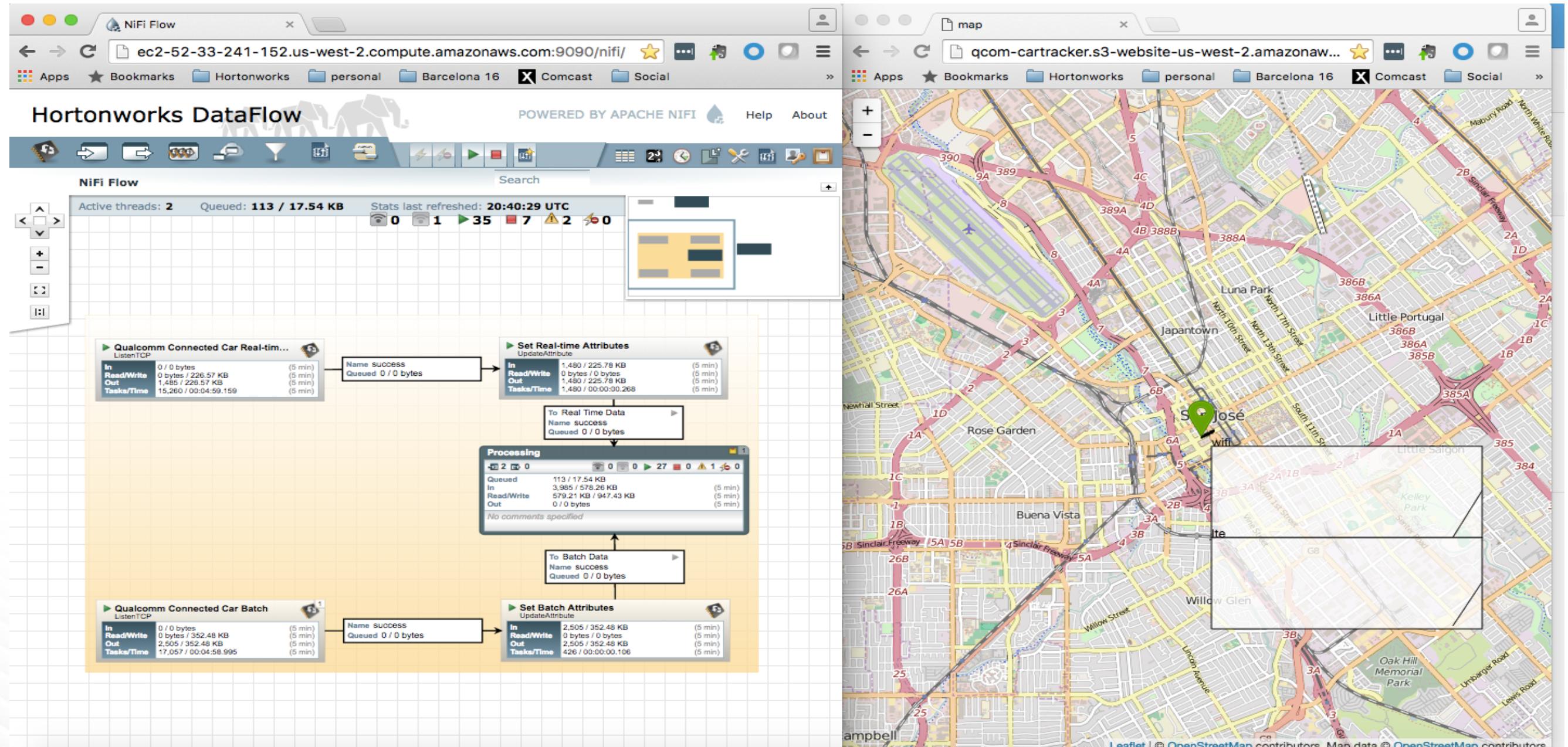
Connectivity Card

Tuner + DSRC Card

MiNiFi on a Connected Car



MiNiFi on a Connected Car

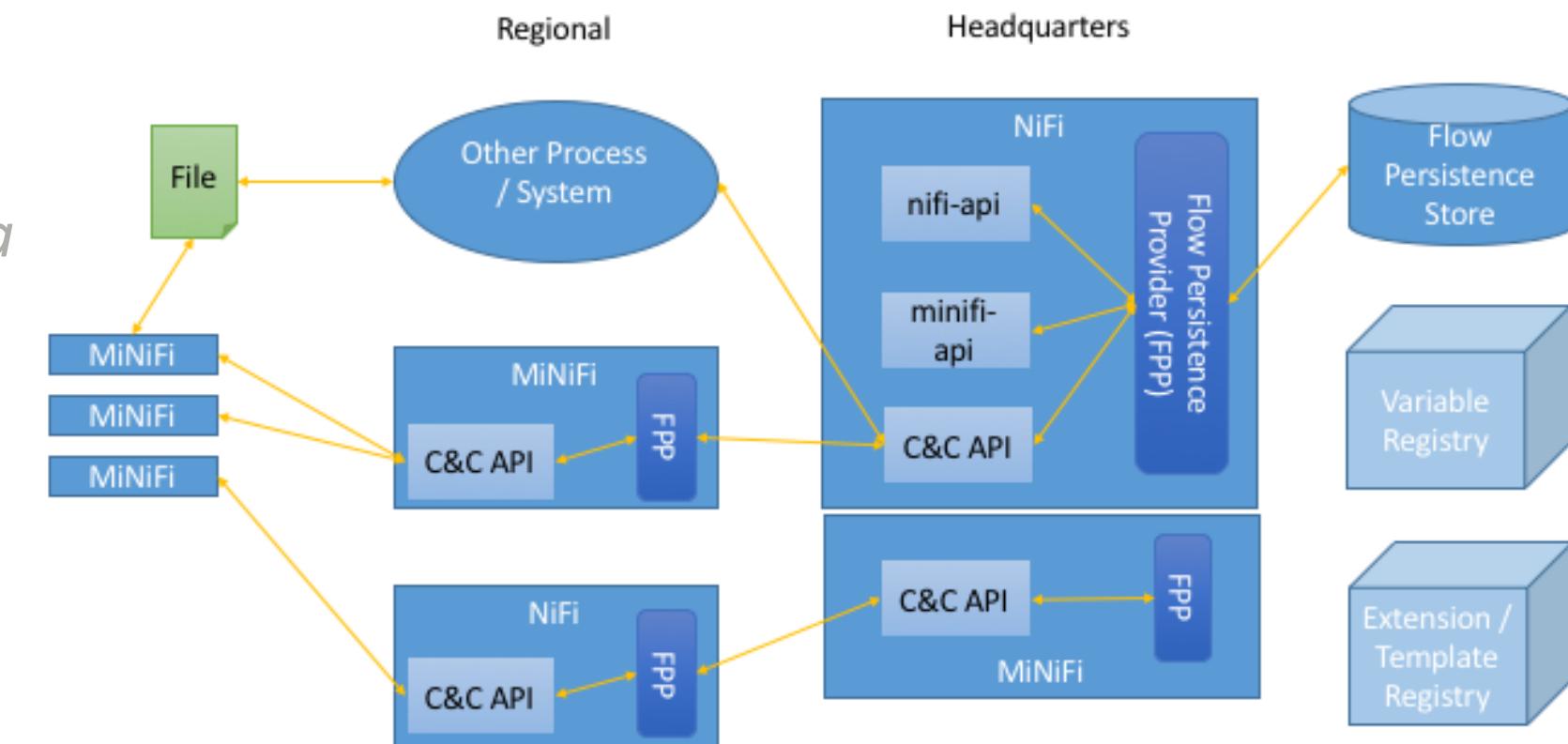


MiNiFi Exfil

- ◆ Site-to-Site
 - ◆ NiFi protocol
 - ◆ Two implementations
 - ◆ Raw socket
 - ◆ HTTP(S) (*Java only*)
 - ◆ Secured with mutual authentication TLS
- ◆ HTTP(S), (S)FTP, JMS, Syslog, File, Email, Process (*Java only*)

MiNiFi Feature Proposals

- ◆ Flow Versioning
 - ◆ Develop flows for class of MiNiFi instances
- ◆ Command & Control (C2) API (*in Java master*)
 - ◆ FileChangelngestor
 - ◆ RestAPIIngestor
 - ◆ PullHTTPIngestor



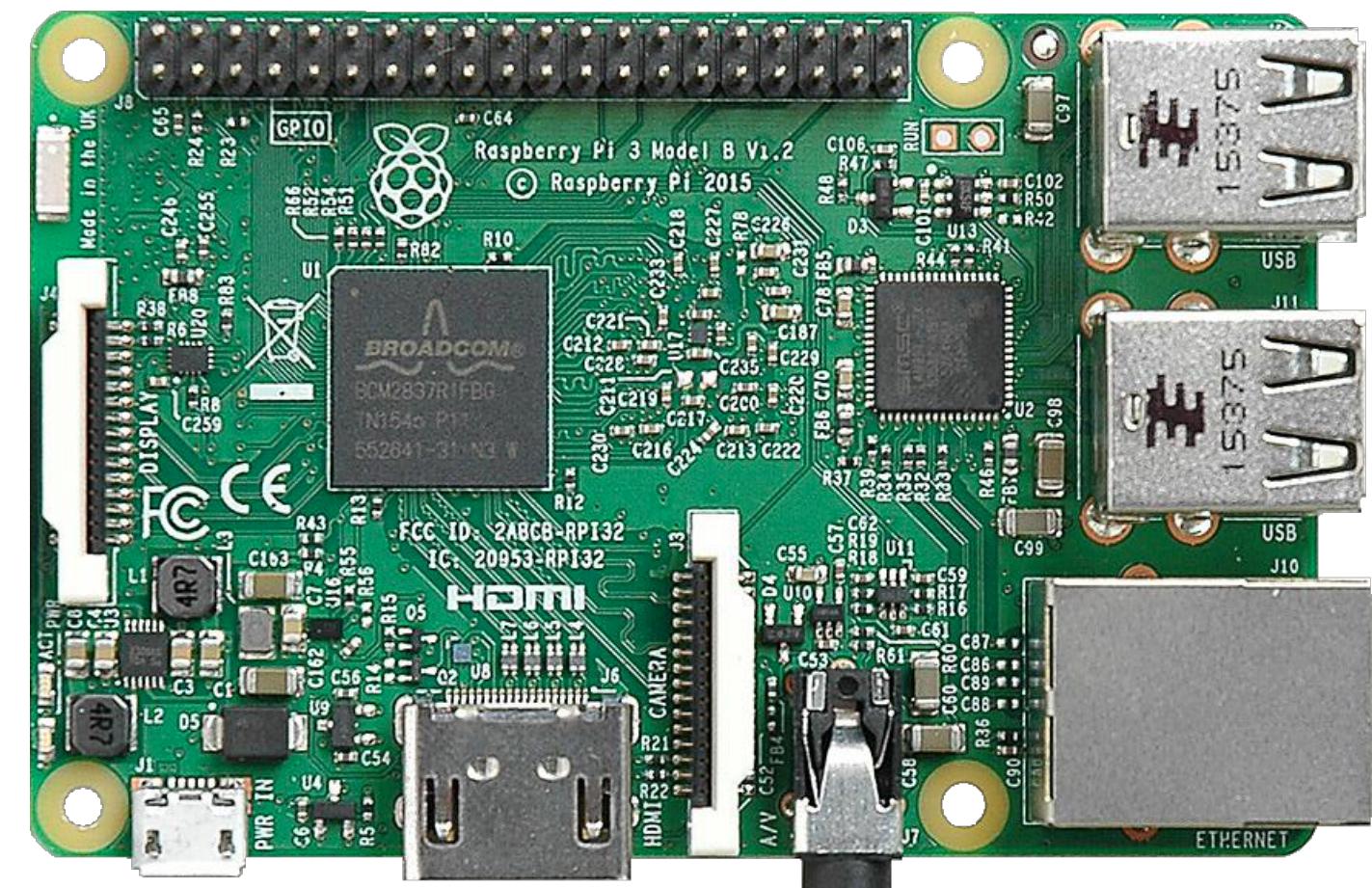
Agenda



- What is dataflow and what are the challenges?*
- Apache NiFi*
- IoT Challenges
- Apache MiNiFi
- Exploration
- Community

Scenario

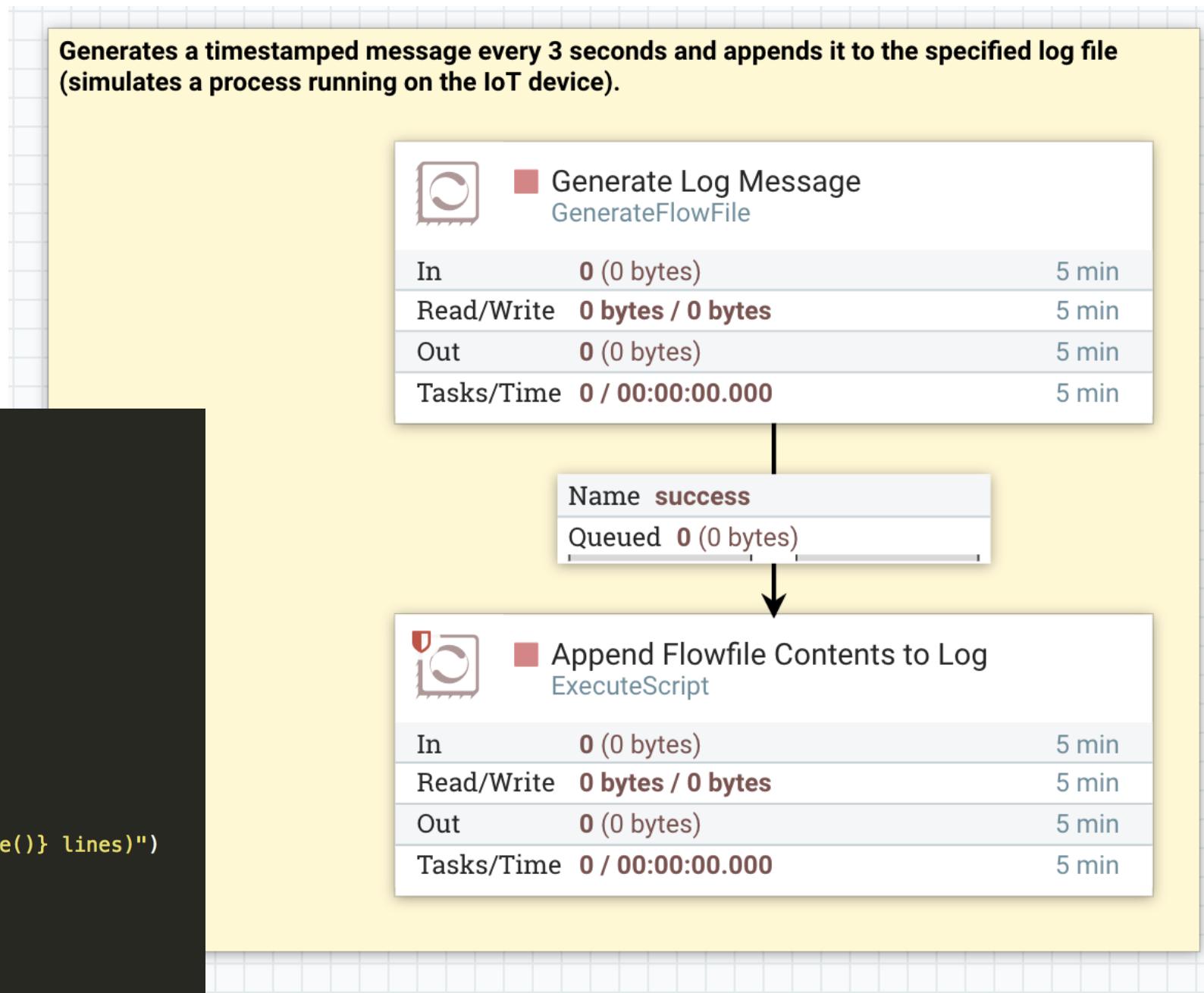
- IoT Device generating log messages
 - Need to encrypt data on device
 - Need to prioritize some data for unreliable network connectivity
 - Transmit data to central node
 - Decrypt data and analyze
 - *Make determinations and modify live flow*



NiFi As Test Harness/Environment

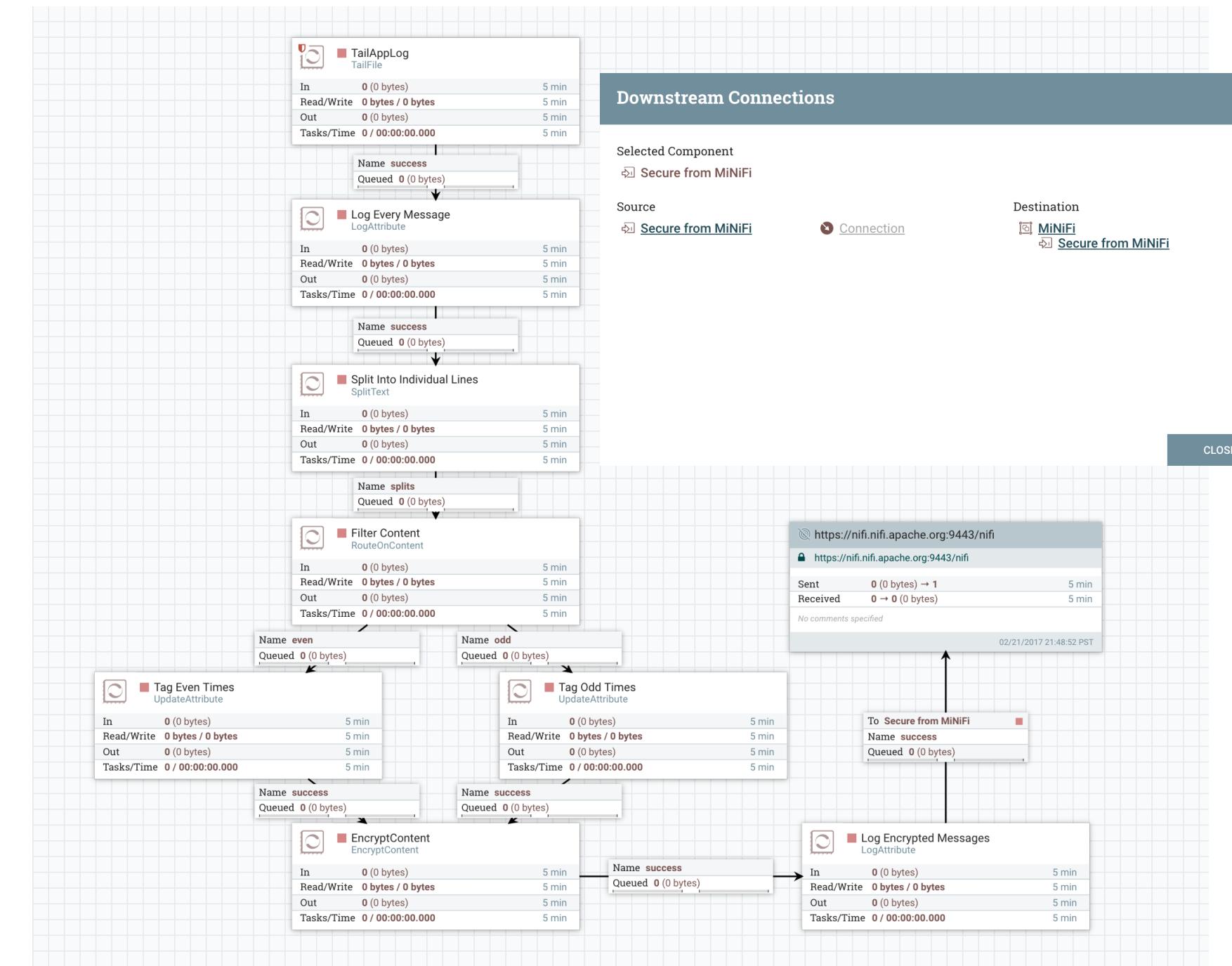
- Simulate the log generation
- Schedule is customizable
- Script can write to dynamic location

```
1 import org.apache.commons.io.IOUtils
2 import java.nio.charset.*
3
4 def flowfile = session.get()
5 if (!flowfile) return
6
7 try {
8     log.info("Received log message from generator")
9
10    def inputStream = session.read(flowfile)
11    def logMessage = IOUtils.toString(inputStream, StandardCharsets.UTF_8)
12    inputStream.close()
13
14    def logFile = new File(logFilePath as String)
15    logFile.append(System.getProperty("line.separator") + logMessage)
16
17    log.info("Wrote message to log file (total: ${logFile.text.split("\n").size()} lines)")
18
19    session.transfer(flowfile, REL_SUCCESS)
20 } catch (Exception e) {
21     log.error(e)
22     session.transfer(flowfile, REL_FAILURE)
23 }
```



Build the MiNiFi Flow

- ◆ Tails a log file
- ◆ Logs the raw contents (can be multiple lines in time window)
- ◆ Splits into individual lines
- ◆ Filters the content
 - ◆ Using parity of the timestamp
- ◆ Prioritizes
- ◆ Encrypts using AES/GCM
- ◆ Exfiles to remote NiFi



Export from NiFi to MiNiFi

- Save as template from NiFi
- Run \$./bin/config.sh transform template.xml config.yml
- MiNiFi flow ready to run*

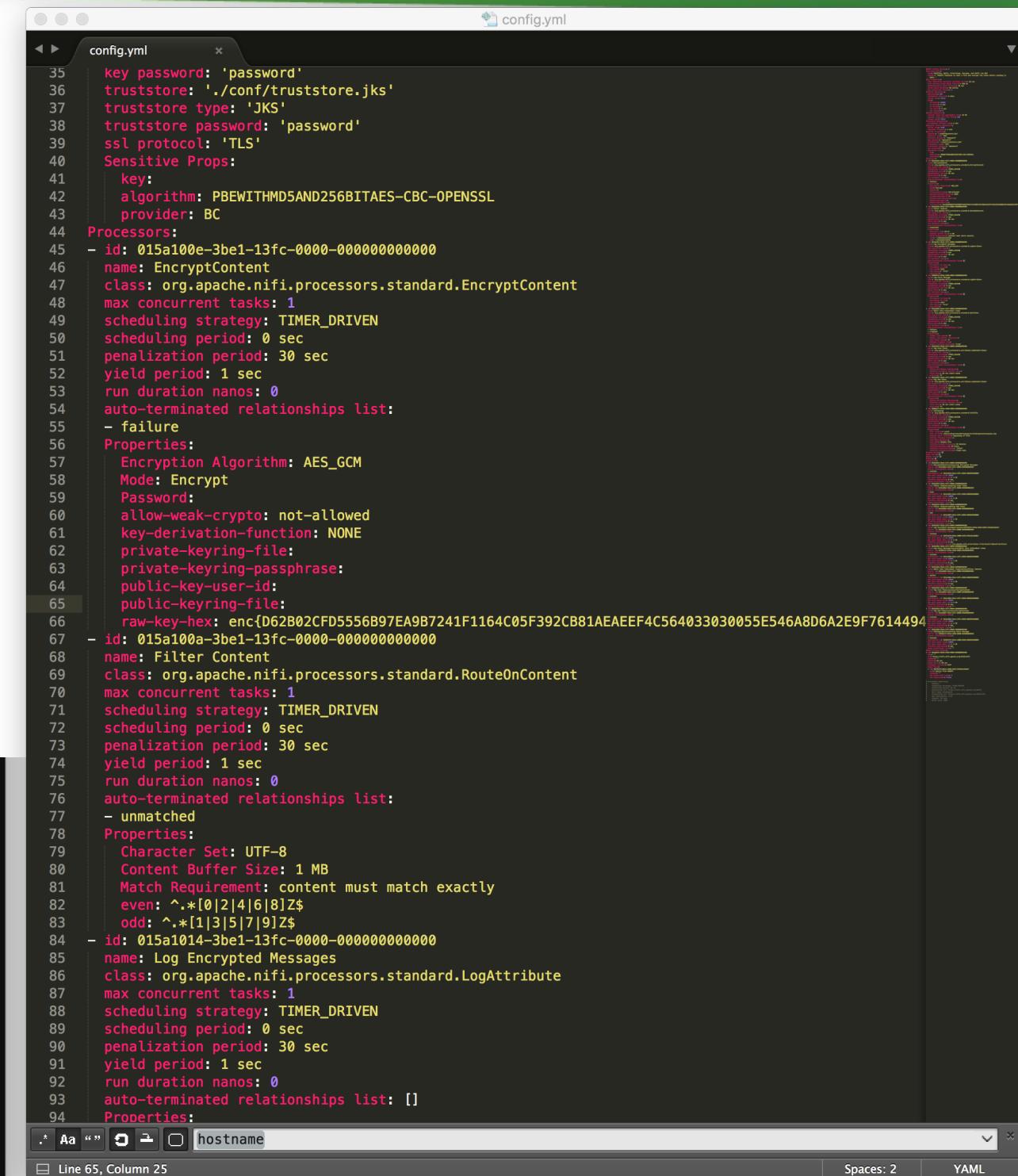
*Still need to set up TLS & encrypted properties

```
hw12203:...inifi-toolkit-assembly/target/minifi-toolkit-0.1.0-bin/minifi-toolkit-0.1.0 (master) alopresto
2s @ 21:54:55 $ ./bin/config.sh transform ~/Downloads/TailFile\,_Split\,_Prioritize\,_Encrypt\,_and_Exfil_via_S2S.xml config.yml

Java home: /Users/alopresto/.jenv/versions/1.8
MiNiFi Toolkit home: /Users/alopresto/Workspace/scratch/release_verification/minifi-java-0.1.0/minifi-0.1.0/minifi-toolkit/minifi-toolkit-assembly/target/minifi-toolkit-0.1.0-bin/minifi-toolkit-0.1.0

No validation errors found in converted configuration.

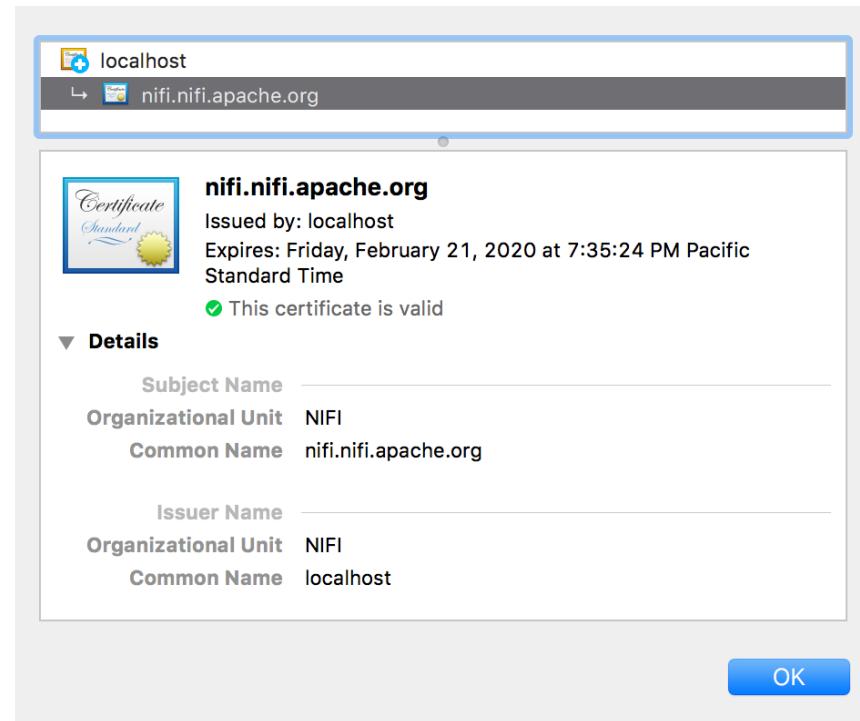
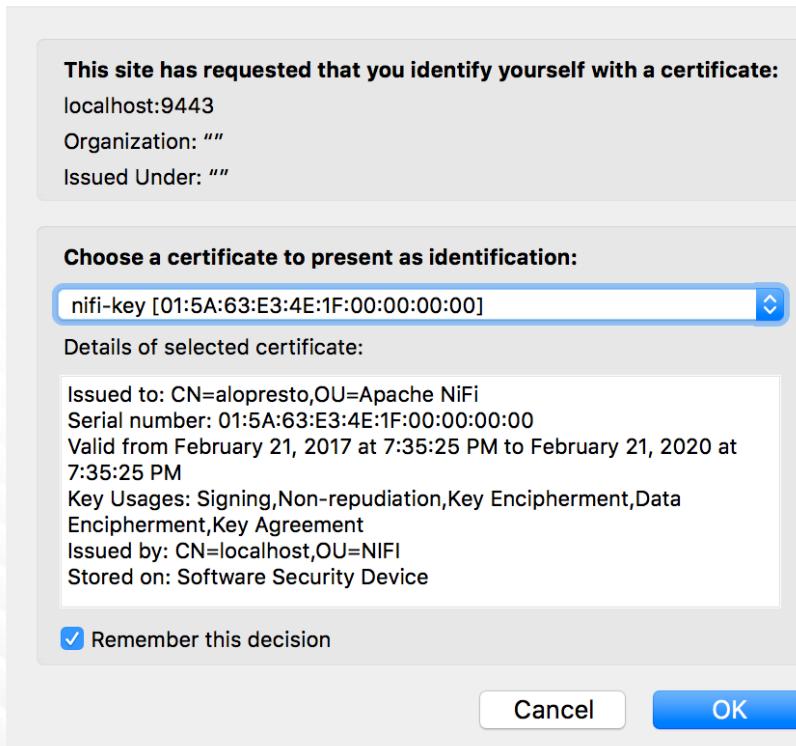
hw12203:...inifi-toolkit-assembly/target/minifi-toolkit-0.1.0-bin/minifi-toolkit-0.1.0 (master) alopresto
41s @ 21:55:37 $ ll
total 104
drwxr-xr-x  8 alopresto  staff  272B Feb 21 21:55 .
drwxr-xr-x  3 alopresto  staff  102B Dec  1 11:13 ..
-rw-r--r--  1 alopresto  staff  18K Nov 30 22:55 LICENSE
-rw-r--r--  1 alopresto  staff  11K Nov 30 22:55 NOTICE
-rw-r--r--  1 alopresto  staff  4.6K Nov 30 22:55 README
drwxr-xr-x  4 alopresto  staff  136B Dec  1 11:13 bin/
-rw-r--r--  1 alopresto  staff  8.9K Feb 21 21:55 config.yml
drwxr-xr-x 83 alopresto  staff  2.8K Dec  1 11:13 lib/
hw12203:...inifi-toolkit-assembly/target/minifi-toolkit-0.1.0-bin/minifi-toolkit-0.1.0 (master) alopresto
10s @ 21:55:47 $
```



```
config.yml
35 key password: 'password'
36 truststore: './conf/truststore.jks'
37 truststore type: 'JKS'
38 truststore password: 'password'
39 ssl protocol: 'TLS'
40 Sensitive Props:
41   key:
42     algorithm: PBEWITHMD5AND256BITAES-CBC-OPENSSL
43     provider: BC
44 Processors:
45 - id: 015a100e-3be1-13fc-0000-000000000000
46   name: EncryptContent
47   class: org.apache.nifi.processors.standard.EncryptContent
48   max concurrent tasks: 1
49   scheduling strategy: TIMER_DRIVEN
50   scheduling period: 0 sec
51   penalization period: 30 sec
52   yield period: 1 sec
53   run duration nanos: 0
54   auto-terminated relationships list:
55 - failure
56   Properties:
57     Encryption Algorithm: AES_GCM
58     Mode: Encrypt
59     Password:
60     allow-weak-crypto: not-allowed
61     key-derivation-function: NONE
62     private-keyring-file:
63     private-keyring-passphrase:
64     public-key-user-id:
65     public-keyring-file:
66     raw-key-hex: enc{D62B02CFD5556B97EA9B7241F1164C05F392CB81AEAEF4C564033030055E546A8D6A2E9F7614494
67 - id: 015a100a-3be1-13fc-0000-000000000000
68   name: Filter Content
69   class: org.apache.nifi.processors.standard.RouteOnContent
70   max concurrent tasks: 1
71   scheduling strategy: TIMER_DRIVEN
72   scheduling period: 0 sec
73   penalization period: 30 sec
74   yield period: 1 sec
75   run duration nanos: 0
76   auto-terminated relationships list:
77 - unmatched
78   Properties:
79     Character Set: UTF-8
80     Content Buffer Size: 1 MB
81     Match Requirement: content must match exactly
82     even: ^.*[0|2|4|6|8]Z$
83     odd: ^.*[1|3|5|7|9]Z$
84 - id: 015a1014-3be1-13fc-0000-000000000000
85   name: Log Encrypted Messages
86   class: org.apache.nifi.processors.standard.LogAttribute
87   max concurrent tasks: 1
88   scheduling strategy: TIMER_DRIVEN
89   scheduling period: 0 sec
90   penalization period: 30 sec
91   yield period: 1 sec
92   run duration nanos: 0
93   auto-terminated relationships list: []
94   Properties:
```

Setting Up Crypto

- NiFi TLS Toolkit makes certificates & keystores simple (*and secure*)
- Copy encrypted property value from `flow.xml.gz` to `config.yml` (*flow repo*)



```
hw12203:...assembly/target/nifi-toolkit-1.2.0-SNAPSHOT-bin/nifi-toolkit-1.2.0-SNAPSHOT (NIFI-3486-RC1) all
opresto
173s @ 19:34:24 $ ./bin/tls-toolkit.sh standalone -n 'nifi.nifi.apache.org' -C 'CN=alopresto, OU=Apache NiFi' -P password -S password -B password -f ../../../../../../nifi-assembly/target/nifi-1.2.0-SNAPSHOT-bin/nifi-1.2.0-SNAPSHOT/conf/nifi.properties -o ../../../../../../nifi-assembly/target/nifi-1.2.0-SNAPSHOT-bin/nifi-1.2.0-SNAPSHOT/conf/
2017/02/21 19:35:23 INFO [main] org.apache.nifi.toolkit.tls.standalone.TlsToolkitStandaloneCommandLine: Using ../../../../../../nifi-assembly/target/nifi-1.2.0-SNAPSHOT-bin/nifi-1.2.0-SNAPSHOT/conf/nifi.properties as template.
2017/02/21 19:35:23 INFO [main] org.apache.nifi.toolkit.tls.standalone.TlsToolkitStandalone: Running standalone certificate generation with output directory ../../../../../../nifi-assembly/target/nifi-1.2.0-SNAPSHOT-bin/nifi-1.2.0-SNAPSHOT/conf
2017/02/21 19:35:24 INFO [main] org.apache.nifi.toolkit.tls.standalone.TlsToolkitStandalone: Generated new CA certificate ../../../../../../nifi-assembly/target/nifi-1.2.0-SNAPSHOT-bin/nifi-1.2.0-SNAPSHOT/conf/nifi-cert.pem and key ../../../../../../nifi-assembly/target/nifi-1.2.0-SNAPSHOT-bin/nifi-1.2.0-SNAPSHOT/conf/nifi-key.key
2017/02/21 19:35:24 INFO [main] org.apache.nifi.toolkit.tls.standalone.TlsToolkitStandalone: Writing new ssl configuration to ../../../../../../nifi-assembly/target/nifi-1.2.0-SNAPSHOT-bin/nifi-1.2.0-SNAPSHOT/conf/nifi.nifi.apache.org
2017/02/21 19:35:24 INFO [main] org.apache.nifi.toolkit.tls.standalone.TlsToolkitStandalone: Successfully generated TLS configuration for nifi.nifi.apache.org 1 in ../../../../../../nifi-assembly/target/nifi-1.2.0-SNAPSHOT-bin/nifi-1.2.0-SNAPSHOT/conf/nifi.nifi.apache.org
2017/02/21 19:35:24 INFO [main] org.apache.nifi.toolkit.tls.standalone.TlsToolkitStandalone: Generating new client certificate ../../../../../../nifi-assembly/target/nifi-1.2.0-SNAPSHOT-bin/nifi-1.2.0-SNAPSHOT/conf/CN=alopresto_OU=Apache_NiFi.p12
2017/02/21 19:35:25 INFO [main] org.apache.nifi.toolkit.tls.standalone.TlsToolkitStandalone: Successfully generated client certificate ../../../../../../nifi-assembly/target/nifi-1.2.0-SNAPSHOT-bin/nifi-1.2.0-SNAPSHOT/conf/CN=alopresto_OU=Apache_NiFi.p12
2017/02/21 19:35:25 INFO [main] org.apache.nifi.toolkit.tls.standalone.TlsToolkitStandalone: tls-toolkit standalone completed successfully
hw12203:...assembly/target/nifi-toolkit-1.2.0-SNAPSHOT-bin/nifi-toolkit-1.2.0-SNAPSHOT (NIFI-3486-RC1) all
opresto
```

Secure Connection

The connection to this site is encrypted and authenticated using a strong protocol (TLS 1.2), a strong key exchange (ECDHE_RSA with P-256), and a strong cipher (AES_256_GCM).

If We Really Have TLS, Why Encrypt?

- ◆ All data transmitted over TLS is encrypted
- ◆ On NiFi, automatically decrypted
- ◆ Attributes visible
- ◆ Content still encrypted because of EncryptContent processor
- ◆ Can serve as secure route for follow-on systems

Configure Processor

SETTINGS SCHEDULING PROPERTIES COMMENTS

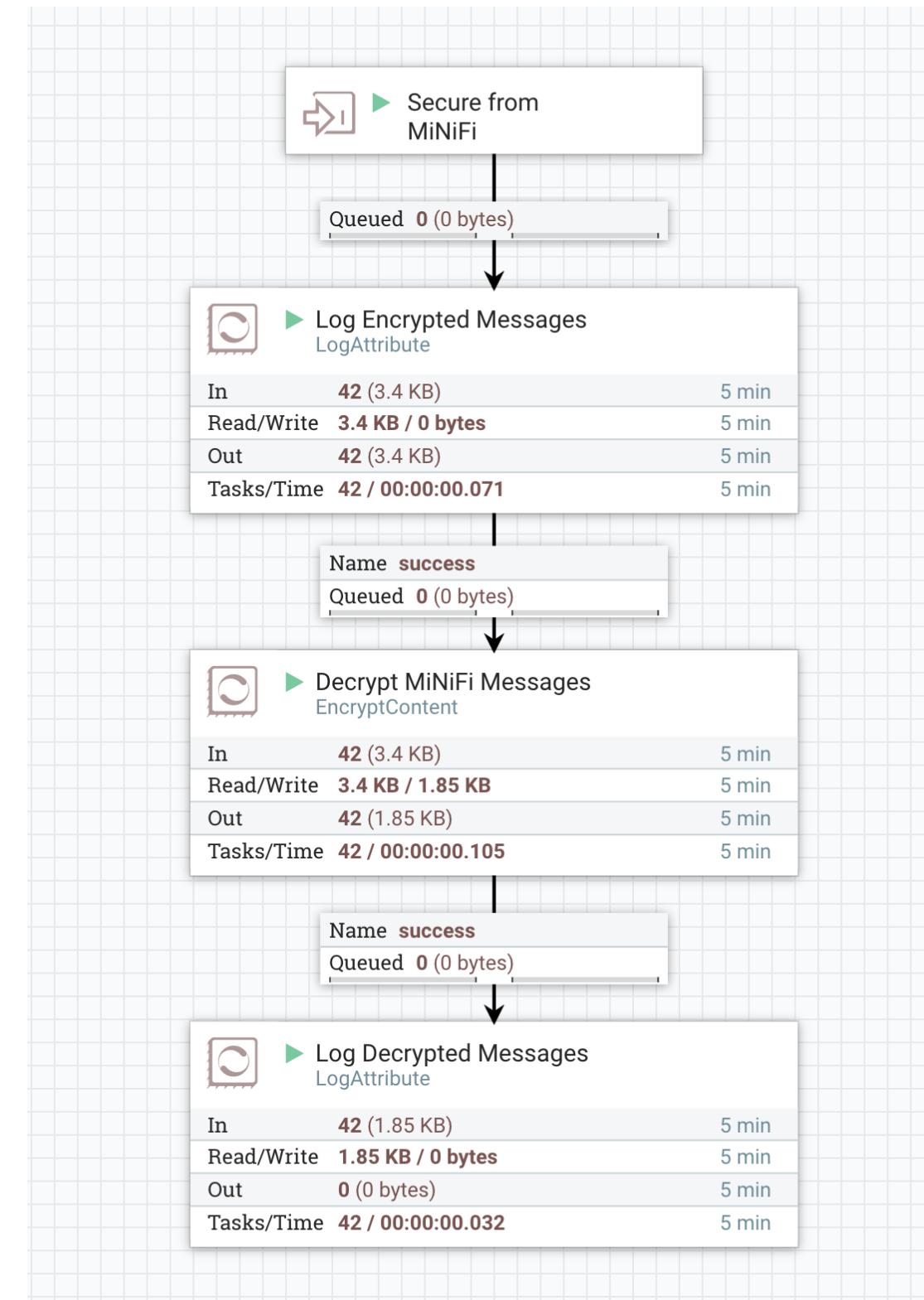
Required field

Property	Value
Mode	Encrypt
Key Derivation Function	None
Encryption Algorithm	AES_GCM
Allow insecure cryptographic modes	Not Allowed
Password	No value set
Raw Key (hexadecimal)	Sensitive value set
Public Keyring File	In keyed encryption, this is the raw key, encoded in hexadecimal
Public Key User Id	Supports expression language: false
Private Keyring File	History: • ***** - 02/21/2017 20:30:46 PST (CN=alopresto, OU=Apache NiFi)
Private Keyring Passphrase	No value set

CANCEL APPLY

Process Data In NiFi

- Receive the data over S2S
- Log the incoming messages
- Decrypt content
- Log again



Does It Work?

NiFi Data Provenance

Displaying 213 of 213
Oldest event available: 02/21/2017 22:14:43 PST

Filter by component name

Date/Time	Type
02/21/2017 22:22:05.079 PST	DROP
02/21/2017 22:22:05.078 PST	DROP
02/21/2017 22:22:05.077 PST	CONTENT_MODIFIED
02/21/2017 22:22:05.076 PST	CONTENT_MODIFIED
02/21/2017 22:22:05.076 PST	CONTENT_MODIFIED
02/21/2017 22:22:05.075 PST	CONTENT_MODIFIED
02/21/2017 22:22:05.074 PST	CONTENT_MODIFIED
02/21/2017 22:22:05.073 PST	CONTENT_MODIFIED
02/21/2017 22:22:05.073 PST	CONTENT_MODIFIED
02/21/2017 22:22:05.072 PST	CONTENT_MODIFIED
02/21/2017 22:22:05.071 PST	CONTENT_MODIFIED
02/21/2017 22:22:05.070 PST	CONTENT_MODIFIED
02/21/2017 22:22:05.069 PST	CONTENT_MODIFIED
02/21/2017 22:22:05.069 PST	CONTENT_MODIFIED
02/21/2017 22:22:05.068 PST	CONTENT_MODIFIED
02/21/2017 22:22:05.068 PST	CONTENT_MODIFIED
02/21/2017 22:22:05.067 PST	DROP
02/21/2017 22:22:05.067 PST	DROP
02/21/2017 22:22:05.067 PST	CONTENT_MODIFIED
02/21/2017 22:22:05.066 PST	DROP
02/21/2017 22:22:05.066 PST	CONTENT_MODIFIED
02/21/2017 22:22:05.066 PST	DROP
02/21/2017 22:22:05.065 PST	CONTENT_MODIFIED
02/21/2017 22:22:05.065 PST	DROP
02/21/2017 22:22:05.065 PST	DROP
02/21/2017 22:22:05.064 PST	CONTENT_MODIFIED
02/21/2017 22:22:05.064 PST	DROP

Provenance Event

DETAILS	ATTRIBUTES	CONTENT
Input Claim Container default Section 1 Identifier 1487744083443-1 Offset 4259 Size 83 bytes	Output Claim Container default Section 1 Identifier 1487744083443-1 Offset 6681 Size 45 bytes	Download View
Download View	Download View	OK

Replay

Connection Id 015a1002-3be1-13fc-98e3-f54ee6183280

	a933c38a-e5b8-4eb2-abc0-91dd03216eec	45 bytes	Log Decrypted Messages
	8c335548-4e0c-47f0-8f3c-f610095815a0	45 bytes	Log Decrypted Messages
	ddacdcb7-bba6-456a-8a9f-94cdead061c4	45 bytes	Decrypt MiNiFi Messages
	49a9fe0f-a906-4886-b8a3-e8cef65a9b4	45 bytes	Log Decrypted Messages

Last updated: 22:22:49 PST

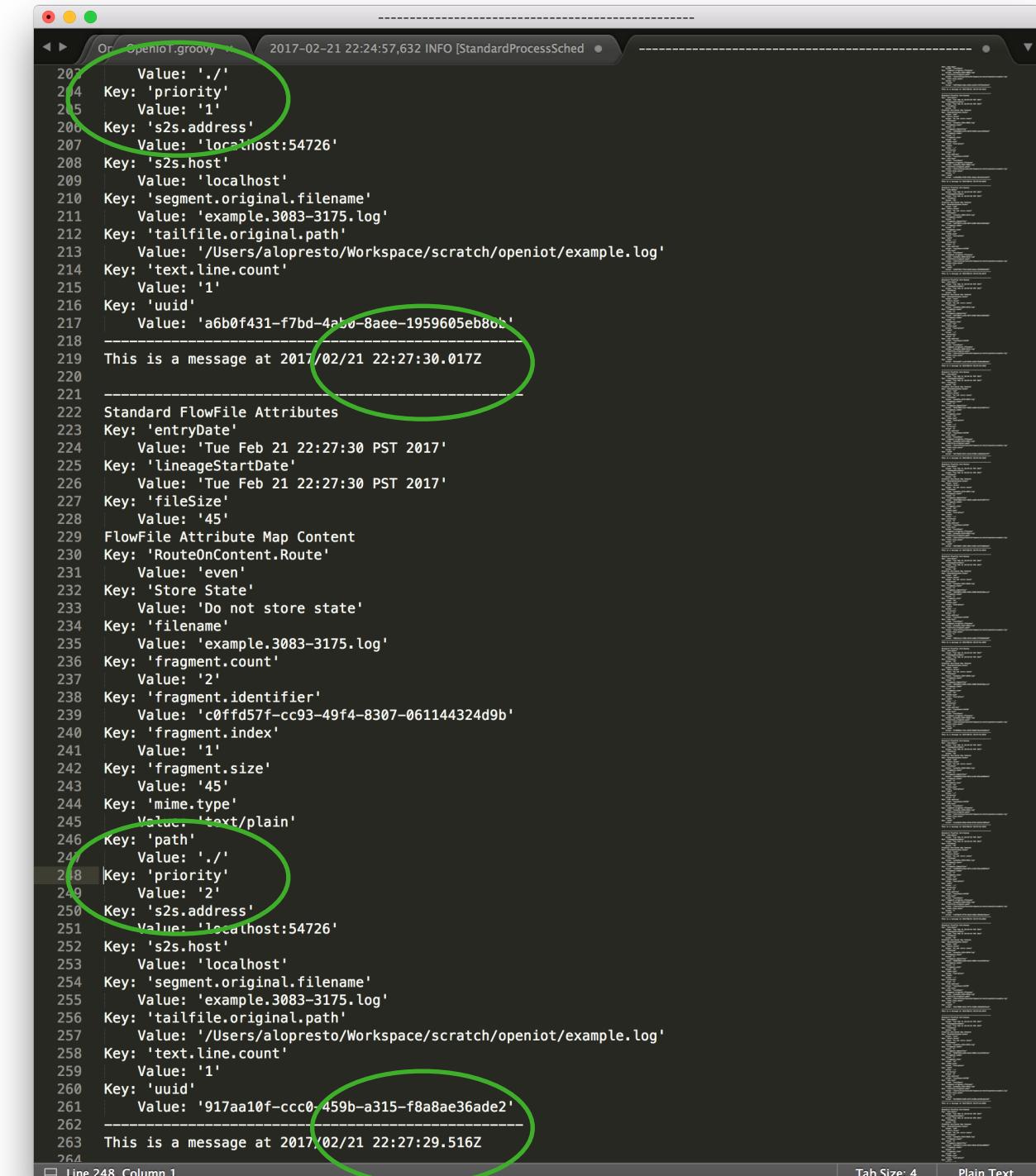
NiFi Flow > MINIFI

TailFile_Split_Prioritize.xml



Prioritization?

- Increase the write frequency
- Check that newer records (within tail window) with higher priority arrive first



```
207     Value: './'
208     Key: 'priority'
209     Value: '1'
210     Key: 's2s.address'
211     Value: 'localhost:54726'
212     Key: 's2s.host'
213     Value: 'localhost'
214     Key: 'segment.original.filename'
215     Value: 'example.3083-3175.log'
216     Key: 'tailfile.original.path'
217     Value: '/Users/alopresto/Workspace/scratch/openiot/example.log'
218     Key: 'text.line.count'
219     Value: '1'
220     Key: 'uuid'
221     Value: 'a6b0f431-f7bd-4a50-8aee-1959605eb86b'
222
223 This is a message at 2017/02/21 22:27:30.017Z
224
225 Standard FlowFile Attributes
226 Key: 'entryDate'
227     Value: 'Tue Feb 21 22:27:30 PST 2017'
228 Key: 'lineageStartDate'
229     Value: 'Tue Feb 21 22:27:30 PST 2017'
230 Key: 'fileSize'
231     Value: '45'
232 FlowFile Attribute Map Content
233 Key: 'RouteOnContent.Route'
234     Value: 'even'
235 Key: 'Store State'
236     Value: 'Do not store state'
237 Key: 'filename'
238     Value: 'example.3083-3175.log'
239 Key: 'fragment.count'
240     Value: '2'
241 Key: 'fragment.identifier'
242     Value: 'c0ffd57f-cc93-49f4-8307-061144324d9b'
243 Key: 'fragment.index'
244     Value: '1'
245 Key: 'fragment.size'
246     Value: '45'
247 Key: 'mime.type'
248     Value: 'text/plain'
249 Key: 'path'
250     Value: './'
251     Key: 'priority'
252     Value: '2'
253     Key: 's2s.address'
254     Value: 'localhost:54726'
255     Key: 's2s.host'
256     Value: 'localhost'
257     Key: 'segment.original.filename'
258     Value: 'example.3083-3175.log'
259     Key: 'tailfile.original.path'
260     Value: '/Users/alopresto/Workspace/scratch/openiot/example.log'
261     Key: 'text.line.count'
262     Value: '1'
263     Key: 'uuid'
264     Value: '917aa10f-ccc0-459b-a315-f8a8ae36ade2'
265
266 This is a message at 2017/02/21 22:27:29.516Z
267
```

Next Steps

- ◆ Window Aggregator
 - ◆ If >60% odd in window, switch prioritization
- ◆ Encrypt with different keys for different tags & send to different follow-on systems
- ◆ Spotty network? Tell MiNiFi to cache low priority and send in batches
- ◆ MiNiFi rollover & pruning of monitored log
- ◆ Exfil MiNiFi provenance data to NiFi

Agenda

What is dataflow and what are the challenges?

Apache NiFi

IoT Challenges

Apache MiNiFi

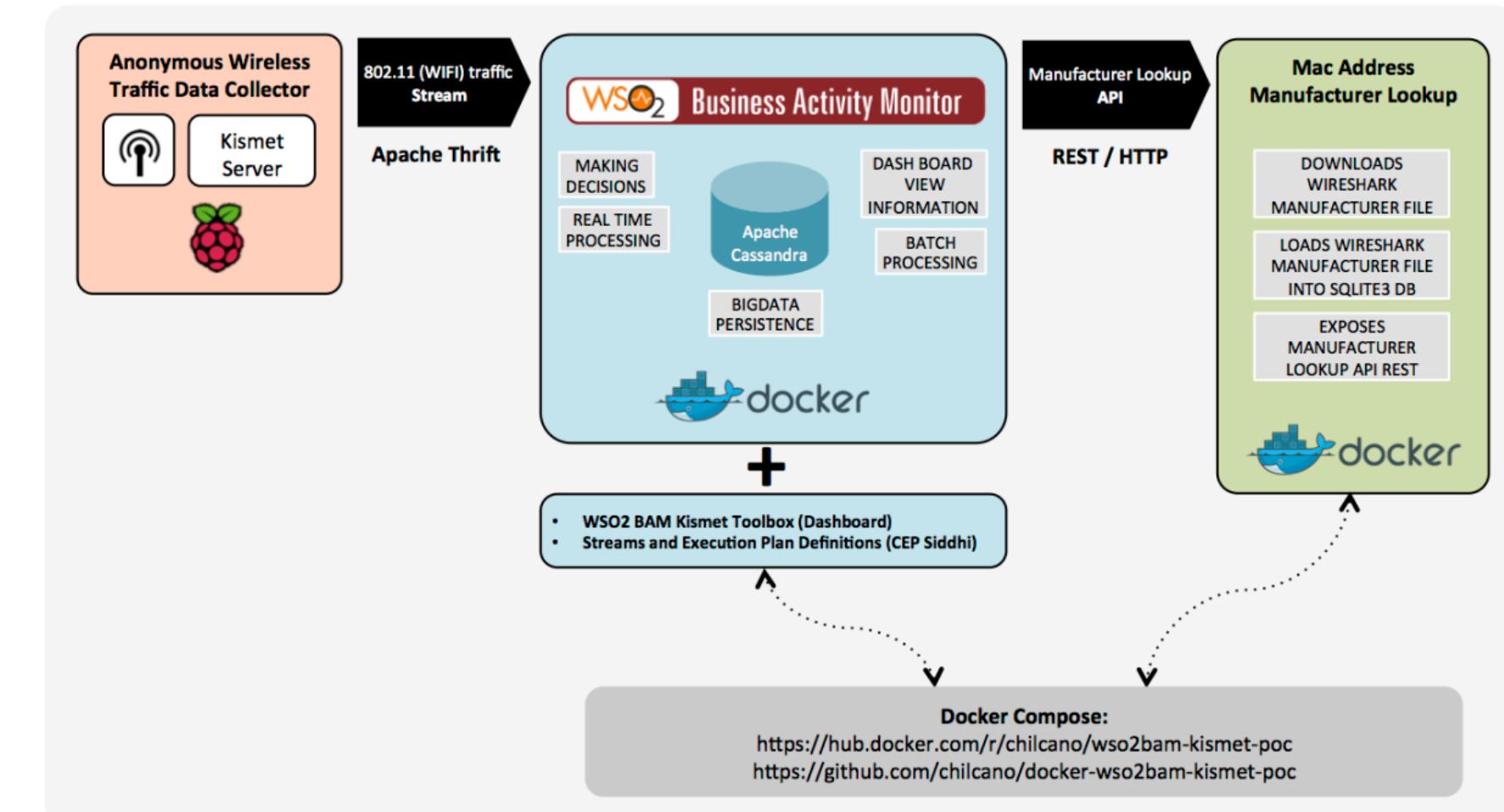
Exploration

Community



Community Example #1

- Roger Carhuatocto
- RP3B, Apache Thrift, Kismet, Apache Cassandra, and more



Community Example #1

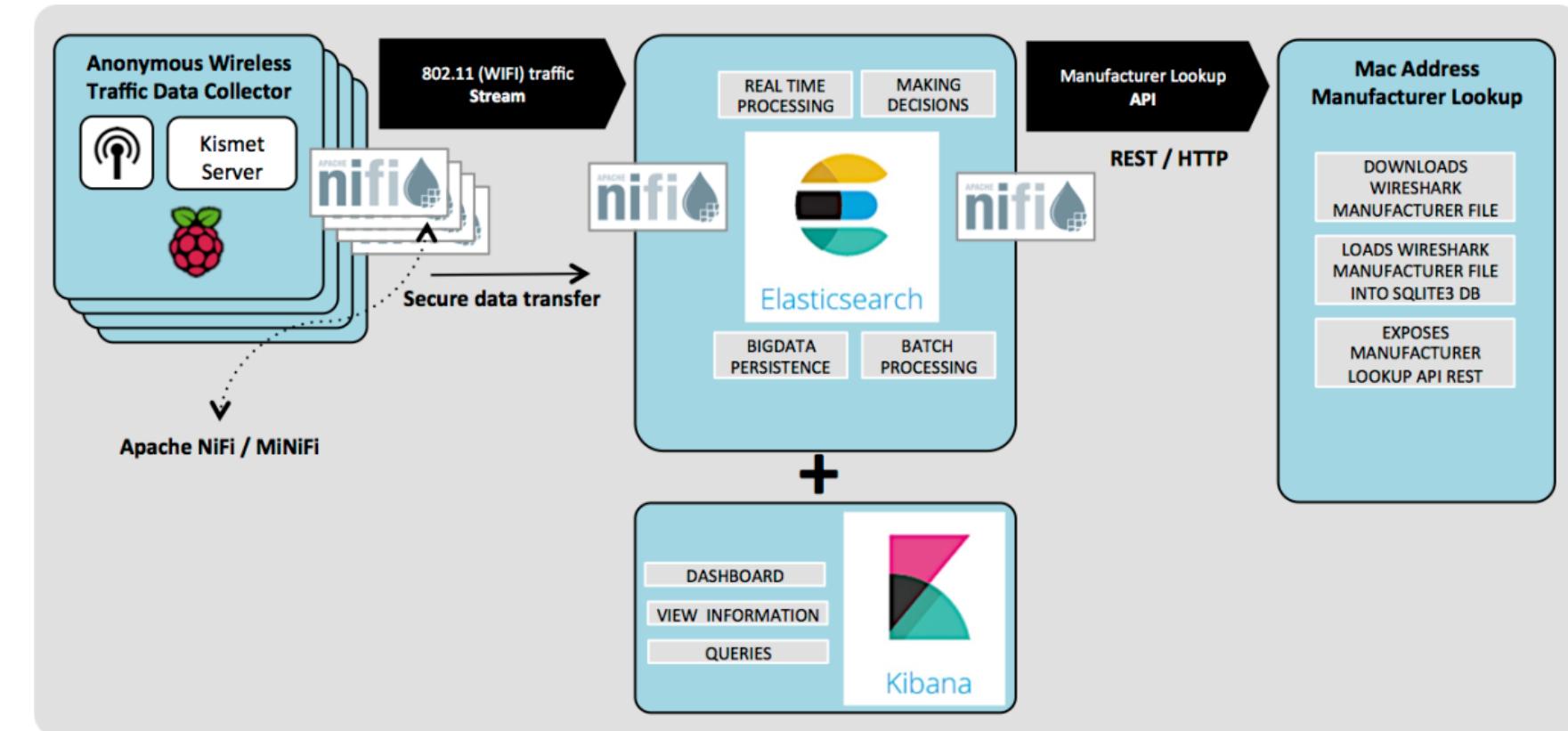
◆ Roger Carhuatocto

◆ RP3B, Apache Thrift, Kismet, Apache Cassandra, and more

- Large scaling.
 - I would like to avoid to deploy Logstash in each Raspberry Pi just to transform in JSON the captured 802.11 (WIFI) traffic and send it to Elasticsearch. Other approach what I want to avoid is to deploy Logstash with the UDP/TCP Input Plugin in the Elasticsearch side, because both choices need parse/transform/filter the captured traffic by using [GROK](#) and Elasticsearch Index Templates for each Logstash instance deployed. What if I have 100 or more Raspberry Pi distributed in different locations?.
- Security.
 - I'm using Kismet installed in each Raspberry Pi to capture 802.11 traffic, by default Kismet sends that traffic over UDP, UDP is faster but not secure. The big problem with Logstash listening UDP traffic over a port is that Logstash is susceptible to DoS attacks and the traffic to be spoofed. I have to update UDP to the "secure UDP", UDP over SSL/TLS for example.
- Monitoring/Tracking.
 - How to monitor if Kismet is running in the Raspberry Pi?, How to know if Raspberry Pi is healthy ?.
- Administrable remotely.
 - Definitely I can't do that in a massively distributed Raspberry Pi's.

Then, what can I do ?....

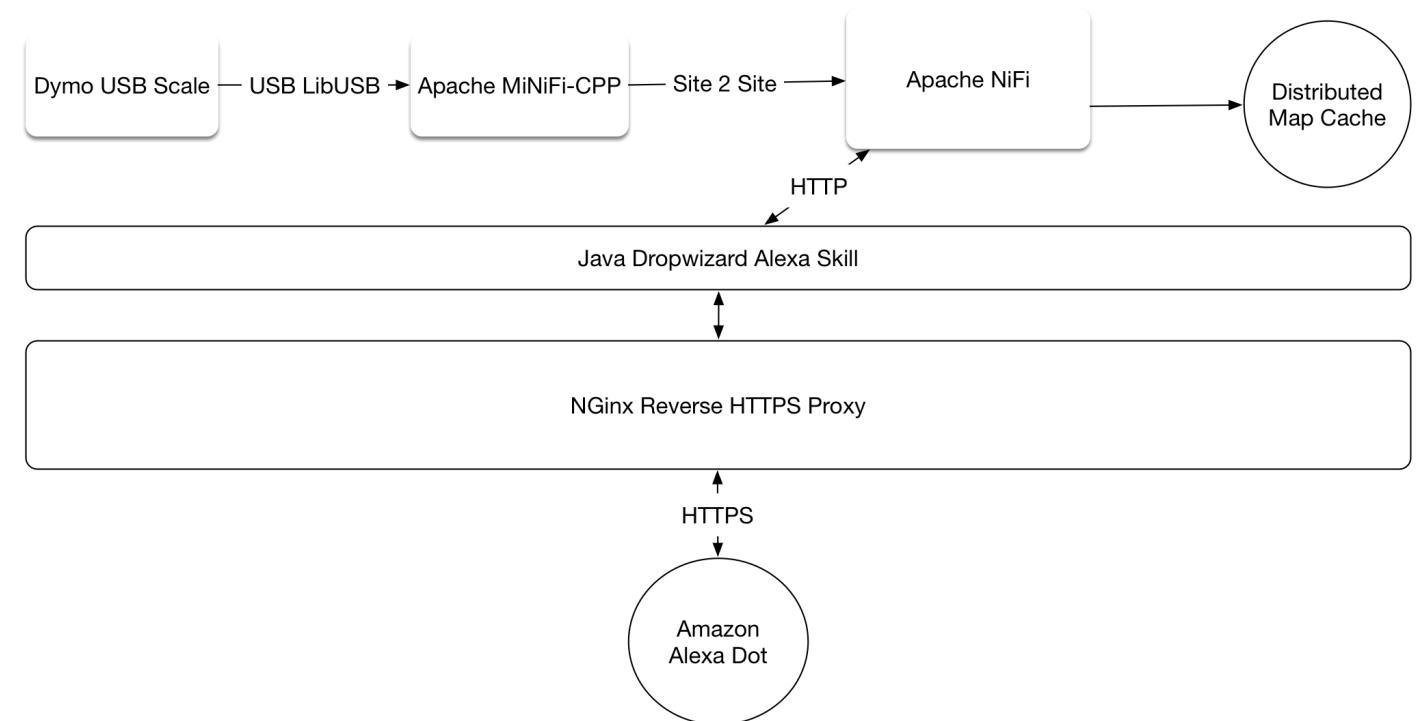
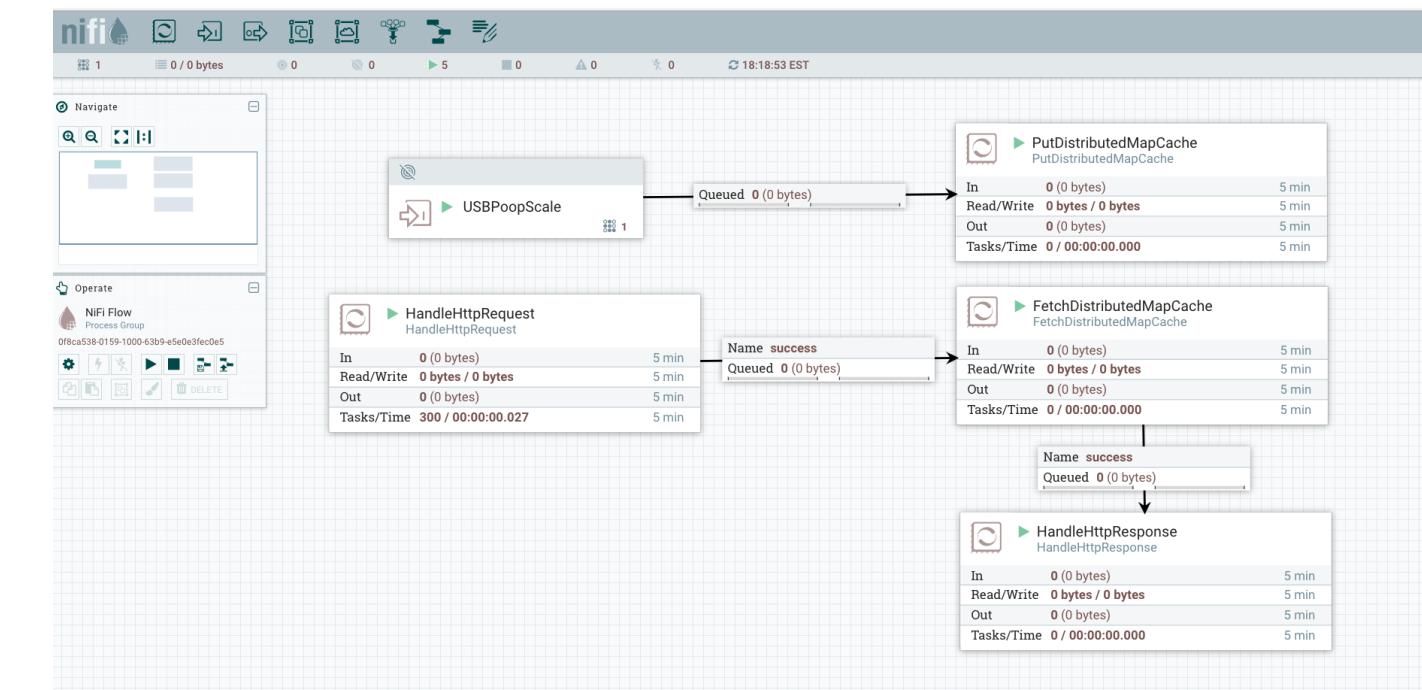
Apache NiFi to the rescue!



Community Example #2

◆ Jeremy Dyer

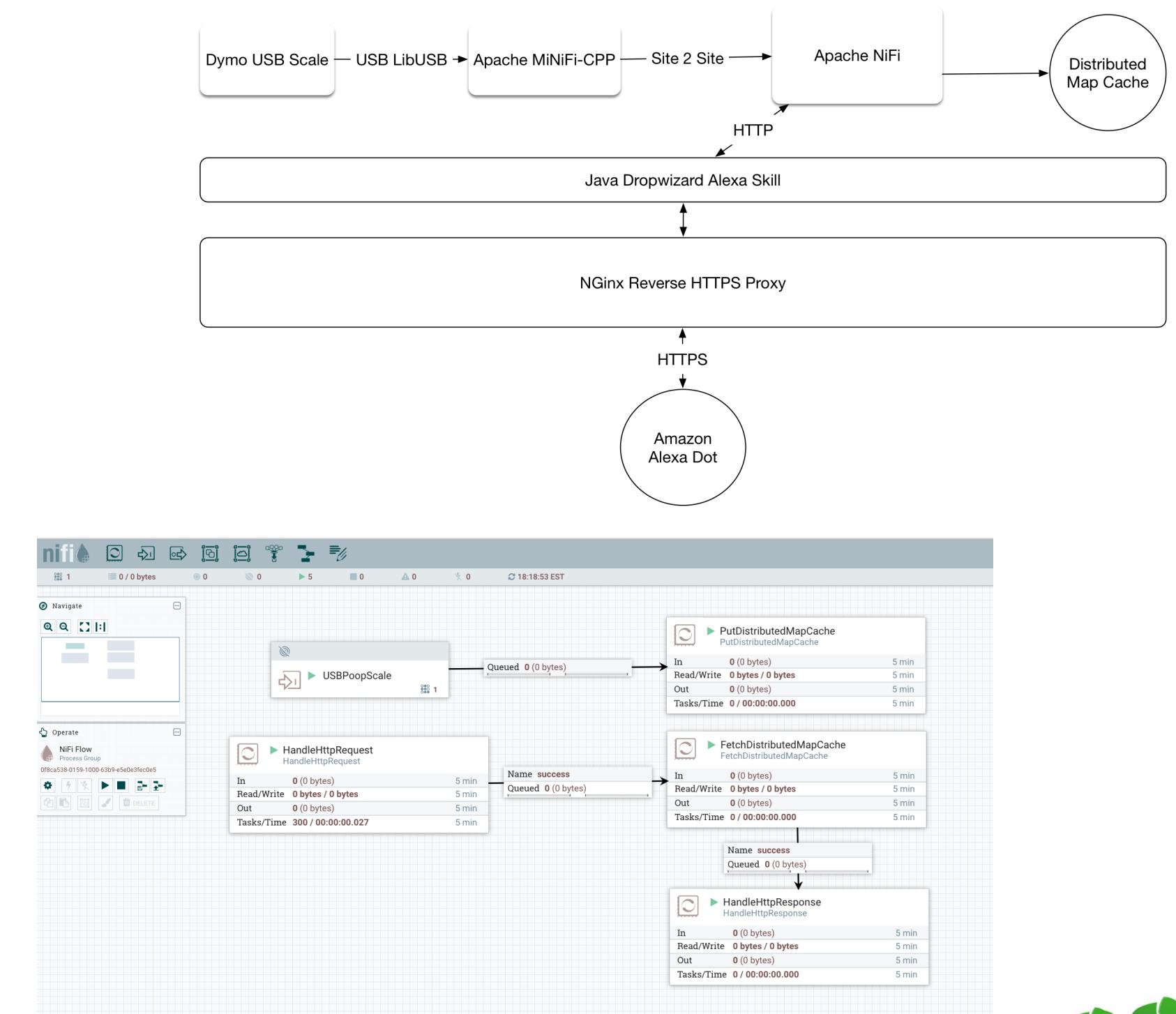
◆ Alexa + MiNiFi + Dyer 2.0



Community Example #2

◆ Jeremy Dyer

◆ Alexa + MiNiFi + Dyer 2.0



Why NiFi & MiNiFi?

- ◆ Moving data is multifaceted in its challenges and these are present in different contexts at varying scopes
 - Inter vs intra, domestically, internationally
- ◆ Provide common tooling and extensions that are needed but be flexible for extension
 - Leverage existing libraries and expansive Java ecosystem for functionality
 - Allow organizations to integrate with their existing infrastructure
- ◆ Empower folks managing your infrastructure to make changes and reason about issues that are occurring
 - Data Provenance to show context and data's journey
 - User Interface/Experience a key component

Healthy Community

apache / nifi
mirrored from <git://git.apache.org/nifi.git>

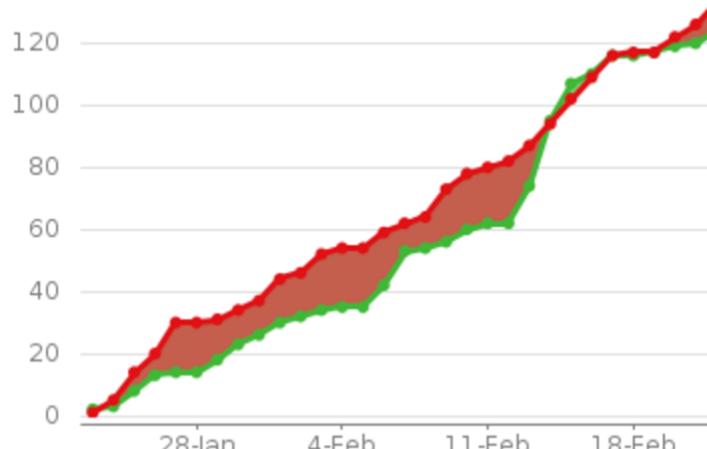
Unwatch 102 Unstar 462 Fork 431

Code Pull requests 57 Projects 0 Pulse Graphs

Mirror of Apache NiFi

3,271 commits 38 branches 44 releases 111 contributors

Issues: 30 Day Summary



Issues: 133 created and 124 resolved

Status Summary

Status	Issues	Percentage
Open	1024	29%
In Progress	19	1%
Reopened	10	1%
Resolved	2329	67%
Closed	65	2%
Patch Available	49	1%

Learn more and join us

Apache NiFi site

<https://nifi.apache.org>

Subproject MiNiFi site

<https://nifi.apache.org/minifi/>

Subscribe to and collaborate at

dev@nifi.apache.org

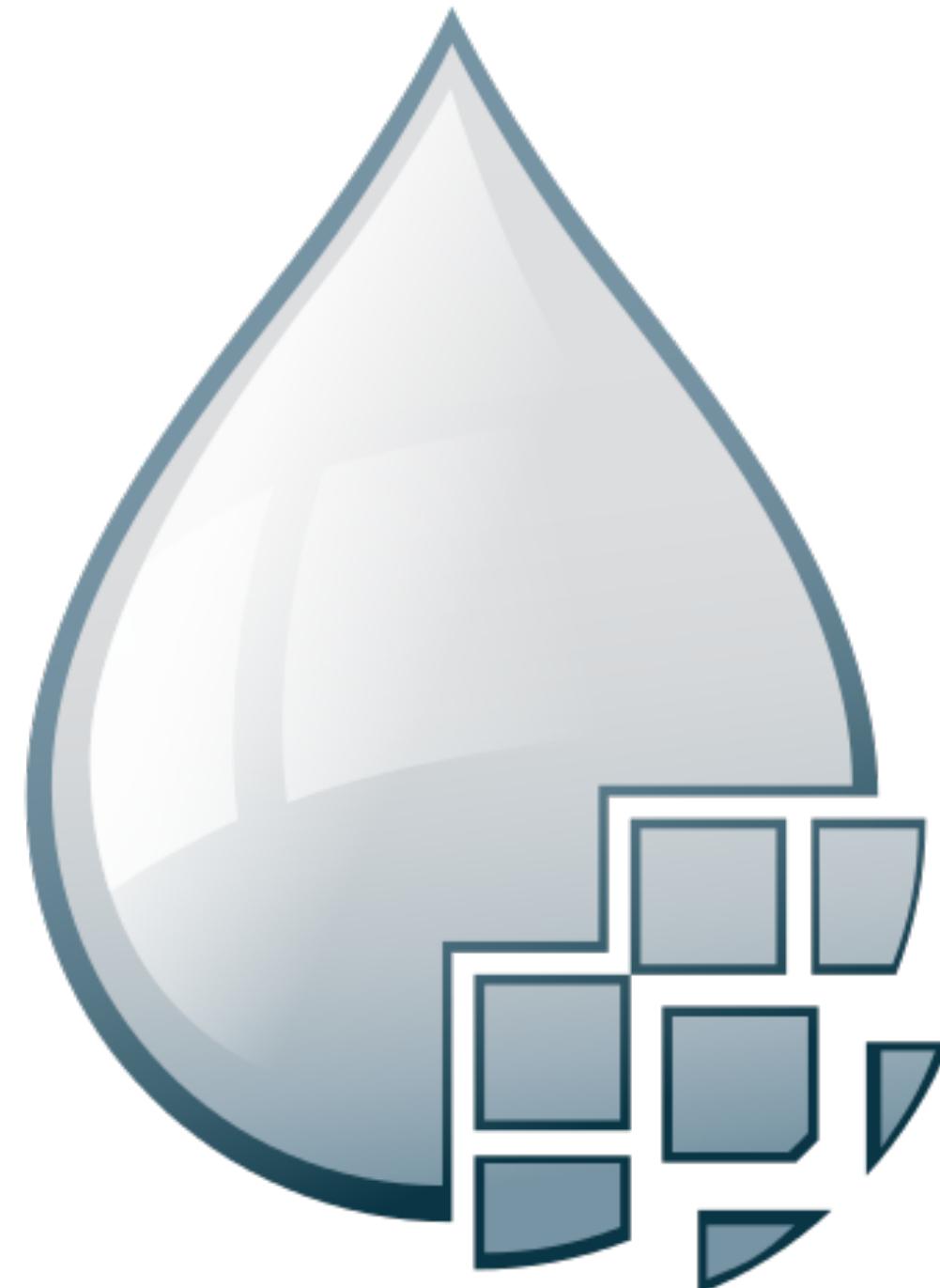
users@nifi.apache.org

Submit Ideas or Issues

<https://issues.apache.org/jira/browse/NIFI>

Follow us on Twitter

[@apachennifi](https://twitter.com/apachennifi)



Thank You

I'm sticking around for discussions/questions

 @yolopey / @apachennifi

alopresto@apache.org

PGP: 70EC B3E5 98A6 5A3F D3C4 BACE 3C6E F65B **2F7D EF69**