



TunedIn:London

Meetup
8th December 2023



Intune Custom Reporting: Where is my SSRS!?

- How it started – Configuration Manager
- How its going - Intune Reporting
 - Monitoring
 - Reporting
 - Endpoint Analytics
- Custom Reporting
 - Diagnostic settings
 - Custom tables
- KQL Queries & Workbooks



TunedIn:London



8th December 2023

About Me (Maurice Daly)



Principal Cloud Architect with CloudWay

Microsoft MVP (Enterprise Mobility) since 2017

Microsoft Certified Trainer since 2020

Blog: MSEndpointMgr(<https://www.msendpointmgr.com>)

X (Twitter):@MoDaly_IT

Focus on endpoint management, through automation including tools such as PowerShell, Graph, and Azure automation.

Formula 1 nut.. and “car enthusiast”

How it started – Configuration Manager

- Configuration Manager
 - Primary endpoint management solution for decades
 - Extensive and extendable in-built reporting
 - Full control over WMI collection
 - SQL queries enabled admins to pull the data they wanted and feed this to Excel/PowerBI etc

The screenshot displays two windows from the Microsoft Configuration Manager interface. The top window, titled 'Lab Client Settings', shows a list of 'Hardware Inventory Classes' with checkboxes. Several checkboxes are checked, including '1394 Controller (Win32_1394Controller)', 'ActiveSync Service (SMS_ActiveSyncService)', 'AMT Agent (SMS_AMTObject)', 'AppV Client Application (AppClientApplication)', 'AppV Client Package (AppClientPackage)', 'AutoStart Software - Asset Intelligence (SMS_AutoStartSoftware)', 'BaseBoard (Win32_BaseBoard)', 'Battery (Win32_Battery)', 'BitLocker Encryption Details (Win32_BitLockerEncryptionDetails)', 'BitLocker Policy (Win32Reg_MBAMPolicy)', 'Boot Configuration (Win32_BootConfiguration)', and 'Browser Helper Object - Asset Intelligence (SMS_BrowserHelperObject)'. The bottom window is a 'SQL Server Reporting Services' report titled 'Computer operating system version history'. It shows a table with columns: NetBIOS Name, Time Stamp, Operating System, Version, CSD Version, Install Date, Last Boot Up Time, Windows Directory, and Description. The table lists several entries for the computer 'LAB-SCCM', showing different operating system versions and installation dates.

NetBIOS Name	Time Stamp	Operating System	Version	CSD Version	Install Date	Last Boot Up Time	Windows Directory	Description
LAB-SCCM	11/24/2023 3:07:38 PM	Microsoft Windows Server 2016 Standard	10.0.14393		6/5/2018 12:36:24 PM	11/24/2023 3:03:16 PM	C:\Windows	
LAB-SCCM	11/19/2023 12:44:22 PM	Microsoft Windows Server 2016 Standard	10.0.14393		6/5/2018 12:36:24 PM	11/19/2023 10:39:36 AM	C:\Windows	
LAB-SCCM	11/13/2023 11:53:25 AM	Microsoft Windows Server 2016 Standard	10.0.14393		6/5/2018 12:36:24 PM	11/13/2023 9:37:14 AM	C:\Windows	
LAB-SCCM	11/3/2023 4:14:57 PM	Microsoft Windows Server 2016 Standard	10.0.14393		6/5/2018 12:36:24 PM	11/3/2023 9:00:43 AM	C:\Windows	
LAB-SCCM	10/31/2023 2:17:24 PM	Microsoft Windows Server 2016 Standard	10.0.14393		6/5/2018 12:36:24 PM	10/31/2023 1:54:45 PM	C:\Windows	
LAB-SCCM	10/20/2023 12:40:56 PM	Microsoft Windows Server 2016 Standard	10.0.14393		6/5/2018 12:36:24 PM	10/20/2023 7:21:20 AM	C:\Windows	
LAB-SCCM	10/16/2023 11:49:17 AM	Microsoft Windows Server 2016 Standard	10.0.14393		6/5/2018 12:36:24 PM	10/16/2023 7:40:32 AM	C:\Windows	
LAB-SCCM	10/10/2023 2:48:21 PM	Microsoft Windows Server 2016 Standard	10.0.14393		6/5/2018 12:36:24 PM	10/10/2023 8:00:07 AM	C:\Windows	
LAB-SCCM	10/2/2023 9:33:23	Microsoft Windows Server	10.0.14393		6/5/2018	10/2/2023 7:46:16 AM	C:\Windows	

How it started – Configuration Manager

Report name	Description
Computers with a specific hard disk size	Displays a list of computers that have hard disks of a specified size.
Computers with low free disk space (less than specified % free)	Displays a list of computers in a specified collection that have less than the specified free disk space.
Computers with low free disk space (less than specified MB free)	Displays a list of computers and disks where the disks are low on space. The amount of free space to check for is specified in MB.
Count physical disk configurations	Displays the number of hard disks inventoried by disk capacity.
Disk information for a specific computer - Logical disks	Displays summary information about the logical disks on a specified computer.
Disk information for a specific computer - Partitions	Displays summary information about the disk partitions on a specified computer.
Disk information for a specific computer - Physical disks	Displays summary information about the physical disks on a specified computer.
History - Logical disk space history for a specific computer	Displays the inventory history for logical disk drives on a specified computer.

[List of reports - Configuration Manager | Microsoft Learn](#)



TunedIn: London

Report name	Description
Hardware 01A - Summary of computers in a specific collection	Displays an Asset Intelligence summary view of computers in a collection you specify.
Hardware 03A - Primary computer users	Displays users and the count of computers on which they're the primary user.
Hardware 03B - Computers for a specific primary console user	Displays all computers for which a specified user is the primary console user.
Hardware 04A - Computers with multiple users (shared)	Displays computers that don't have a primary user because no one user has a signed-in time greater than 66%.
Hardware 05A - Console users on a specific computer	Displays all of the console users on a specified computer.
Hardware 06A - Computers for which console users could not be determined	Helps administrative users identify computers that need to have security logging turned on.
Hardware 07A - USB devices by manufacturer	Displays USB devices, grouped by manufacturer.
Hardware 07B - USB devices by manufacturer and description	Displays USB devices, grouped by manufacturer and description.
Hardware 07C - Computers with a specific USB device	Displays all the computers with a specified USB device.
Hardware 07D - USB devices on a specific computer	Displays all USB devices on a specified computer.
Hardware 08A - Hardware that is not ready for a software upgrade	Displays hardware that doesn't meet the minimum hardware requirements.
Hardware 09A - Search for computers	Displays a summary of computers matching keyword filters. These filters are computer name, Configuration Manager site, domain, top console user, operating system, manufacturer, or model.
Hardware 10A - Computers in a specified collection that have changed during a specified timeframe	Displays a list of computers in a specified collection where a hardware class has changed during a specified time period.
Hardware 10B - Changes on a specified computer within a specified timeframe	Displays the classes that have changed on a specified computer within a specified time period.
License 01A - Microsoft Volume License ledger for Microsoft license statements	Displays an inventory of all Microsoft software titles that are available from the Microsoft Volume Licensing program.
License 01B - Microsoft Volume License ledger item by sales channel	Identifies and displays sales channel for inventoried Microsoft Volume License software.
License 01C - Computers with a specific Microsoft Volume License ledger item and sales channel	Identifies and displays computers that have a specified item from the Microsoft Volume license ledger.
License 01D - Microsoft Volume License ledger products on a specific computer	Identifies and displays all Microsoft Volume license ledger items on a specified computer.
License 02A - Count of licenses nearing expiration by time ranges	Displays a count of licenses nearing expiration by a specified time range. The displayed products have their licenses managed by the Software Licensing Service.
License 02B - Computers with licenses nearing expiration	Displays the specified computers with licenses that are nearing expiration.
License 02C - License information on a specific computer	Displays products on a specified computer that have their



mber 2023

How it started – Configuration Manager

Report name	Description
Computers with a specific hard disk size	Displays a list of computers that have hard disks of a specified size.
Computers with low free disk space (less than specified % free)	Displays a list of computers in a specified collection that have less than the specified free disk space.
Computers with low free disk space (less than specified MB free)	Displays a list of computers and disks where the disks are low on space. The amount of free space to check for is specified in MB.
Count physical disk configurations	Displays the number of hard disks inventoried by disk capacity.
Disk information for a specific computer - Logical disks	Displays summary information about the logical disks on a specified computer.
Disk information for a specific computer - Partitions	Displays summary information about the disk partitions on a specified computer.
Disk information for a specific computer - Physical disks	Displays summary information about the physical disks on a specified computer.
History - Logical disk space history for a specific computer	Displays the inventory history for logical disk drives on a specified computer.

[List of reports - Configuration Manager | Microsoft Learn](#)



TunedIn: London

Report name	Description
Hardware 01A - Summary of computers in a specific collection	Displays an Asset Intelligence summary view of computers in a collection you specify.
Hardware 03A - Primary computer users	Displays users and the count of computers on which they're the primary user.
Hardware 03B - Computers for a specific primary console user	Displays all computers for which a specified user is the primary console user.
Hardware 04A - Computers with multiple users (shared)	Displays computers that don't have a primary user because no one user has a signed-in time greater than 66%.
Hardware 05A - Console users on a specific computer	Displays all of the console users on a specified computer.
Hardware 06A - Computers for which console users could not be determined	Helps administrative users identify computers that need to have security logging turned on.
Hardware 07A - USB devices by manufacturer	Displays USB devices, grouped by manufacturer.
Hardware 07B - USB devices by manufacturer and description	Displays USB devices, grouped by manufacturer and description.
Hardware 07C - Computers with a specific USB device	Displays all the computers with a specified USB device.
Hardware 07D - USB devices on a specific computer	Displays all USB devices on a specified computer.
Hardware 08A - Hardware that is not ready for a software upgrade	Displays hardware that doesn't meet the minimum hardware requirements.
Hardware 09A - Search for computers	Displays a summary of computers matching keyword filters. These filters are computer name, Configuration Manager site, domain, top console user, operating system, manufacturer, or model.
Hardware 10A - Computers in a specified collection that have changed during a specified timeframe	Displays a list of computers in a specified collection where a hardware class has changed during a specified time period.
Hardware 10B - Changes on a specified computer within a specified timeframe	Displays the classes that have changed on a specified computer within a specified time period.
License 01A - Microsoft Volume License ledger for Microsoft license statements	Displays an inventory of all Microsoft software titles that are available from the Microsoft Volume Licensing program.
License 01B - Microsoft Volume License ledger item by sales channel	Identifies and displays sales channel for inventoried Microsoft Volume License software.
License 01C - Computers with a specific Microsoft Volume License ledger item and sales channel	Identifies and displays computers that have a specified item from the Microsoft Volume license ledger.
License 01D - Microsoft Volume License ledger products on a specific computer	Identifies and displays all Microsoft Volume license ledger items on a specified computer.
License 02A - Count of licenses nearing expiration by time ranges	Displays a count of licenses nearing expiration by a specified time range. The displayed products have their licenses managed by the Software Licensing Service.
License 02B - Computers with licenses nearing expiration	Displays the specified computers with licenses that are nearing expiration.
License 02C - License information on a specific computer	Displays products on a specified computer that have their



mber 2023

How it started – Configuration Manager

Report name	Description
Computers with a specific hard disk size	Displays a list of computers that have hard disks of a specified size.
Computers with low free disk space (less than	Displays a list of computers in a specified

Report name	Description
Hardware 01A - Summary of computers in a specific collection	Displays an Asset Intelligence summary view of computers in a collection you specify.
Hardware 03A - Primary computer users	Displays users and the count of computers on which they're the primary user.

Hardware 03B - Computers for a specific primary console

471 Built-In Reports

Physical disks	physical disks on a specified computer.
History - Logical disk space history for a specific computer	Displays the inventory history for logical disk drives on a specified computer.

[List of reports - Configuration Manager | Microsoft Learn](#)

Hardware 10A - Computers in a specified collection that have changed during a specified timeframe	Displays a list of computers in a specified collection where a hardware class has changed during a specified time period.
Hardware 10B - Changes on a specified computer within a specified timeframe	Displays the classes that have changed on a specified computer within a specified time period.
License 01A - Microsoft Volume License ledger for Microsoft license statements	Displays an inventory of all Microsoft software titles that are available from the Microsoft Volume Licensing program.
License 01B - Microsoft Volume License ledger item by sales channel	Identifies and displays sales channel for inventoried Microsoft Volume License software.
License 01C - Computers with a specific Microsoft Volume License ledger item and sales channel	Identifies and displays computers that have a specified item from the Microsoft Volume license ledger.
License 01D - Microsoft Volume License ledger products on a specific computer	Identifies and displays all Microsoft Volume license ledger items on a specified computer.
License 02A - Count of licenses nearing expiration by time ranges	Displays a count of licenses nearing expiration by a specified time range. The displayed products have their licenses managed by the Software Licensing Service.
License 02B - Computers with licenses nearing expiration	Displays the specified computers with licenses that are nearing expiration.
License 02C - License information on a specific computer	Displays products on a specified computer that have their

How it started – Configuration Manager

- (What were) the benefits of SQL Reporting Services
 - Ability to customise the look and feel of your reports
 - Corporate branding
 - Exportable Code
 - Allowing you to copy to other environments
 - Community Support
 - Shared repositories
 - Multiple resources available to Configuration Manager admins
 - No code writing (if that is not your thing)
 - Internal Sharing
 - Linked / shared rights to reports



TunedIn:London



8th December 2023

How its going – Microsoft Intune

- **Intune native reporting**
 - Monitoring node(s)
 - Device Monitors
 - Application Monitors
 - **Reports**
 - Generated via API pulls
 - **Endpoint Analytics**
 - Analytics based reporting on system behaviour



Exportable in CSV format
TunedIn:London



How its going – Microsoft Intune

- Intune native reporting

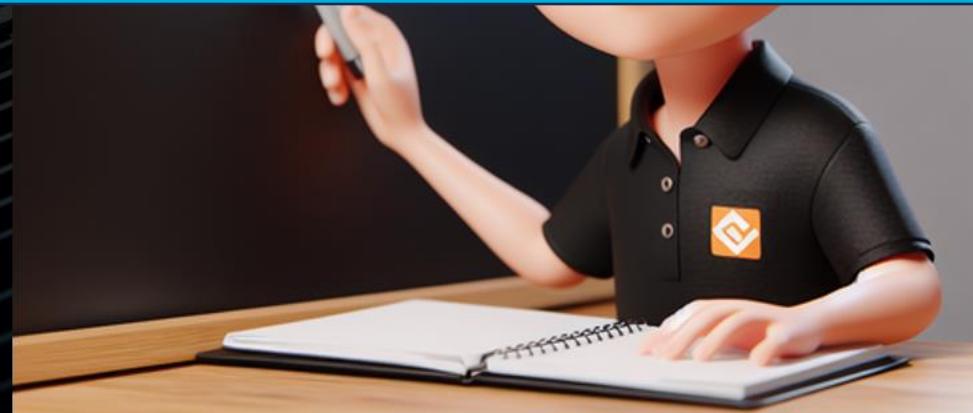


108 Built-In Reports

(I counted everything including summaries)

behaviour

- Exportable in CSV format



How its going – Microsoft Intune



The trouble with comparing
Apples with Oranges

- 471 reports in Configuration Manager
- 108 “reports” in Intune
- But how many reports do you actually use?
- Does Intune provide all the data you are looking for?



Realisation – Microsoft Intune Reporting

- Microsoft Intune provides reporting for general use scenarios
- Reports might be sufficient, but in most cases will never check all boxes
- Microsoft can't cover every scenario
- What can we do??
 - Complain about it (Check Reddit)
 - Enable co-management (Legacy FTW)
 - Get over it and do something better than the above..



Log Analytics – Your “SSRS Replacement”

- Log Analytics is a function within Azure that provides the ability to query datasets stored in tables..
This sounds familiar..
- Log Analytics uses a query language which provides the ability to cross reference and join tables for extensive datasets..
Also sounds familiar..
- Log Analytics provides the ability to export or link data from other platforms including Excel and PowerBI..
OK you get where I am going..



TunedIn:London



8th December 2023

Log Analytics – Your “SSRS Replacement”

Azure Monitor integration reports (Specialist)

You can customize your own reports to get the data you want. The data in your reports will optionally be available via Azure Monitor using Log Analytics and Azure Monitor workbooks. These solutions allow you to create custom queries, configure alerts, and make dashboards to show the device compliance data in the manner you want. Additionally, you can retain the activity logs in your Azure storage account, integrate with the reports using security information and event management (SIEM) tools, and correlate the reports to Microsoft Entra activity logs. Azure Monitor workbooks can be used in addition to importing dashboards for custom reporting needs.

ⓘ Note

Complex reporting functionality require an Azure subscription.

“Specialist”... Sounds like this is difficult

Probably means I need to be some kind of “rocket scientist” to use this..

Log Analytics – Your “SSRS Replacement”



You

Do you have to be a rocket scientist to use Azure log analytics?



ChatGPT

No, you don't have to be a rocket scientist to use Azure Log Analytics. Azure Log Analytics is a cloud-based service provided by Microsoft Azure that helps you collect and analyze data generated by resources in your cloud and on-premises environments. While it involves working with data and queries, you don't need an advanced technical background to get started.

Azure Log Analytics provides a user-friendly interface and query language for analyzing log data. The Query language used in Azure Log Analytics is called Kusto Query Language (KQL), and it's designed to be relatively easy to learn. You can use it to write queries to retrieve and analyze log data.





You

Do you have to be a rocket scientist to use Azure log analytics?



ChatGPT

No, you don't have to be a rocket scientist to use Azure Log Analytics. Azure Log Analytics is a cloud-based service provided by Microsoft Azure that helps you collect and analyze data generated by resources in your cloud and on-premises environments. While it involves working with data and queries, you don't need an advanced technical background to get started.

Azure Log Analytics provides a user-friendly interface and query language for analyzing log data. The Query language used in Azure Log Analytics is called Kusto Query Language (KQL), and it's designed to be relatively easy to learn. You can use it to write queries to retrieve and analyze log data.



Going custom – Microsoft Intune

- **Custom reporting is possible**
 - Step 1: Obtain contributor access to an Azure subscription / Resource group to create a Log Analytics Workspace.

Alternatively ask your Azure admin to provision a Log Analytics Workspace for you.

- Step 2: Enable Diagnostic Logging
- Step 3: Enable Windows Update Reports

- Now it's time to learn something new.. **KQL**



TunedIn:London



8th December 2023

Diagnostic Logging – Microsoft Intune

Diagnostic setting ...

Save Discard Delete Feedback

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. [Learn more about the different log categories and contents of those logs](#)

Diagnostic setting name IntuneDiags

Logs

Categories

- AuditLogs
- OperationalLogs
- DeviceComplianceOrg
- Devices
- Windows365AuditLogs

Destination details

Send to Log Analytics workspace

Subscription Microsoft

Log Analytics workspace (northeurope)

Archive to a storage account

Stream to an event hub

Send to partner solution

KQL Basics – Log Analytics

Writing queries in KQL is simpler than SQL (IMO)

- Start querying your data:
 - *Search*
 - *Where*
 - *Limit/Take*
 - *Count*
 - *Project*
 - *Distinct*
 - *Render*
 - *Order/Sort/Top*
 - *Summarize*

```
1 IntuneDevices
2 | project-away DeviceId
```

Results Chart

TimeGenerated [UTC]	OperationName	Result	DeviceName	UPN
> 07/12/2023, 04:07:41.240	Devices	None	LAB-DC	
> 07/12/2023, 04:07:41.256	Devices	None	LAB-SCCM	
> 07/12/2023, 04:07:41.287	Devices	None	INTUNE-9595	maurice.daly@msendpointm...
> 07/12/2023, 04:07:41.303	Devices	None	DESKTOP-TA43FN8	maurice.daly@msendpointm...
> 07/12/2023, 04:07:41.334	Devices	None	DESKTOP-1MKCI1U	maurice.daly@msendpointm...
> 07/12/2023, 04:07:41.365	Devices	None	INTUNE-8186	maurice.daly@msendpointm...
> 07/12/2023, 04:08:41.370	Devices	Completed		



TunedIn: London

Demo 1: Intune Log Analytics Tables



8th December 2023

Log Analytics – Custom Data Methods

- Azure Monitoring Agent
- Microsoft Monitoring Agent (Legacy)
 - For those early adopters who opted to install the Microsoft Monitoring Agent (MMA), please note:

 **Important**

The legacy **Log Analytics agent** will be deprecated by August 2024. After this date, Microsoft will no longer provide any support for the Log Analytics agent. [Migrate to Azure Monitor agent](#) before August 2024 to continue ingesting data.



Supported REST API's
TunedIn:London



8th December 2023

Custom Data – Log Analytics Custom Tables

- Custom Data Ingestion
 - Data posted via RESTFUL API in JSON format
 - Can be posted to the HTTP Data Collector API using the workspace ID and key
 - Be careful to secure these details
 - Soon to be deprecated (2026)

⚠ Note

The Azure Monitor HTTP Data Collector API has been deprecated and will no longer be functional as of 9/14/2026. It's been replaced by the [Logs ingestion API](#).



TunedIn:London

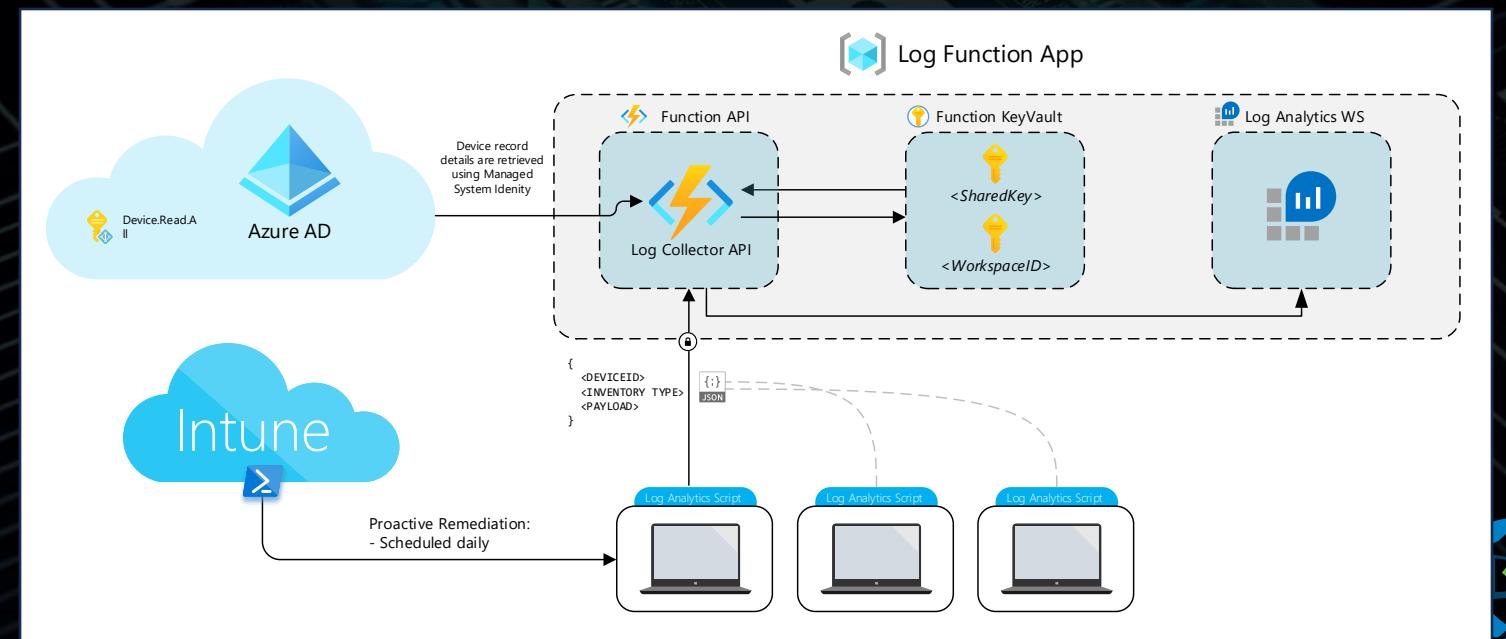


8th December 2023

Going Custom – Log Analytics Custom Tables

- **MSEndpointMgr Function**
 - Current version uses the HTTP DC API but secures the workspace details in Azure Key Vault

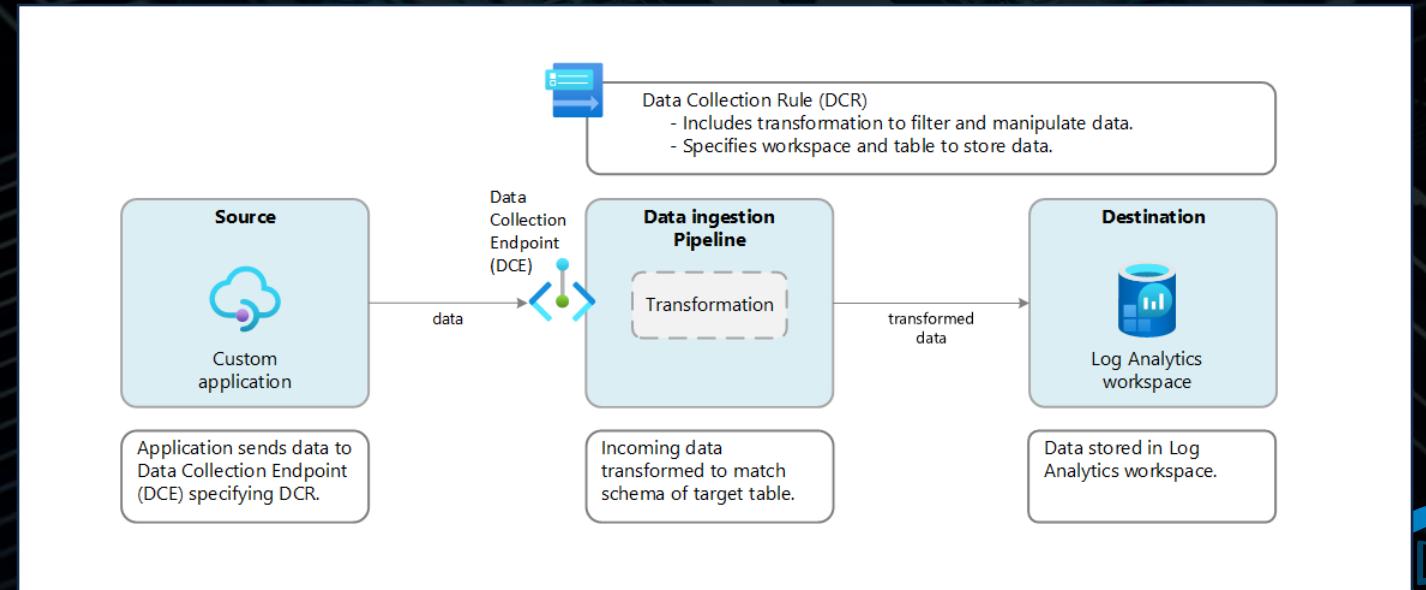
Securing Intune Enhanced Inventory with Azure Function - MSEndpointMgr



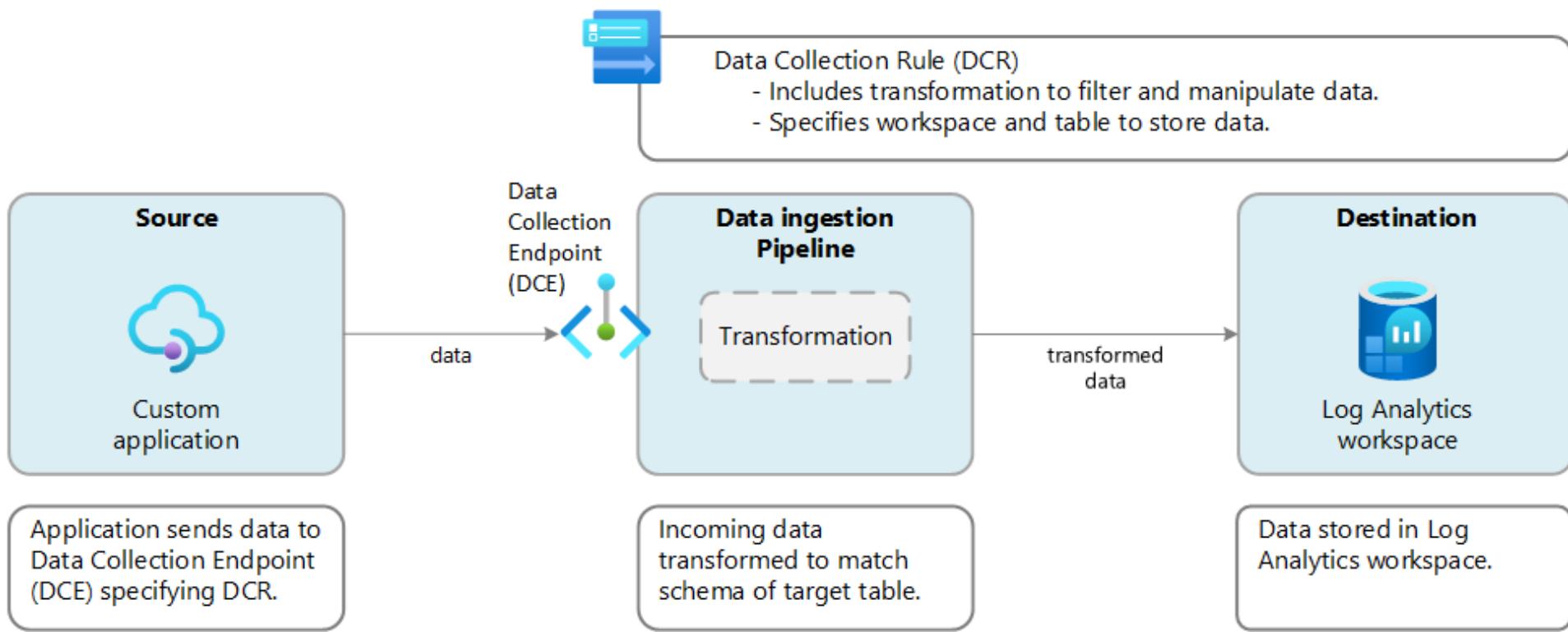
Going custom – Log Analytics Custom Tables

- **New - Log Ingestion API**
 - Newest method, leveraging data collection endpoint (DCE) and data collection rule (DCR) to ingest and even transform data prior to it being written to the custom tables
 - **Requires table schema to be defined prior to posting data**

[Logs Ingestion API in Azure Monitor - Azure Monitor | Microsoft Learn](#)



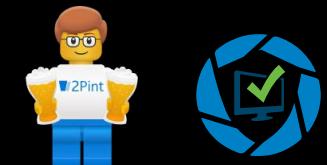
Going custom – Log Analytics Custom Tables





TunedIn: London

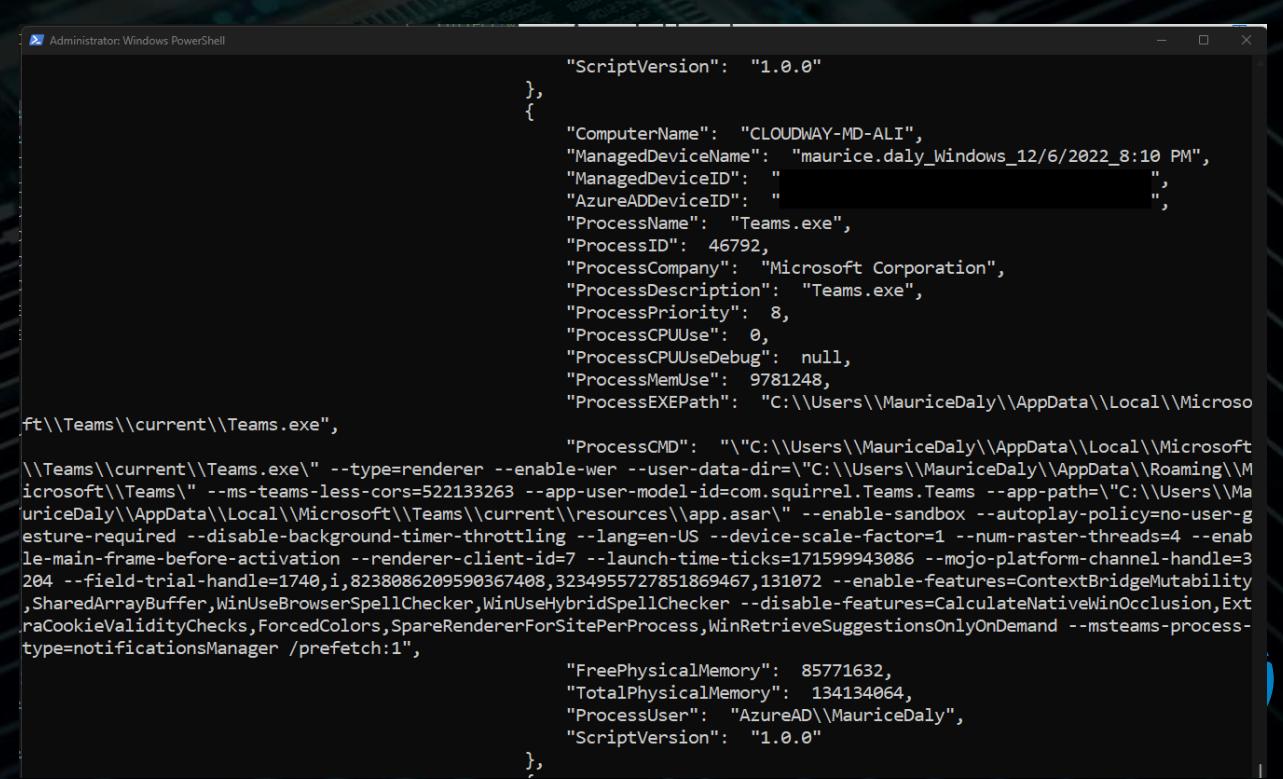
Demo 2: Custom Data



8th December 2023

Going custom – Log Analytics Custom Tables

- **Example Scenario & Payload:** Task Manager Processes
 - Devices are running slow, and we see a large consumption of RAM across our devices
 - We suspect the issues are due to X
 - PowerShell to the rescue
- **PowerShell obtained values;**
 - Process Name
 - Process ID
 - Process CPU Use
 - Process MEM Use
 - Free Physical Memory
 -



```
Administrator: Windows PowerShell
ScriptVersion": "1.0.0"
},
{
"ComputerName": "CLOUDWAY-MD-ALI",
"ManagedDeviceName": "maurice.daly_Windows_12/6/2022_8:10 PM",
"ManagedDeviceID": "",
"AzureADDeviceID": "",
"ProcessName": "Teams.exe",
"ProcessID": 46792,
"ProcessCompany": "Microsoft Corporation",
"ProcessDescription": "Teams.exe",
"ProcessPriority": 8,
"ProcessCPUUse": 0,
"ProcessCPUUseDebug": null,
"ProcessMemUse": 9781248,
"ProcessEXEPath": "C:\\\\Users\\\\MauriceDaly\\\\AppData\\\\Local\\\\Microso
ft\\\\Teams\\\\current\\\\Teams.exe",
"ProcessCMD": "\"C:\\\\Users\\\\MauriceDaly\\\\AppData\\\\Local\\\\Microsoft
\\\\Teams\\\\current\\\\Teams.exe\" --type=renderer --enable-wer --user-data-dir=\"C:\\\\Users\\\\MauriceDaly\\\\AppData\\\\Local\\\\Microsoft\\\\Teams\\\\current\\\\resources\\\\app.asar\" --enable-sandbox --autoplay-policy=no-user-g
esture-required --disable-background-timer-throttling --lang=en-US --device-scale-factor=1 --num-raster-threads=4 --enab
le-main-frame-before-activation --renderer-client-id=7 --launch-time-ticks=171599943086 --mojo-platform-channel-handle=3
204 --field-trial-handle=1740,i,8238086209590367408,3234955727851869467,131072 --enable-features=ContextBridgeMutability
,SharedArrayBuffer,WinUseBrowserSpellChecker,WinUseHybridSpellChecker --disable-features=CalculateNativeWinOcclusion,Ext
raCookieValidityChecks,ForcedColors,SpareRendererForSitePerProcess,WinRetrieveSuggestionsOnlyOnDemand --msteams-process-
type=notificationsManager /prefetch:1",
"FreePhysicalMemory": 85771632,
"TotalPhysicalMemory": 134134064,
"ProcessUser": "AzureAD\\\\MauriceDaly",
"ScriptVersion": "1.0.0"
},
```

Going custom – Log Analytics Custom Tables

```
1 ProcessResources_CL  
2 | summarize arg_max(TimeGenerated, *) by ManagedDeviceID_g, ProcessCMD_s, ProcessCompany_s  
3 | where ProcessCMD_s !has "User"  
4 | summarize count() by ProcessCMD_s, ProcessCompany_s  
5 | order by count_ desc
```

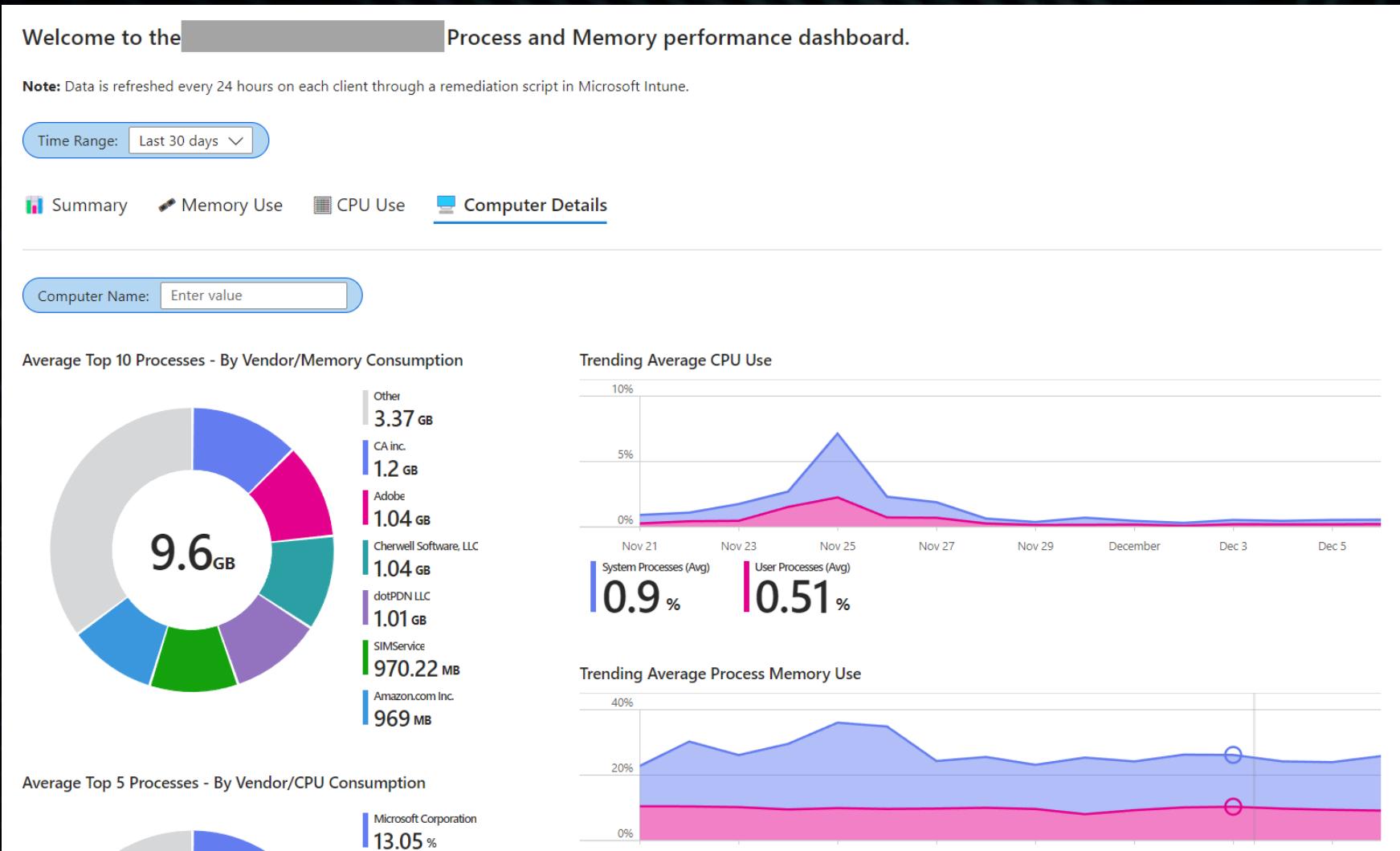
Results Chart

 Showing the first 30,000 results. [Learn more](#) on how to narrow down the result set.

ProcessCMD_s	ProcessCompany_s	count
> "C:\Program Files (x86)\ResearchMonitor\Agent\SvcBoot.exe"	TRGRP, Inc.	1099
> "C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeClickToRun.exe..."	Microsoft Corporation	1099
> C:\WINDOWS\System32\svchost.exe -k NetworkService -p -s NlaSvc	Microsoft Corporation	1099
> "C:\Program Files\AppSense\Management Center\Communications Agent\Cca.exe"	Ivanti	1098
> "C:\Program Files\AppSense\Environment Manager\Agent\EmCoreService.exe"	Ivanti	1098
> C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s SysMain	Microsoft Corporation	1098
> C:\WINDOWS\system32\wbem\unsecapp.exe -Embedding	Microsoft Corporation	1098
> C:\WINDOWS\CCM\CcmExec.exe	Microsoft Corporation	1097
> "C:\Program Files (x86)\Enable Business Solutions\Enable Revenue Manager\ERMS....	Blue Car Technologies Limited	1097



Going custom – Log Analytics Workbooks



Going custom – Log Analytics Workbooks

Intune Devices (Win...) **2.15 k**

Reported Device **1.19 k**

Unique System Proc... **69 k**

Unique User Process... **133 k**

Highest Process Use
TmCCSF.exe
Trend Micro Inc.

Highest Memory Use
SIMService.exe
SIMService

Average Free Memory - By Total Ram

Unique System Processes - By Vendor

Vendor	Processes
Microsoft Corporation	34.5 k
Trend Micro Inc.	22.6 k
Ivanti	8.37 k
Cisco Systems, Inc.	1.63 k
Unknown	1.21 k
Other	689
Microsoft	171

Unique User Processes - By Vendor

Vendor	Processes
Microsoft Corporation	80.4 k
Cisco Systems, Inc.	14.2 k
Adobe Systems Incorporated	13.6 k
Other	11.6 k
Cisco WebEx LLC	5.39 k
Unknown	4.32 k
Sound Research, Corp.	3.99 k

Top 10 Devices - With Free Memory Issues

Computer Na...	OS	CPU	Memo...	Free Memory	Free Memory %
	Microsoft Windows 10 Enterprise	12th Gen Intel(R) Core(TM) i7-1265U	16	0.08	0.5%
	Microsoft Windows 10 Enterprise	12th Gen Intel(R) Core(TM) i7-1265U	16	0.11	0.69%
	Microsoft Windows 10 Enterprise	11th Gen Intel(R) Core(TM) i7-1165G7 @ 2.80GHz	16	0.12	0.75%
	Microsoft Windows 10 Enterprise	12th Gen Intel(R) Core(TM) i7-1265U	16	0.14	0.88%
	Microsoft Windows 10 Enterprise	12th Gen Intel(R) Core(TM) i7-1265U	16	0.17	1.06%
	Microsoft Windows 10 Enterprise	11th Gen Intel(R) Core(TM) i7-1185G7 @ 3.00GHz	16	0.17	1.06%
	Microsoft Windows 10 Enterprise	12th Gen Intel(R) Core(TM) i7-1265U	16	0.2	1.25%
	Microsoft Windows 10 Enterprise	Intel(R) Core(TM) i7-10510U CPU @ 1.80GHz	16	0.21	1.31%
	Microsoft Windows 10 Enterprise	12th Gen Intel(R) Core(TM) i7-1265U	16	0.22	1.38%

TUNEDIN
MEETUPS

TUNEDIN. LONDON

8th December 2023

Going custom – Log Analytics Workbooks

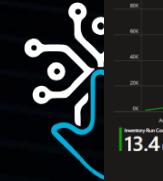
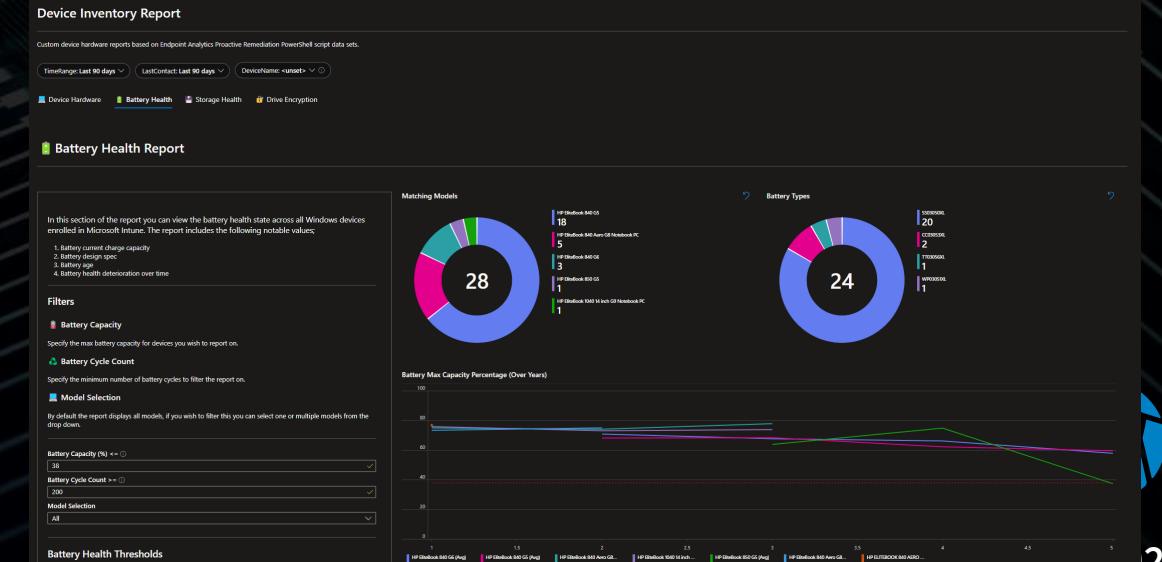
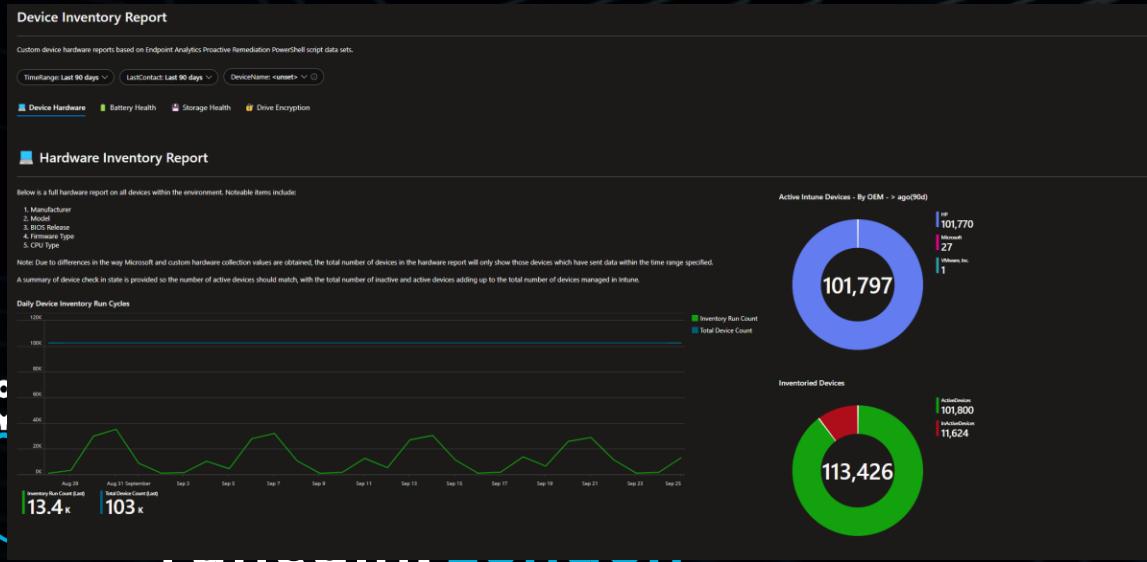
Top 10 Devices - CPU Process Spikes							...		
OS	↑↓	CPU	↑↓	Memo...	↑↓	Description	↑↓	CPU Usage ↑↓	Vendor
Microsoft Windows 10 Enterprise		12th Gen Intel(R) Core(TM) i7-1265U		16		dsagent.exe		98.55%	Trend Micro Inc.
Microsoft Windows 10 Enterprise		Intel(R) Core(TM) i7-4770 CPU @ 3.40GHz		8		TMBMSRV.exe		98.02%	Trend Micro Inc.
Microsoft Windows 10 Enterprise		11th Gen Intel(R) Core(TM) i7-1165G7 @ 2.80GHz		16		WmiPrvSE.exe		94.85%	Microsoft Corpora
Microsoft Windows 10 Enterprise		11th Gen Intel(R) Core(TM) i7-1165G7 @ 2.80GHz		16		msedge.exe		93.5%	Microsoft Corpora
Microsoft Windows 10 Enterprise		12th Gen Intel(R) Core(TM) i7-1265U		16		OUTLOOK.EXE		90.32%	Microsoft Corpora
Microsoft Windows 10 Enterprise		11th Gen Intel(R) Core(TM) i7-1165G7 @ 2.80GHz		16		powershell.exe		90.1%	Microsoft Corpora
Microsoft Windows 10 Enterprise		Intel(R) Core(TM) i7-4770 CPU @ 3.40GHz		8		WmiPrvSE.exe		89.38%	Microsoft Corpora
Microsoft Windows 10 Enterprise		12th Gen Intel(R) Core(TM) i7-1265U		16		dsagent.exe		88.42%	Trend Micro Inc.
Microsoft Windows 10 Enterprise		11th Gen Intel(R) Core(TM) i7-1165G7 @ 2.80GHz		16		powershell.exe		88.4%	Microsoft Corpora
Microsoft Windows 10 Enterprise		Intel(R) Core(TM) i7-8565U CPU @ 1.80GHz		16		EXCEL.EXE		87.9%	Microsoft Corpora

Going custom – Log Analytics Workbooks

Top 10 CPU Processes - User Environment							
Time Generated	Vendor	Description	Path	CPU Perc...			
27/11/2023, 00:00:00.000	Cisco Webex LLC	atmgr.exe	appdata\local\webex\webex64\meetin...	38.5%			
26/11/2023, 00:00:00.000	Cisco Webex LLC	atmgr.exe	appdata\local\webex\webex64\meetin...	29.5%			
05/12/2023, 00:00:00.000	Cisco Webex LLC	atmgr.exe	data\local\webex\webex64\meetings\...	26.53%			
06/12/2023, 00:00:00.000	Cisco Webex LLC	atmgr.exe	appdata\local\webex\webex64\meetin...	24.32%			
07/12/2023, 00:00:00.000	Cisco Webex LLC	atmgr.exe	appdata\local\webex\webex64\meetin...	22.6%			
05/12/2023, 00:00:00.000	Microsoft Corporation	explorer.exe	C:\WINDOWS\explorer.exe	21.98%			
Top 10 CPU Processes - System Environment							
Time Generated	Vendor	Description	Path	CPU Perc...			
06/12/2023, 00:00:00.000	Microsoft Corporation	TiWorker.exe	C:\WINDOWS\winsxs\amd64_microsoft-windows-servicin...	48.75%			
25/11/2023, 00:00:00.000	Trend Micro Inc.	dsagent.exe	C:\WINDOWS\system32\dgagent\DSAGENT.exe	29.05%			
01/12/2023, 00:00:00.000	Trend Micro Inc.	TmCCSF.exe	C:\Program Files (x86)\Trend Micro\OfficeScan Client\CCS...	22.58%			
07/12/2023, 00:00:00.000	Trend Micro Inc.	TmCCSF.exe	C:\Program Files (x86)\Trend Micro\OfficeScan Client\CCS...	17.11%			
06/12/2023, 00:00:00.000	Trend Micro Inc.	TmCCSF.exe	C:\Program Files (x86)\Trend Micro\OfficeScan Client\CCS...	15.91%			

Going custom – Log Analytics Custom Tables

- **Example Scenario & Payload: Device Inventory**
 - We need a better way of keeping track of device
 - We need to report on encryption states
 -on battery health
 -winre version information



Device Inventory Report

Custom device hardware reports based on Endpoint Analytics Proactive Remediation PowerShell script data sets.

TimeRange: Last 90 days ▾ LastContact: Last 90 days ▾ DeviceName: <unset> ▾ ⓘ

Device Hardware Battery Health Storage Health Drive Encryption

Battery Health Report

In this section of the report you can view the battery health state across all Windows devices enrolled in Microsoft Intune. The report includes the following notable values;

1. Battery current charge capacity
2. Battery design spec
3. Battery age
4. Battery health deterioration over time

Filters

Battery Capacity

Specify the max battery capacity for devices you wish to report on.

Battery Cycle Count

Specify the minimum number of battery cycles to filter the report on.

Model Selection

By default the report displays all models, if you wish to filter this you can select one or multiple models from the drop down.

Battery Capacity (%) <= ⓘ

38

Battery Cycle Count >= ⓘ

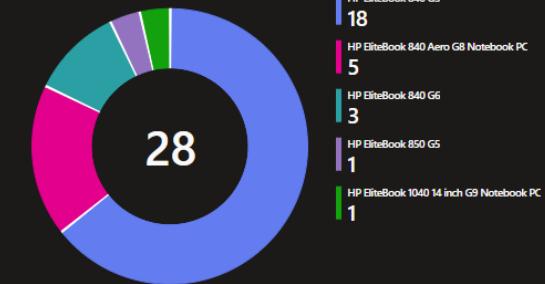
200

Model Selection

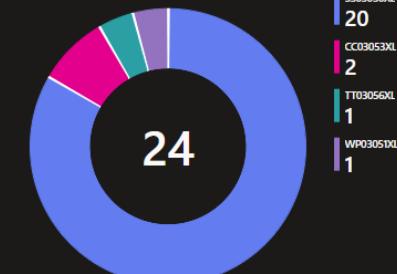
All

Battery Health Thresholds

Matching Models



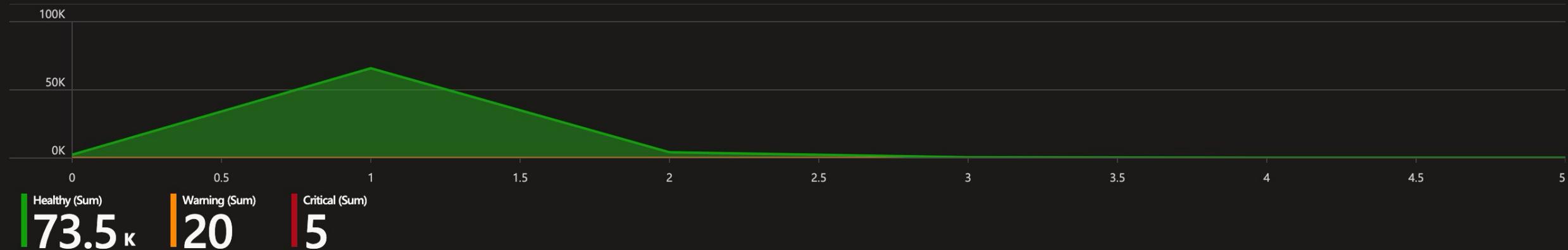
Battery Types



Battery Max Capacity Percentage (Over Years)



Battery Age Profile - > ago(90d)



Model Battery Status

ComputerName...↑↓	Model_s	↑↓	BatteryDate	↑↓	BatteryAgeDays	↑↓	BatteryCurrentMaxCapacity	↑↓	BatteryFullChargedCapacity↑↓	BatteryDesign...
	HP EliteBook 840 Aero G8 Notebook PC		28-08-2021		✓ 761		! 0%			23
	HP EliteBook 840 G5		14-08-2018		! 1871		! 9.4%			4724
	HP EliteBook 840 G6		23-09-2019		⚠ 1466		! 12.4%			6191
	HP EliteBook 850 G5		19-10-2018		⚠ 1805		! 15.2%			8512
	HP EliteBook 830 G5		08-11-2018		⚠ 1785		! 17.6%			8801
	HP EliteBook 840 G5		08-09-2018		! 1846		⚠ 20.2%			10118
	HP EliteBook 830 G5		08-11-2018		⚠ 1785		⚠ 23.2%			11608



TunedIn: London

Demo 3: KQL Workbooks



8th December 2023

Go & Get Building – Log Analytics FTW

- YOU are once again a “Report Builder”
- Script your own reporting destiny
 - As we just saw, PowerShell is your friend. If you can get useful values in a script, you can transform the data into something reportable
 - Remediations are your frequency limitation (and you need to be licensed of course)
- Use Azure Monitor to trigger actions, such as Teams Webhook notifications on events



TunedIn: London



8th December 2023

Go & Get Building – Useful Links

- Microsoft

- [Log Analytics agent data sources in Azure Monitor - Azure Monitor | Microsoft Learn](#)
- [Logs Ingestion API in Azure Monitor - Azure Monitor | Microsoft Learn](#)
- [Sample code to send data to Azure Monitor using Logs ingestion API - Azure Monitor | Microsoft Learn](#)
- [Connect computers by using the Log Analytics gateway - Azure Monitor | Microsoft Learn](#)
- [Kusto Query Language \(KQL\) overview - Azure Data Explorer & Real-Time Analytics | Microsoft Learn](#)

Go & Get Building – Useful Links

- **Azure Monitor Community (GitHub)**
 - [GitHub - microsoft/AzureMonitorCommunity](https://github.com/microsoft/AzureMonitorCommunity): An open repo for Azure Monitor queries, workbooks, alerts and more
- **MSEndpointMgr**
 - [Windows Update Compliance Workbook Community Edition – MSEndpointMgr](#)
 - [Intune BIOS Update Compliance Reporting – MSEndpointMgr](#)
 - [Log Analytics & AppLocker - Better Together – MSEndpointMgr](#)



TunedIn:London



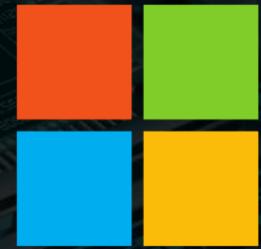
8th December 2023

Q&A

Thank you again to our Sponsors



TunedIn:London



Microsoft

8th December 2023



TunedIn: London

Thank you!



8th December 2023