Operationel Logning og Overvågning

Claus Albøge / Lead Solution Architect / Netic

Trifork & Netic

FinTech

bankdata · YOUNG · VOCALINK

Digital Health

xsana · GeriMedica · DANISH HEALTH DATA AUTHORITY

Smart Building

GRUNDFOS · Danfoss · kamstrup

Smart Enterprise	ERHVERVSSTYRELSEN · VIKING · Vestas
Cyber Protection	Cyber Protection kunder foretrækker fortrolighed
Cloud Operations	AALBORG UNIVERSITET · University of Zurich · JYSK

Netic i tal.

2002
Stiftet

146
Medarbejdere

181
Mio. i omsætning i 2021

29,8%
Gn.snitlig årlig vækst (seneste 5 år)

6
Antal Børsen Gazelle priser

5
Antal Datacentre

Agenda.

- Logs.
- Logning.
- Log Management.
- Overvågning.
- Spørgsmål?

1 Logs

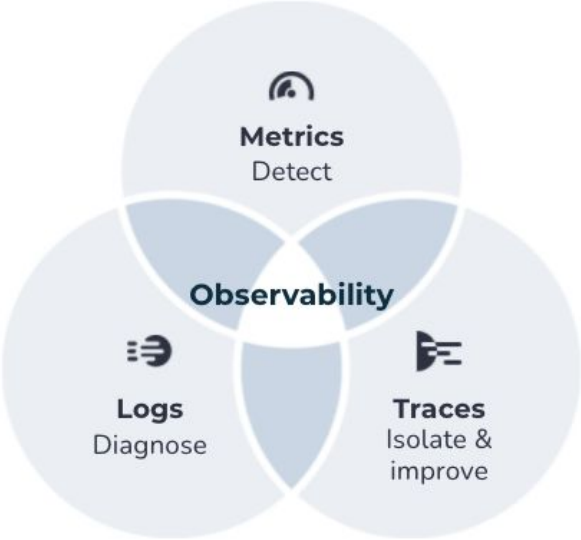
netic
A TRIFORK COMPANY

Definition.

Log *er en idempotent registrering af en diskret hændelse i et system. Logs indeholder typisk information, der kan besvare 'hvem', 'hvad', 'hvor', hvordan' og 'hvornår' for en given hændelse.*

Metrics *er numeriske repræsentationer at et systems tilstand, typisk målt over et tidsinterval.*

Tracing *giver mulighed for at repræsentere en forespørgsels tilstand i løbet af dets livscyklus på tværs af forskellige komponenter i et system.*



Logtyper.

Transaktionslog	Log der beskriver ændring i et databasesystem, før selve ændringen i databasen foretages.
Systemlog*	Fælles betegnelse for alle tekniske logs. Denne typer af logs har ofte til formål at **bistå ved fejlfinding** af systemet. Det er fagsystemet, som selv sørger for at oprette, vedligeholde og udfylde de relevante systemlogs.
Revisionslog*	Formålet med denne log er opsamling af, hvordan **systemet er blevet anvendt** på et givent tidspunkt. Herunder opsamling af **hvilke informationer tilgås af hvilke brugere**. Krav direkte udledt af Persondataloven og tilsvarende krav om revisionsspor og **sikring mod uretmæssig tilgang til personfølsomme oplysninger**.
Afregningslog*	Logning til **brug for afregning**. Loggen skal indeholde tilstrækkelige information for at kunne beregne afregning for brug i en given periode.
Verifikationslog*	Logning af events i forbindelse med udrulning og **ændringer i de fysiske miljøer**. Muliggør verifikation af om ændringer er udrullet korrekt.
Driftslog*	Logning fra de fysiske miljøer inkl. operativsystem, netværksudstyr med videre, som kan **danne grundlag for fejlsøgning**.

**) Eksempel fra Kombit Standardkontrakt - Underbilag 2F - Logning v. 1.0*

Logeksempler.

Applikation	2021-08-25T04:04:57.166Z error: Order XYZ1234 from User 42 is in received state. Cannot update delivered date after receiving
Middleware	23:58:33,675 INFO [org.jboss.as.server.deployment.scanner] (MSC service thread 1-4) WFLYDS0013: Started FileSystemDeploymentService for directory /opt/jboss/keycloak/standalone/deployments
Webserver	23.40.43.75 - - [25/Aug/2021:06:04:57 +0200] "POST /order.php?id=xyz1234 HTTP/1.1" 200 396 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.120 Safari/537.36"
Database	2021-08-25T04:00:00.052247Z 6 [System] [MY-013172] [Server] Received SHUTDOWN from user boot. Shutting down mysqld (Version: 8.0.23-0ubuntu0.20.04.1).
Linux (OS)	May 23 11:17:01 proxmox01 CRON[6918]: (root) CMD (cd / && run-parts --report /etc/cron.hourly)

Windows (OS)	<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
	  <System>
	  <Provider Name="Microsoft-Windows-Security-Auditing"
	  Guid="{54849625-5478-4994-A5BA-3E3B0328C30D}" />
	  <EventID>4624</EventID>
	  [...]
	  <Channel>Security</Channel>
	  <Computer>USER-WORKSTATION</Computer>
	  </System>
	  <EventData>
	  <Data Name="SubjectUserSid">S-1-5-18</Data>
	  [...]
	  </EventData>
	</Event>

Virtualisering	[2008-07-26 10:09:56.601 'vm:/vmfs/volumes/485a72e0-dd49e4f1-796c-001517761286/Nostalgia/Nostalgia.vmx' 123898800 info] State Transition (VM_STATE_RECONFIGURING -> VM_STATE_OFF)
Netværk	%ASA-6-302013: Built outbound TCP connection 937 for OUTSIDE:23.40.43.75/443 (23.40.43.75/443) to INSIDE:192.168.1.10/54396 (192.168.0.111/54396)

2 Logning

netic
A TRIFORK COMPANY

Definition.

***Logning**: at registrere en hændelse eller aktivitet i et (IT-)system.*

Udfordringer.

Mange standardsystemer kommer allerede med en fast defineret logningsløsning. Men for applikationer, man selv udvikler, er der ofteste en række ting, man skal tage stilling til.

- Hvad skal man logge?
  - Kontekst
  - Personfølsom information
  - Detaljeniveau
- Formatering
  - Struktureret vs Ustruktureret
  - Tidsstempler
- Performance Impact

Kontekst.

Gør loggen brugbar ved at inkludere kontekst (hvem, hvad, hvor og hvordan)

- `{“message”: “The database is down”}` **VS**
- `{“message”: “Failed to get users preferences for user id=1. Configuration Database db03 not responding. Will retry again in 5 minutes.”}` **VS**

Gerne som tags eller metadata

- `{“message”: “Failed to get users preferences for user id=1. Configuration Database not responding. Will retry again in 5 minutes.”, “user_id”: 1, “database”: ”Configuration Database”, “database_host”: ”db03”}`

Følsom Information.

Undlad så vidt muligt følsom information (CPR nummer, Credentials, osv)

- **Anonymisering**
  - *“uigenkaldelig i den betydning, at der ikke findes en måde for nogen til at tilknytte oplysningerne til en fysisk person igen”*
- **Pseudonymisering**
  - *“at personoplysningerne ikke længere kan henføres til en bestemt registreret uden brug af supplerende oplysninger”*

Detaljeniveau.

Definer detaljeniveau - og gør det konfigurerbart (så det kan ændres runtime)

- `DEBUG` - Bruges til fejlretning. Beskederne er specifikt rettet mod applikationens udviklere.
- `INFO` - Informationsmeddelelser, der ikke angiver nogen fejl.
- `WARN` - Angiver et potentielt problem, men uden indflydelse på brugeroplevelsen.
- `ERROR` - Angiver et alvorligt problem med en vis indvirkning på brugeroplevelsen.
- `FATAL` - Angiver fatale fejl, hvor brugeroplevelsen er stærkt påvirket.

Syslog opererer med 8 niveauer (Severity Levels):

- `EMERG`, `ALERT`, `CRIT`, `ERR`, `WARNING`, `NOTICE`, `INFO` og `DEBUG.`

Formattering.

Log i et struktureret format

- JSON
- KeyValue
- XML

Kan altid ‘konverteres’ til noget, der er læsbart for et menneske - den anden vej er knap så nemt…

```
<134>Jun 01 20:34:55 app42.example.com testapp: Something happened
```

RFC 3164 & RFC 5424

VS

```
{
    "time": 1654115695,
    "host": "app42.example.com",
    "source": "testapp",
    "event": {
        "message": "Something happened",
        "severity": "INFO"
        "facility": "Local0"
    }
}
```

Tidsstempler.

Benyt RFC-3339 (ISO-8601) til tidsstempler

Jun 02 14:20:42	MMM dd HH:mm:ss
Jun 02 2022 14:20:42	MMM dd yyyy HH:mm:ss
Jun 02 14:20:42 2010	MMM dd HH:mm:ss yyyy
Jun 02 12:20:42 +0000	MMM dd HH:mm:ss ZZZZ
Jun 2, 2022 2:20:42 PM	MMM dd, yyyy hh:mm:ss a
Jun 02 12:20:42 +0000 2022	MMM dd HH:mm:ss ZZZZ yyyy
22-06-02 14:20:42	yy-MM-dd HH:mm:ss
06/02/22 12:20:42 +0000	MM/dd/yy HH:mm:ss ZZZZ
02/Jun/2022:08:20:42 -0400	dd/MMM/yyyy:HH:mm:ss ZZZZ
2022 Jun 02 05:20:42.808 PDT	yyyy MMM dd HH:mm:ss.SSS zzz
2022 Jun 02 18:**05**:42.808 NPT	yyyy MMM dd HH:mm:ss.SSS zzz
2022-06-02T12:20:42+0000	yyyy-MM-dd'T'HH:mm:ssZZZZ
2022-06-02T14:20:42,808+02:00	**yyyy-MM-dd'T'HH:mm:ss.SSSZZZZ**

Performance.

Overvej påvirkning af performance

- Overdreven logning kan have performancemæssig negative effekt på applikationen og dermed brugeroplevelsen.
- Logning skal altid være asynkront og bør ikke blokere applikationen.

  - med mindre…

Undlad at opfinde din egen løsning!

Benyt et eksisterende lognings framework

- Serilog for .NET applikationer: https://serilog.net/
- LogBack for Java applikationer: https://logback.qos.ch/
- Zerolog for Go applikationer: https://github.com/rs/zerolog
- … og mange flere

Undlad at logge direkte til et Log Management system

Benyt en standardiseret informations model

- Eksempelvis Splunk CIM (Common Information Model)
  - “src_ip” **VS** “source_ip”, “ip”, “src”, “from”, “OUTSIDE”, mf

3 Log Management

netic
A TRIFORK COMPANY

Definition.

***Log Management**: at indsamle, behandle, gemme og opbevare logs i et centralt system, der giver mulighed for at analysere logs, med det formål at skabe indsigt.*

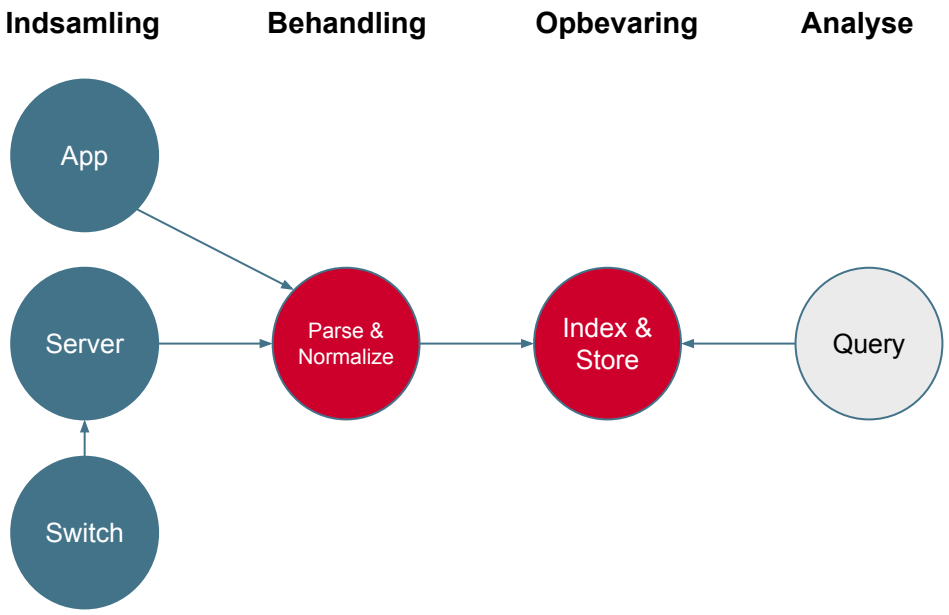
Indsigt.

Applikation	2021-08-25T04:01:57.166Z error: Order XYZ1234 from User 42 is in received state. Cannot update delivered date after receiving
Middleware	23:58:33,675 INFO [org.jboss.as.server.deployment.scanner] (MSC service thread 1-4) WFLYDS0013: Started FileSystemDeploymentService for directory /opt/jboss/keycloak/standalone/deployments
Webserver	23.40.43.75 - - [25/Aug/2021:06:01:57 +0200] "POST /order.php?id=xyz1234 HTTP/1.1" 500 396 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.120 Safari/537.36"
Database	2021-08-25T04:00:01.052247Z 6 [System] [MY-013172] [Server] Received SHUTDOWN from user boot. Shutting down mysqld (Version: 8.0.23-0ubuntu0.20.04.1).
Linux (OS)	May 23 11:17:01 proxmox01 CRON[6918]: (root) CMD (cd / && run-parts --report /etc/cron.hourly)

Windows (OS)	<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
	  <System>
	  <Provider Name="Microsoft-Windows-Security-Auditing"
	  Guid="{54849625-5478-4994-A5BA-3E3B0328C30D}" />
	  <EventID>4624</EventID>
	  [...]
	  <Channel>Security</Channel>
	  <Computer>USER-WORKSTATION</Computer>
	  </System>
	  <EventData>
	  <Data Name="SubjectUserSid">S-1-5-18</Data>
	  [...]
	  </EventData>
	</Event>

Virtualisering	[2021-08-25 04:00:56.601 'vm:/vmfs/volumes/485a72e0-dd49e4f1-796c-001517761286/db01/db01.vmx' 123898800 info] State Transition (VM_STATE_RECONFIGURING -> VM_STATE_OFF)
Netværk	%ASA-6-302013: Built outbound TCP connection 937 for OUTSIDE:23.40.43.75/443 (23.40.43.75/443) to INSIDE:192.168.1.10/54396 (192.168.0.111/54396)

Log Management System.



Udfordringer.

- **Integritet**: Hvordan sikre jeg at logs ikke går tabt undervejs?

- **Retention:** Hvor længe skal hvilke logs opbevares?

- **Skalering**:
  - **Ingest**: Hvor mange logs kan håndteres pr sekund?
  - **Opbevaring**: Hvor meget fylder logs fra 180 dage?
  - **Søgning / Latenstid**: Hvor lang tid går der inden nyeste log bliver søgbar?
  - **Søgning / Hastighed**: Hvor hurtigt kan jeg søge på tværs af alle logs?

- **Adgangskontrol**: Hvem har adgang til hvilke logs? - Er der persondata i mine logs?

Indsamling.

- **Opsamling**
  - Fil
  - Syslog
  - EventLog
- **Berigelse**
  - Tags & Metadata
  - Server, Miljø, Logtype, mm
- **Transformation**
  - Tidsstempel
  - JSON
- **Afsendelse**
  - Protokol
  - Buffering
  - Gensendelse
  - Kryptering

VECTOR BY DATADOG

beats

fluentd

rsyslog

NXLog

Behandling & Opbevaring.

- Parsing
- Transformation
- Indeksering
  - “Schema on Write”
  - “Schema on Read”
- Komprimering
- Opbevaring
  - Replika
  - Tiering
  - Retention
- Adgangskontrol
  - RBAC
  - Repo / View / Index

Analyse.

Søgning og analyse via dedikeret søgesprog

- Filtre
  - Felter
  - Fritekst
- Operatører
  - Sammenligning
  - Logiske
- Funktioner

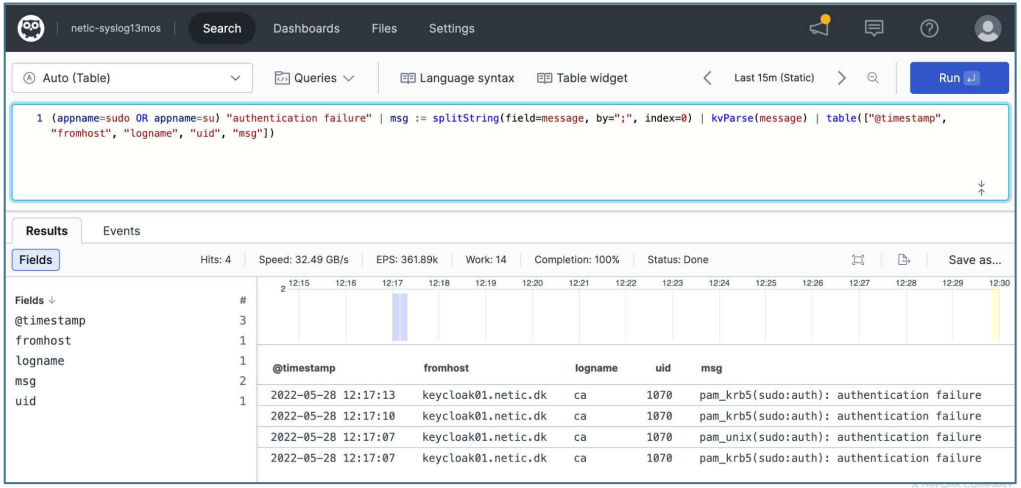
Query Function	Description
avg()	Calculates the average for a field of a set of events.
base64Decode()	Performs Base64 decoding of a field.
cidr()	Filters events using CIDR subnets.
count()	Counts given events.
drop()	Removes attributes or columns from a result set.
eval()	Creates a new field by evaluating the provided expression.
format()	Formats a string using printf-style.
groupBy()	Groups events by specified fields and executes aggregate functions…
hash()	Computes a non-cryptographic hash of a list of fields.
ioc:lookup()	Look up IOCs (indicators of compromise).
kvParse()	Key-value parse events.
length()	Returns the number of characters in a string field.
lookup()	Enhances events with metadata.
math:sqrt()	Calculates the rounded positive square root of a double field.
max()	Finds the largest number for the specified field over a set of events.
min()	Finds the smallest number for the specified field over a set of events.
parseJson()	Parses specified fields as JSON.
parseTimestamp()	Parses a string into a timestamp.
parseUrl()	Extracts URL components from a field.
regex()	Extracts new fields using a regular expression.
rename()	Renames a given field.
sample()	Samples the event stream.
sort()	Sorts events by their fields.
split()	Splits an event structure created by json array into distinct events.
table()	Used to create a widget to present the data in a table.
top()	Finds the top results based on a given field.

Søgning.

@rawstring:

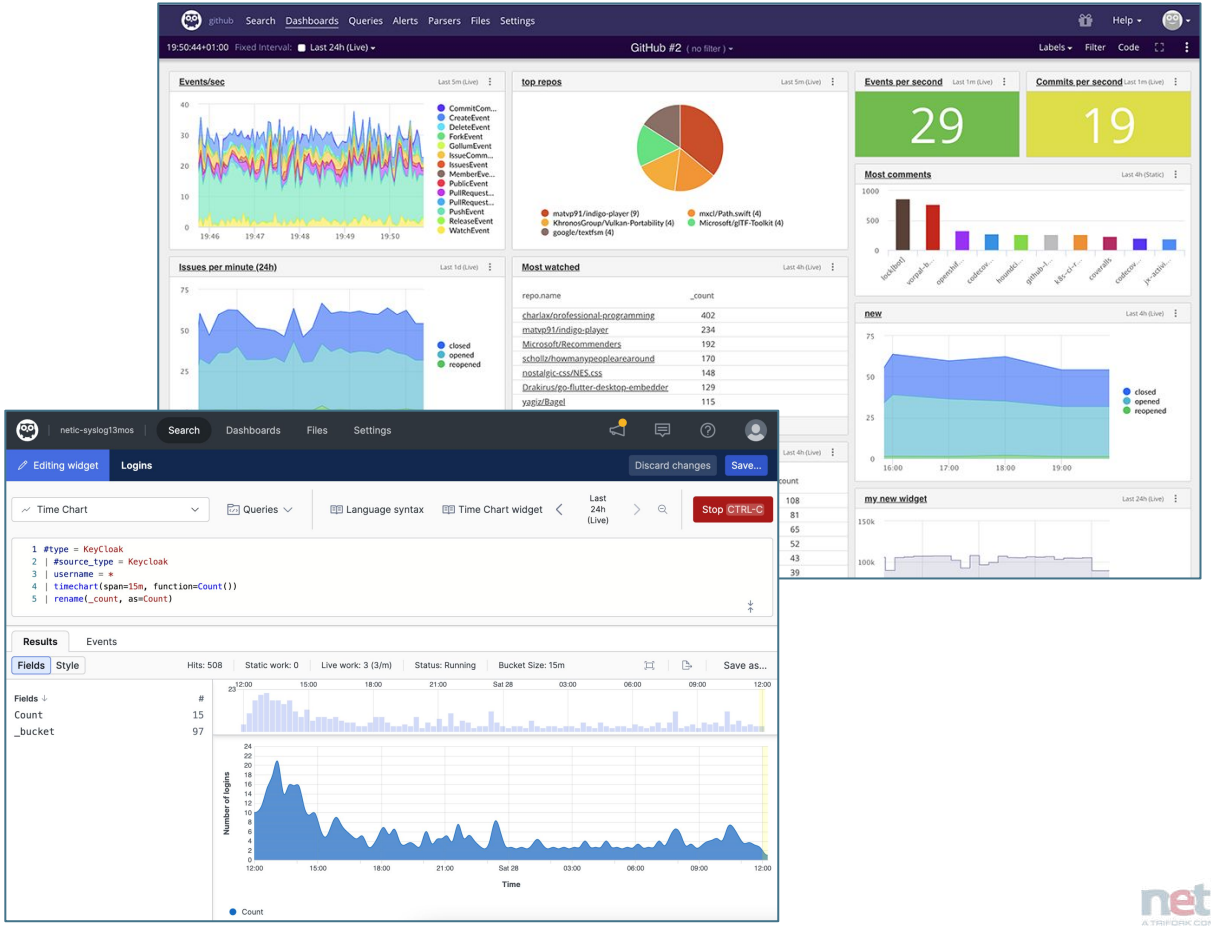

```
{
  "@timestamp.nanos": 0,
  "appname": "sudo",
  "facility": "10",
  "fromhost": "keycloak01.netic.dk",
  "fromhostip": "77.243.58.152",
  "headers": {},
  "host": "keycloak01.netic.dk",
  "loghost": "syslog01.netic.dk",
  "message": "pam_krb5(sudo:auth): authentication
failure; logname=ca uid=1070 euid=0 tty=/dev/pts/0
 ruser=ca rhost=",
  "message_key": null,
  "offset": 13415190408,
  "partition": 4,
  "severity": "5",
  "source": "syslog",
  "source_type": "syslog",
  "syslogtag": "sudo:",
  "topic": "netic-hc-syslog"
}
```


```
(appname=sudo OR appname=su) "authentication failure" |
msg := splitString(field=message, by=";", index=0) |
kvParse(message) |
table(["@timestamp", "fromhost", "logname", "uid", "msg"])
```



Anvendelse.

- Dashboards
  - Hurtigt overblik
- Grafer
  - Visualisering
  - Hurtig indblik
  - Drilldowns



4 Overvågning

netic
A TRIFORK COMPANY

Alarmer.

Benyt så vidt muligt **metrics** (systemets tilstand målt over tid) til alarmering.
Metrics kan komme fra logs (de fleste grafer på forrige slide var log based metrics).

- Antal ERRORS målt over tidsinterval > X
- Trends vs Threshold
  - “Disk løber fuld om X timer” **VS** “Disk 90% fuld”
- Optimer Incident Processen ved at berige alarmer med:
  - Links til Runbooks
  - Links til Dashboard
  - Links til CMDB
  - …

Alarmer.

Det er selvfølgeligt muligt at alarmere på baggrund af **logs** (diskrete hændelser)
… eller mangel på logs.

- Periodiske søgninger vs streaming / real-time søgninger
- Udfordringer i flere Log Management Systemer:
  - State: Er en alarm stadig aktiv? (Er incident resolved?)
  - Correlation Id: Er der tale om samme alarm?
- Løsning: Integration til Notification Management system
  - Opsgenie
  - PagerDuty
  - … webhook i monitoreringssystem
- Bonus: Mulighed for links direkte til søgning i Log Management system for hurtigere fejlsøgning.

5

Spørgsmål?

netic
A TRIFORK COMPANY

netic
A TRIFORK COMPANY

Tak for jeres tid!

Alfred Nobels vej 25, DK-9220 Aalborg Ø * Tlf. 77 77 08 88

netic.dk

company/netic-as