



Anatoly Kulakov

Structured Logging



Why logging?

- **Troubleshooting & Remediation**
- Where did the problem occur?
- **Performance & Cost**
- How my changes impact overall performance?
- **Learning & Improvement**
- Can I detect or prevent this problem in the future?
- **Trends**
- Do I need to scale?
- **Customer Experience**
- Are my customers getting a good experience?

U731A
8CTB
8HDI
KM8A
H8MA
3E1A8
E1E8
H8X
E8K8
E1E3E

C:\Documents and Settings\myak\My Documents\UBCD4\WIN\...
Path = C:\Documents and Settings\myak\My Documents\UBCD4\WIN\...

RegistryPermissions: entered
RegistryPermissions: exiting
OutputPath: entered
ing old output directory: C:\Documents and Settings\myak\My Documents\UBCD4\WIN\...
OutputPath: entered
wanted dir is C:\Documents and Settings\myak\My Documents\UBCD4\WIN\...
ing unwanted dir to C:\Documents and Settings\myak\Local Settings\Temp\...
ing worker thread.
OutputPath: exiting
ing new output directory: C:\Documents and Settings\myak\My Documents\UBCD4\WIN\...

OutputPath: entered
OutputPath: exiting
Delete: entered
systemRegFile: entered
systemRegFile: exiting
empDir: entered
empDir: entered
wanted dir is C:\Documents and Settings\myak\Local Settings\Temp\...
ing unwanted dir to C:\Documents and Settings\myak\Local Settings\Temp\...

Log Viewer

File Edit Help

Logger Tree

Refine focus on:

ID	Timestamp	Level
1036	2003-12-17 02:33:20,868	ERROR
1037	2003-12-17 02:33:20,868	ERROR
1038	2003-12-17 02:33:20,868	ERROR
1039	2003-12-17 02:33:20,868	ERROR
1040	2003-12-17 02:33:20,868	ERROR
1041	2003-12-17 02:33:20,868	ERROR
1042	2003-12-17 02:33:20,868	ERROR
1043	2003-12-17 02:33:20,868	ERROR
1044	2003-12-17 02:33:20,868	ERROR

Log Viewer

File Edit Help

Logger Tree

Refine focus on:

ID	Timestamp	Level
1036	2003-12-17 02:33:20,868	ERROR
1037	2003-12-17 02:33:20,868	ERROR
1038	2003-12-17 02:33:20,868	ERROR
1039	2003-12-17 02:33:20,868	ERROR
1040	2003-12-17 02:33:20,868	ERROR
1041	2003-12-17 02:33:20,868	ERROR
1042	2003-12-17 02:33:20,868	ERROR
1043	2003-12-17 02:33:20,868	ERROR
1044	2003-12-17 02:33:20,868	ERROR

830 Rows

Ship	Label	Value
NULL		
anero	RJ	
NULL		

Time Stamp

Level	Thread	Message
ERROR	4656	at System.Web.S...
COMPRESSION	5292	Loading Master Tic...
WARN	5292	Loading FeeTickets...
WARN	4656	Loading FeeTickets...

ERROR

Time Stamp	Machine Name	User Name
8/22/2008 3:10:43 PM	wyny	UBS

CAIT.Log Method Error Line 43

C:\Case\CAIT-Branch-2.3.0.0\STM_FL_RISK\Struct_Cred\scs\CAIT\CAITLog.cs

WebException: The request failed with HTTP status 503: Service Unavailable.
Web.Services.Protocols.SoaHttpProtocol.ReadResponse(SoapResponse response, Stream responseStream, Boolean asyncCall)

Log Viewer

File Edit Help

Logger Tree

Refine focus on:

ID	Timestamp	Level
1036	2003-12-17 02:33:20,868	ERROR
1037	2003-12-17 02:33:20,868	ERROR
1038	2003-12-17 02:33:20,868	ERROR
1039	2003-12-17 02:33:20,868	ERROR
1040	2003-12-17 02:33:20,868	ERROR
1041	2003-12-17 02:33:20,868	ERROR
1042	2003-12-17 02:33:20,868	ERROR
1043	2003-12-17 02:33:20,868	ERROR
1044	2003-12-17 02:33:20,868	ERROR

Log Viewer

File Edit Help

Logger Tree

Refine focus on:

ID	Timestamp	Level
1036	2003-12-17 02:33:20,868	ERROR
1037	2003-12-17 02:33:20,868	ERROR
1038	2003-12-17 02:33:20,868	ERROR
1039	2003-12-17 02:33:20,868	ERROR
1040	2003-12-17 02:33:20,868	ERROR
1041	2003-12-17 02:33:20,868	ERROR
1042	2003-12-17 02:33:20,868	ERROR
1043	2003-12-17 02:33:20,868	ERROR
1044	2003-12-17 02:33:20,868	ERROR

Gamut Log Viewer - Aube.log | File Size: OMB | 2011-05-15 18:25:17.7624 - 2011-05-15 18:26:29.8004

Date	Time	Delta	Process Id	Thread Id	Message
5/15/2011	6:25:17 PM	762	7860	8	Logger loaded!
5/15/2011	6:25:39 PM	81	21319	8	Open file: C:\Steve\LogViewer\LogViewer\bin\Release\DummyManager.dll
5/15/2011	6:25:39 PM	401	320	7860	MDI child load!
5/15/2011	6:25:39 PM	536	135	7860	Form Load
5/15/2011	6:25:39 PM	543	7	7860	Activated
5/15/2011	6:25:39 PM	764	221	7860	Opening log file: C:\Steve\LogViewer\LogViewer\bin\Release\DummyManager.dll
5/15/2011	6:25:39 PM	773	9	7860	Apply log file change: GamutLogViewer\LogViewer\bin\Release\DummyManager.dll
5/15/2011	6:25:39 PM	789	16	7860	LogFile created

Log Viewer

File Edit Help

Logger Tree

Refine focus on:

ID	Timestamp	Level
1036	2003-12-17 02:33:20,868	ERROR
1037	2003-12-17 02:33:20,868	ERROR
1038	2003-12-17 02:33:20,868	ERROR
1039	2003-12-17 02:33:20,868	ERROR
1040	2003-12-17 02:33:20,868	ERROR
1041	2003-12-17 02:33:20,868	ERROR
1042	2003-12-17 02:33:20,868	ERROR
1043	2003-12-17 02:33:20,868	ERROR
1044	2003-12-17 02:33:20,868	ERROR

Log Viewer

File Edit Help

Logger Tree

Refine focus on:

ID	Timestamp	Level
1036	2003-12-17 02:33:20,868	ERROR
1037	2003-12-17 02:33:20,868	ERROR
1038	2003-12-17 02:33:20,868	ERROR
1039	2003-12-17 02:33:20,868	ERROR
1040	2003-12-17 02:33:20,868	ERROR
1041	2003-12-17 02:33:20,868	ERROR
1042	2003-12-17 02:33:20,868	ERROR
1043	2003-12-17 02:33:20,868	ERROR
1044	2003-12-17 02:33:20,868	ERROR

Log Viewer

File Edit Help

Logger Tree

Refine focus on:

ID	Timestamp	Level
1036	2003-12-17 02:33:20,868	ERROR
1037	2003-12-17 02:33:20,868	ERROR
1038	2003-12-17 02:33:20,868	ERROR
1039	2003-12-17 02:33:20,868	ERROR
1040	2003-12-17 02:33:20,868	ERROR
1041	2003-12-17 02:33:20,868	ERROR
1042	2003-12-17 02:33:20,868	ERROR
1043	2003-12-17 02:33:20,868	ERROR
1044	2003-12-17 02:33:20,868	ERROR

Log Viewer

File Edit Help

Logger Tree

Refine focus on:

ID	Timestamp	Level
1036	2003-12-17 02:33:20,868	ERROR
1037	2003-12-17 02:33:20,868	ERROR
1038	2003-12-17 02:33:20,868	ERROR
1039	2003-12-17 02:33:20,868	ERROR
1040	2003-12-17 02:33:20,868	ERROR
1041	2003-12-17 02:33:20,868	ERROR
1042	2003-12-17 02:33:20,868	ERROR
1043	2003-12-17 02:33:20,868	ERROR
1044	2003-12-17 02:33:20,868	ERROR

UBCD4WIN-Log-bkp.txt - TracerX Log Viewer

File Edit View Help

Session	Line #	Level	Logger	Th#	ThName
1	3,724	Info	BuildProgressControl	1	Main
1	3,725	Info	BuildProgressControl	1	Main
1	3,726	Info	BuildProgressControl	2	Worker
1	3,727	Info	BuildProgressControl	2	Worker
1	3,728	Info	BuildProgressControl	2	Worker
1	3,728.1	Info	BuildProgressControl	2	Worker
1	3,728.2	Info	BuildProgressControl	2	Worker
1	3,728.3	Info	BuildProgressControl	2	Worker
1	3,728.4	Info	BuildProgressControl	2	Worker
1	3,728.5	Info	BuildProgressControl	2	Worker
1	3,728.6	Info	BuildProgressControl	2	Worker
1	3,728.7	Info	BuildProgressControl	2	Worker
1	3,729	Info	Registry	2	Worker
1	3,730	Info	Registry	2	Worker
1	3,731	Info	BuildProgressControl	2	Worker
1	3,732	Info	BuildProgressControl	2	Worker

Log Viewer

File Edit Help

Logger Tree

Refine focus on:

ID	Timestamp	Level
1036	2003-12-17 02:33:20,868	ERROR
1037	2003-12-17 02:33:20,868	ERROR
1038	2003-12-17 02:33:20,868	ERROR
1039	2003-12-17 02:33:20,868	ERROR
1040	2003-12-17 02:33:20,868	ERROR
1041	2003-12-17 02:33:20,868	ERROR
1042	2003-12-17 02:33:20,868	ERROR
1043	2003-12-17 02:33:20,868	ERROR
1044	2003-12-17 02:33:20,868	ERROR

Log Viewer

File Edit Help

Logger Tree

Refine focus on:

ID	Timestamp	Level
1036	2003-12-17 02:33:20,868	ERROR
1037	2003-12-17 02:33:20,868	ERROR
1038	2003-12-17 02:33:20,868	ERROR
1039	2003-12-17 02:33:20,868	ERROR
1040	2003-12-17 02:33:20,868	ERROR
1041	2003-12-17 02:33:20,868	ERROR
1042	2003-12-17 02:33:20,868	ERROR
1043	2003-12-17 02:33:20,868	ERROR
1044	2003-12-17 02:33:20,868	ERROR

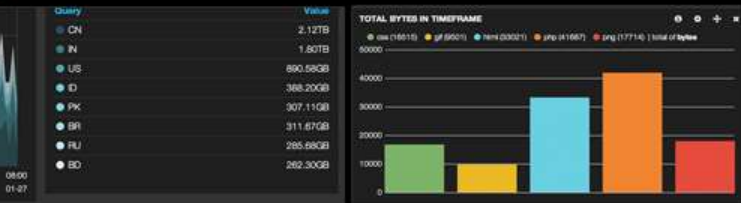
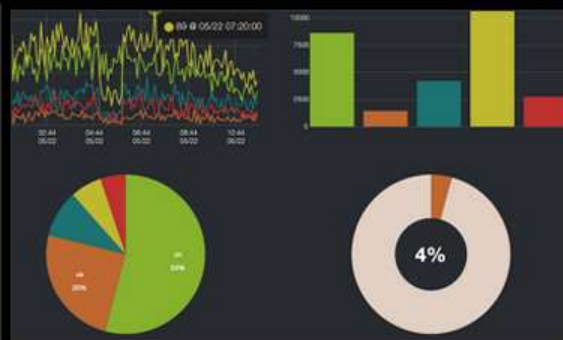
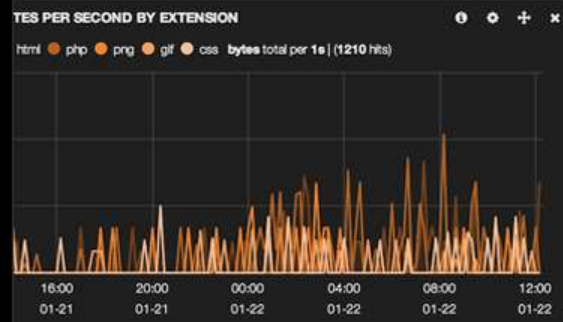
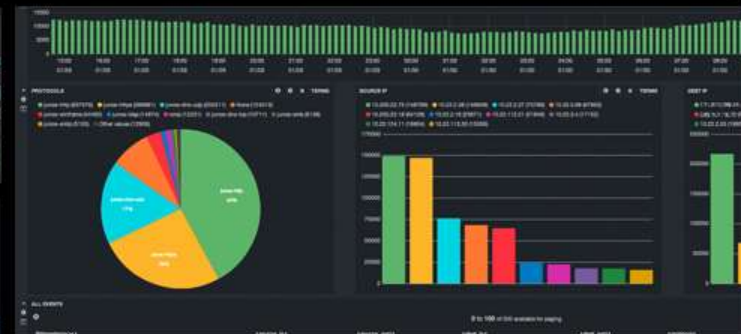
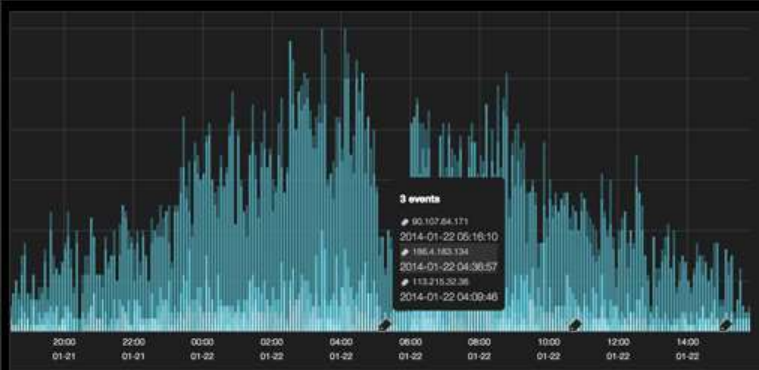


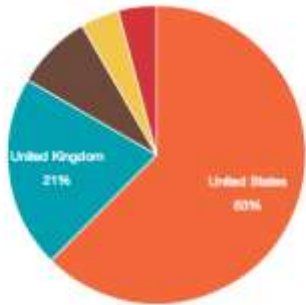
ELASTIC
SEARCH



logstash

kibana

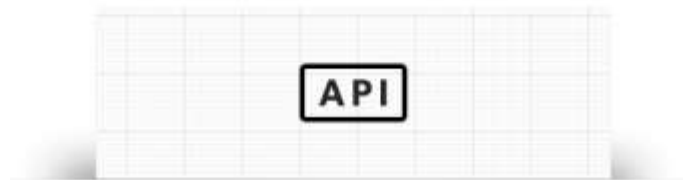




Real-Time
Advanced Analytics



High Availability



Developer-Friendly,
RESTful API



Schema-Free



Full-Text Search



Build on top of
Apache Lucene

Inputs

- File
- TCP
- UDP
- HTTP
- WebSocket
- Syslog
- IRC
- IMAP

Filters

- Grok
- GeoIP
- Filetr
- Tags
- DNS
- Aggregate
- JSON
- XML

Outputs

- Elasticsearch
- Graphite
- Nagios
- Riemann
- DataDog
- Redis
- Riak
- MongoDB



ELASTIC
SEARCH



logstash

kibana

S3_ACCESS_LOG %{WORD:owner} %{NOTSPACE:bucket} [%{HTTPDATE:timestamp}] %{IP:clientip}
%{NOTSPACE:requester} %{NOTSPACE:request_id} %{NOTSPACE:operation} %{NOTSPACE:key}
(?:"%{S3_REQUEST_LINE}"|-) (?:%{INT:response:int}|-) (?:-|%{NOTSPACE:error_code}) (?:%{INT:bytes:int}|-)
(?:%{INT:object_size:int}|-) (?:%{INT:request_time_ms:int}|-) (?:%{INT:turnaround_time_ms:int}|-) (?:%{QS:referrer}|-)
(?:"%{QS:agent}"?|-) (?:-|%{NOTSPACE:version_id}) ELB_URIPATHPARAM
%{URIPATH:path}(?:%{URIPARAM:params})?

ELB_URI %{URIPROTO:proto}://(?:%{USER}(?:[:^@]*)?@)?(?:%{URIHOST:urihost})?(?:%{ELB_URIPATHPARAM})?

ELB_REQUEST_LINE (?:%{WORD:verb} %{ELB_URI:request}(?:
HTTP/%{NUMBER:httpversion})?|%{DATA:rawrequest})

ELB_ACCESS_LOG %{TIMESTAMP_ISO8601:timestamp} %{NOTSPACE:elb} %{IP:clientip}:%{INT:clientport:int}
(?:(%{IP:backendip}:%{INT:backendport:int})|-) %{NUMBER:request_processing_time:float}
%{NUMBER:backend_processing_time:float} %{NUMBER:response_processing_time:float} %{INT:response:int}
%{INT:backend_response:int} %{INT:received_bytes:int} %{INT:bytes:int} "%{ELB_REQUEST_LINE}

CISCOFW106001 %{CISCO_DIRECTION:direction} %{WORD:protocol} connection %{CISCO_ACTION:action} from
%{IP:src_ip}/%{INT:src_port} to %{IP:dst_ip}/%{INT:dst_port} flags %{GREEDYDATA:tcp_flags} on interface
%{GREEDYDATA:interface}

CISCOFW106006_106007_106010 %{CISCO_ACTION:action} %{CISCO_DIRECTION:direction} %{WORD:protocol}
(?:from|src) %{IP:src_ip}/%{INT:src_port}(\(%{DATA:src_fwuser}\))?(?:to|dst)
%{IP:dst_ip}/%{INT:dst_port}(\(%{DATA:dst_fwuser}\))?(?:on interface %{DATA:interface})|due to
%{CISCO_REASON:reason})

```
class LoggedInEvent
{
    string    Name
    IPAddress Address
    string[]  Roles
}
```

A
P
P

```
String.Format(
    "User {0} logged in
    from {1}
    with {2} roles", ... )
```

L
o
g

User Guest logged in from 127.0.0.1 with [Admin, God] roles

```
{
    string    Name
    string    Address
    string[]  Roles
}
```

E
S

Logstash



WHAT IF I TOLD YOU



THAT THERE'S A BETTER WAY TO LOG

Event Viewer

File Action View Help

Event Viewer (Local)

- Custom Views
- Windows Logs
 - Application
 - Security
 - Setup
 - System
 - Forwarded Events
- Applications and Services Logs
- Subscriptions

Security Number of events: 70 881 (!) New events available

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	14.11.2015 16:20:03	Microsoft Windows sec...	4648	Logon
Audit Failure	14.11.2015 16:15:12	Microsoft Windows sec...	4656	File System
Audit Success	14.11.2015 16:15:11	Microsoft Windows sec...	4611	Security System Extensi...
Audit Failure	14.11.2015 16:15:11	Microsoft Windows sec...	4656	File System
Audit Success	14.11.2015 16:15:11	Microsoft Windows sec...	4611	Security System Extensi...
Audit Failure	14.11.2015 15:51:24	Microsoft Windows sec...	4673	Sensitive Privilege Use
Audit Success	14.11.2015 15:50:02	Microsoft Windows sec...	4648	Logon
Audit Success	14.11.2015 15:43:38	Microsoft Windows sec...	4648	Logon

Actions

- Security
- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Clear Log...
- Filter Current Log...
- Properties

Event Properties - Event 4648, Microsoft Windows security auditing.

General Details

☐ Friendly View ☒ XML View

```

<Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords>
<TimeCreated SystemTime="2015-11-14T11:49:59.597538800Z" />
<EventRecordID>1865084</EventRecordID>
<Correlation />
<Execution ProcessID="912" ThreadID="55236" />
<Channel>Security</Channel>
<Computer>AKulak.paladyne.com</Computer>
<Security />
</System>
- <EventData>
  <Data Name="SubjectUserSid">S-1-5-21-3474699846-2331608753</Data>
  <Data Name="SubjectUserName">AKulakov</Data>
  <Data Name="SubjectDomainName">P</Data>
  <Data Name="SubjectLogonId">0x550b5</Data>
  <Data Name="LogonGuid">{00000000-0000-0000-0000-000000000000}</Data>
  <Data Name="TargetUserName">kulakov</Data>
  <Data Name="TargetDomainName">b</Data>
  <Data Name="TargetLogonGuid">{00000000-0000-0000-0000-000000000000}</Data>
  <Data Name="TargetServerName">X.com</Data>
  <Data Name="TargetInfo">X.com</Data>
  <Data Name="ProcessId">0xd5c</Data>
  <Data Name="ProcessName">C:\Program Files\Microsoft Office\Office15\OUTLOOK.EXE</Data>
  <Data Name="IpAddress"></Data>
  <Data Name="IpPort"></Data>
</EventData>
  
```

Copy Close

Structure log

- Windows Event Log
- Event Tracing for Windows (ETW)
- Semantic Logging Application Block (SLAB)
- Microsoft.Framework.Logging (ASP.NET)
- Splunk, Graylog2

name=Guest, address=127.0.0.1, role=Admin

Serilog

Serilog is built with
powerful structured
event data in mind



```
String.Format(
    "User {0} logged in from {1} with {2} roles",
    Name, Address, Roles)
```



S
e
r
i
l
o
g

```
Log.Information(
    "User {UserName} logged in
    from {RemoteAddress}
    with {SecurityRoles} roles",
    Name, Address, Roles)
```

E
v
e
n
t

```
{
    EventType = UserLoggedIn
    UserName = "Guest"
    RemoteAddress = "127.0.0.1"
    SecurityRoles = ["Admin", ...]
}
```


Structured Data

- Simple, Scalar Values
- Collections
- Dictionaries
- Objects
- String format specifier
- Stringification and Destructuring

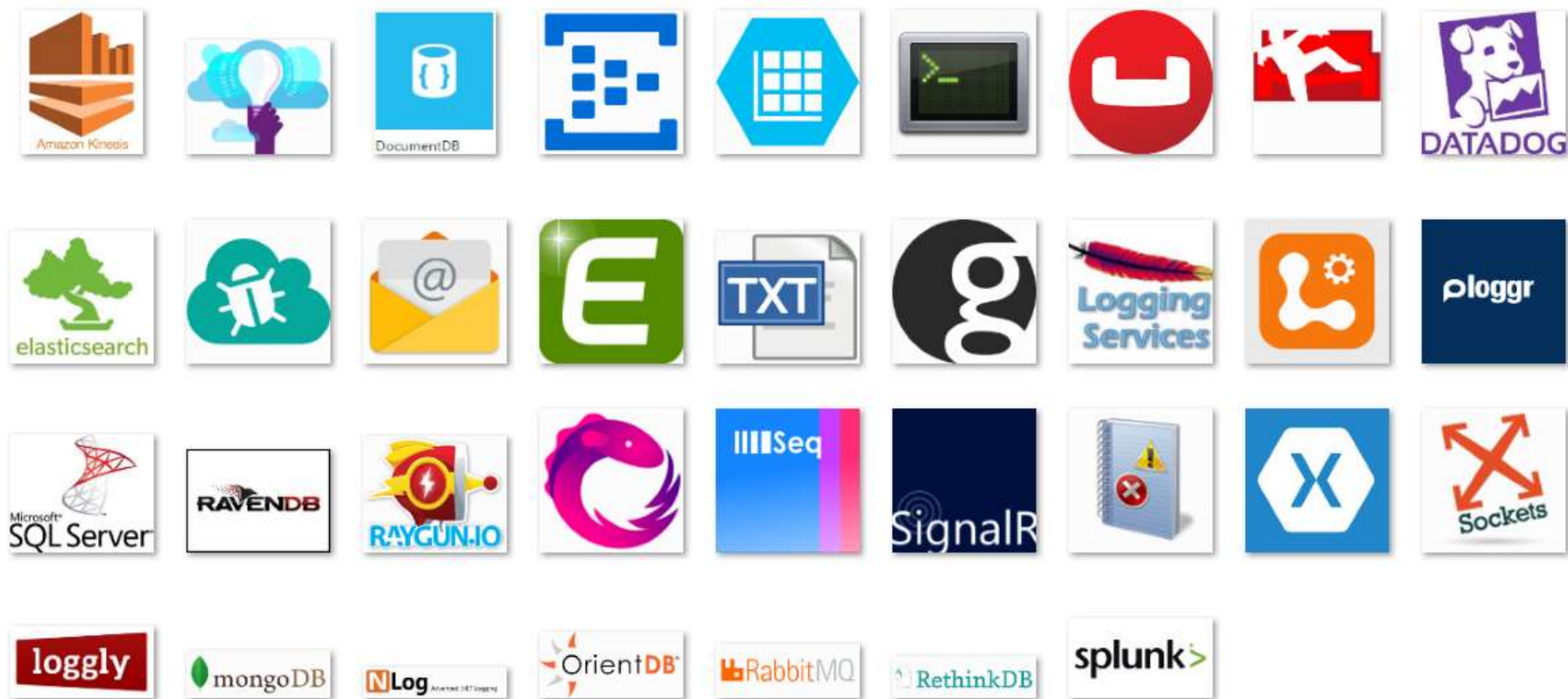
Enrichment

- MachineName
- UserName
- ProcessId
- ThreadId
- ASP ClientHostIP
- ASP UserAgent

LogContext

```
public class RequestContextMiddleware
{
    public async Task Invoke(IDictionary<string, object> environment)
    {
        using (LogContext.PushProperty("RequestId", Guid.NewGuid()))
        {
            await next(environment);
        }
    }
}
```

Sinks



Demo powered by



Serilog



PowerShell



GraphViz

Demo powered by



Microsoft®
SQL Server®



Serilog

Seq

- Quick install
- Built with .NET
- C#-like queries over structured data
- Filters and dashboards
- Lightweight but powerful
- HTTP API
- Seq Apps



Demo powered by

Seq



Serilog

The screenshot displays the Seq application interface. The top navigation bar includes links for 'dash', 'events', 'help', 'settings', and a user profile 'nblumhardt'. A search bar at the top left contains the filter 'Hostname == "ae789cc0.cloudapp.net" && E'. Below the search bar, a list of log events is shown, each with a timestamp and a message. The messages include eligibility checks, user logins, and transaction commits. On the right side, a sidebar titled 'This is the signal bar. You can apply and switch between existing signals, or create a new one by moving filters with the [X] button to the left.' contains a 'SIGNALS' section. This section lists several signals: 'None', 'Errors', 'Patient Portal', 'Production', 'Slow Requests', and 'Staging'. The 'Patient Portal' and 'Production' signals are highlighted in yellow. At the bottom of the sidebar, there is a link 'Create or add a signal...'.

Timestamp	Message
09-Jun-2015 12:48:29.940	Eligibility check for HIS-9514-f6eed0 returned ("AcceptAfter":"2015-06-26","Category":"OSTR-C")
09-Jun-2015 12:48:29.924	● Execution time of 180ms exceeded budget of 30ms; query SELECT ct.contact_id, p.scheduled_admission_dt, p.preadmission_status fro...
09-Jun-2015 12:48:29.917	User bthompson logged on as contact HIS-9514-f6eed0
09-Jun-2015 12:48:29.910	● Transaction committed in 1209ms
09-Jun-2015 12:48:29.900	● Uptime 32.10:19:59 - threads: 141, working set 312093kB
09-Jun-2015 12:48:29.894	Writing updated indications to EHR HIS-5d1f-dbf7e1
09-Jun-2015 12:48:29.879	Eligibility check for HIS-b564-ec20d5 returned ("AcceptAfter":"2015-06-11","Category":"PSCD")
09-Jun-2015 12:48:29.862	Eligibility check for HIS-0477-44f2c2 returned ("AcceptAfter":"2015-06-26","Category":"OSTR-C")
09-Jun-2015 12:48:29.817	● Execution time of 180ms exceeded budget of 30ms; query SELECT ct.contact_id, p.scheduled_admission_dt, p.preadmission_status fro...
09-Jun-2015 12:48:29.808	User diam logged on as contact HIS-0477-44f2c2
09-Jun-2015 12:48:29.801	● Transaction committed in 1199ms
09-Jun-2015 12:48:29.792	● Uptime 32.10:19:59 - threads: 131, working set 312093kB
09-Jun-2015 12:48:29.786	Writing updated indications to EHR HIS-6d1c-96c067
09-Jun-2015 12:48:29.769	Eligibility check for HIS-47e8-1c5da0 returned ("AcceptAfter":"2015-06-11","Category":"PSCD")
09-Jun-2015 12:48:29.765	● Failed to log on user HIS-eb9a-20aea2

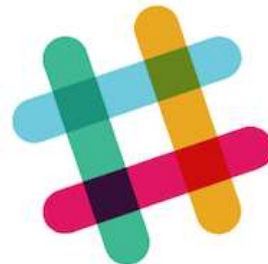
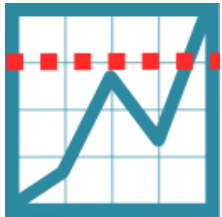
SIGNALS

- 0=0 None
- 0=0 Errors
- 0=0 Patient Portal
- 0=0 Production
- 0=0 Slow Requests
- 0=0 Staging

[Create or add a signal...](#)

Seq Apps

- FirstOfType
- Timeout
- Thresholds
- FileArchive
- Replication
- Email
- YouTrack
- Slack
- HipChat



In conclusion



VS

NLog



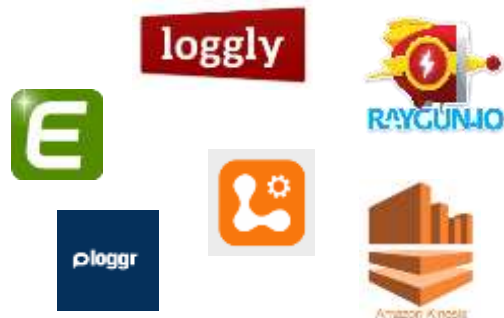
In conclusion



vs



elastic



Graphite



Resources

- Serilog (serilog.net)
- Seq (getseq.net)
- Nicholas Blumhardt (nblumhardt.com)
- FSharp (github.com/destructurama/fsharp)
- JavaScript (github.com/structured-log/structured-log)



Resources

- Anatoly.Kulakov@outlook.com
- twitter.com/KulakovT
- github.com/AnatolyKulakov
- SpbDotNet.org

