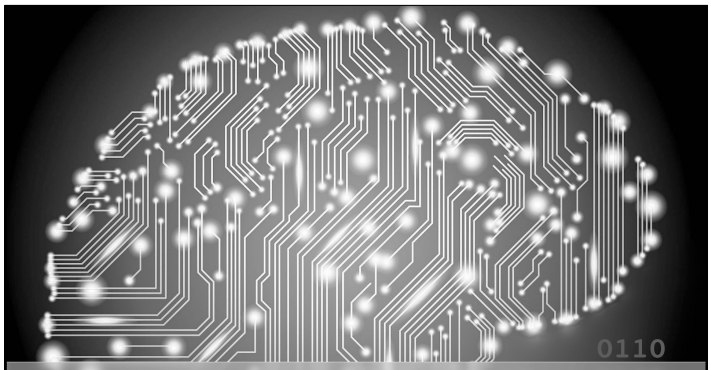


Monitoring Logs > Technobabble
Kevin Capwell – META
Pat Zielke – Viroqua

Logs > Technobabble

School District of Onalaska

- Kevin Capwell
  fmr → Data Systems Director (24 years)
- Enrollment: 3,166
- Total Staff: 415
- Buildings:
  High School, Middle School, three Elementary Schools, District Office, Pupil Service and School Nutrition (~12 sq. mi.)
- Computers: Desktop 1400, Chrome-books 1400, Other mobile 200.

Logs > Technobabble

Viroqua Area Schools

- Pat Zielke
  Technology Coordinator – 19 years
- Enrollment: 1,191
- Total Staff: 184
- Buildings:
  Shared High School/Middle School a separate Elementary all on the same campus.
- Computers: Desktop 400, Chrome-books 200, Other mobile 90.

Logs > Technobabble

Kev and Pat have a security chat…

- Security comes in layers
- Passwords – good, bad and ugly!
- Patch / vulnerability scan (Nessus)
- Penetration testing (Kali)
- Incoming / outgoing traffic (SNMP)
- Centralized tools with integrated management (Netsight, OneView)
- Monitor top user statistics
- Check / test backups / offsite
- Logs, Logs, Logs!

Logs > Technobabble

Log Monitoring

Log management tools analyze logs and discovers issues by using rules to automate the review of these logs in real time, and point out events that might represent problems or threats. The system alert you via email or text when something suspicious is detected.

Logs > Technobabble

Our first example: Scalyr

SCALYR

- Used in monitoring, alerting, forensics and log analysis
- Pricing: startup ($19/mo), silver ($99/mo), gold ($249/mo), and platinum ($499/mo)
- Built by the creator of Google Docs
- Completes nearly all queries in less than 1 second
- No complex query language
- Data is stored in the cloud

Logs > Technobabble

Scalyr agent installation

[redacted]

SCALYR AGENT

The Scalyr Agent is a daemon which you can install on each of your servers. It uploads logs and system metrics to Scalyr. This is our se
agent, designed to be easy to install and manage, with minimal dependencies and resource requirements.

The agent can run on versions of Python back to 2.4, which is present on most servers. Resource requirements vary by workload; in o
installations, the agent generally uses less than 15 MB RAM and 2% of CPU.

INSTALLATION

For standard installation instructions, go to the Agent Installation page.

[redacted]

Logs > Technobabble

Scalyr agent configuration

[redacted]

CONFIGURATION

To configure the Linux agent, edit the following file:

```
/etc/scalyr-agent-2/agent.json
```

For Windows, edit this file:

```
C:\Program Files (x86)\Scalyr\config\agent.json
```

The agent will notice the new configuration within 30 seconds. There is no need to restart the agent.

[redacted]

Logs > Technobabble

Scalyr agent configuration (pt 2)

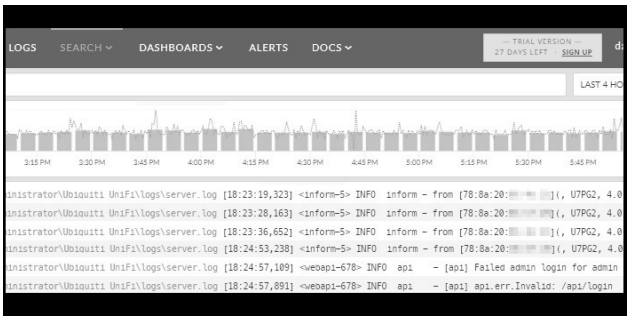
[redacted]

```
  api_key: "This is where you put key",

  // Fields describing this server. These fields are attached to each log message, and
  // can be used to filter data from a particular server or group of servers.
  server_attributes: {
     // Fill in this field if you'd like to override the server's hostname.
     // serverHost: "REPLACE THIS",

     // You can add whatever additional fields you'd like.
     // tier: "production"
  }

  // Log files to upload to Scalyr. You can use '*' wildcards here.
  logs: [
 { path: "C:\\Users\\Administrator\\Ubiquiti UniFi\\logs\\server.log", attributes:
{parser: "accessLog"} }
```

[redacted]

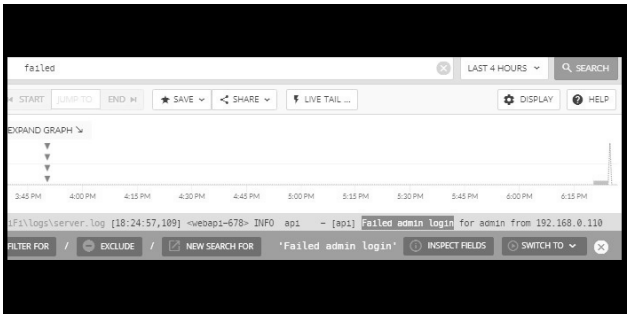
Logs > Technobabble

Presenting Scalyr data…



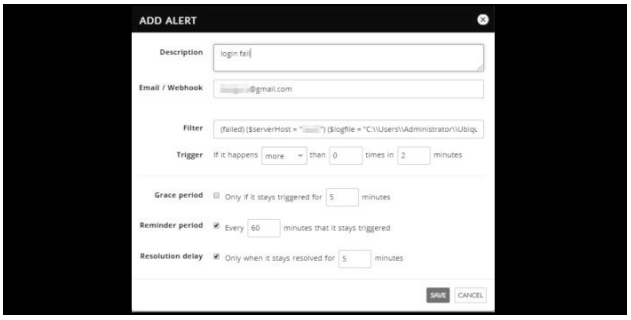
Logs > Technobabble

Searching Scalyr…



Logs > Technobabble

Creating a Scalyr alert.



Logs > Technobabble

Trigger Expression Syntax

- [Function]:[Time]([Attr where] [Filter])

- count: Matching events over time
- countPerSecond: Matching events per second
- mean: The average field value
- Functions can be combined using the following operators: + - * / < > <= >= && || !

Logs > Technobabble

Trigger Expression - Examples

- mean:1m(latency where path == '/home') > 200 && count:1m(path == '/home') >= 20

- count:1m('server error') > count:1m(success) * 0.1

- mean:5m(bytes where path == '/home') < 100

Logs > Technobabble

JSON Cloud Config File

```
alerts: [
   {
     alertAddress: "user@example.edu",
     description: "Login fail",
     trigger: "count:1 minutes(('Failed admin
login for admin') ($serverHost = \"myServ\")
($logfile = \"C:\\\\Users\\Administrator\\Ubiquiti
UniFi\\logs\\server.log\")) > 0"
```

Logs > Technobabble

JSON Cloud Config File (pt 2)

```
alertAddress: "user@example.edu",
    description: "test",
    renotifyPeriodMinutes: 60,
    resolutionDelayMinutes: 5,
    trigger: "count:2 minutes(('Failed admin
login') ($serverHost = \"myServ\") ($logfile
= \"C:\\\\Users\\\\Administrator\\\\Ubiquiti
UniFi\\\\logs\\\\server.log\")) > 0"
```


Logs > Technobabble

JSON Cloud Config File (pt 3)

```
//Scalyr Test
/*   {
    alertAddress: "jim+spock@scalyr.com",
    description: "test log",
    trigger: "count:1min(\"a\") > 0",
    gracePeriodMinutes: "",
    renotifyPeriodMinutes: "",
    resolutionDelayMinutes: ""
```


Logs > Technobabble

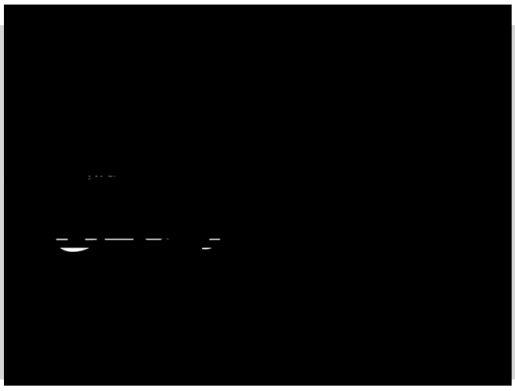
Scalyr is built around security

- All communication, uses SSL.
- Scalyr agent doesn't act as root, no external instructions, and it can redact data.
- Safe tools: Java instead of C/C++, eliminate SQL injection, avoid XSS; input sanitization.
- Scalyr API uses tokens that you can rotate or revoke at any time. The agent only allows to upload data.

Logs > Technobabble

Scalyr live demo!

Logs > Technobabble



Logs > Technobabble

Our second example: Nagios LS

Nagios® Log Server™

- Collect multiple logs in one location
- Pricing: 500 mb/day (free), one installation ($1,995), 2-instance ($4,995) for fail-over / load balance
- Log information can be "Googled"
- Alerts: email, SNMP Trap, execute custom scripts, or forward to Nagios
- Installed on: Windows, VMWare (OVA 32, 64-bit), Red Hat / CentOS
- Data is stored locally

Logs > Technobabble

Let's use Open Source

- CentOS is a community-developed and supported alternative to RHEL. It is similar to Red Hat Enterprise Linux but lacks the enterprise-level support. CentOS is more or less a free replacement for RHEL.
- CentOS 7 System requirements: Updates through June 30th, 2024 1GB/logical CPU, 10GB/20GB (storage)
- Firewall has been disabled.

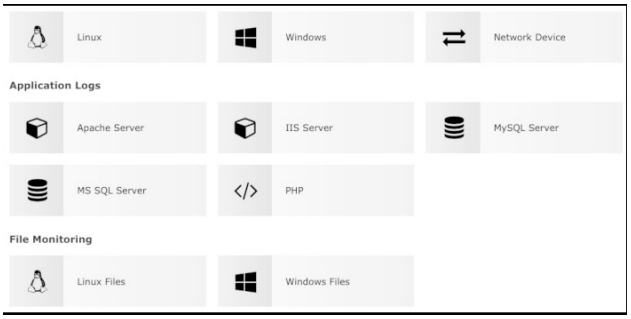
Logs > Technobabble

Installation of Nagios LS

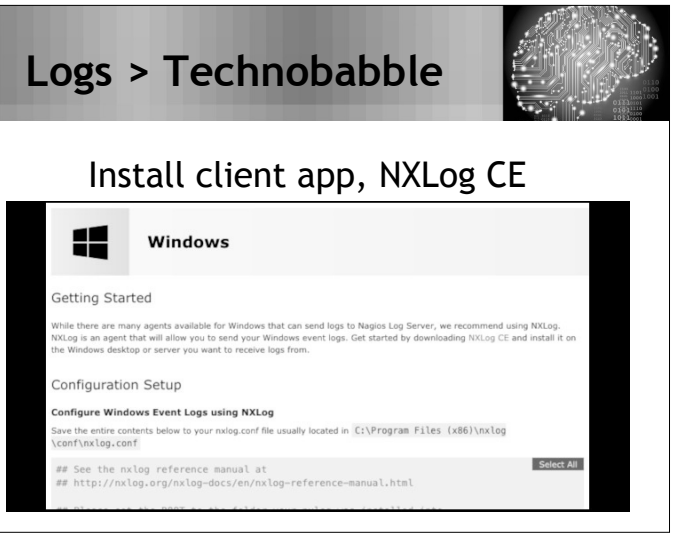
- A minimal installation of CentOS 7.
- cd /tmp
- wget https://assets.nagios.com/downloads/nagios-log-server/nagioslogserver-latest.tar.gz
- tar -zxvf nagioslogserver-latest.tar.gz
- cd nagioslogserver
- ./fullinstall
- If firewall is enabled, the installer will set the appropriate ports.

Logs > Technobabble

What can connect with Nagios LS?

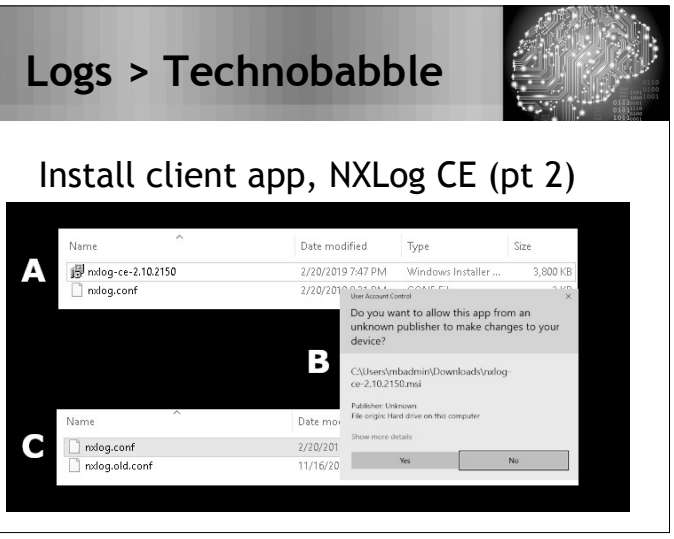


Logs > Technobabble



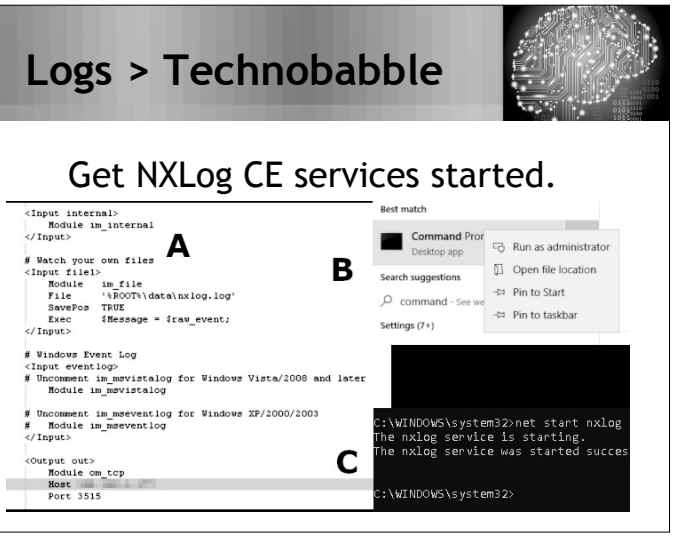
Install client app, NXLog CE

Logs > Technobabble



Install client app, NXLog CE (pt 2)

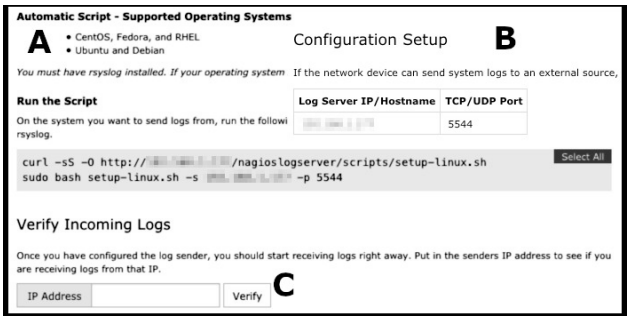
Logs > Technobabble



Get NXLog CE services started.

Logs > Technobabble

Connect all clients and verify.



Logs > Technobabble

Nagios LS Dashboard

Logs > Technobabble

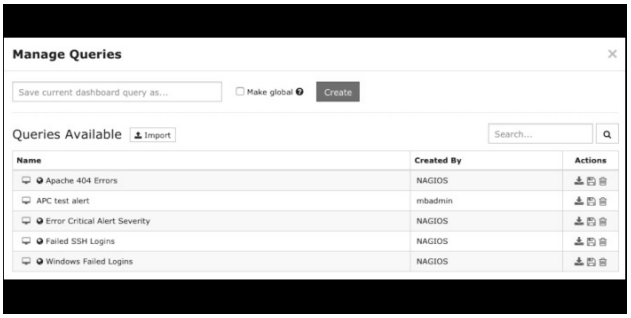
Nagios LS search window.

Logs > Technobabble

Search results, graph and details.

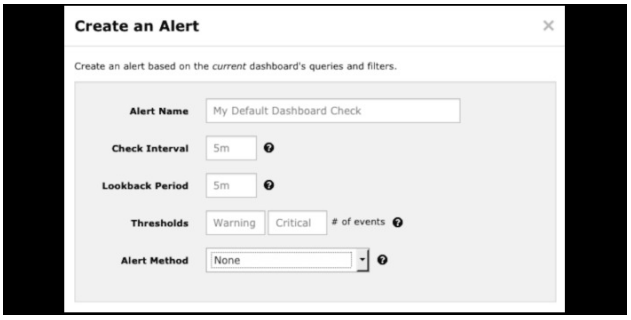
Logs > Technobabble

Nagios LS - saving your queries.



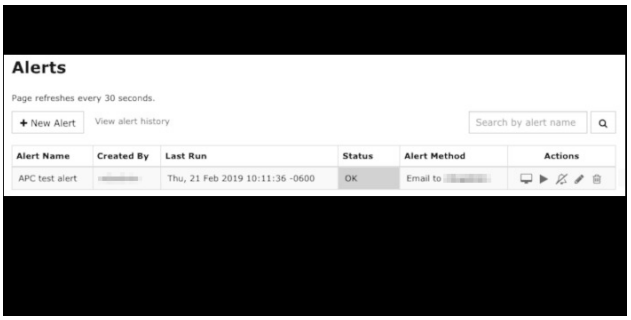
Logs > Technobabble

Nagios LS – saving an alert.



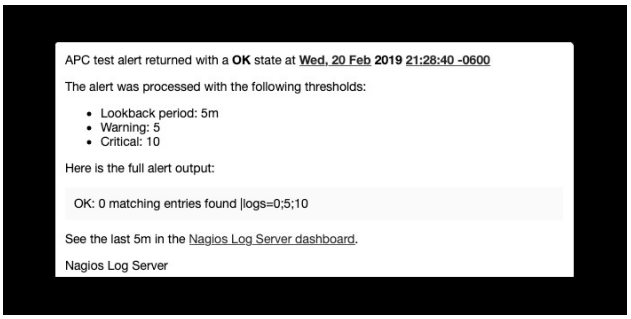
Logs > Technobabble

Nagios LS – active alert.



Logs > Technobabble

Nagios LS – alert example.



Logs > Technobabble

Questions?

Pat Zielke
Viroqua School District
pzielke@viroqua.k12.wi.us

Kevin Capwell
Midwest Educational Technology Association
kcapwell@brainstormk20.com