HOW TO ESTIMATE AND REDUCE AZURE SENTINEL DATA INGESTION COSTS? CAN WE TRUST AZURE CALCULATOR?

Jair Santanna (jair.santanna@northwave.nl)

16/04/2021

INTRODUCTION

- The overall goal is **how to reduce Azure Sentinel data ingestion-related costs?.**
- Sentinel usage cost is based on data ingestion in: Azure Sentinel and LogAnalytics (LA).
- More info on Azure Sentinel ingestion at https://azure.microsoft.com/en-us/pricing/details/azure-sentinel/
- More info on LogAnalytics ingestion at https://azure.microsoft.com/en-us/pricing/details/monitor/
- Both ingestion models (For Sentinel and LA) give discount for data reservation.
- PROBLEM: as both models are different, to discover a precise estimated price is difficult/variable.

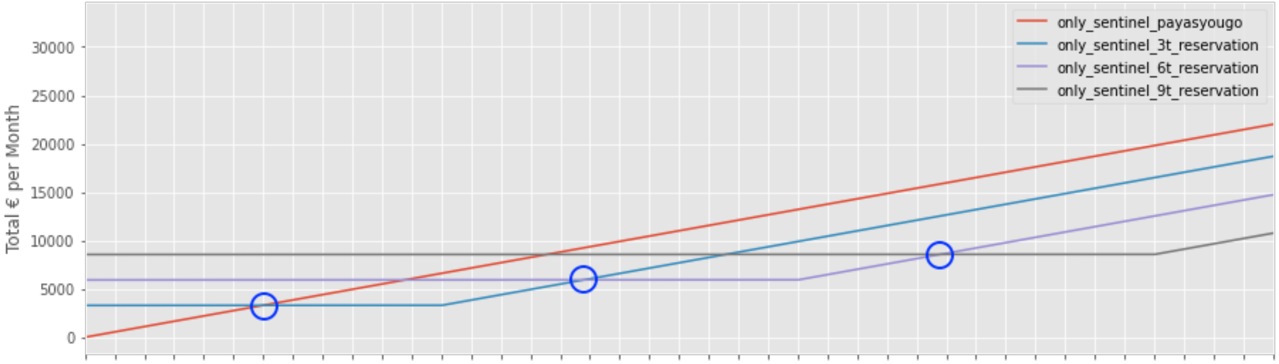
The following slides cover:

- When should you reserve data in Sentinel and LA?
- How much will you pay per month if we reserve data?
- How much cost each GB when you reserve logs in Sentinel and LA?
- Can we trust the Azure Calculator?

WHEN SHOULD YOU RESERVE DATA IN SENTINEL AND LA?

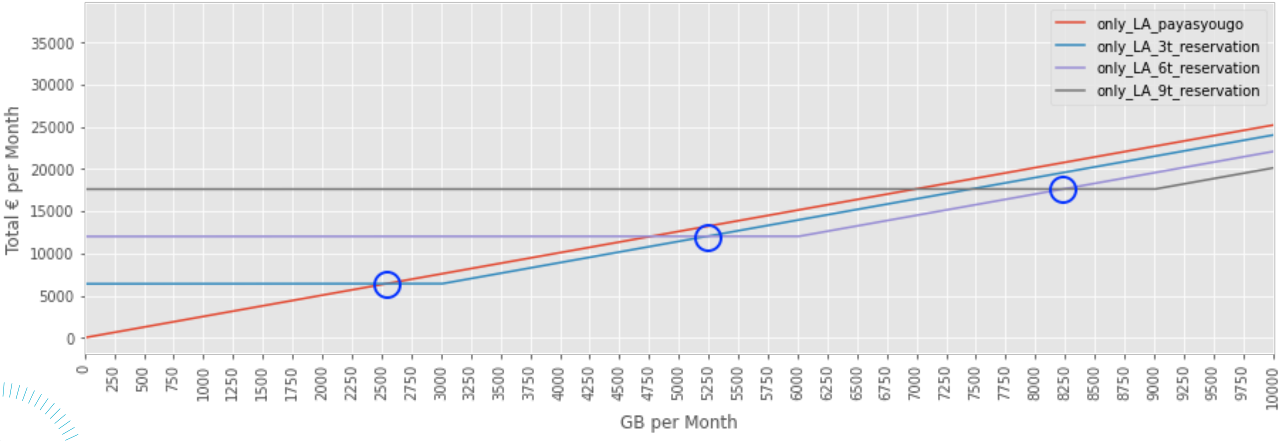
Price/month per GB/month

Based on: https://azure.microsoft.com/en-us/pricing/details/azure-sentinel/ (West Europe)



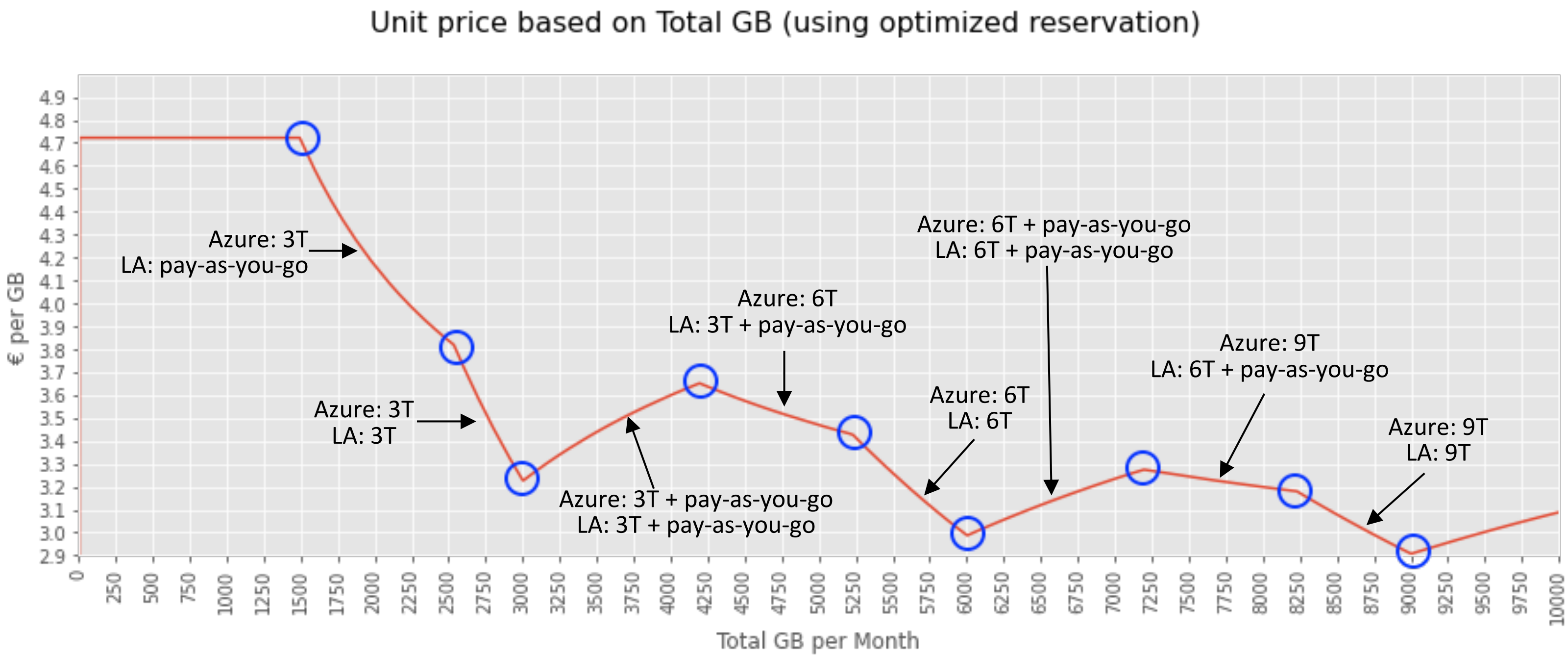
- From 1495GB it is cheaper to use 3T reservation (100GB/day)
- From 4196GB it is cheaper to use 6T reservation (200GB/day)
- From 7196GB it is cheaper to use 9T reservation (300GB/day)

Based on: https://azure.microsoft.com/en-us/pricing/details/monitor/ (West Europe)



- From 2536GB it is cheaper to use 3T reservation (100GB/day)
- From 5231GB it is cheaper to use 6T reservation (200GB/day)
- From 8231GB it is cheaper to use 9T reservation (300GB/day)

HOW MUCH COST EACH GB WHEN I RESERVE LOGS IN SENTINEL AND LA?



Unit price based on Total GB (using optimized reservation)

Azure: 3T
LA: pay-as-you-go

Azure: 3T
LA: 3T

Azure: 3T + pay-as-you-go
LA: 3T + pay-as-you-go

Azure: 6T
LA: 3T + pay-as-you-go

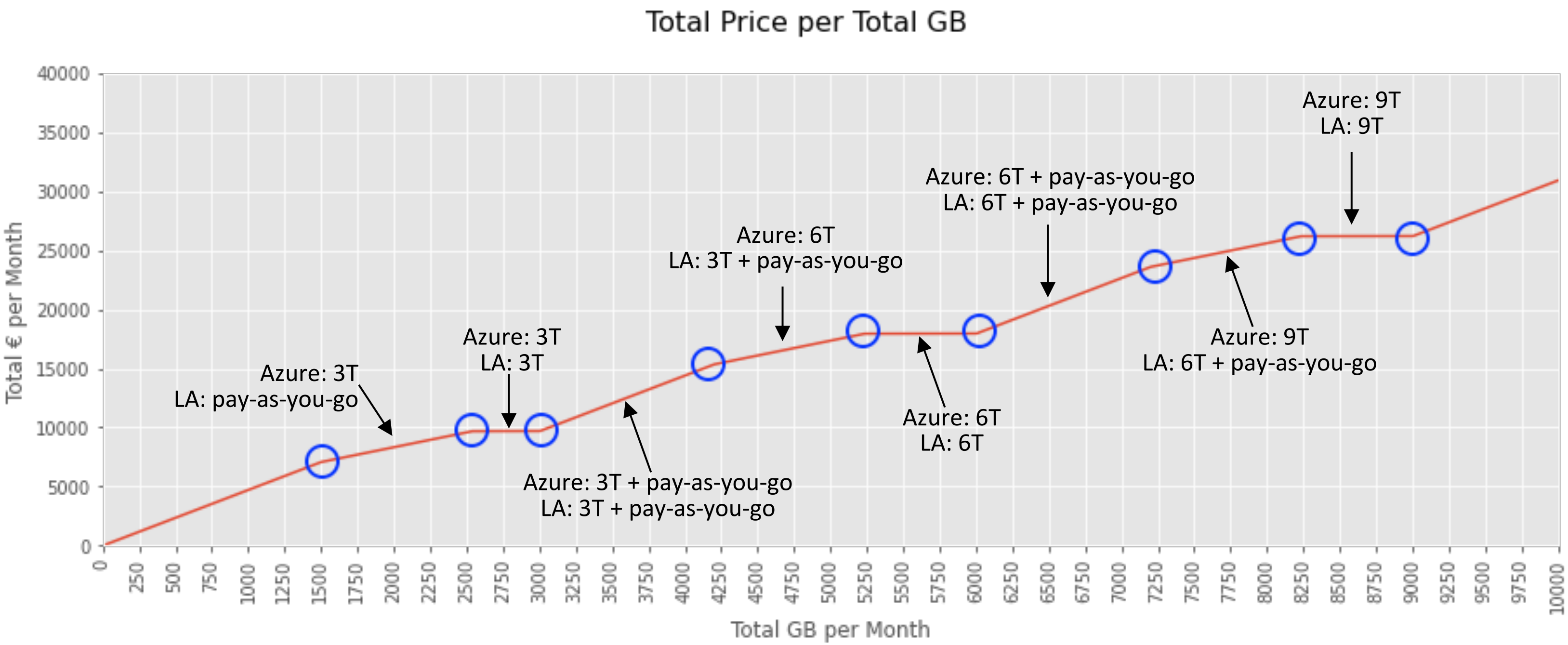
Azure: 6T
LA: 6T

Azure: 6T + pay-as-you-go
LA: 6T + pay-as-you-go

Azure: 9T
LA: 6T + pay-as-you-go

Azure: 9T
LA: 9T

HOW MUCH WE WILL PAY PER MONTH IF WE RESERVE DATA?



Azure: 9T
LA: 9T

Azure: 6T + pay-as-you-go
LA: 6T + pay-as-you-go

Azure: 6T
LA: 3T + pay-as-you-go

Azure: 3T
LA: 3T

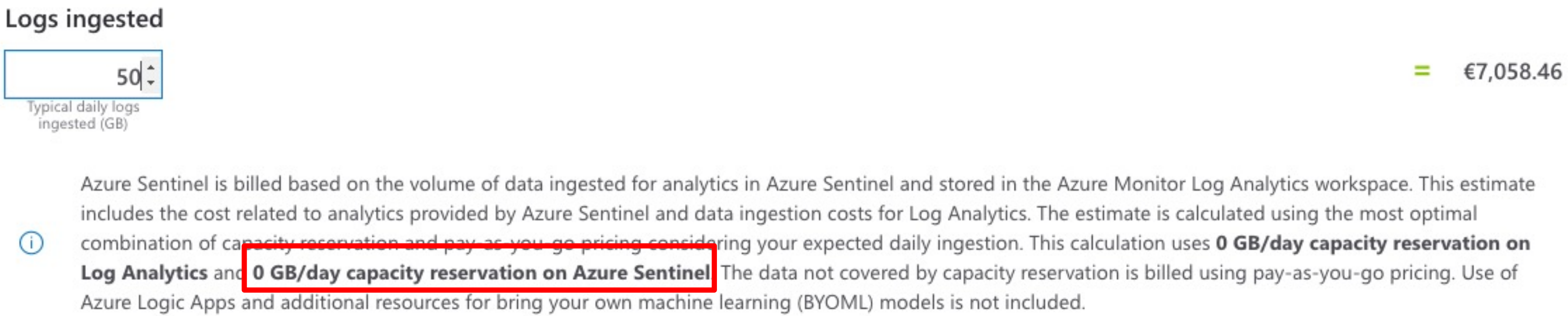
Azure: 9T
LA: 6T + pay-as-you-go

Azure: 3T
LA: pay-as-you-go

Azure: 6T
LA: 6T

Azure: 3T + pay-as-you-go
LA: 3T + pay-as-you-go

CAN WE TRUST THE AZURE CALCULATOR? (SOME ERROS)



Logs ingested

50

Typical daily logs ingested (GB)

= €7,058.46

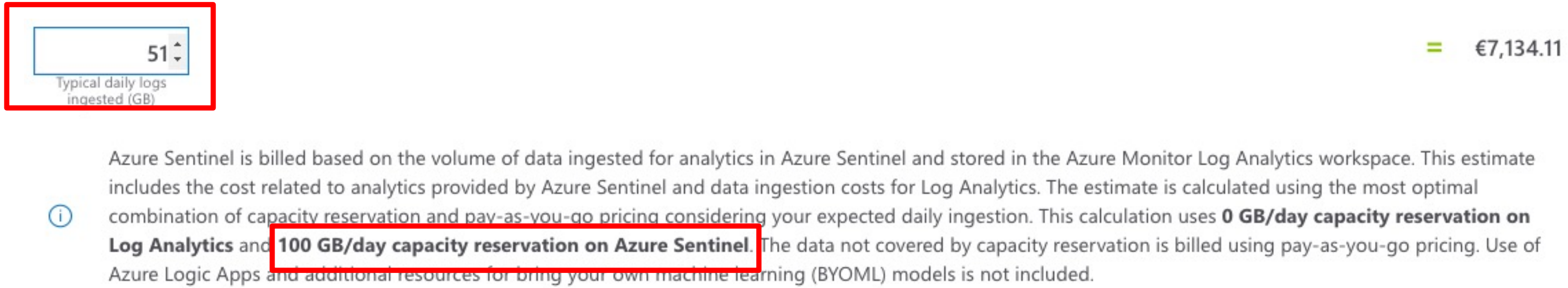
Azure Sentinel is billed based on the volume of data ingested for analytics in Azure Sentinel and stored in the Azure Monitor Log Analytics workspace. This estimate includes the cost related to analytics provided by Azure Sentinel and data ingestion costs for Log Analytics. The estimate is calculated using the most optimal combination of capacity reservation and pay-as-you-go pricing considering your expected daily ingestion. This calculation uses **0 GB/day capacity reservation on Log Analytics** and **0 GB/day capacity reservation on Azure Sentinel**. The data not covered by capacity reservation is billed using pay-as-you-go pricing. Use of Azure Logic Apps and additional resources for bring your own machine learning (BYOML) models is not included.

With pay-as-you-go: 50*30days* €2.20 = 3.300

With 100GB/day reservation: 30days* €109.63 = 3.288,9

Magic number?!

50*30*2,1926=3.288,9



51

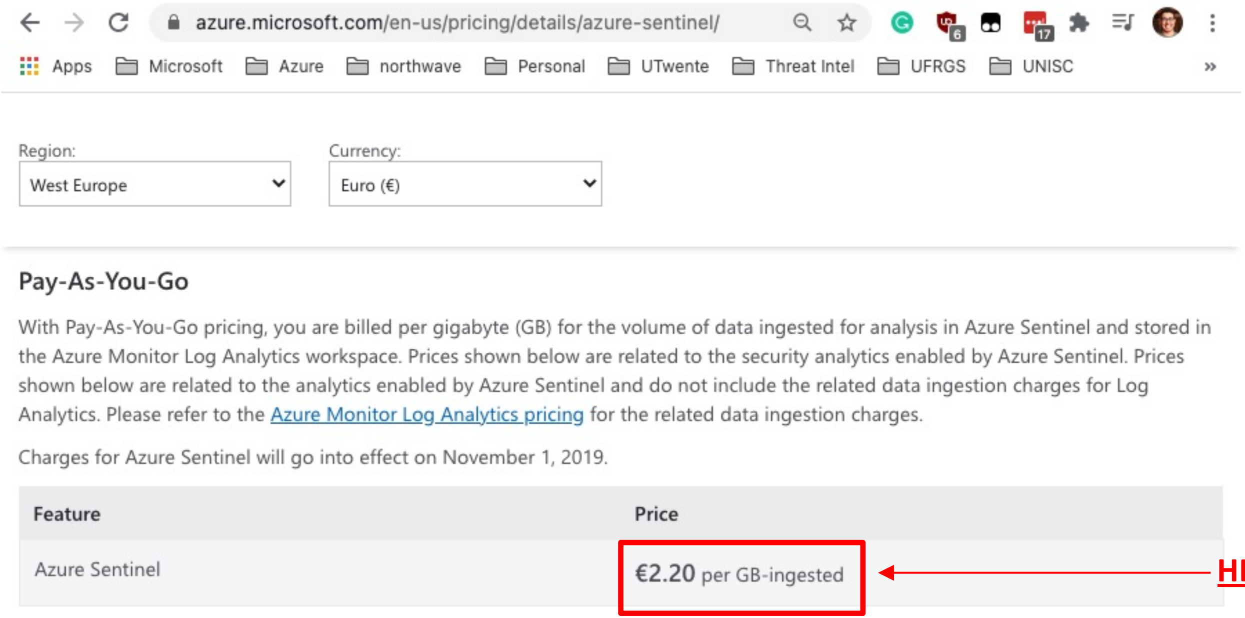
Typical daily logs ingested (GB)

= €7,134.11

Azure Sentinel is billed based on the volume of data ingested for analytics in Azure Sentinel and stored in the Azure Monitor Log Analytics workspace. This estimate includes the cost related to analytics provided by Azure Sentinel and data ingestion costs for Log Analytics. The estimate is calculated using the most optimal combination of capacity reservation and pay-as-you-go pricing considering your expected daily ingestion. This calculation uses **0 GB/day capacity reservation on Log Analytics** and **100 GB/day capacity reservation on Azure Sentinel**. The data not covered by capacity reservation is billed using pay-as-you-go pricing. Use of Azure Logic Apps and additional resources for bring your own machine learning (BYOML) models is not included.

The same applies to LA price

CAN WE TRUST THE AZURE CALCULATOR? (SOME ERROS)



Region: West Europe

Currency: Euro (€)

Pay-As-You-Go

With Pay-As-You-Go pricing, you are billed per gigabyte (GB) for the volume of data ingested for analysis in Azure Sentinel and stored in the Azure Monitor Log Analytics workspace. Prices shown below are related to the security analytics enabled by Azure Sentinel. Prices shown below are related to the analytics enabled by Azure Sentinel and do not include the related data ingestion charges for Log Analytics. Please refer to the Azure Monitor Log Analytics pricing for the related data ingestion charges.

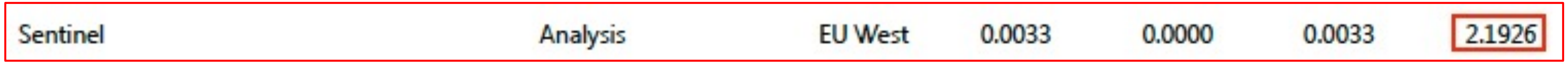
Charges for Azure Sentinel will go into effect on November 1, 2019.

Feature	Price
Azure Sentinel	€2.20 per GB-ingested

HERE IS THE ERROR!

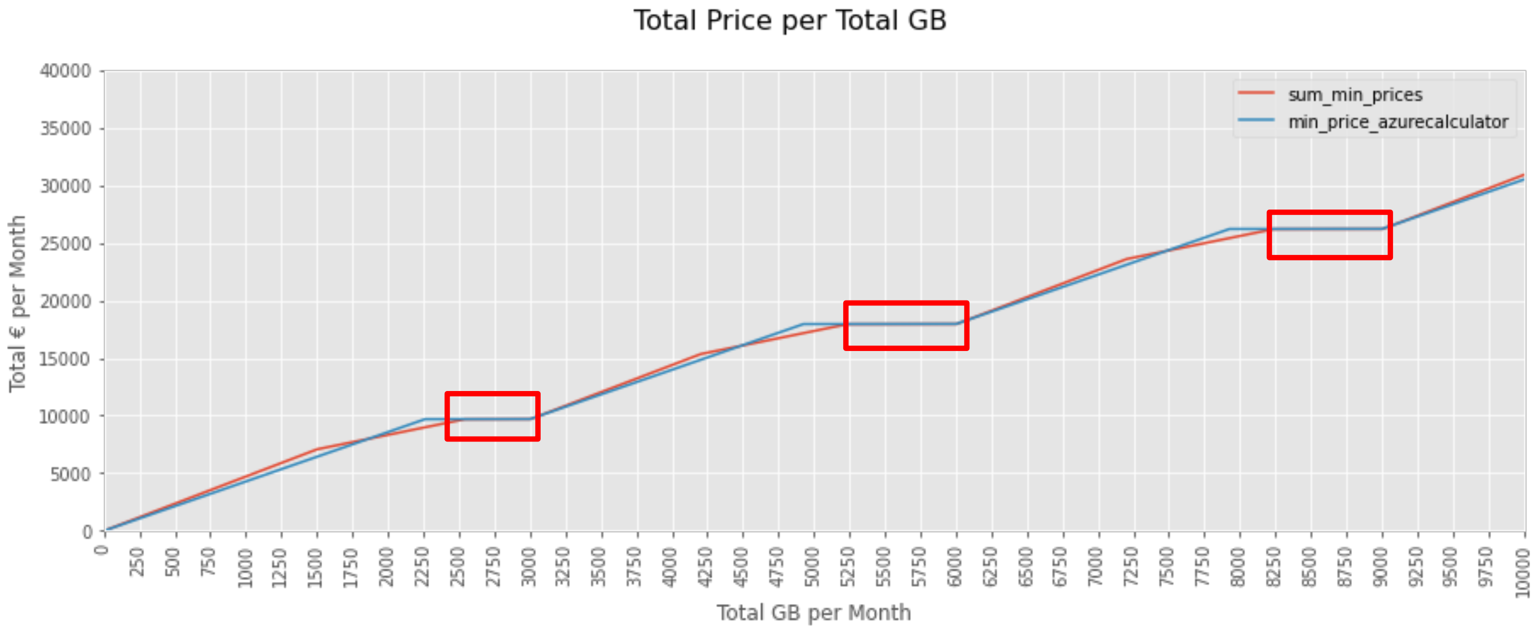
Real invoice!

Magic number!



Sentinel	Analysis	EU West	0.0033	0.0000	0.0033	2.1926

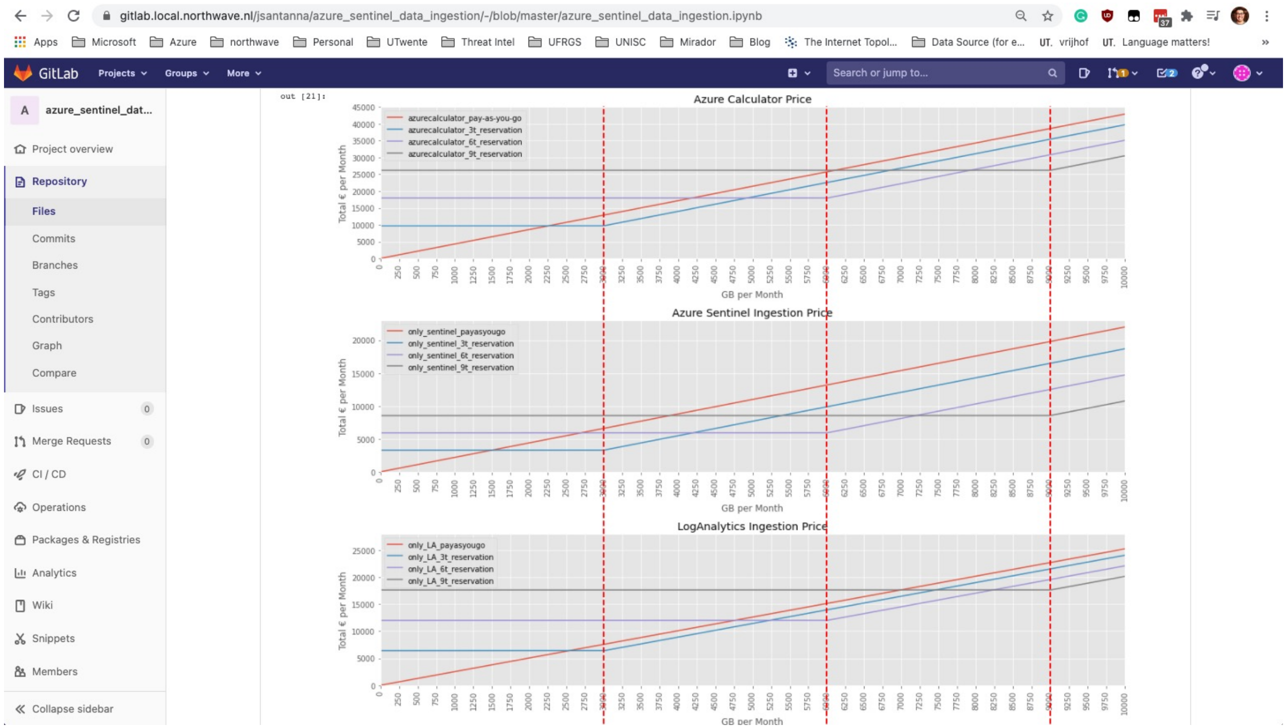
CAN WE TRUST THE AZURE CALCULATOR? (SOME ERROS)



This proves that, overall, we can trust the Azure Calculator!

It is not 100% but the error will be a couple of Euros in the end bill.

ALL OUR CALCULATIONS ARE PUBLICLY AVAILABLE



https://github.com/jjsantanna/sentinel_versus_azure_calculator
/blob/master/sentinel_versus_azure_calculator.ipynb

HOW TO ESTIMATE AND REDUCE AZURE SENTINEL DATA INGESTION COSTS? CAN WE TRUST AZURE CALCULATOR?

Jair Santanna (jair.santanna@northwave.nl)

16/04/2021