# Choosing the Right Sink to Enable Analysis



Erik Dahl
PRINCIPAL ARCHITECT

@dahlsailrunner www.knowyourtoolset.com



# Overview



Review goals of logging

**Exploration of available sinks** 

- Multiple categories

Considerations for choosing a sink

**Demo: SQL Server** 

Demo: Elasticsearch (ELK stack)

**NOTE:** No ASP.NET Core entries in the

demos



# Goals of Logging

#### Improve "Fixability"

Full details in the logs

Easily accessible

Minimize "Can't reproduce"

# **Understand Applications**

Most-used features

Speed of key activities

Time(s) for max concurrency

Frequency of errors

Key customer usage

#### **Prioritize Work**

What to fix first

What to speed up

Deflect squeaky wheels

Base decisions on usage and/or customer



#### Databases - NoSQL

Amazon
DynamoDB
Azure
DocumentDB
Azure
TableStorage
Couchbase

CouchDB
Elasticsearch
LiteDB
MongoDB
OrientDB
RavenDB
RethinkDB

#### Databases - SQL

Serilog

Sinks

SQL Server SQLite PostgreSQL

#### Files

File Rolling File Alternative Rolling File

#### Monitoring Services

Amazon
CloudWatch
Application
Insights
Azure (Log)
Analytics
DataDog
Exceptionless
Glimpse
Loggly

LogEntries
Logmatic.io
Loggr
New Relic
Raygun
Scalyr
Seq
Splunk
Stackify
Sumo Logic

#### Messaging - Platforms

Akka Actor
Amazon Kinesis
Azure EventHubs
Azure Web Jobs
Fluentd
Google Cloud PubSub
Log4Net
NLog

#### Messaging - Raw

HTTP
Network
Observable
RabbitMQ
SignalR
UDP
XSockets

#### Collaboration

Email MS Teams Slack YouTrack

#### Windows

Console
Event Log
Trace
TextWriter
Xamarin



# Sink Considerations

#### **Database**

Pricing based on licensing for database and storage requirements

Identify a review and analysis tool

May need to build your own tool(s)

Likely need to define purge or archival process

User accessibility is simpler

#### **Monitoring Service**

Pricing based on number of log entries and number of users (often monthly)

Review and analysis is part of solution

May need to configure some views

User accessibility needs to be managed by someone



# Demo



#### **SQL** Server sink

- Write log entries to the sink
- Confirm entries with queries
- Review entries with a custom web app
- Review entries with an SSRS report



### Demo



#### Elasticsearch sink

- Use a Docker image to host the ELK stack
- Write log entries to the sink
- Confirm entries with Sense
- Configure Kibana with an index pattern
- Explore Discovery within Kibana
- Explore Visualization and Dashboards within Kibana



# Summary



Discussed overall goals of logging

Built a logging platform using Serilog

Established guiding principles

- Types of things to log
- Information to include

Applied it to many application types

- Included logging via API

Reviewed available sinks

More detailed look at SQL Server and ELK stack

