

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



Kevin 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 discover 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 alerts you via email or text when something suspicious is detected.

Logs > Technobabble



Our first example: 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

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 our 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](#).

Logs > Technobabble



Scalyr agent configuration

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.

Logs > Technobabble



Scalyr agent configuration (pt 2)

```
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",

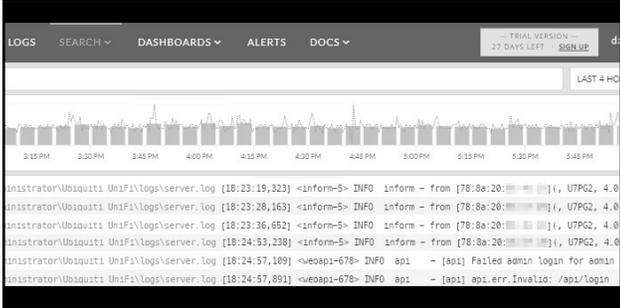
  // You can add whatever additional fields you'd like.
  // tier: "production"
}

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

Logs > Technobabble



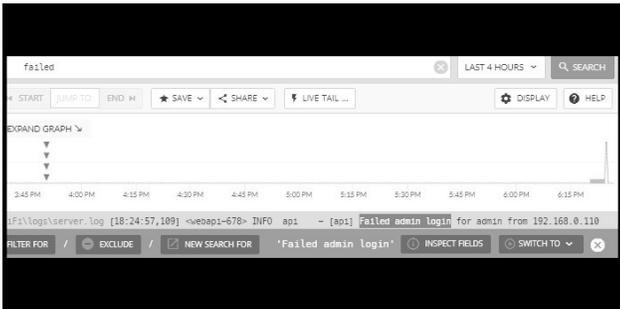
Presenting Scalyr data...



Logs > Technobabble



Searching Scalyr...



Logs > Technobabble



Creating a Scalyr alert.

The screenshot shows the 'ADD ALERT' configuration form in Scalyr. The 'Description' field contains 'login fail'. The 'Email / Webhook' field contains 'admin@gmail.com'. The 'Filter' field contains the query: '[failed] (serverhost = "mail") (logfile = "C:\Users\Administrator\Ubiloq...'. The 'Trigger' is set to 'more' than 0 times in 2 minutes. The 'Grace period' is set to 5 minutes. The 'Reminder period' is checked and set to 60 minutes. The 'Resolution delay' is checked and set to 5 minutes. 'SAVE' and 'CANCEL' buttons are at the bottom.

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.

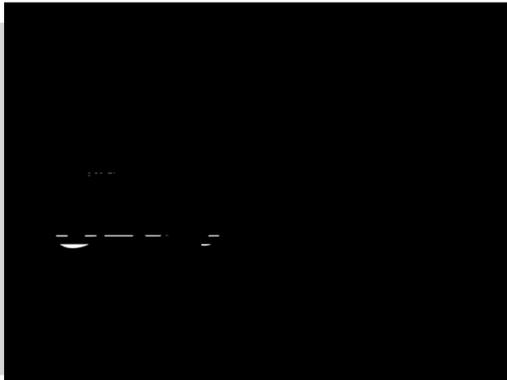
Logs > Technobabble



Scalyr live demo!

**GOING
LIVE!**

Logs > Technobabble



Logs > Technobabble



Our second example: Nagios LS



- 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?

Linux	Windows	Network Device
Application Logs		
Apache Server	IIS Server	MySQL Server
MS SQL Server	PHP	
File Monitoring		
Linux Files	Windows Files	

Logs > Technobabble



Install client app, NXLog CE

Windows

Getting Started

While there are many agents available for Windows that can send logs to Nagios Log Server, we recommend using NXLog. NXLog is an agent that will allow you to send your Windows event logs. Get started by downloading NXLog CE and install it on the Windows desktop or server you want to receive logs from.

Configuration Setup

Configure Windows Event Logs using NXLog

Save the entire contents below to your nxlog.conf file usually located in C:\Program Files (x86)\nxlog\conf\nxlog.conf.

```
## See the nxlog reference manual at
## http://nxlog.org/nxlog-docs/en/nxlog-reference-manual.html
```

Select All

Logs > Technobabble



Install client app, NXLog CE (pt 2)

A

Name	Date modified	Type	Size
nxlog-ce-2.10.2150	2/20/2019 7:47 PM	Windows Installer ...	3,800 KB
nxlog.conf	2/20/2019 10:03 AM	User Account Control	3,410 B

B

Do you want to allow this app from an unknown publisher to make changes to your device?

C:\Users\mbadmin\Downloads\nxlog-ce-2.10.2150.msi

Publisher: Unknown
File origin: Hard drive on this computer

Show more details

Yes No

C

Name	Date modified
nxlog.conf	2/20/2019
nxlog.old.conf	11/16/2018

Logs > Technobabble



Get NXLog CE services started.

```
<input internal>
  Module im_internal
</input>
# Watch your own files
<input file!>
  Module im_file
  File 'C:\ROOT\data\nxlog.log'
  SavePos TRUE
  Exec $Message = $raw_event;
</input>
# Windows Event Log
<input eventlog!>
# Uncomment im_msvistalog for Windows Vista/2008 and later
  Module im_msvistalog
# Uncomment im_mseventlog for Windows XP/2000/2003
  Module im_mseventlog
</input>
<output out!>
  Module om_tcp
  Host '192.168.1.100'
  Port 3515
```

A

B

Best match

- Command Prompt (Desktop app) [Run as administrator]
- Search suggestions [Open file location]
- command - See we... [Pin to Start]
- Settings (+) [Pin to taskbar]

C

```
C:\WINDOWS\system32>net start nxlog
The nxlog service is starting.
The nxlog service was started succes
```

```
C:\WINDOWS\system32>
```

Logs > Technobabble



Connect all clients and verify.

Automatic Script - Supported Operating Systems

- CentOS, Fedora, and RHEL
- Ubuntu and Debian

Configuration Setup

You must have rsyslog installed. If your operating system If the network device can send system logs to an external source,

Run the Script

On the system you want to send logs from, run the following rsyslog.

Log Server IP/Hostname	TCP/UDP Port
<input type="text"/>	5544

```
curl -sS -O http://[redacted]/nagioslogserver/scripts/setup-linux.sh  
sudo bash setup-linux.sh -s [redacted] -p 5544
```

Verify Incoming Logs

Once you have configured the log sender, you should start receiving logs right away. Put in the senders IP address to see if you are receiving logs from that IP.

IP Address <input type="text"/>	Verify
---------------------------------	--------

Logs > Technobabble



Nagios LS Dashboard

A 4
Unique Hosts Report

1
Alert Manage

1
Unique Hosts

Showing logs received from hosts in the last 24 hours.
Amount of hosts: 4



IP Address (Hostname)	Log Count
[redacted]	38,158
[redacted]	2,887
[redacted]	995
[redacted]	1

Not Sending

This is a list of hosts that Log Server has received logs from in Last sending check was Thu, 21 Feb 2019 10:00:01 -0600.

IP Address (Hostname)	Last Sending Check
[redacted]	Wed, 20 Feb 2019 21:00:02 -0600

Logs > Technobabble



Nagios LS search window.

The screenshot shows the Nagios LS search interface. At the top, there are navigation tabs: Home, Dashboard, Alerting, Configuration, Help, Admin. Below that, there are search filters for 'Hosts' and 'Log Count'. A dropdown menu is open, showing time range options: Last 5m, Last 15m, Last 1h, Last 2h, Last 6h, Last 12h, Last 24h, Last 7d, Last 7d, Last 30d, Auto-Refresh, and Custom.

Logs > Technobabble



Search results, graph and details.

The screenshot displays the Nagios LS interface. At the top, there is a bar chart titled 'EVENTS OVER TIME' showing event frequency over a period. Below the chart is a table of 'ALL EVENTS' with columns for '@timestamp', 'host', 'type', and 'message'. A search filter is applied to the 'message' column, showing results for '6.399971] cli', '6.399959] cli', and '6.370034] cli'. An 'Actions' menu is visible on the right side of the table.

Logs > Technobabble



Nagios LS - saving your queries.

The screenshot shows the 'Manage Queries' dialog box in Nagios LS. It includes a text input field for 'Save current dashboard query as...', a 'Make global' checkbox, and a 'Create' button. Below this is a table of 'Queries Available' with columns for 'Name', 'Created By', and 'Actions'. The table lists several queries such as 'Apache 404 Errors', 'APC test alert', 'Error Critical Alert Seventy', 'Failed SSH Logins', and 'Windows Failed Logins'.

Logs > Technobabble



Nagios LS - saving an alert.

The screenshot displays the 'Create an Alert' dialog box. It contains several configuration fields: 'Alert Name' (My Default Dashboard Check), 'Check Interval' (5m), 'Lookback Period' (5m), 'Thresholds' (Warning, Critical, # of events), and 'Alert Method' (None). Each field has a help icon to its right.

Logs > Technobabble



Nagios LS - active alert.

Alerts

Page refreshes every 30 seconds.

[+ New Alert](#) [View alert history](#)

Alert Name	Created By	Last Run	Status	Alert Method	Actions
APC test alert		Thu, 21 Feb 2019 10:11:36 -0600	OK	Email to [redacted]	

Logs > Technobabble



Nagios LS - alert example.

APC test alert returned with a **OK** state at **Wed, 20 Feb 2019 21:28:40 -0600**

The alert was processed with the following thresholds:

- Lookback period: 5m
- Warning: 5
- Critical: 10

Here is the full alert output:

```
OK: 0 matching entries found |logs=0;5;10
```

See the last 5m in the [Nagios Log Server dashboard](#).

Nagios Log Server

Logs > Technobabble



Questions?



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

Kevin Capwell
Midwest Educational Technology Association
kcapwell@brainstormk20.com
