Business Observability – Demo (DQL Input Visible)

Introdução

Este notebook demonstra como a **observabilidade de logs** pode ser usada não apenas para troubleshooting técnico, mas também para gerar **insights de negócio em tempo real**.

Aqui analisamos duas aplicações:

- **Legacy app** → dados não estruturados
- **Modern app** → logs estruturados

E mostramos como falhas impactam diretamente métricas críticas:

- Pedidos processados
- Pagamentos recusados
- Indisponibilidade de estoque

Introdução

Este notebook demonstra como a **observabilidade de logs** pode ser usada não apenas para troubleshooting técnico, mas também para gerar **insights de negócio em tempo real**.

Aqui analisamos duas aplicações:

- **Legacy app** → dados não estruturados
- **Modern app** → logs estruturados

E mostramos como falhas impactam diretamente métricas críticas:

- Pedidos processados
- Pagamentos recusados
- Indisponibilidade de estoque

Repositório público desta demo

Visão dos 10 Logs Mais Recentes

Validação dos últimos eventos ingeridos no dataset **demo**.
Cada log já está enriquecido com `service.name` e `severity`, facilitando correlação entre sistemas.

> 💡 Insight: confirma ingestão em tempo real e o pipeline de enriquecimento.

Explore logs

```
fetch logs, from:"2025-08-24 08:00:00", to:"2025-08-24 11:00:00"
| fieldsAdd bucket = "Demo"
| filter service.name == "modern-app" or service.name == "legacy-app"
| fields timestamp, service.name, severity, content
| sort timestamp desc
| limit 10
```

10 records Executed at: 8/24/2025, 11:03:45, Timeframe: 08:00:00 – 11:00:00, Scanned bytes: 282 kB

timestamp	service.name	severity	content
8/24/2025, 10:59:55 AM	modern-app	INFO	Periodic log: 72 orders processed, 24 errors (Payment F
8/24/2025, 10:58:55 AM	modern-app	INFO	Periodic log: 72 orders processed, 24 errors (Payment F
8/24/2025, 10:57:55 AM	modern-app	INFO	Periodic log: 72 orders processed, 24 errors (Payment F
8/24/2025, 10:56:55 AM	modern-app	INFO	Periodic log: 72 orders processed, 24 errors (Payment F
8/24/2025, 10:55:55 AM	modern-app	INFO	Periodic log: 72 orders processed, 24 errors (Payment F
8/24/2025, 10:54:55 AM	modern-app	INFO	Periodic log: 72 orders processed, 24 errors (Payment F
8/24/2025, 10:53:55 AM	modern-app	INFO	Periodic log: 72 orders processed, 24 errors (Payment F
8/24/2025, 10:52:55 AM	modern-app	INFO	Periodic log: 72 orders processed, 24 errors (Payment F
8/24/2025, 10:51:55 AM	modern-app	INFO	Periodic log: 72 orders processed, 24 errors (Payment F
8/24/2025, 10:50:55 AM	modern-app	INFO	Periodic log: 72 orders processed, 24 errors (Payment F

Tendência de Pedidos Processados vs Falhas

Distribuição de logs por severidade ao longo do tempo:

- **INFO** → pedidos processados com sucesso
- **WARN** → falhas de negócio (ex.: estoque)
- **ERROR** → falhas críticas (ex.: pagamento)

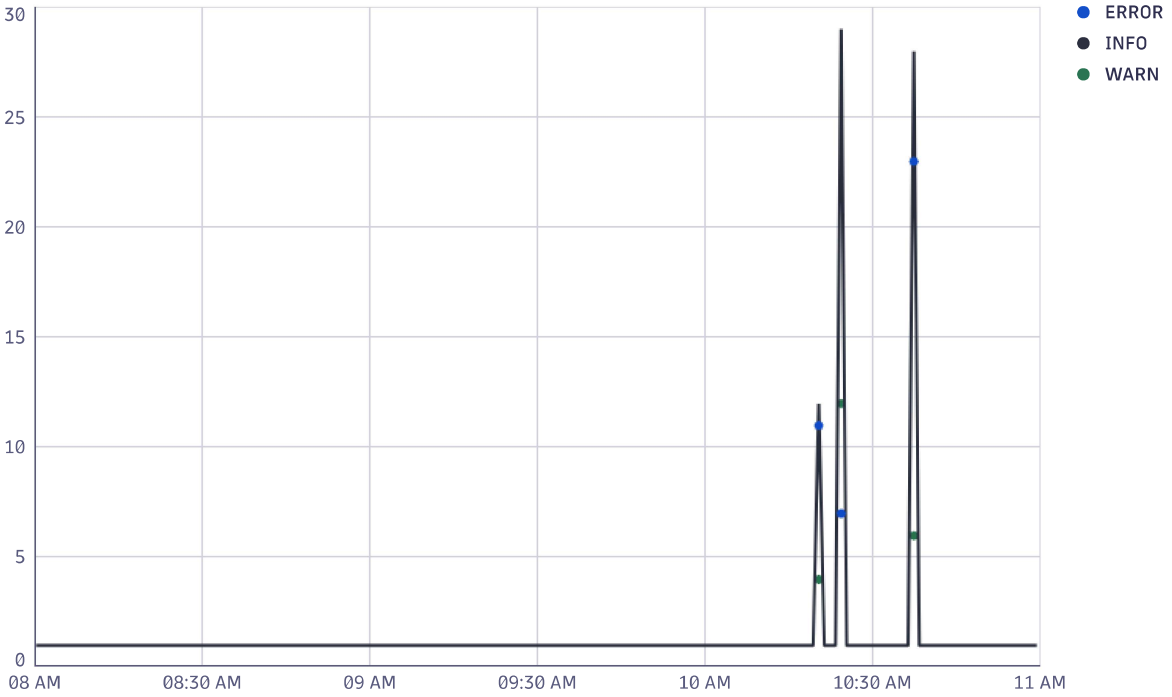
> 💡 Insight: mostra a evolução temporal dos principais KPIs de negócio, permitindo identificar picos anômalos.

Explore logs

```
fetch logs, from:"2025-08-24 08:00:00", to:"2025-08-24 11:00:00"| fieldsAdd bucket="De
| filter service.name == "modern-app" or service.name == "legacy-app"
| filter isNotNull(severity)
| fields timestamp, service.name, severity, content
| makeTimeseries count(), interval: 1m, by: { severity }

```

3 records Executed at: 8/24/2025, 11:03:51, Timeframe: 08:00:00 – 11:00:00, Scanned bytes: 279 kB



Causas de Falhas (Business Failures)

Ranking das falhas mais recorrentes:

- **Pagamentos recusados**
- **Indisponibilidade de estoque**
- Outros erros críticos

> 💡 Insight: permite priorizar se a dor maior está no financeiro (gateway de pagamento) ou operacional (estoque).

Legacy App

Explore logs

```
fetch logs, from:"2025-08-24 08:00:00", to:"2025-08-24 11:00:00"| fieldsAdd bucket="De
| filter service.name == "legacy-app"
| filterOut status == "NONE"
| summarize total = count(), by: { service.name, content, status }
| sort total desc
```

67 records Executed at: 8/24/2025, 11:03:57, Timeframe: 08:00:00 – 11:00:00, Scanned bytes: 129 kB

service.name	content	total	status
legacy-app	Order failed due to out of stock (Order ID: 2023)	1	WARN
legacy-app	Order failed due to out of stock (Order ID: 2349)	1	WARN
legacy-app	Order failed due to out of stock (Order ID: 2414)	1	WARN
legacy-app	Order failed due to out of stock (Order ID: 3513)	1	WARN
legacy-app	Order failed due to out of stock (Order ID: 3713)	1	WARN
legacy-app	Order failed due to out of stock (Order ID: 3877)	1	WARN
legacy-app	Order failed due to out of stock (Order ID: 4827)	1	WARN
legacy-app	Order failed due to out of stock (Order ID: 5673)	1	WARN
legacy-app	Order failed due to out of stock (Order ID: 5674)	1	WARN
legacy-app	Order failed due to out of stock (Order ID: 5968)	1	WARN
legacy-app	Order failed due to out of stock (Order ID: 6044)	1	WARN
legacy-app	Order failed due to out of stock (Order ID: 6479)	1	WARN
legacy-app	Order failed due to out of stock (Order ID: 7075)	1	WARN
legacy-app	Order failed due to out of stock (Order ID: 7385)	1	WARN
legacy-app	Order failed due to out of stock (Order ID: 7745)	1	WARN
legacy-app	Order failed due to out of stock (Order ID: 8543)	1	WARN
legacy-app	Order failed due to out of stock (Order ID: 9756)	1	WARN

Modern App

Explore logs

```
fetch logs, from:"2025-08-24 08:00:00", to:"2025-08-24 11:00:00"| fieldsAdd bucket="De
| filter service.name == "modern-app"
| filterOut status == "NONE"
| summarize total = count(), by: { service.name, content, status }
| sort total desc
```

67 records Executed at: 8/24/2025, 11:05:32, Timeframe: 08:00:00 – 11:00:00, Scanned bytes: 258 kB

service.name	content	total	statu
modern-app	Periodic log: 28 orders processed, 6 errors (Payment Failures: 3, Ou…	140	INFO
modern-app	Periodic log: 72 orders processed, 24 errors (Payment Failures: 16, …	23	INFO
modern-app	Periodic log: 56 orders processed, 15 errors (Payment Failures: 8, O…	12	INFO
modern-app	Periodic log: 35 orders processed, 7 errors (Payment Failures: 4, Ou…	4	INFO
modern-app	Order 13329 failed: Payment declined trace_id=82e81093dec3ac1ad18fc5…	1	ERRO
modern-app	Order 14503 failed: Payment declined trace_id=6b064e75294df3c1f2b99e…	1	ERRO
modern-app	Order 183195 failed: Out of stock trace_id=c3fb46395a2e8fbf3cd6c8c3f…	1	WAR
modern-app	Order 220695 failed: Payment declined trace_id=aada469526fcfbf361983…	1	ERRO
modern-app	Order 253004 failed: Payment declined trace_id=3a8c5d45c4ddc6bb68b03…	1	ERRO
modern-app	Order 375571 failed: Payment declined trace_id=9ff804d17f5f52e07e655…	1	ERRO
modern-app	Order 386709 failed: Out of stock trace_id=f9c6bcbb830777d77e0d7f126…	1	WAR
modern-app	Order 388917 failed: Payment declined trace_id=d6decdfd160984c7fd27a…	1	ERRO
modern-app	Order 458588 failed: Payment declined trace_id=6df8b11bbe60df9f01658…	1	ERRO
modern-app	Order 499578 failed: Out of stock trace_id=358d14dd0853a87baac27b63a…	1	WAR
modern-app	Order 565641 failed: Payment declined trace_id=b2e3072b352b22884ffb0…	1	ERRO
modern-app	Order 651905 failed: Payment declined trace_id=b058bb7c88eb150294fa9…	1	ERRO

Porcentagem por Tipos de Falhas

Explore logs

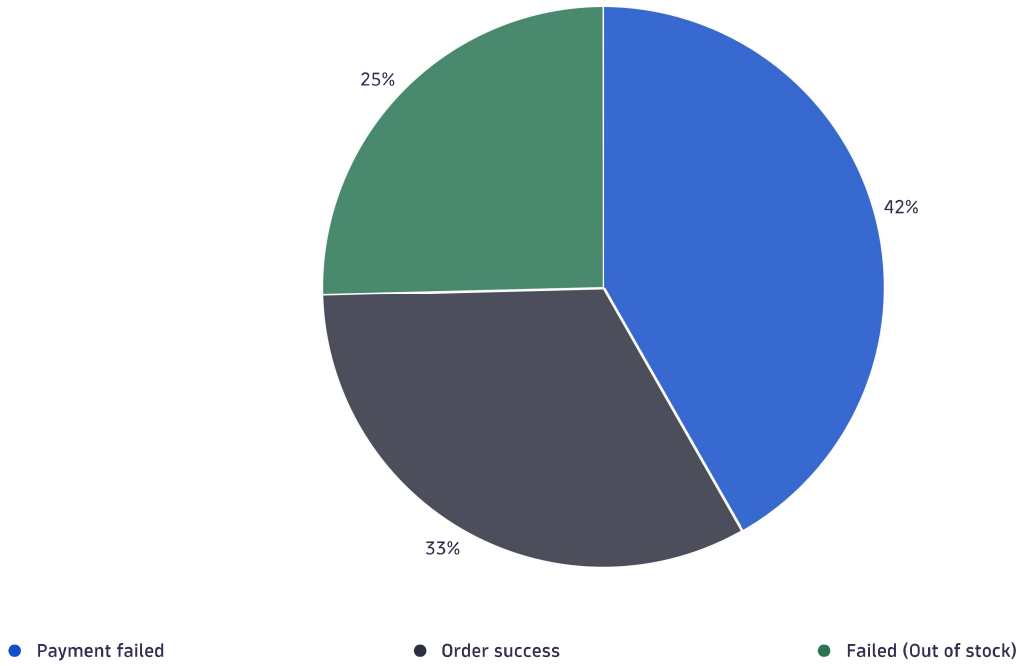
```
fetch logs, from:"2025-08-24 08:00:00", to:"2025-08-24 11:00:00"| fieldsAdd bucket="De
| filter service.name == "legacy-app"
| summarize total = countIf(contains(lower(content), "payment failed for order"))
| fieldsAdd category = "Payment failed"
| append [
    fetch logs, from:"2025-08-24 08:00:00", to:"2025-08-24 11:00:00"| fieldsAdd bucket

    | filter service.name == "legacy-app"
    | summarize total = countIf(contains(lower(content), "order processed successfully
    | fieldsAdd category = "Order success"
]
| append [
    fetch logs, from:"2025-08-24 08:00:00", to:"2025-08-24 11:00:00"| fieldsAdd bucket

    | filter service.name == "legacy-app"
    | summarize total = countIf(contains(lower(content), "out of stock"))
    | fieldsAdd category = "Failed (Out of stock)"
]
| fields category, total
| sort total desc

```

3 records Executed at: 8/24/2025, 11:06:42, Timeframe: 08:00:00 – 11:00:00, Scanned bytes: 387 kB



Comparativo Legacy vs Modern App

A comparação entre as duas aplicações revela um contraste crítico:

- **Legacy App** → taxa de sucesso **97%** (opera de forma estável, poucas falhas)
- **Modern App** → taxa de sucesso **apenas 19%** (mais de 8 em cada 10 pedidos falham)

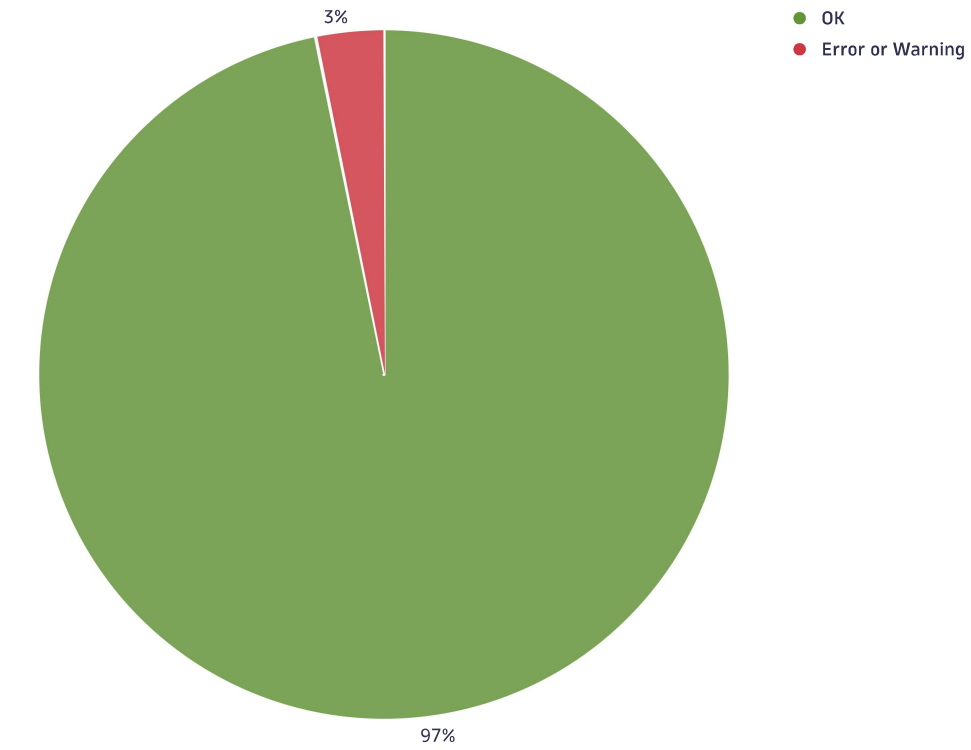
> 🚨 **Alerta**: Apesar de adotar uma arquitetura moderna, o novo sistema apresenta uma taxa de insucesso **muito superior** ao legado.
> Isso reforça a necessidade urgente de revisão de design, testes de resiliência e análise de dependências externas.

Explore logs

```
fetch logs, from:"2025-08-24 06:00:00", to:"2025-08-24 11:00:00"| fieldsAdd bucket="De
| filter service.name == "legacy-app"
| fieldsAdd status = if(status == "NONE", "OK", else:"Error or Warning")
| summarize total=count(), by: { status }
| sort total desc

```

2 records Executed at: 8/24/2025, 11:07:59, Timeframe: 06:00:00 – 11:00:00, Scanned bytes: 4 MB

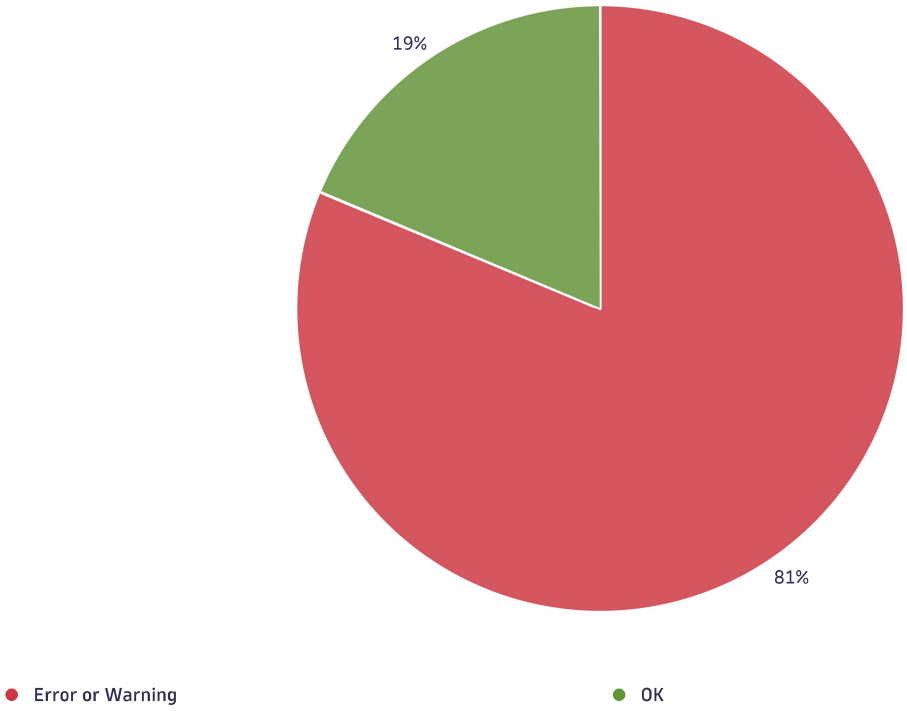


Explore logs

```
fetch logs, from:"2025-08-24 06:00:00", to:"2025-08-24 11:00:00"| fieldsAdd bucket="De
| filter service.name == "modern-app"
| fieldsAdd status = if(status == "NONE", "OK", else:"Error or Warning")
| summarize total=count(), by: { status }
| sort total desc

```

2 records Executed at: 8/24/2025, 11:11:28, Timeframe: 06:00:00 – 11:00:00, Scanned bytes: 384 kB



Resumo Executivo

Nesta demo, partimos de **eventos técnicos (logs)** e extraímos **métricas de negócio**:

- Quantidade de pedidos processados
- Percentual de falhas de pagamento
- Impacto da indisponibilidade de estoque

Esse é o diferencial da **observabilidade moderna**: transformar telemetria em **insights para o negócio**.
O mesmo modelo pode ser estendido para **conversão, churn e NPS**, conectando **TI e negócio** em tempo real

> 💡 Observação:
> Para este caso de uso, os logs poderiam ser transformados em **BizEvents já no pipeline de ingestão**.
> Benefícios:
>
> - **Redução de custo** de armazenamento no Grail com métricas, possibilitando um maior e melhor uso do Grail com dados relevantes.
> - **Maior performance** nas consultas, já que apenas campos de negócio relevantes (`order_id` , `status` , `amount`) seriam mantidos.