Maximizing Observability with Dynatrace Log Management

Karl Svensson

Karl.svensson@dynatrace.com

Me, Karl Svensson

- Delivery Architect for Dynatrace professional services
- Based in Espoo(Helsinki Area) in Finland
- Grew up in Malmö, Sweden
- Master of science in computer science from Lund Technical University
- Developed & architected bank software for 10 years at Crosskey Banking Solutions
- 6 years at Digia as Integration Architect & Cloud Architect
- 1 year as Cloud Architect at Bradleys Oy
- 1 AWS certification(Associate Architect), 2 GCP (Professional Architect), 4 Splunk (Splunk Architect), 2 Dynatrace (Professional)
- Full professional proficiency in Swedish, Finnish, English & German

Dubai HOTs

AMAR NATH SARASWAT • 1st
Digital Transformation Architect - AiOps, Observability, Automation, ...
1w • Edited •

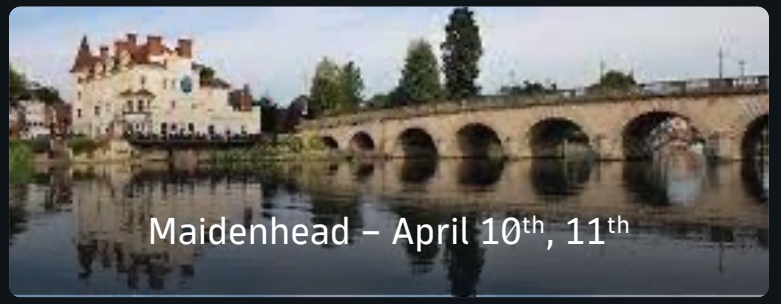
Thanks to the Dynatrace team for organizing the incredible training session!

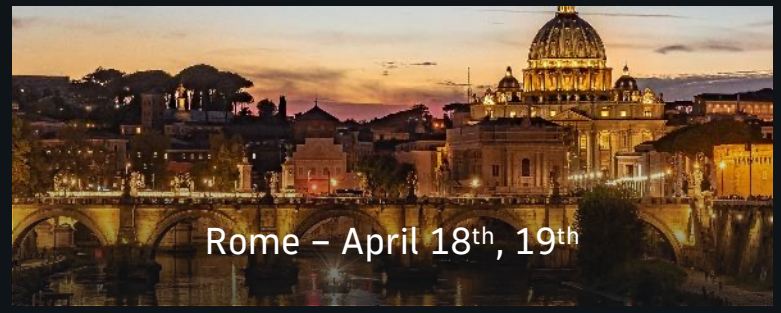
🚀 Your dedication to empowering professionals with cutting-edge monitoring and observability tools is truly commendable. The insights gained are invaluable and will undoubtedly elevate our knowledge to new heights.

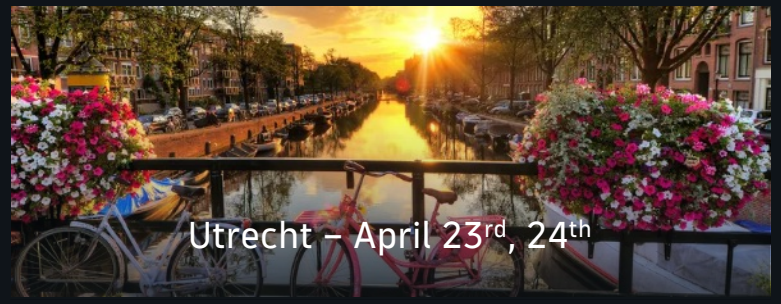
Moreover, it was enjoyable to connect with Yuan Sun (孙远) Karl Svensson Danilo Vukotic Anton Freyberg Hani Hannoun Paul Hashem

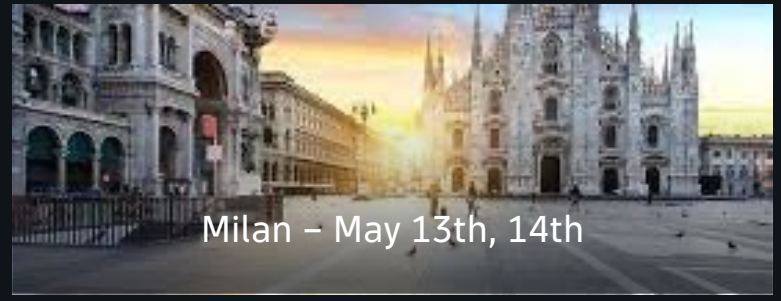
Looking forward to continued collaboration and success together! #Dynatrace #Gratitude #ContinuousImprovement 🌟

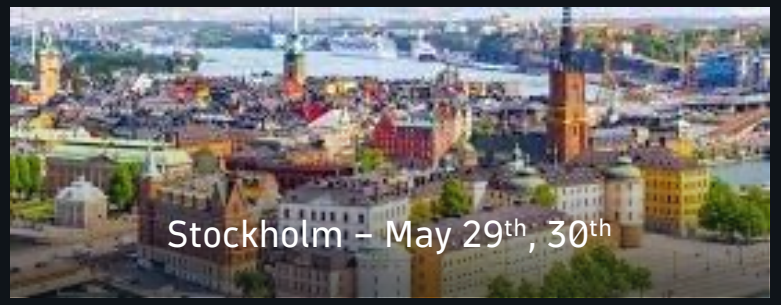
EMEA HoT Labs

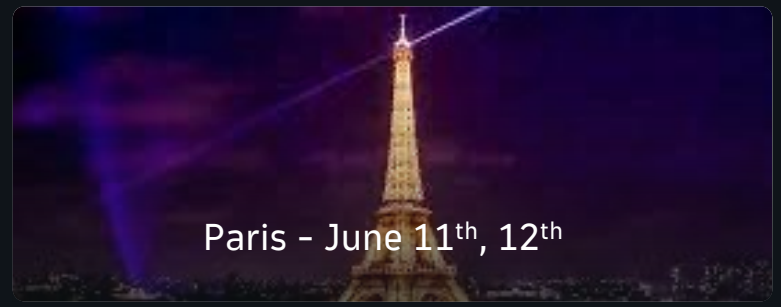






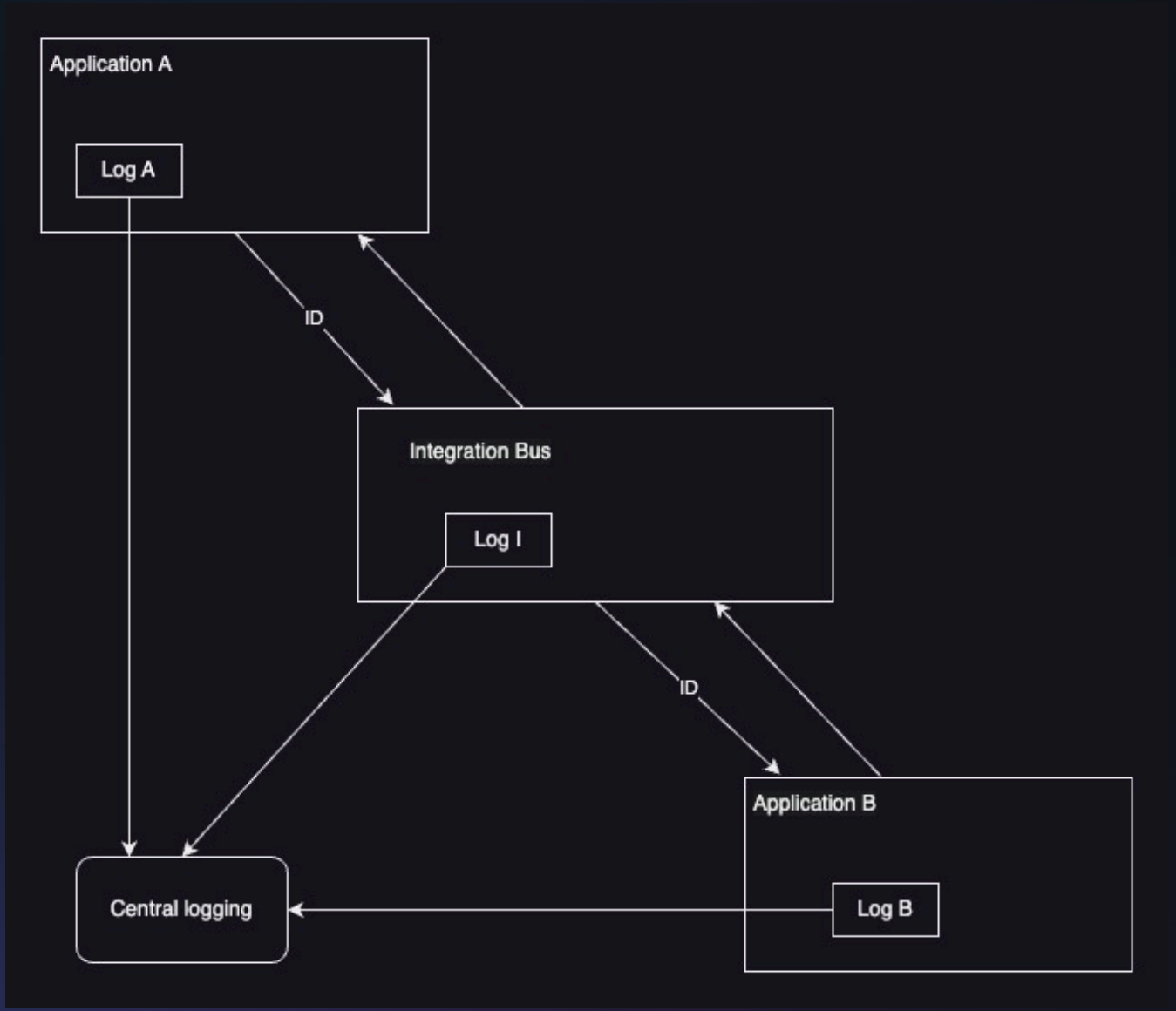






https://www.dynatrace.com/services-support/ace-services/global-hot-labs/

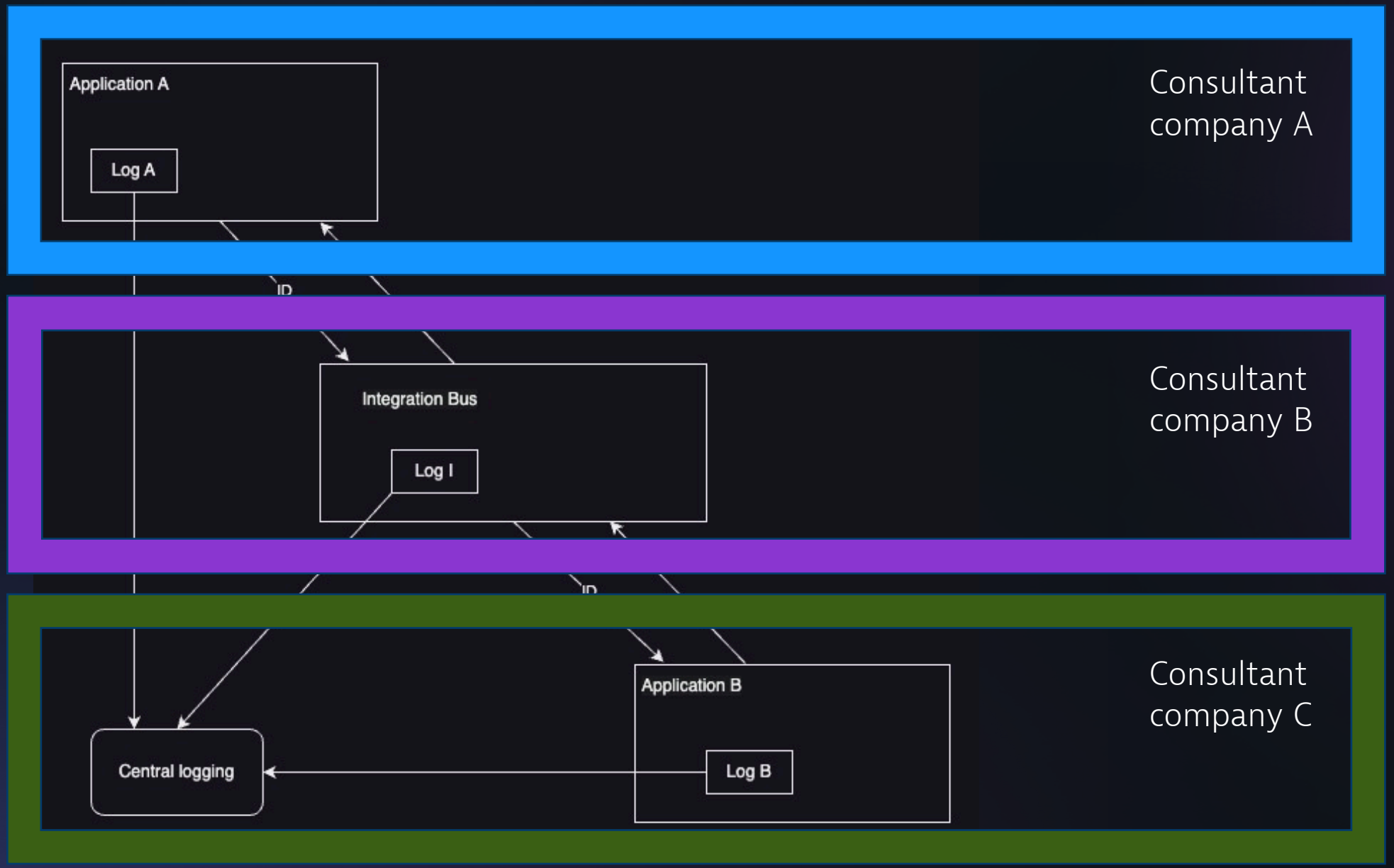
Logs: the way I used to do it



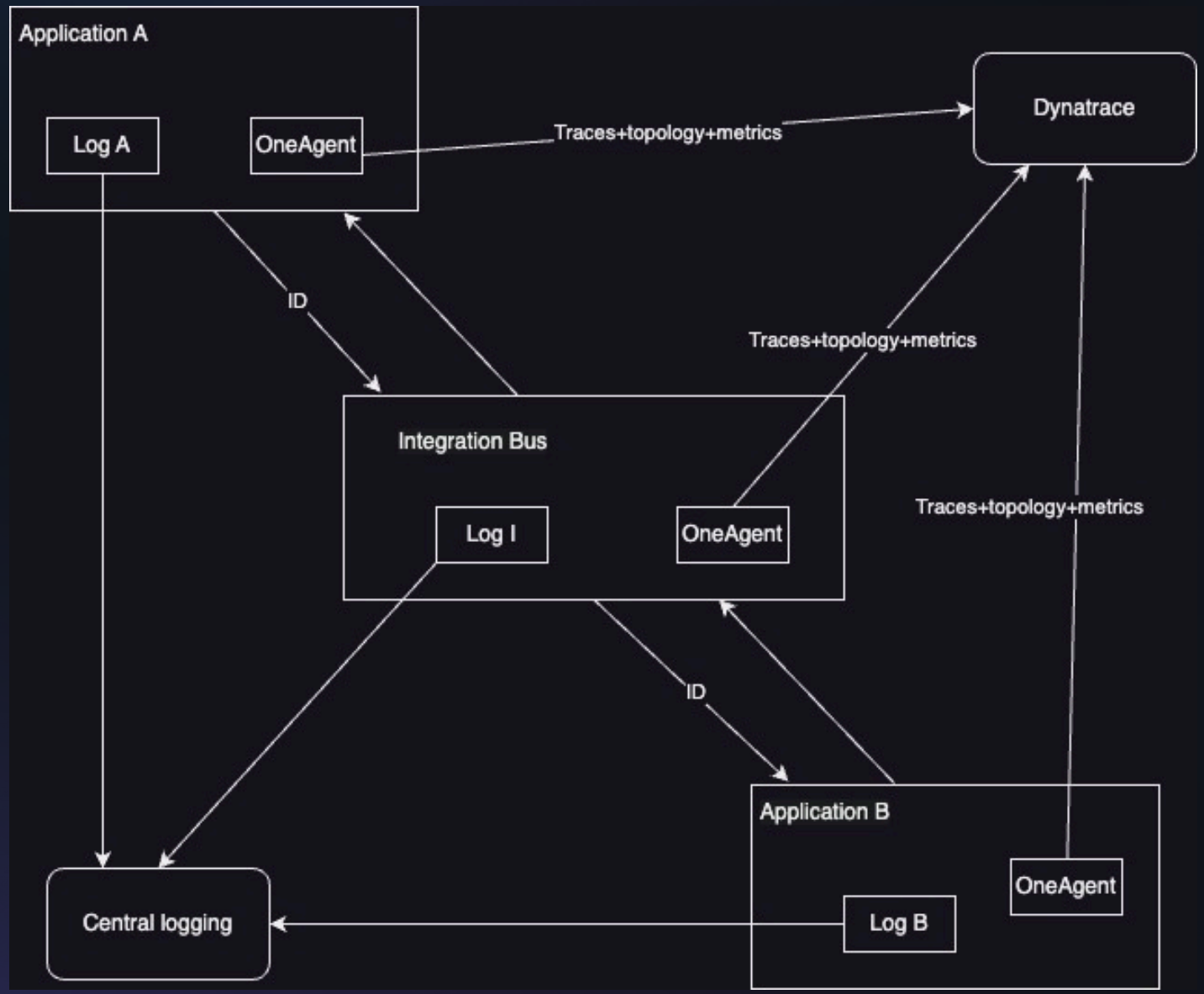
Query:

...id...

Logs: Challenge

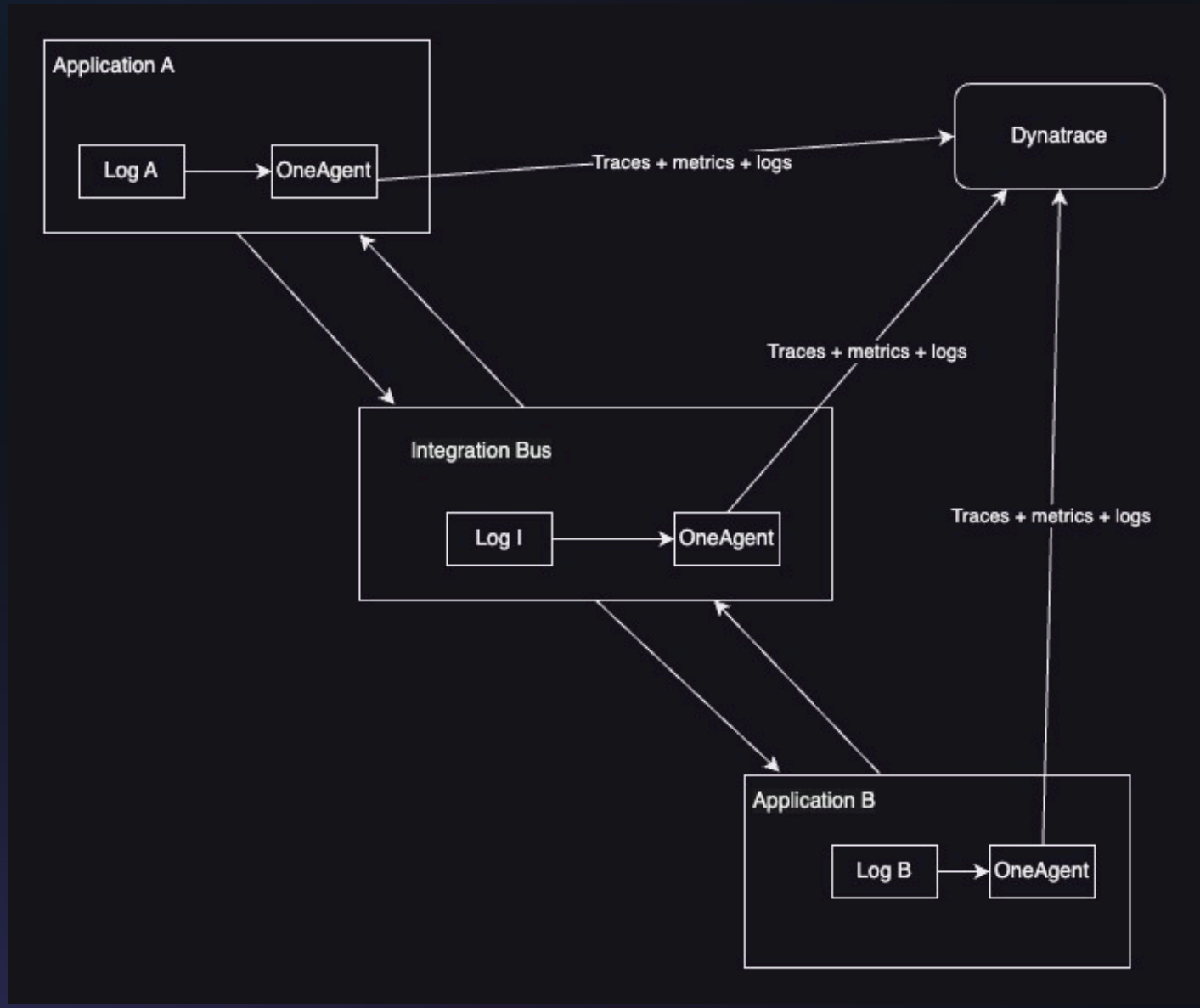


Add APM with Dynatrace



Trace example

Traces, metrics & logs with one tool and one query language

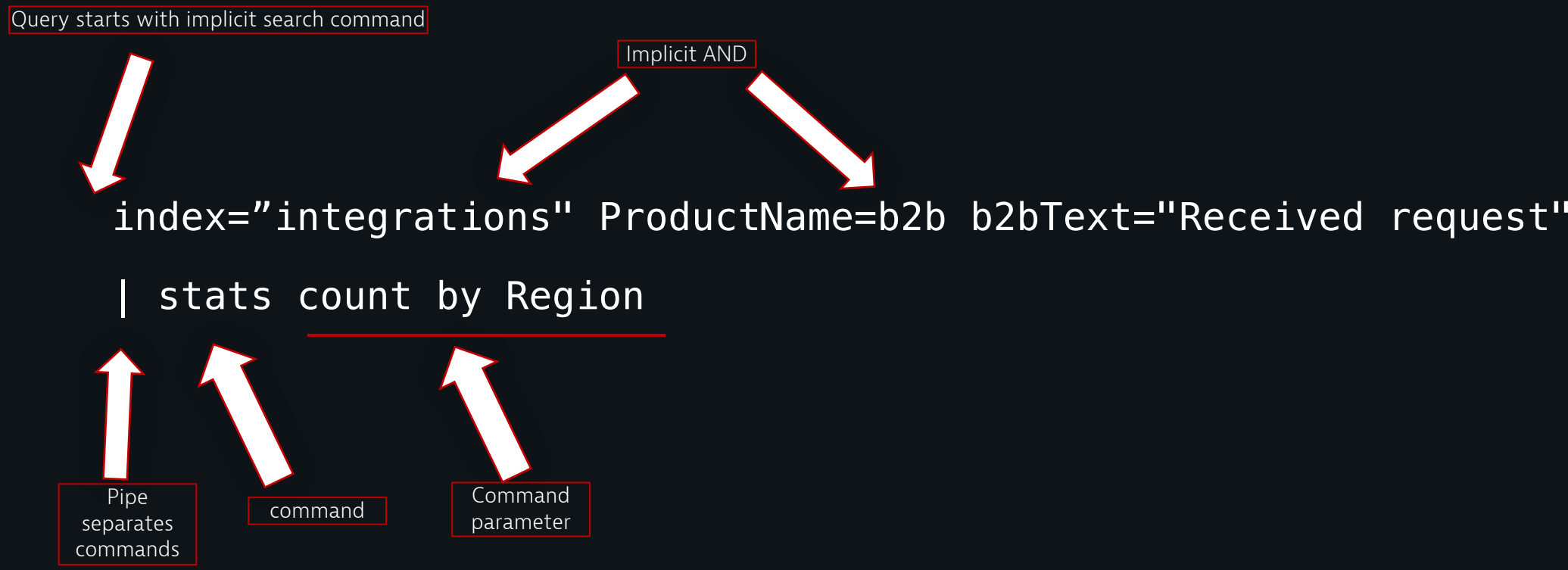


Trace + logs example

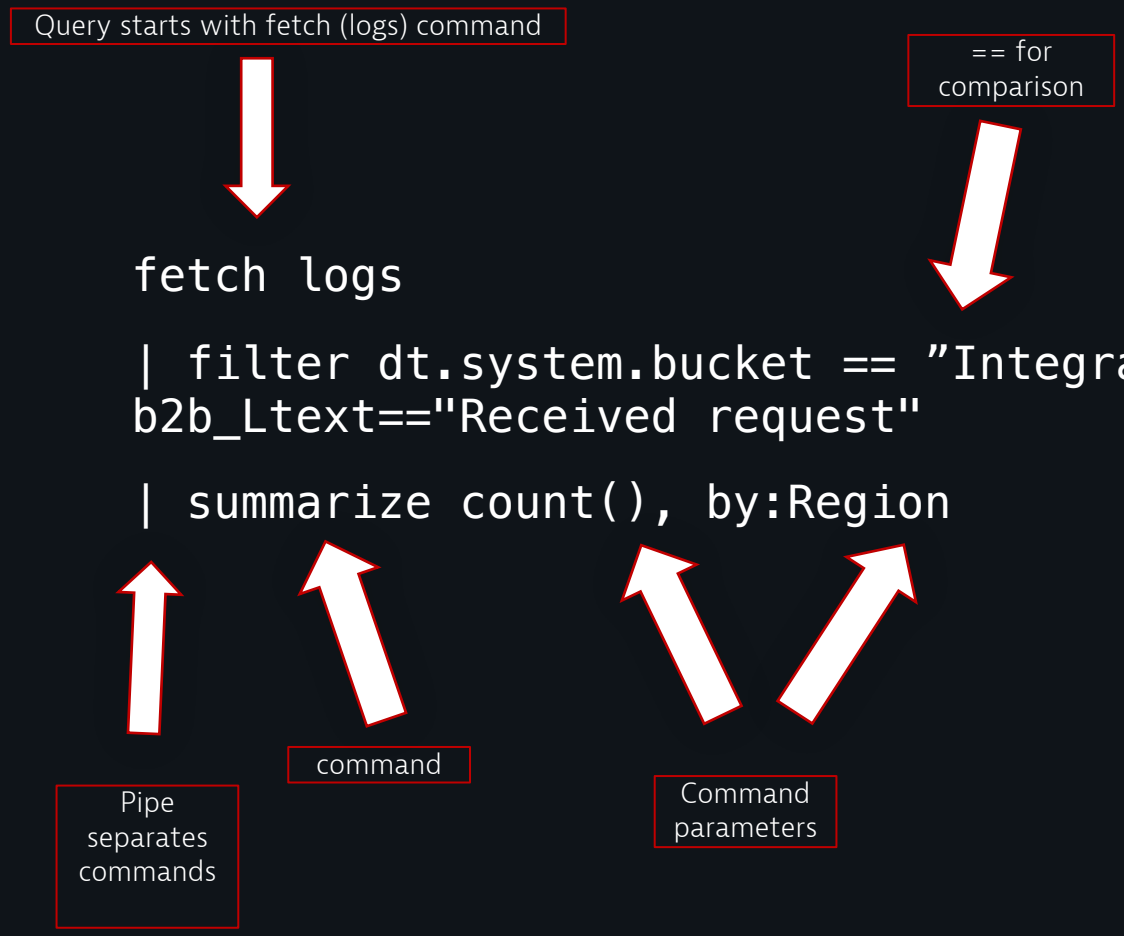
Splunk -> Grail migration project for very large EU customer

- Current ingest: **~500** TB / 24h
- Hundreds of dashboards, alerts and inputs
- Lots of people to train. About 500 people attended some of the trainings

SPL basic structure



DQL basic structure



Complex logs DQL example 1

```
fetch logs, from:now()-1d

| filter dt.entity.host == ”HOSTNAME”

| fieldsadd F1 = trim(F1)

| filter (F1=="Received request from Partner" or F1=="Message sent to Partner" or F1=="Received error response from Integration System")

| fieldsadd KCM_Status=if((b2b_Type=="Request" and root=="AddOrder"),"Request",else:if((b2b_Type=="Response" and root=="OrderPending"),"OrderPending",else:if(((b2b_Type=="Response" and root=="OrderRejected") or F1=="Received error response from Integration System"),"OrderRejected",else:if((root=="OrderStatusUpdate" and CompletionCode=="510"),"OrderAcknowledged",else:null)))) | filter (F1=="Received request from Partner" or F1=="Message sent to Trading Partner" or F1=="Received error response from Integration System") and category=="L3B"

| fieldsadd Request=if(KCM_Status="Request",_time,NULL)

| fieldsadd OrderAcknowledged=if(KCM_Status="OrderAcknowledged",_time,NULL)

| fieldsadd Today=unixSecondsFromTimestamp(now())

| summarize CompletionCode1=takelast(CompletionCode), Today=takelast(Today), _time=takelast(unixSecondsFromTimestamp(timestamp)), LineStatus1=takelast(LineStatus), RequestDt=takelast(Request), OrderAcknowledged=takelast(OrderAcknowledged), by:BuyersID

| fieldsadd Diff = Today-RequestDt

| fieldsadd Diff=round(toDouble(Diff)/86400)

| filter CompletionCode1==510 and LineStatus1=="Acknowledged" and Diff>0
```

Logs DQL live example

Problems / things that needed solving

- User training in DQL syntax and SPL to DQL translation needed
- Quite much work was needed to translate queries and build new dashboards with corresponding functionality as in Splunk
- Users were not used to DT logs license model, query costs needed controlling and policing. Buckets helped.

Demo of Cloud tags dashboard

Simply smarter clouds