Monitoring Dell | Command Update with Modern Management

Integration Dell Management Tools in Microsoft Log Analytics

Author: Sven Riebe

Contents

Monitoring Dell Management Tools

We have been providing management tools to help manage a Dell client for many years. All these tools offer the possibility to query information via CLI (Command Line Interface) or GUI (Graphical User Interface). In this blog I will take a closer look at what you can do with this information in modern management. I will focus on a feature of the Microsoft Azure service called Log Analytics. We will look at how to collect relevant data from the clients and monitor it in the form of a dashboard. Microsoft Log Analytics is a paid service that charges depending on the amount of data, so I recommend checking the Microsoft license agreements before rebuilding my solution. The advantage I see in Log Analytics is that I can bring any data from a client into a custom table and then analyze it as needed. I will describe this and give you the

opportunity to use my PowerShell scripts and JSON (Java Script Object Notation) files for your environment.

Concept of Custom logging with Log Analytics

Microsoft Log Analytics has the possibility to process logs of other solutions. I will make use of this here. I build on a project from https://www.systanddeploy.com/ and use the functions for uploading to Log Analytics.

Click on the link to get more information about the setup of Log Analytics.

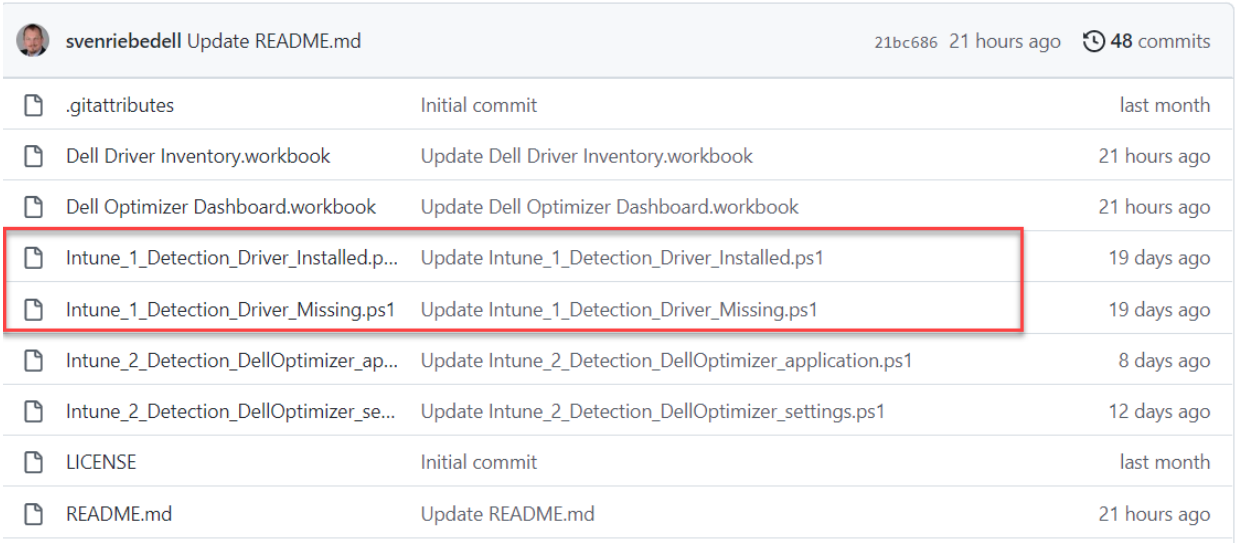
https://www.systanddeploy.com/2021/11/starting-with-log-analytics-part-1.html

https://www.systanddeploy.com/2022/05/starting-with-log-analytics-part-2.html

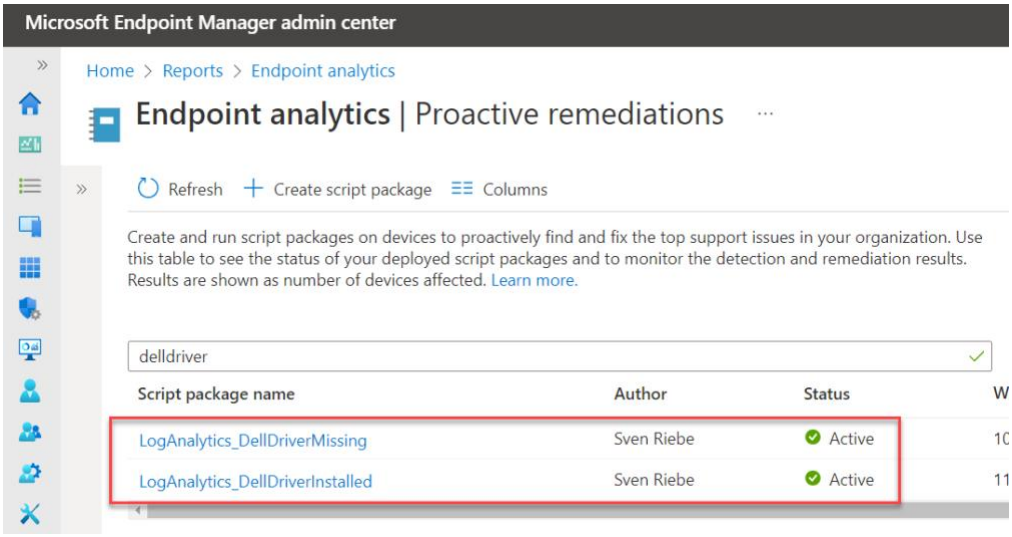
The platform is up and running and the upload works. Now I start with the adaptation of the scripts for the Dell Management Tools and create a script for the Dell Command Update to read the driver inventory and a script for the scan for new drivers.

You can find the scripts here on my GitHub repository.

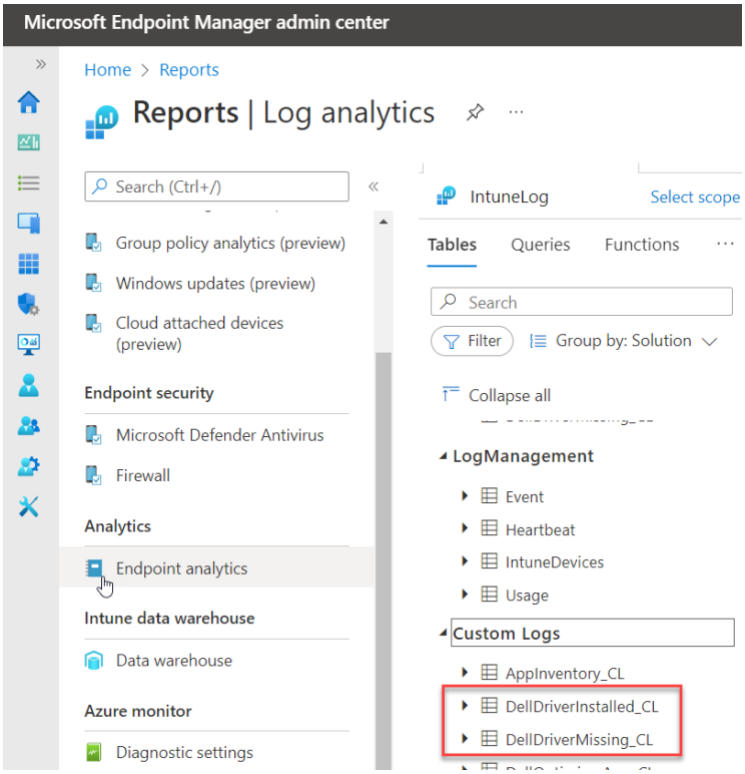
https://github.com/svenriebedell/LogAnalytics



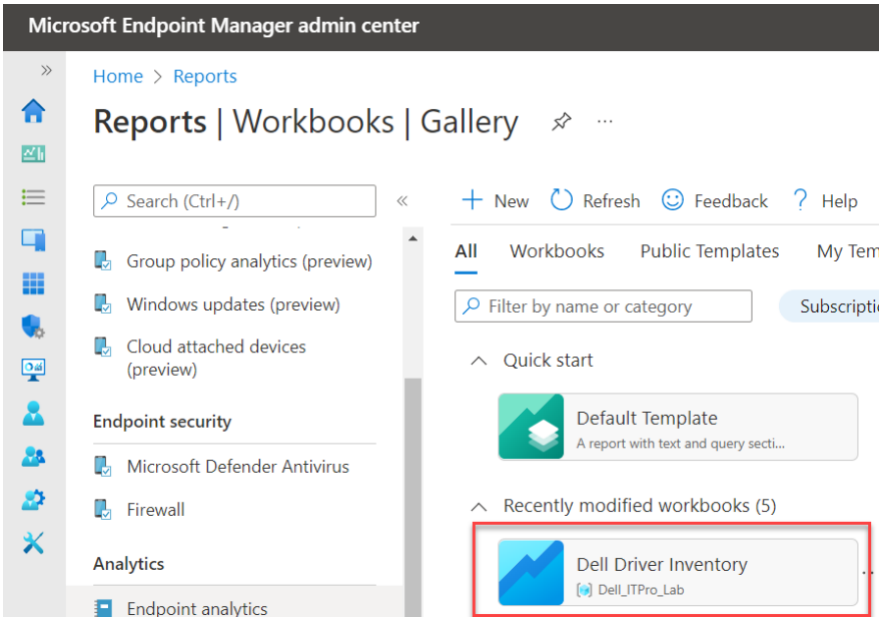
These scripts need to run regularly to request data from the device and then write it to the Custom Table in Log Analytics. In my case, I use the Microsoft Endpoint Manager - Endpoint Analytics feature and run both scripts as remediation once a day. (Since the update catalog is not updated daily, other times can be set).



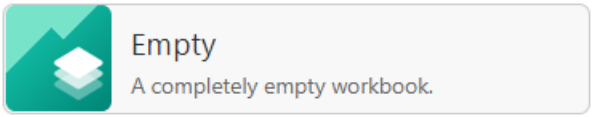
Provided the script runs correctly, please remember to install the Dell Command Update beforehand, we will have new tables available.



This data can now be queried via KQL (Kusto Query Language) Query or, best of all, converted into a dashboard for administrators.



If you have not done so yet, click Empty and create a new dashboard.

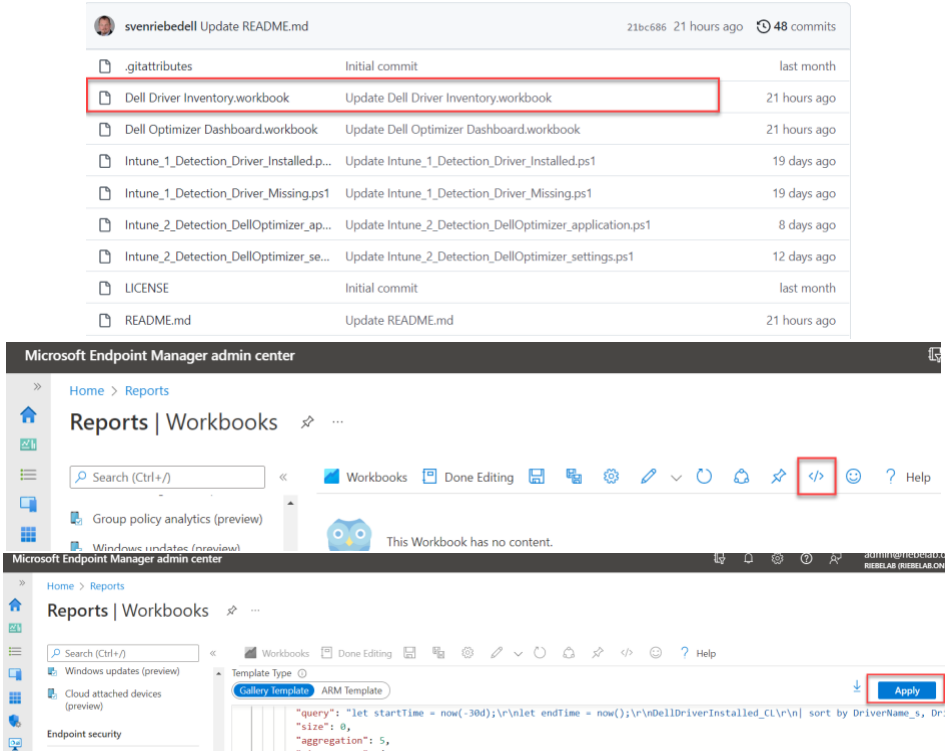


The necessary design with queries can also be found on GitHub and only needs to be copied and pasted. Direct import of a workbook is currently not yet available in the UI (User Interface).

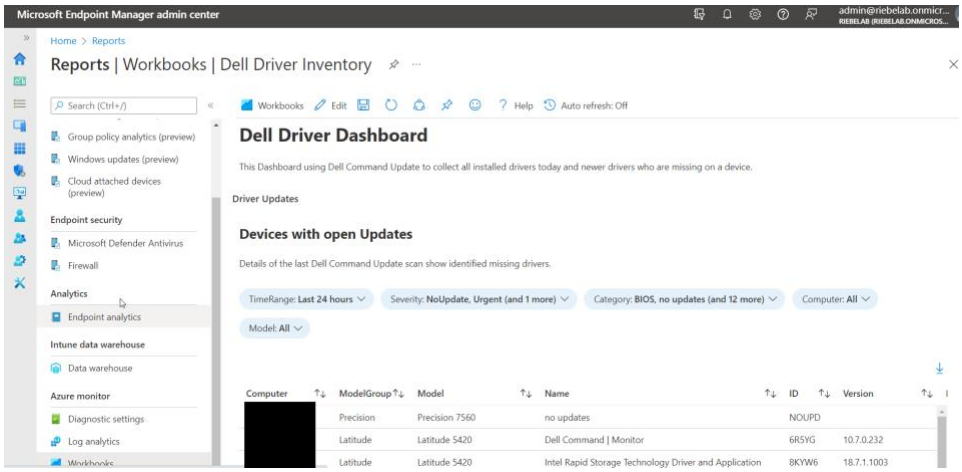
Click ‘</>’

Copy and Paste Full text of Dell Driver Inventory.workbook to replace existing line

Click ‘Apply’



The Dell Driver Dashboard is just ready to use. You can still refine the results with filters or customize the KQL queries to create other views.



Process generates a Dashboard

Collect Data

- Using PowerShell Script
- Script running as Detection script in Microsoft Endpoint Manager on regular base.
- Alternative by Task planer or other solutions

Transform to JSON

- Same PowerShell script transform Array to JSON

Upload to Log Analytics

- Same PowerShell script upload data (you need a resource ID from Log Analytics)

Generate Custom Table

- Generated by Log Analytics based on JSON File

Build a query set and save

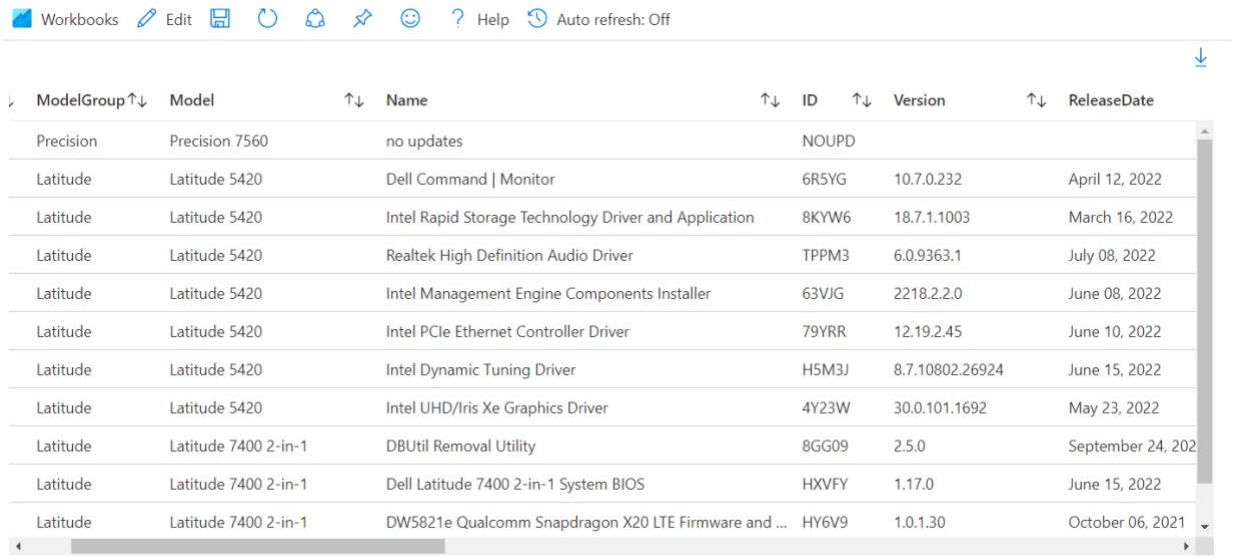
- Using KQL queries and save as Workbook for later monitoring

Explaining the dashboard

The dashboard has two main parts.

1. open/missing updates
2. existing drivers.

In the first part of the missing updates, we use the data from the scan engine of Dell Command Update. Based on the package IDs we search the Device Update catalog for the other information like version, release date, category, etc. which is all relevant information for this driver.



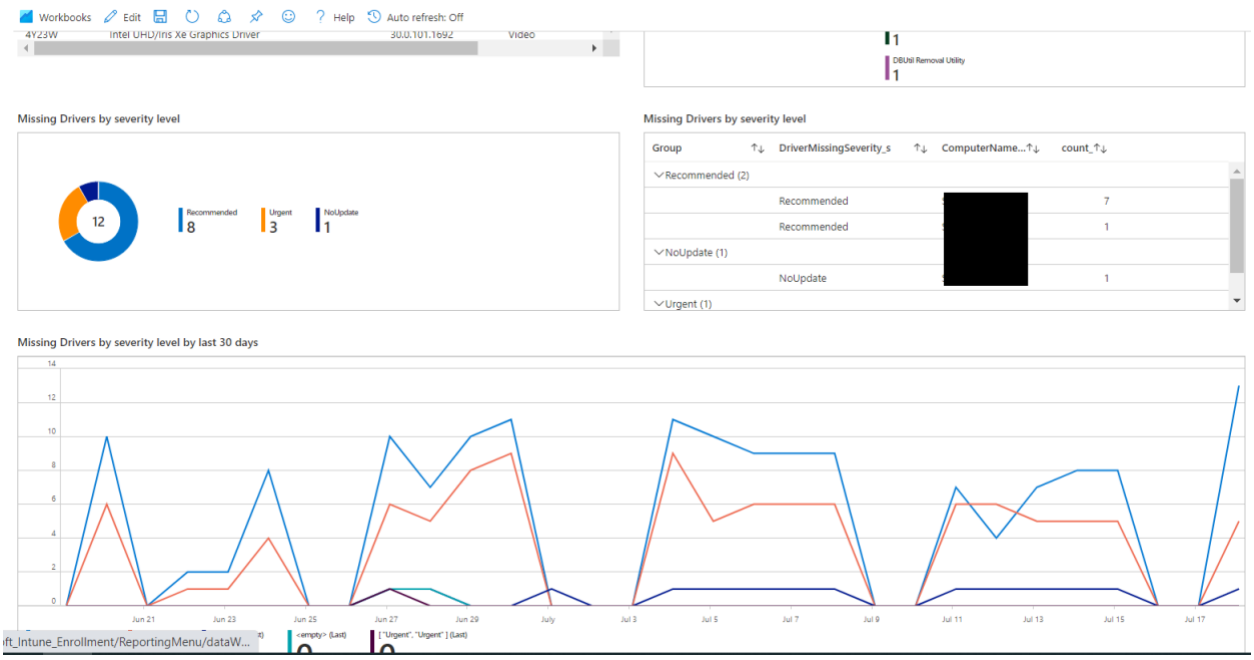
ModelGroup	Model	Name	ID	Version	ReleaseDate
Precision	Precision 7560	no updates	NOUPD		
Latitude	Latitude 5420	Dell Command | Monitor	6R5YG	10.7.0.232	April 12, 2022
Latitude	Latitude 5420	Intel Rapid Storage Technology Driver and Application	8KYW6	18.7.1.1003	March 16, 2022
Latitude	Latitude 5420	Realtek High Definition Audio Driver	TPPM3	6.0.9363.1	July 08, 2022
Latitude	Latitude 5420	Intel Management Engine Components Installer	63VJG	2218.2.2.0	June 08, 2022
Latitude	Latitude 5420	Intel PCIe Ethernet Controller Driver	79YRR	12.19.2.45	June 10, 2022
Latitude	Latitude 5420	Intel Dynamic Tuning Driver	H5M3J	8.7.10802.26924	June 15, 2022
Latitude	Latitude 5420	Intel UHD/Iris Xe Graphics Driver	4Y23W	30.0.101.1692	May 23, 2022
Latitude	Latitude 7400 2-in-1	DBUtil Removal Utility	8GG09	2.5.0	September 24, 202
Latitude	Latitude 7400 2-in-1	Dell Latitude 7400 2-in-1 System BIOS	HXVFY	1.17.0	June 15, 2022
Latitude	Latitude 7400 2-in-1	DW5821e Qualcomm Snapdragon X20 LTE Firmware and ...	HY6V9	1.0.1.30	October 06, 2021

Since we use the scan engine of the Dell Command Update, we can also detect missing firmware updates for docking stations via this path if one is connected to the device during the scan.

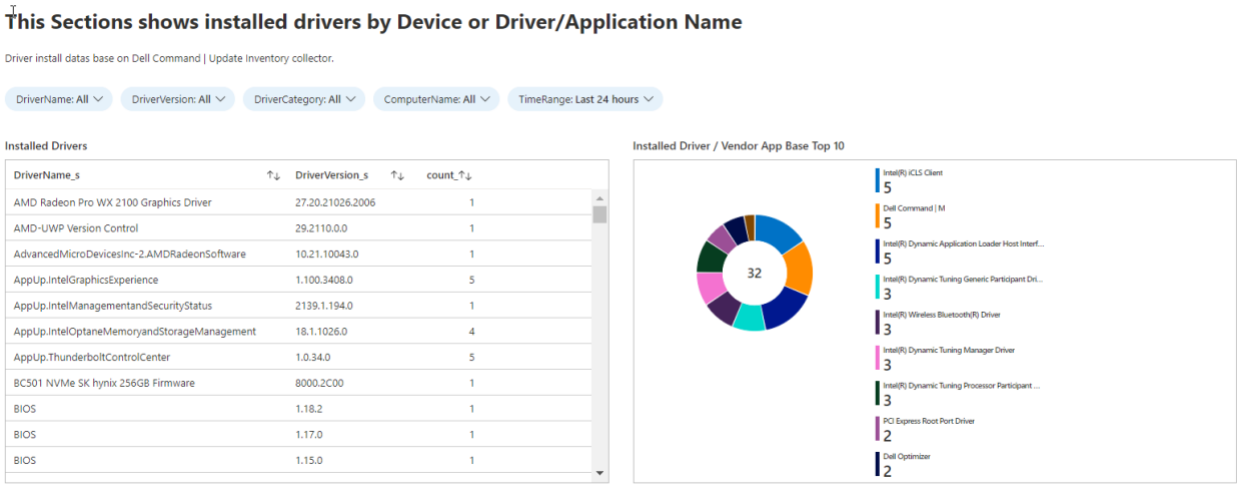
If a device has no updates that need to be installed, the driver name "no updates" appears.

ModelGroup	Model	Name	ID	Version	ReleaseDate
Precision	Precision 7560	no updates	NOUPD		

The Update section includes a couple of other useful Grids and Views.



To make good decisions when analyzing errors, it is important to know the basis of the client. Dell Command Update brings an inventory collector with the data we have with the second script also in a table. Here we can tell which driver is installed in which version or was installed x-days ago. With other grids and charts this area gives a good overview of the actual situation of the client.



Thx for reading. I hope you have enjoyed it, and I am happy to hear your feedback and ideas. 😊

The next Log Analytics projects you will be able to find here in this blog. I am planning a Dashboard for Dell Optimizer and Dell BIOS (Basic Input Output System) Settings/Security in the next step.