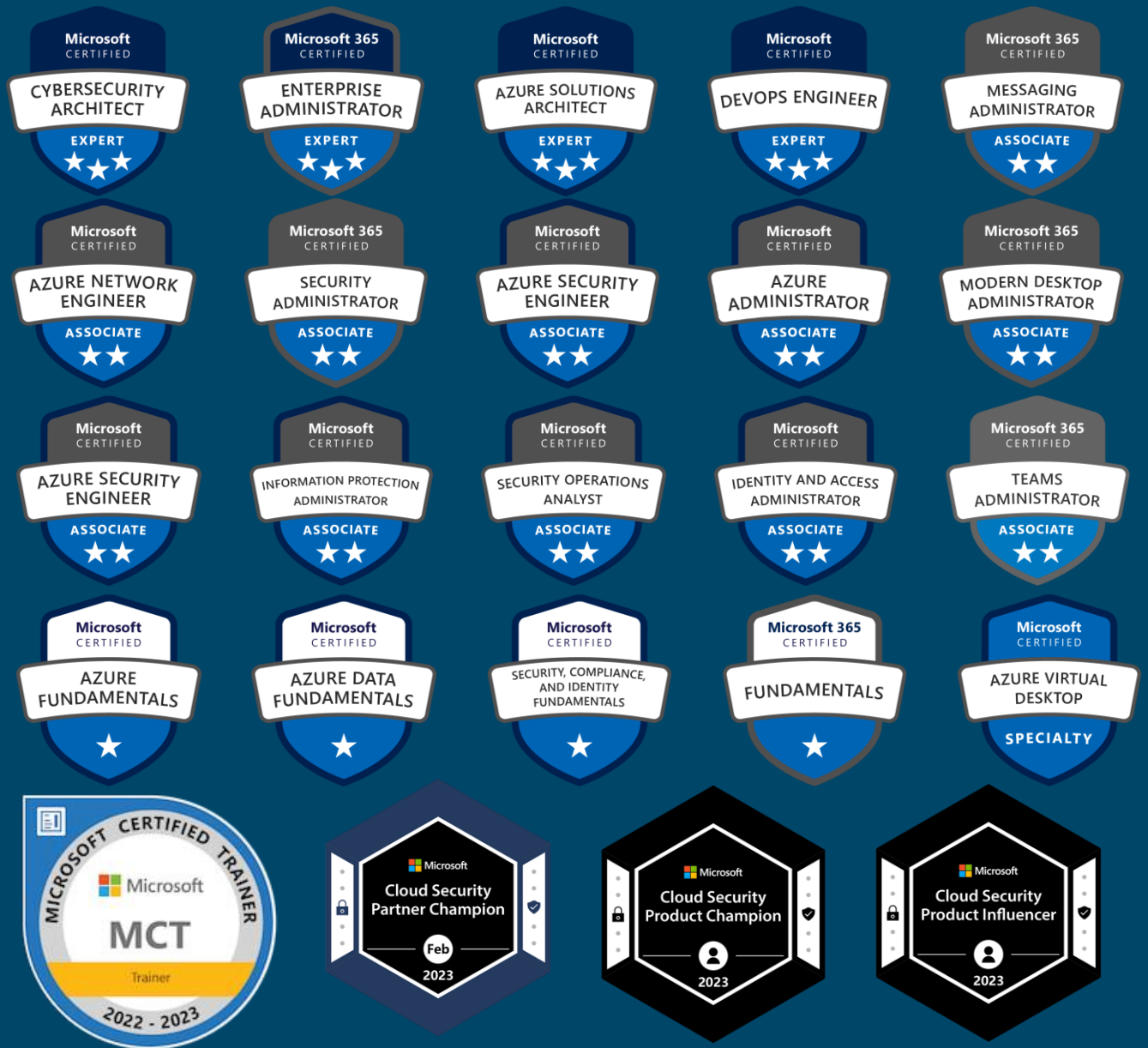
Client Insight using Next-Generation Azure Log Capabilities

Morten Knudsen

Microsoft® Most Valuable Professional

My LinkedIn Profile (connect)

Speaker – Morten Knudsen



About | Morten Knudsen

Microsoft MVP Security & Azure Hybrid MVP

Microsoft Certified Trainer

Cloud & Security Architect

Microsoft Sentinel Black Belt

Microsoft Defender Black Belt

Microsoft Cloud Security Influencer

Microsoft Sentinel Influencer

Microsoft Defender for Cloud Influencer

MVP Microsoft® Most Valuable Professional

Award Categories
Security

First year awarded:
2023

Number of MVP Awards:
1


Microsoft
Microsoft
Microsoft


Microsoft

Session Objective – hopefully something for all ☺

Audience - we come from different background? Competency?

Introduction & Inspiration

- How you can use the Microsoft technologies to build your own cool log integrations to work with facts – for a little cost, compared to value
- Get inspired about Azure Logging capabilities - use-cases
- try out **showcase**, **ClientInspector** – ready-to-use – free - community ☺

How-to migrate from Azure Logging V1 --> V2 - End of support (Aug 24)?

- MMA → AMA
- HTTP Data Collector REST API → Azure Log Ingestion Pipeline, Log Ingestion API, Transformation and Azure Data Collection Rules (End of support announcement soon)
- Azure LogAnalytics custom tables v1 → v2
- Data manipulation – Schema/Table Management - Data Transformation – Data Upload
- "AnyConnector" → Introduction to your new helper → AzLogDcrIngestPS PS module
- Where can I get more information ?

Showcase: Good Security demands to be and stay in control with the fundamentals !

Data Source/In

WMI

CIM

REST APIs

CSV

JSON

XML

Powershell cmdlets – get-mppreference

Registry

Files

Integration HR system

Security-portal (Advanced Hunting)- REST API

Logfiles

SQL performance counters

Databaser

Defender for Endpoint (MDE)

..

..

Data Collection

Pending Windows Updates

Members Local Admins

Bitlocker config

Window firewall settings

Hardware Serial Number

OS Last Restart

..

Desired State Dashboards (KPIs)

Computers with wrong/missing Bitlocker config

Computers with pending updates released more than 40 days ago

Unexpected shutdowns during last 24 hours

Incomplete Office update channel

Incompliant Real Protection antivirus

Computer not refreshing Group Policies during last 7 days

CLIENT KPI STATUS | MANAGED D...

Shared dashboard

Create | Upload | Refresh | Full screen | Edit | Manage sharing | Export | Clone | Assign tags | Delete | Feedback

Auto refresh : Off | UTC Time : Past 24 hours

OTHER PRIMARY ANTIVIRUS (SECURITY CENTER) | CLIENTS | C...
log-platform-management-client-p (@ 3/19 3:11 PM)
3

INCOMPLIANT BITLOCKER | CLIENTS | COUNT
log-platform-management-client-p (@ 3/19 3:11 PM)
465

NO RESTART MORE THAN 7 DAYS DAY | CLIENTS | COUNT
log-platform-management-client-p (@ 3/19 3:11 PM)
8

LAST GROUP POLICY REFRESH MORE THAN 7 DAYS AGO | CLIE...
log-platform-management-client-p (@ 3/19 3:11 PM)
0

INCOMPLIANT LAPS | CLIENTS | COUNT
log-platform-management-client-p (@ 3/19 3:11 PM)
15

INCOMPLIANT DEFENDER AV | CLIENTS | COUNT
log-platform-management-client-p (@ 3/19 3:11 PM)
73

UNSUPPORTED WINDOWS OS BUILD, MDE | CLIENTS | COUNT
log-platform-management-client-p (@ 3/19 3:11 PM)
34

SOON UNSUPPORTED WINDOWS OS BUILD, MDE | CLIENTS | ...
log-platform-management-client-p (@ 3/19 3:11 PM)
1

DEVICES WITH NON-STANDARD MEMBERS LOCAL ADMINS G...
log-platform-management-client-p (@ 3/19 3:11 PM)
2,332

DEVICES WITH HIGH SEVERITY VULNERABILITIES >9 | CLIENTS ...
log-platform-management-client-p (@ 3/19 3:11 PM)
7

UPDATING O365 OFFICE NOT ENABLED | CLIENTS | COUNT
log-platform-management-client-p (@ 3/19 3:11 PM)
572

INCOMPLIANT UPDATE CHANNEL O365 OFFICE | CLIENTS | CO...
log-platform-management-client-p (@ 3/19 3:11 PM)
0

LEGACY OFFICE | CLIENTS | COUNT
log-platform-management-client-p (@ 3/19 3:11 PM)
0

STANDALONE OFFICE 2016 | CLIENTS | COUNT
log-platform-management-client-p (@ 3/19 3:11 PM)
0

INCOMPLIANT WINDOWS FIREWALL | CLIENTS | COUNT
log-platform-management-client-p (@ 3/19 3:11 PM)
1

LAST WINDOWS UPDATE MORE THAN 40 DAYS AGO | CLIENT...
log-platform-management-client-p (@ 3/19 3:11 PM)
134

CLIENTS WITH PENDING UPDATES OLDER THAN 40 DAYS | CLI...
log-platform-management-client-p (@ 3/19 3:11 PM)
33

CLIENTS WITH PENDING UPDATES OLDER THAN 40 DAYS, NO ...
log-platform-management-client-p (@ 3/19 3:11 PM)
25

UNEXPECTED SHUTDOWNS | CLIENTS | COUNT
log-platform-management-client-p (@ 3/19 3:11 PM)
819

DEVICES WITH COLLECTION ISSUES (FIX WMI) | CLIENTS | COU...
log-platform-management-client-p (@ 3/19 3:11 PM)
14

DEVICES WITH CRITICAL OR HIGH RISKY BROWSER EXT | CLIE...
log-platform-management-client-p (@ 3/19 3:11 PM)
552

DEVICES WITH EXPIRED CERTIFICATES, PERSONAL, EXCL. MEM...
log-platform-management-client-p (@ 3/19 3:11 PM)
2,307

DEVICES WITH SOON TO EXPIRE CERTIFICATES (60 DAYS), PER...
log-platform-management-client-p (@ 3/19 3:11 PM)
316

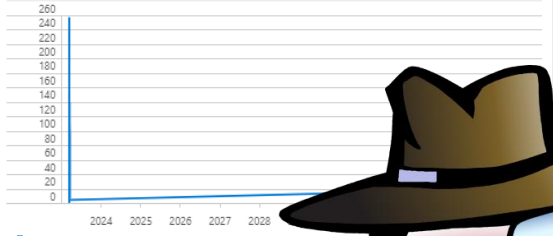
DEVICES WITH HIGH SEVERITY VULNERABILITY > 9 | CLIENTS | TIME 7 DAYS
log-platform-management-client-p (@ 3/19 3:11 PM)

total (Avg)
4.67

NO RESTART MORE THAN 7 DAYS DAY | CLIENTS | TIME 1 MONTH COLLECTI...
log-platform-management-client-p (@ 3/19 3:11 PM)

total (Avg)
1

UNEXPECTED SHUTDOWNS | CLIENTS | TIME 7 DAYS
log-platform-management-client-p (@ 3/19 3:11 PM)

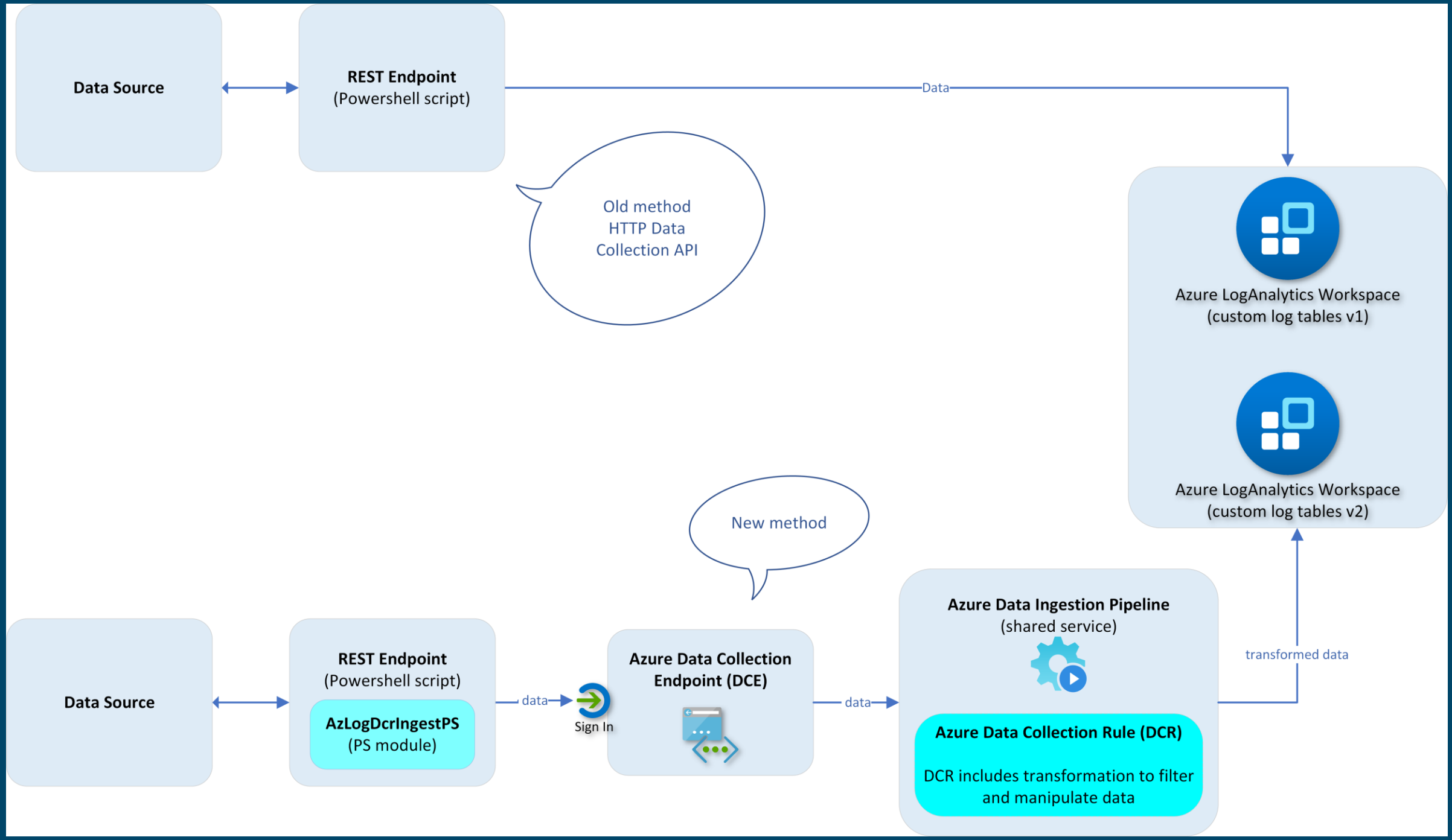


total (Avg)
86

Showcase (how/what):

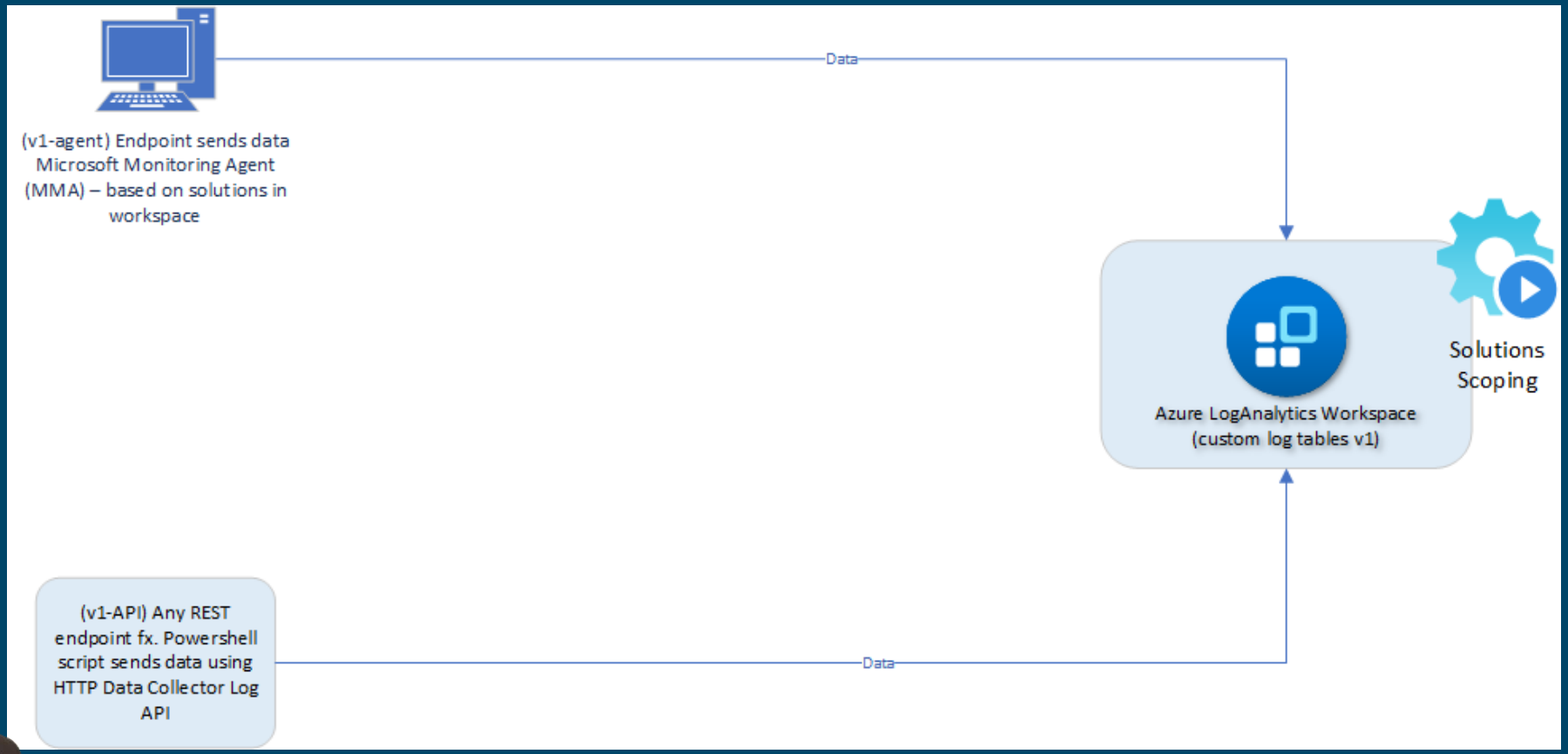
ClientInspector PS-script
Azure LogAnalytics tables
14x Azure Workbooks
15x Azure Dashboards
AzLogDcrIngestPS

Price per month:
Daily collection from 500 clients
= USD 27 (DKK 200) / month


Data Source
REST Endpoint
(Powershell script)
Data
Old method
HTTP Data
Collection API
Azure LogAnalytics Workspace
(custom log tables v1)
Azure LogAnalytics Workspace
(custom log tables v2)
New method
Data Source
REST Endpoint
(Powershell script)
AzLogDcrIngestPS
(PS module)
data
Sign In
Azure Data Collection
Endpoint (DCE)
data
Azure Data Ingestion Pipeline
(shared service)
Azure Data Collection Rule (DCR)
DCR includes transformation to filter
and manipulate data
transformed data

“V1” (legacy)

- Custom tables (v1)
- LA Solutions
- MMA
- Azure Monitor HTTP Data Collector API

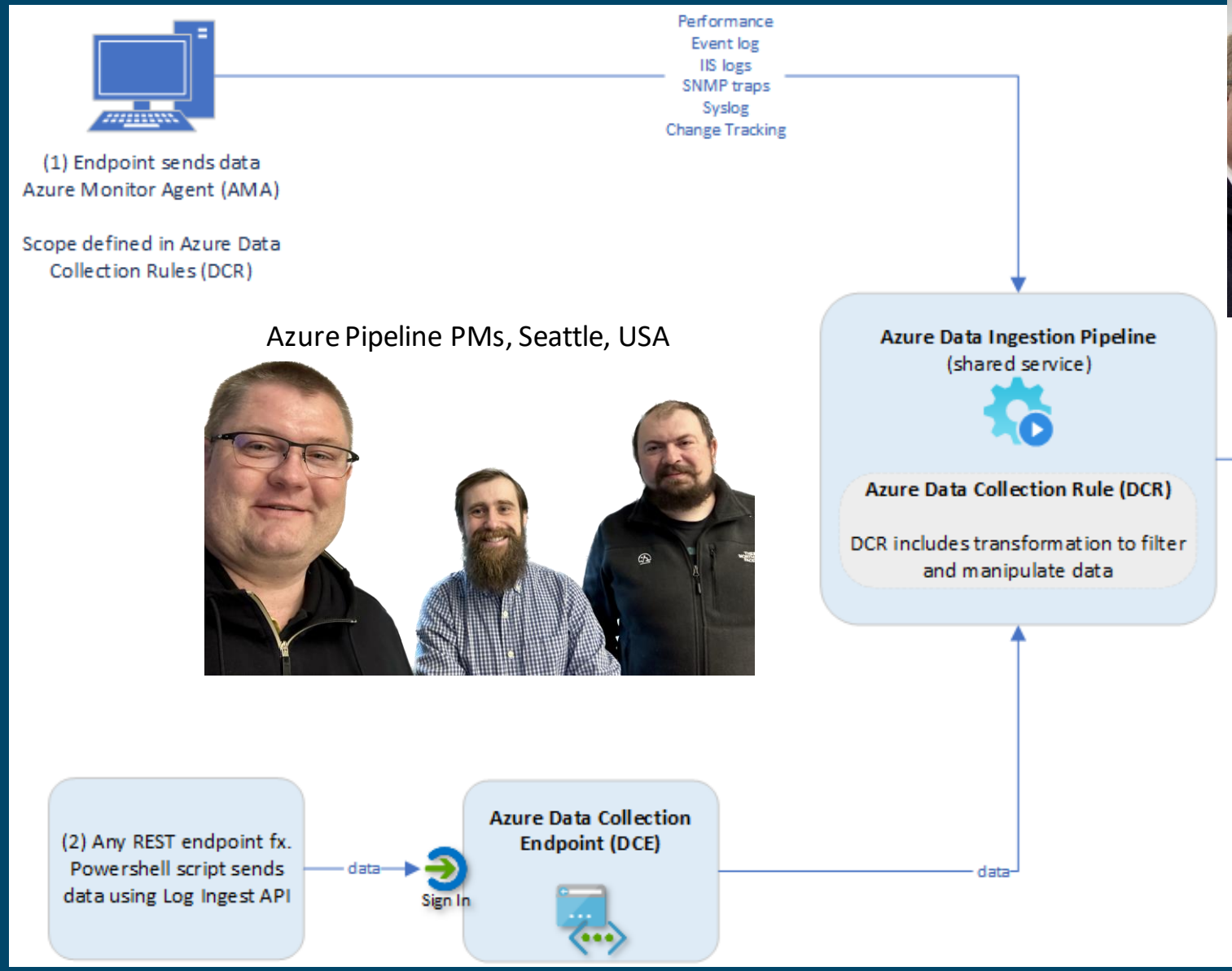


> **Note**
>
> The Azure Monitor HTTP Data Collector API is in public preview.

Response from product team
”Data Collector API was never officially released or considered “complete”
We are going to update Data Collector API documentation as part of its deprecation cycle”

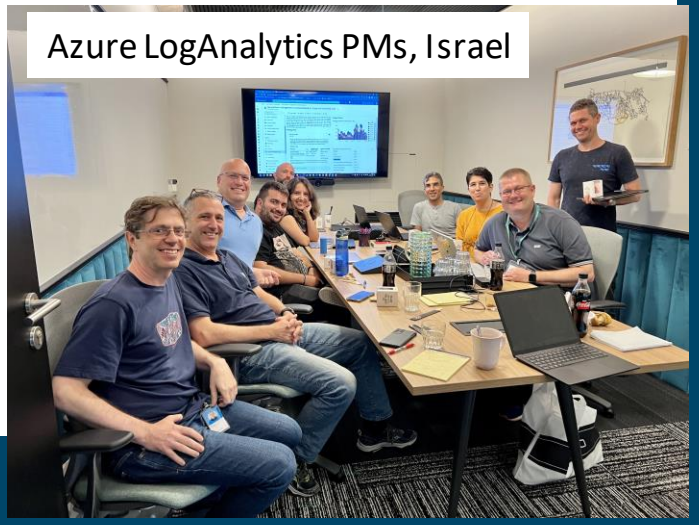
“V2”

Azure Pipeline
DCRs
Transformation
DCEs
Custom tables (v2)



Azure DCR PMs & Dev Lead, Seattle, USA

Azure LogAnalytics PMs, Israel



Azure Logging V2 – current data sources

More capabilities are coming – I'm so excited ☺

Performance metrics & telemetry

Performance Counters (SQL)

Eventlogs

Standard/Platform metrics/Telemetry (AzPaaS)

IIS logs

Windows Fw Logs

Text logs

Change Tracking

Custom Logs (Ingestion API)

Custom metrics/telemetry (custom AzApp)

SNMP Traps

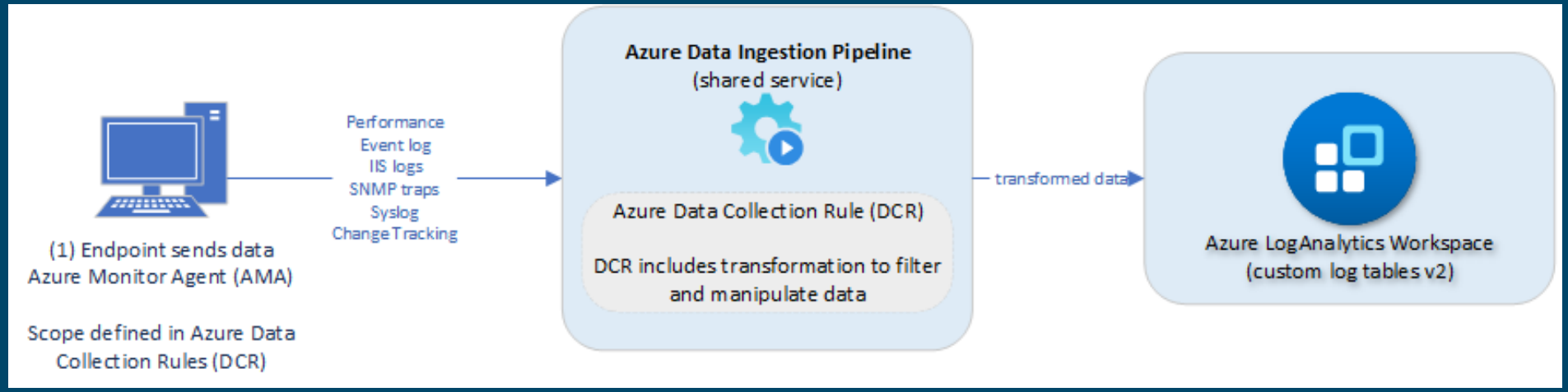
Platform logs (diagnostics)

Activity logs

Standard Logs (Ingestion API)

Meet the Azure Monitor PMs (Seattle, USA)

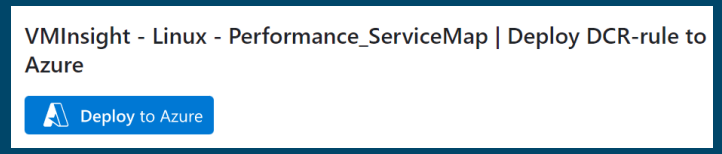
I'm fan ☺



- remove data before being sent into LogAnalytics (remove "noice" data/cost optimization, GDPR/compliance)
- add data before being sent into LogAnalytics
- merge data before being sent into LogAnalytics
- better data quality (array data), as array data is converted into dynamic - whereas the old MMA-method would convert array data into strings
- support to send to other destinations
- support for file-based logs collection (txt-logs, Windows Firewall logs)
- advanced support for advanced collection of performance data (including new collection type like SQL performance counters)
- support for SNMP traps logs collection
- security is based on Azure AD RBAC
- naming of data columns are prettier, as they contain the actual name - and not for example ComputerName_s indicating it is a string value

My contribution to get you started with Azure Logging v2 ??

12 new blogs + AzureLogLibrary.net (templates)

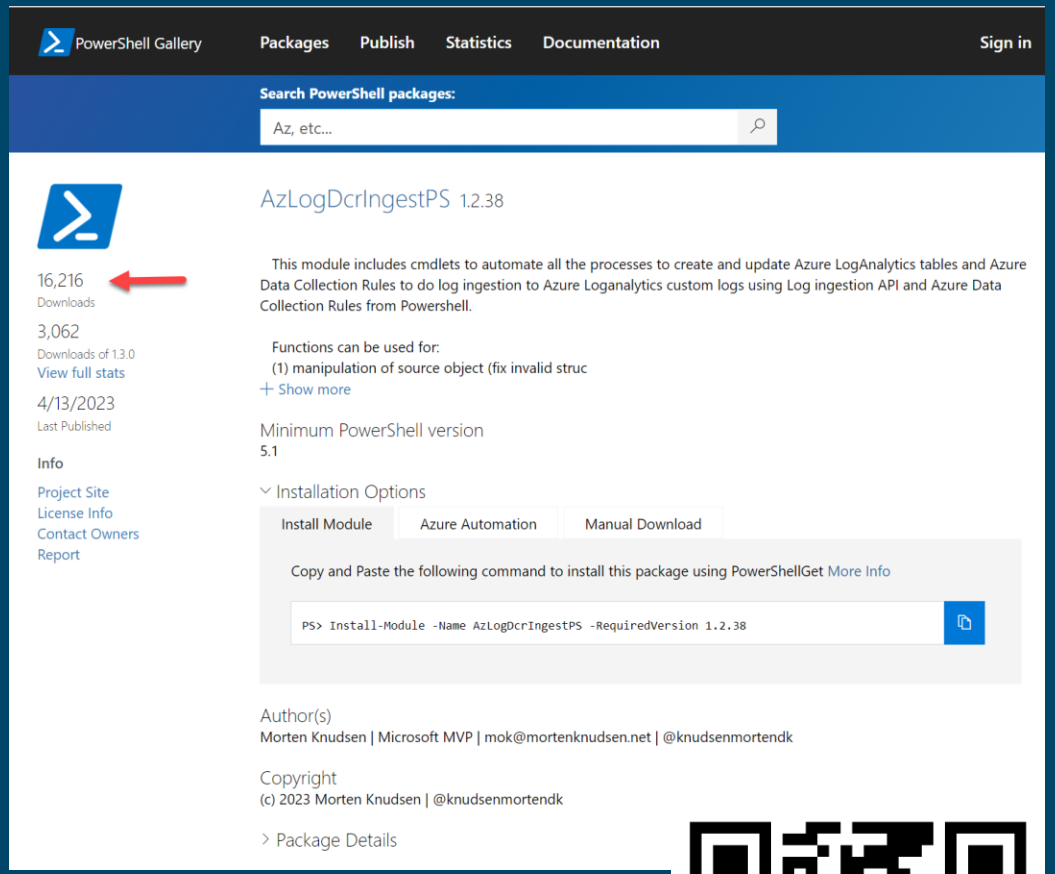


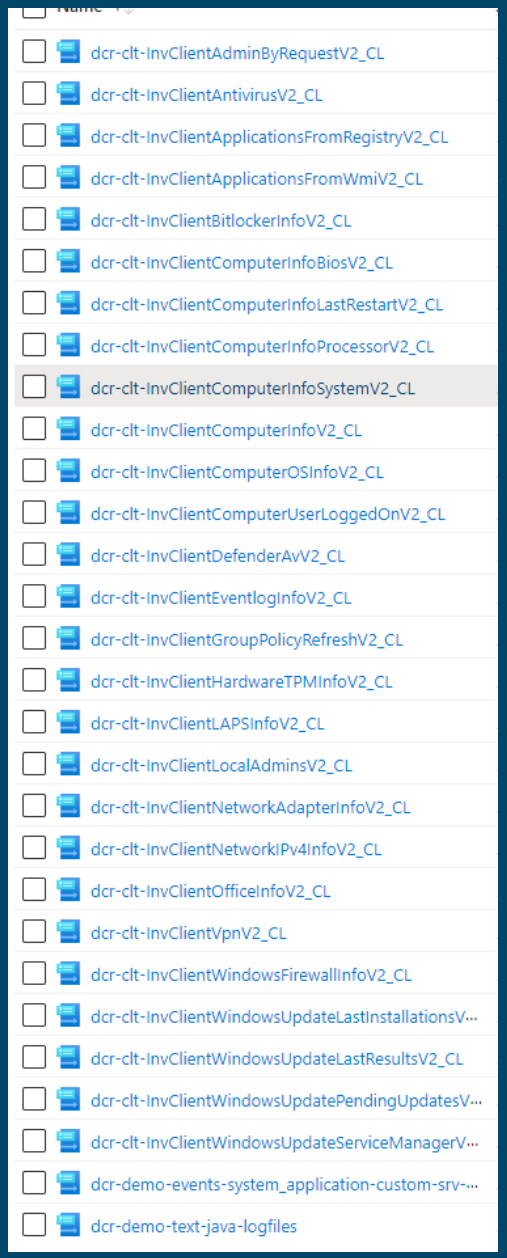
Topic	Link
Understanding Azure logging capabilities in depth	https://mortenknudsen.net/?p=1433
How to do data transformation using Workspace transformation for legacy upload methods	https://mortenknudsen.net/?p=1436
Understanding the fundamentals of log-collection with Azure Monitor Agent & Azure Data Collection Rules	https://mortenknudsen.net/?p=1438
Understanding Azure Data Collection Endpoint	https://mortenknudsen.net/?p=1442
Collecting Security events using Azure Monitor Agent	https://mortenknudsen.net/?p=1444
Collecting System & Application events using Azure Monitor Agent	https://mortenknudsen.net/?p=1446
Collecting Performance data using Azure Monitor Agent, VMInsights and ServiceMap	https://mortenknudsen.net/?p=1449
Collecting IIS logs using Azure Monitor Agent	https://mortenknudsen.net/?p=1451
Collecting text logs using Azure Monitor Agent	https://mortenknudsen.net/?p=1453
Collecting Syslogs using Azure Monitor Agent	https://mortenknudsen.net/?p=1455
Collecting CEF Syslogs using Azure Monitor Agent	https://mortenknudsen.net/?p=1457
Tutorial – How to make data transformations using Data Collection Rules?	https://mortenknudsen.net/?p=1440

Challenges with v2 technologies
compared to V1

25 functions
+6000 lines of code

- Schema
  - Req: Creation of DCR + tables before sending data
  - Req: Data Collection EndPoint must exist
  - Req: Schema for data must be defined in both DCR and custom table (v2)
  - Naming conventions & limitations / Prohibited names
  - Handle new properties in source object (merge, overwrite)
  - Property changes -True (string) → True (Boolean) – "internal server 500"
- Upload changes (32 mb -> 1 mb) per JSON (batches, calculations)
- Data manipulations of source data (filtering, remove)
- DCR limitations with large schema
  - create with limited schema first, then full schema
- Azure seconds - timing / delays – dependencies
- Platform – no-internet access, TLS incompatibility





Home > Monitor | Data Collection Rules >

dcr-clt-InvClientComputerInfoSystemV2_CL

Data collection rule | Directory: 2linkIT

Search

Delete

- Overview
- Activity log
- Access control (IAM)
- Tags

Settings

- Locks

Configuration

- Data sources
- Resources

Automation

- Tasks (preview)
- Export template

Support + troubleshooting

- New Support Request

Essentials

Resource group (move)	: rg-dcr-log-management-client
Status	: Provisioned
Location	: West Europe
Subscription (move)	: 2LINKIT CLOUD (MS SPONSOF
Subscription ID	: fce4f282-fcc6-43fb-94d8-bf17
Tags (edit)	: Click here to add tags

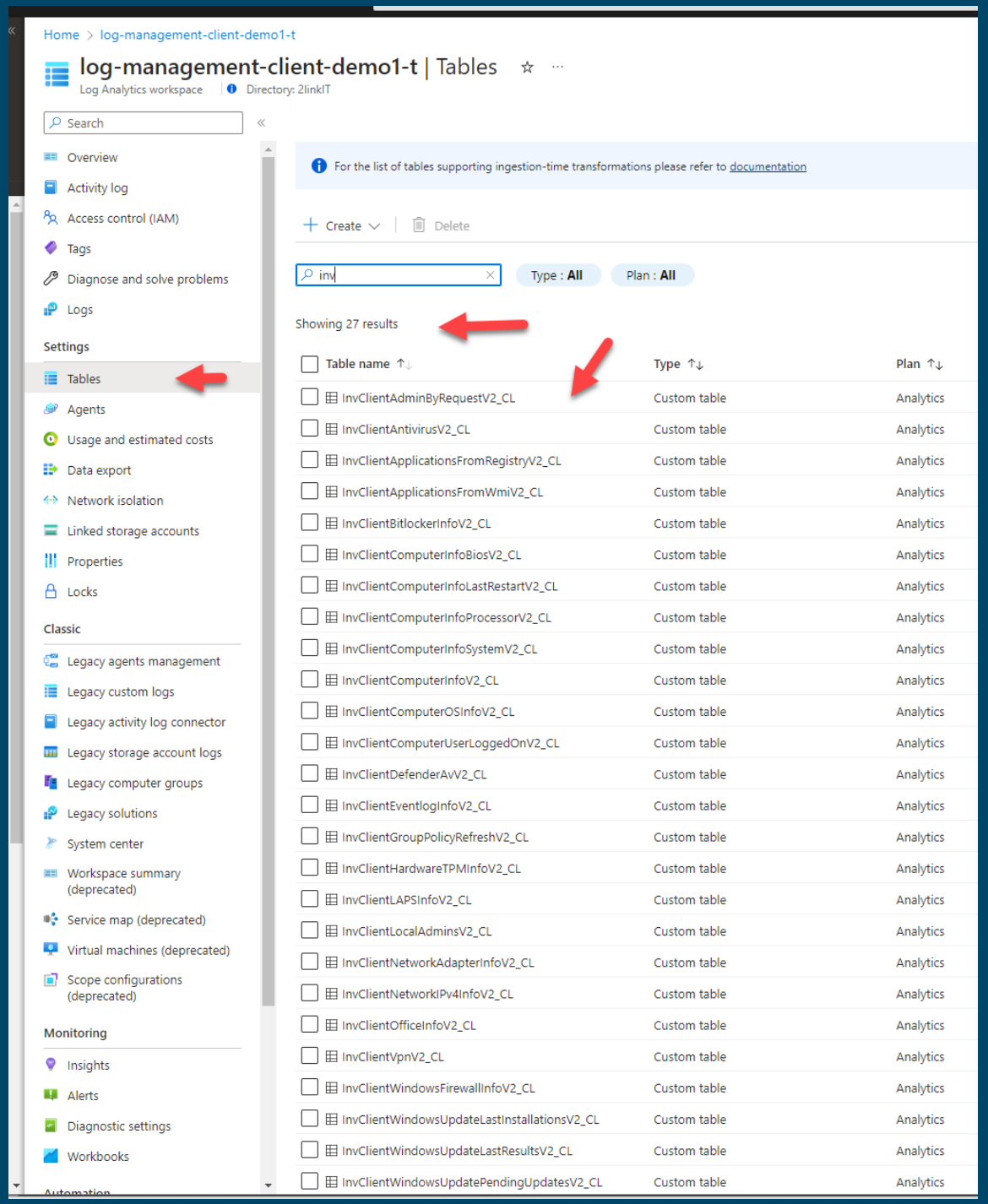
Resource JSON

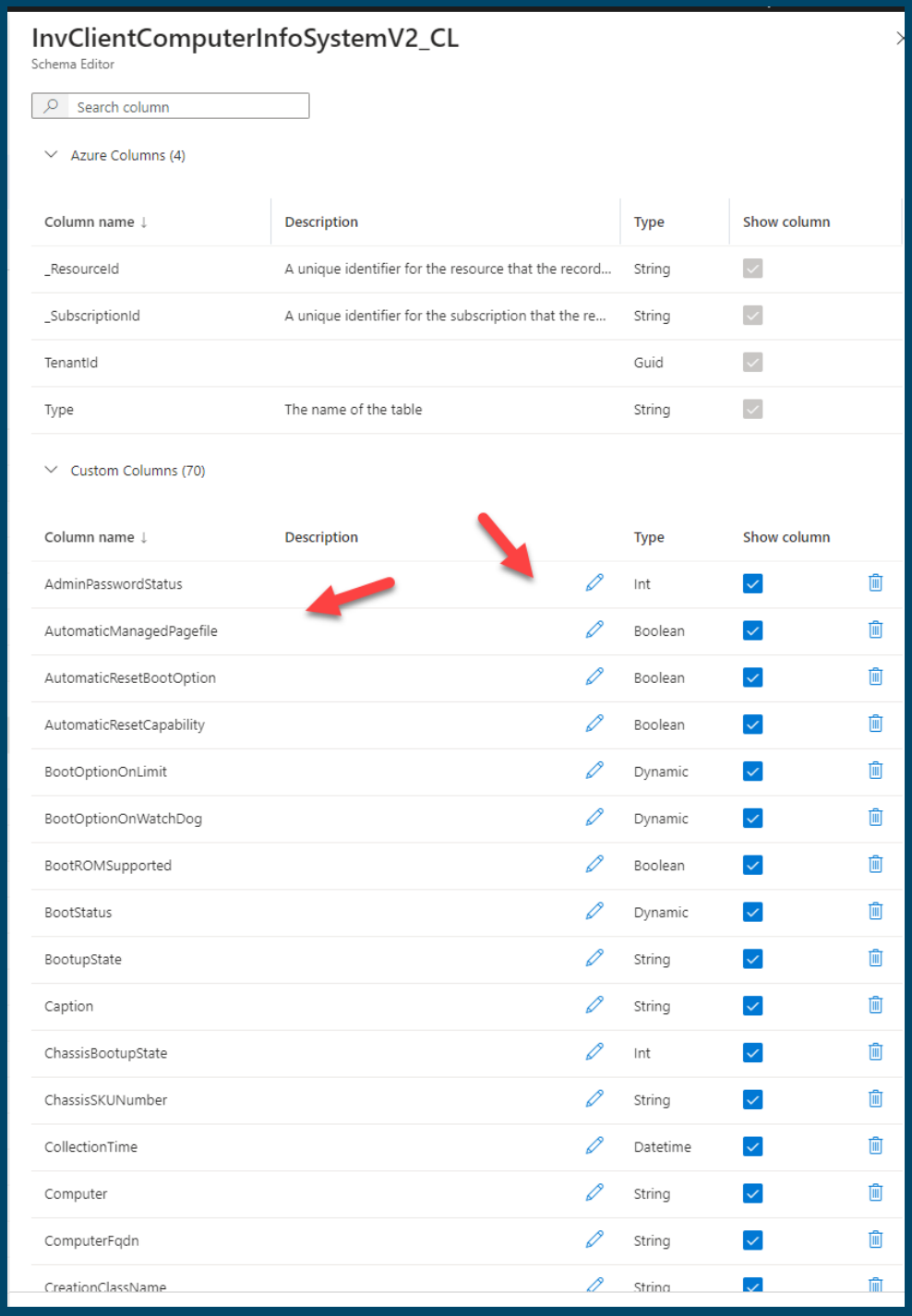
dcr-clt-InvClientComputerInfoSystemV2_CL

Resource ID: /subscriptions/fce4f282-fcc6-43fb-94d8-bf1701b862c3/resourceGroups/rg-dcr-log-management-client-demo1-t/providers/microsoft.insights/dataCol...

API version: 2022-06-01

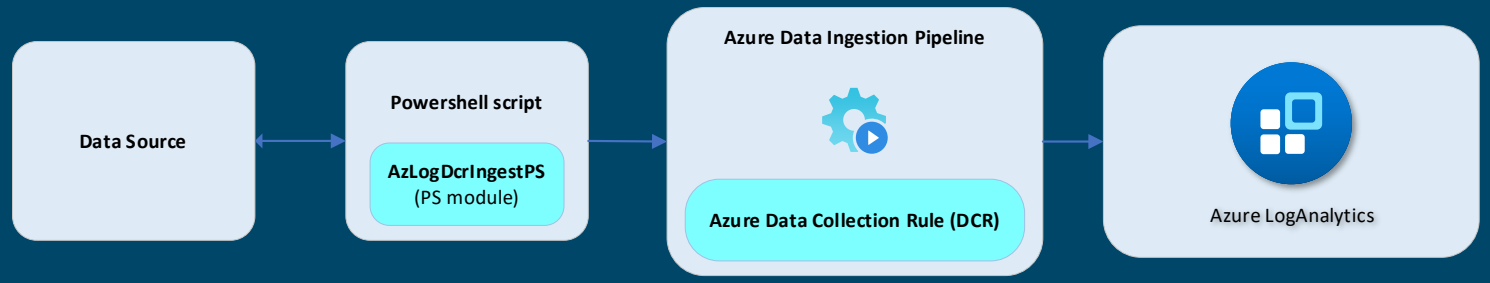

```
{
    "properties": {
        "immutableId": "dcr-857e7b752da1400bac1e302c194bf1f3",
        "dataCollectionEndpointId": "/subscriptions/fce4f282-fcc6-43fb-94d8-bf1701b862c3/resourceGroups/rg-dce-log-management-client
        "streamDeclarations": {
            "Custom-InvClientComputerInfoSystemV2_CL": {
                "columns": [
                    {
                        "name": "AdminPasswordStatus",
                        "type": "int"
                    },
                    {
                        "name": "AutomaticManagedPagefile",
                        "type": "boolean"
                    },
                    {
                        "name": "AutomaticResetBootOption",
                        "type": "boolean"
                    },
                    {
                        "name": "AutomaticResetCapability",
                        "type": "boolean"
                    },
                    {
                        "name": "BootOptionOnLimit",
                        "type": "dynamic"
                    },
                    {
                        "name": "BootOptionOnWatchDog",
                        "type": "dynamic"
                    },
                    {
                        "name": "BootROMSupported",
                        "type": "boolean"
                    },
                    {
                        "name": "BootStatus",
                        "type": "dynamic"
                    },
                    {
                        "name": "BootupState",
                        "type": "string"
                    },
                    {
                        "name": "Caption",
                        "type": "string"
                    },
                    {
                        "name": "ChassisBootupState",
                        "type": "int"
                    },
                    {
                        "name": "ChassisSKUNumber",
                        "type": "string"
                    },
                    {
```


Home > log-management-client-demo1-t
log-management-client-demo1-t | Tables
Log Analytics workspace | Directory: 2linkIT
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Logs
Settings
Tables
Agents
Usage and estimated costs
Data export
Network isolation
Linked storage accounts
Properties
Locks
Classic
Legacy agents management
Legacy custom logs
Legacy activity log connector
Legacy storage account logs
Legacy computer groups
Legacy solutions
System center
Workspace summary (deprecated)
Service map (deprecated)
Virtual machines (deprecated)
Scope configurations (deprecated)
Monitoring
Insights
Alerts
Diagnostic settings
Workbooks
For the list of tables supporting ingestion-time transformations please refer to documentation
Create
Delete
inv
Type : All
Plan : All
Showing 27 results
Table name
Type
Plan
InvClientAdminByRequestV2_CL Custom table Analytics
InvClientAntivirusV2_CL Custom table Analytics
InvClientApplicationsFromRegistryV2_CL Custom table Analytics
InvClientApplicationsFromWmiV2_CL Custom table Analytics
InvClientBitlockerInfoV2_CL Custom table Analytics
InvClientComputerInfoBiosV2_CL Custom table Analytics
InvClientComputerInfoLastRestartV2_CL Custom table Analytics
InvClientComputerInfoProcessorV2_CL Custom table Analytics
InvClientComputerInfoSystemV2_CL Custom table Analytics
InvClientComputerInfoV2_CL Custom table Analytics
InvClientComputerOSInfoV2_CL Custom table Analytics
InvClientComputerUserLoggedOnV2_CL Custom table Analytics
InvClientDefenderAvV2_CL Custom table Analytics
InvClientEventlogInfoV2_CL Custom table Analytics
InvClientGroupPolicyRefreshV2_CL Custom table Analytics
InvClientHardwareTPMInfoV2_CL Custom table Analytics
InvClientLAPSInfoV2_CL Custom table Analytics
InvClientLocalAdminsV2_CL Custom table Analytics
InvClientNetworkAdapterInfoV2_CL Custom table Analytics
InvClientNetworkIPv4InfoV2_CL Custom table Analytics
InvClientOfficeInfoV2_CL Custom table Analytics
InvClientVpnV2_CL Custom table Analytics
InvClientWindowsFirewallInfoV2_CL Custom table Analytics
InvClientWindowsUpdateLastInstallationsV2_CL Custom table Analytics
InvClientWindowsUpdateLastResultsV2_CL Custom table Analytics
InvClientWindowsUpdatePendingUpdatesV2_CL Custom table Analytics

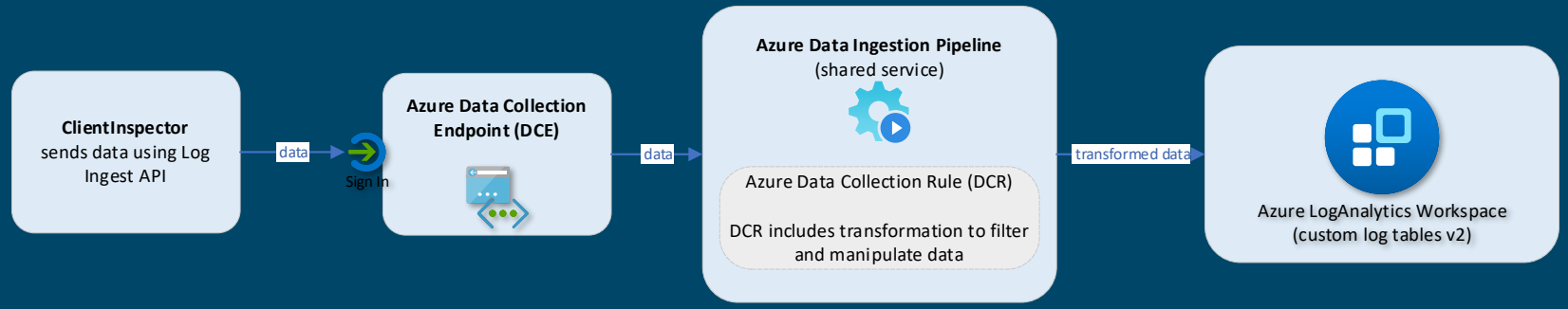

InvClientComputerInfoSystemV2_CL
Schema Editor
Search column
Azure Columns (4)
Column name
Description
Type
Show column
_ResourceId A unique identifier for the resource that the record... String
_SubscriptionId A unique identifier for the subscription that the re... String
TenantId Guid
Type The name of the table String
Custom Columns (70)
Column name
Description
Type
Show column
AdminPasswordStatus Int
AutomaticManagedPagefile Boolean
AutomaticResetBootOption Boolean
AutomaticResetCapability Boolean
BootOptionOnLimit Dynamic
BootOptionOnWatchDog Dynamic
BootROMSupported Boolean
BootStatus Dynamic
BootupState String
Caption String
ChassisBootupState Int
ChassisSKUNumber String
CollectionTime Datetime
Computer String
ComputerFqdn String
CreationClassName String

Use-Case | “AnyConnector” | AzLogDcrIngestPS

- Pull - Retrieve data from any 3rd party source using PS script (intermediate)



- Push - Collect data from endpoint - send data from endpoint (ClientInspector)



Detect local printers – replace with large multi-function printers (prepare business case)

PC replacement – yearly budget – Lenovo / Dell warranty

Cisco SecureX integration (REST API) – get alerts over

Cisco Prime (REST API) – wifi connectivity – which APs + SSID are users connecting to

SQL monitoring (WhoAmI)

WINDOWS UPDATE | CLIENTS | M...

Shared dashboard

Auto refresh : **Off** | UTC Time : **Past 24 hours**

PENDING UPDATES OLDER THAN 40 DAYS | CLIENTS | COUNT

log-management-client-demo1-t (@ 3/23 7:19 PM)

5

PENDING UPDATES, NO DRV, OLDER THAN 40 DAYS | CLIENTS | COUNT

log-management-client-demo1-t (@ 3/23 7:19 PM)

3

LAST WINDOWS UPDATE MORE THAN 40 DAYS AGO | CLIENTS...

log-management-client-demo1-t (@ 3/23 7:19 PM)

0

PENDING UPDATES OLDER THAN 40 DAYS | CLIENTS | SUM BY CLIENTS

log-management-client-demo1-t (@ 3/23 7:19 PM)

Search

Computer	total
STRV-ACW-LT-01	7
STRV-MEW-DT-02	6
STRV-CEW-LT-03	4
STRV-ACW-DT-01	2
STRV-MOK-LT-02	1

PENDING UPDATES, NO DRV, OLDER THAN 40 DAYS | CLIENTS | SUM BY CLIE...

log-management-client-demo1-t (@ 3/23 7:19 PM)

Search

Computer	total
STRV-ACW-LT-01	3
STRV-MEW-DT-02	2
STRV-CEW-LT-03	1

UPDATE SOURCE MICROSOFT UPDATE | CLIENTS | COUNT

log-management-client-demo1-t (@ 3/23 7:19 PM)

8

UPDATE SOURCE WINDOWS UPDATE | CLIENTS | LIST

log-management-client-demo1-t (@ 3/23 7:19 PM)

0

PENDING UPDATES OLDER THAN 40 DAYS | CLIENTS | LIST

log-management-client-demo1-t (@ 3/23 7:19 PM)

Search

Computer	UserLoggedOn	Title_	UpdateClassification	UpdateKBPublished	LastDeploymentChangeTime	CollectionTime	TimeGenerated	AutoDownload	AutoSelection	AutoSel
STRV-ACW-DT-01	2LINKIT\Anne	Lenovo Ltd. - Firmware - 1.0.0.110	Drivers	11/25/2022, 12:00:00 AM	11/25/2022, 12:00:00 AM	3/21/2023, 1:13:04 PM	3/21/2023, 1:13:08 PM	2	1	false
STRV-ACW-DT-01	2LINKIT\Anne	Hewlett-Packard - Imaging - Null Print - HP Photosmart 6...	Drivers	9/2/2018, 12:00:00 AM	9/2/2018, 12:00:00 AM	3/23/2023, 6:52:01 PM	3/23/2023, 6:52:03 PM	2	1	false
STRV-ACW-LT-01	2LINKIT\Anne	Apple, Inc. - USBDevice - 486.0.0.0	Drivers	11/20/2020, 12:00:00 AM	11/20/2020, 12:00:00 AM	3/22/2023, 12:15:17 PM	3/22/2023, 12:15:26 PM	2	1	false
STRV-ACW-LT-01	2LINKIT\Anne	Sikkerhedsopdatering 08-2022 til Windows 11 22H2 for x...	Security Updates	11/10/2022, 12:00:00 AM	11/10/2022, 12:00:00 AM	3/22/2023, 12:15:17 PM	3/22/2023, 12:15:26 PM	2	1	true
STRV-ACW-LT-01	2LINKIT\Anne	Microsoft Azure Information Protection Unified Labeling ...	Updates	11/28/2022, 12:00:00 AM	11/28/2022, 12:00:00 AM	3/22/2023, 12:15:17 PM	3/22/2023, 12:15:26 PM	0	0	false
STRV-ACW-LT-01	2LINKIT\Anne	Intel Corporation - System - 2.14.101.1	Drivers	11/1/2022, 12:00:00 AM	11/1/2022, 12:00:00 AM	3/22/2023, 12:15:17 PM	3/22/2023, 12:15:26 PM	2	1	false
STRV-ACW-LT-01	2LINKIT\Anne	Intel Corporation - SoftwareComponent - 2.17.100.2	Drivers	2/11/2023, 12:00:00 AM	2/11/2023, 12:00:00 AM	3/22/2023, 12:15:17 PM	3/22/2023, 12:15:26 PM	2	1	false
STRV-ACW-LT-01	2LINKIT\Anne	Lenovo - System - 1.2.0.11	Drivers	2/7/2023, 12:00:00 AM	2/7/2023, 12:00:00 AM	3/22/2023, 12:15:17 PM	3/22/2023, 12:15:26 PM	2	1	false
STRV-ACW-LT-01	2LINKIT\Anne	2023-01 Opdatering til Windows 11 Version 22H2 til x64-...	Critical Updates	1/18/2023, 12:00:00 AM	1/18/2023, 12:00:00 AM	3/22/2023, 12:15:17 PM	3/22/2023, 12:15:26 PM	2	1	true
STRV-CEW-LT-03	2LINKIT\Caroline	Realtek - Extension - 10.44.0.2	Drivers	11/11/2021, 12:00:00 AM	11/11/2021, 12:00:00 AM	3/23/2023, 2:04:46 PM	3/23/2023, 2:04:48 PM	2	1	false
STRV-CEW-LT-03	2LINKIT\Caroline	Lenovo - System - 1.2.0.11	Drivers	2/7/2023, 12:00:00 AM	2/7/2023, 12:00:00 AM	3/23/2023, 2:04:46 PM	3/23/2023, 2:04:48 PM	2	1	false

LOCAL ADMINS | CLIENTS | MANA...

Shared dashboard

Create | Upload | Refresh | Full screen | Edit | Manage sharing

Auto refresh : **Off** | UTC Time : **Past 24 hours**

DEVICES WITH NON-STANDARD MEMBERS LOCAL ADMINS G...

log-management-client-demo1-t (@ 3/23 7:21 PM)

8

DEVICES WITH NON-STANDARD MEMBERS LOCAL ADMINS GROUP | CLIENT...

log-management-client-demo1-t (@ 3/23 7:21 PM)

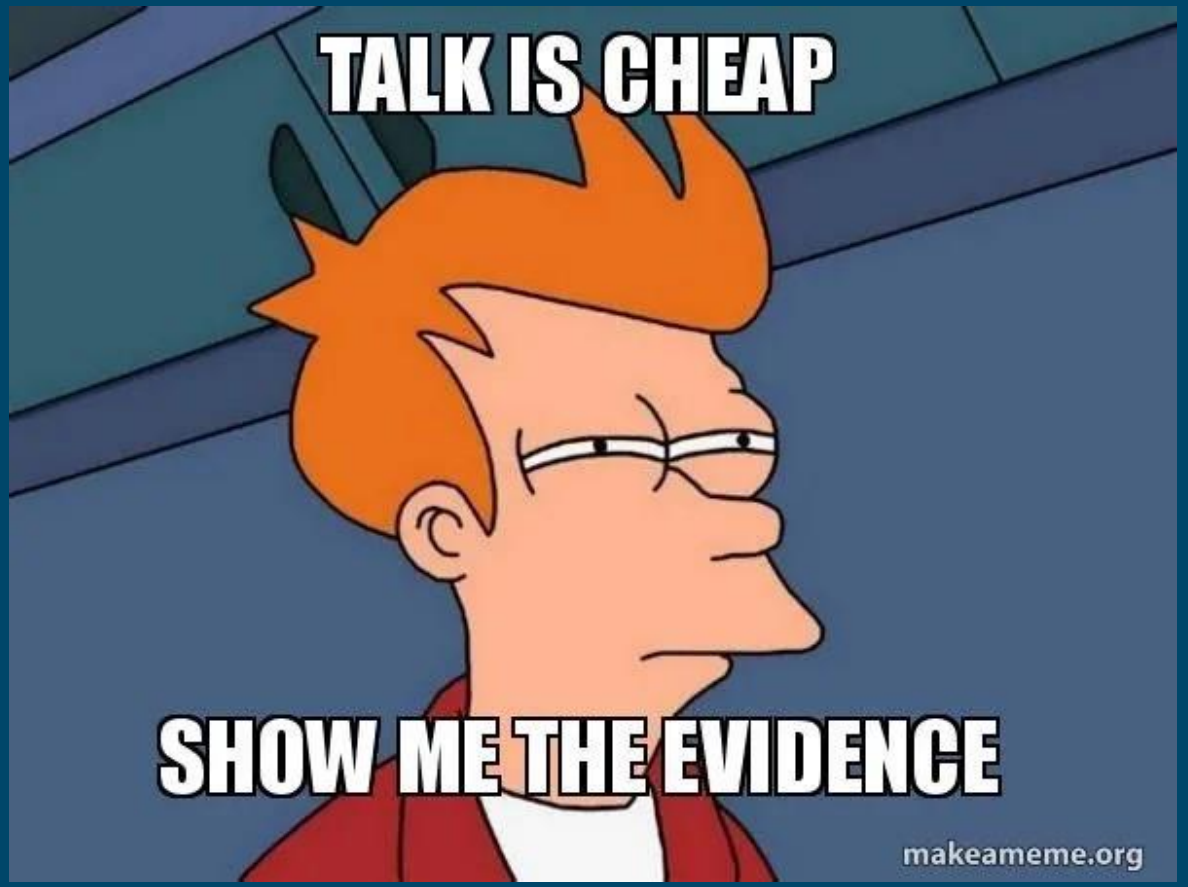
Computer
STRV-ACW-DT-01
STRV-MOK-LT-02
HEIM-NEW-DT-01
STRV-MOK-DT-02
STRV-CEW-LT-03
STRV-MEW-LT-02
STRV-MEW-DT-02

MEMBERS LOCAL ADMINS GROUP | CLIENTS | GROUPED

log-management-client-demo1-t (@ 3/23 7:21 PM)

Search

Group	Computer	UserLoggedOn
2LINKIT/Anne (2)		
WORKGROUP/STRV-MOK-LT-02/Morten Knudsen (1)		
2LINKIT/mok (2)		
2LINKIT/Niels.Waltorp (1)		
WORKGROUP/STRV-MOK-DT-02/mok (1)		
2LINKIT/Caroline (1)		
2LINKIT/magnus (2)		
WORKGROUP/STRV-ACW-LT-01/annew (1)		



INCOMPLIANT BITLOCKER | CLIENTS | COUNT

2

BITLOCKER COMPLIANT | CLIENTS | LIST

Search

Computer	UserLoggedOn	CollectionTime	OSDisk_DriveLetter	OSDisk_EncryptionPercentage	OSDisk_VolumeStatus	OSDisk_ProtectionStatus	OSDisk_CapacityGB	OSDisk_KeyProtector
STRV-ACW-DT-01	2LINKIT\Anne	3/23/2023, 6:52:33 PM	C:	100	1	1	235.475586	[{"KeyProtectorId":"{E19D31BA-B09E-4C44-B64C-D17FFE...
STRV-ACW-LT-01	2LINKIT\Anne	3/22/2023, 12:15:40 PM	C:	100	1	1	475.692383	[{"KeyProtectorId":"{2D3A1901-580A-474C-8C30-B8DCBE...
STRV-CEW-LT-03	2LINKIT\Caroline	3/23/2023, 2:04:53 PM	C:	100	1	1	475.897461	[{"KeyProtectorId":"{51FA6A6E-E255-44D4-B6E7-52EADC...
STRV-MEW-LT-02	2LINKIT\magnus	3/23/2023, 1:02:26 PM	C:	100	1	1	475.897461	[{"KeyProtectorId":"{27A4640A-A7D4-4865-BF34-6CB1F2...
STRV-MOK-DT-02	2LINKIT\mok	3/23/2023, 6:52:26 PM	C:	100	1	1	952.827148	[{"KeyProtectorId":"{384EB343-1213-4FF1-97E7-3F8926C7...
STRV-MOK-LT-02	2LINKIT\mok	3/23/2023, 3:55:53 PM	C:	100	1	1	952.660156	[{"KeyProtectorId":"{AB739D6B-C832-4EE0-834A-862D9A...

BITLOCKER INCOMPLIANT | CLIENTS | LIST

Search

Computer	UserLoggedOn	CollectionTime	OSDisk_DriveLetter	OSDisk_EncryptionPercentage	OSDisk_VolumeStatus	OSDisk_ProtectionStatus	OSDisk_CapacityGB	OSDisk_KeyProtector
HEIM-NEW-DT-01	2LINKIT\Niels.Waltorp	3/23/2023, 6:38:19 PM	C:	0	0	0	921.5879	[]
STRV-MEW-DT-02	2LINKIT\magnus	3/22/2023, 9:35:30 PM	C:	0	0	0	943.7178	[]

INVENTORY | CLIENTS | MANAGED...
Shared dashboard

+ Create | Upload | Refresh | Full screen | Edit | Manage sharing | Export | Clone | Assign tags | Delete | Feedback

Auto refresh : **Off** | UTC Time : **Past 24 hours**

STRV-MOK-DT-02	2LINKIT\mok	3/19/2023, 3:40:45 PM	LENOVO	11D1003VMX	STRV-MOK-DT-02	[{"Description":"Bluetooth Device (Personal Area Network...	true	16
STRV-MOK-LT-02	2LINKIT\mok	3/19/2023, 12:50:51 PM	Microsoft Corporation	Surface Book 3	STRV-MOK-LT-02	[{"Description":"ExpressVPN TAP Adapter","ConnectionID"...	true	8

INVENTORY OVERVIEW (OS) | CLIENTS | LIST
log-management-client-demo1-t (@ 3/19 4:15 PM)

Search

Computer	UserLoggedOn	CollectionTime	OsArchitecture	OsBootDevice	OsBuildNumber	OsBuildType	OsCodeSet	OsCountryCode	OsCurrentTimeZone	OsDataExecutionPrevention32BitA...	OsDataExecutionPreventionAvailab...	OsDataExecutionPreventio
STRV-ACW-DT-01	2LINKIT\Anne	3/19/2023, 3:44:11 PM	64-bit	\Device\HarddiskVolume1	22000	Multiprocessor Free	1252	45	60	true	true	true
STRV-ACW-DT-01	2LINKIT\Anne	3/19/2023, 3:44:11 PM	64-bit	\Device\HarddiskVolume1	22000	Multiprocessor Free	1252	45	60	true	true	true
STRV-ACW-DT-01	2LINKIT\Anne	3/19/2023, 3:44:11 PM	64-bit	\Device\HarddiskVolume1	22000	Multiprocessor Free	1252	45	60	true	true	true
STRV-ACW-DT-01	2LINKIT\Anne	3/19/2023, 3:44:11 PM	64-bit	\Device\HarddiskVolume1	22000	Multiprocessor Free	1252	45	60	true	true	true
STRV-ACW-DT-01	2LINKIT\Anne	3/19/2023, 3:44:11 PM	64-bit	\Device\HarddiskVolume1	22000	Multiprocessor Free	1252	45	60	true	true	true

INVENTORY OVERVIEW (WINDOWS) | CLIENTS | LIST
log-management-client-demo1-t (@ 3/19 4:15 PM)

Search

Computer	UserLoggedOn	CollectionTime	OsName	OsVersion	WindowsVersion	WindowsProductName	WindowsProductId	WindowsCurrentVersion	WindowsBuildLabEx	WindowsSystemRoot	WindowsRegisteredOw
STRV-ACW-DT-01	2LINKIT\Anne	3/19/2023, 3:44:11 PM	Microsoft Windows 11 Enterprise	10.0.22000	2009	Windows 10 Enterprise	00330-80000-00000-AA875	6.3	22000.1.amd64fre.co_release.210604-1628	C:\WINDOWS	2LINKIT
STRV-MOK-DT-02	2LINKIT\mok	3/19/2023, 3:40:45 PM	Microsoft Windows 11 Enterprise	10.0.22621	2009	Windows 10 Enterprise	00330-80000-00000-AA032	6.3	22621.1.amd64fre.ni_release.220506-1250	C:\WINDOWS	mok
STRV-MOK-LT-02	2LINKIT\mok	3/19/2023, 12:50:51 PM	Microsoft Windows 11 Enterprise	10.0.22621	2009	Windows 10 Enterprise	00330-80000-00000-AA845	6.3	22621.1.amd64fre.ni_release.220506-1250	C:\WINDOWS	Morten Knudsen

OFFICE | CLIENTS | MANAGED DAS...
Shared dashboard

Create | Upload | Refresh | Full screen | Edit | Manage sharing | Export | Clone | Assign tags | Delete | Feedback

Auto refresh : **Off** | UTC Time : **Past 24 hours**

Last updated: a few seconds ag

UPDATING O365 OFFICE NOT ENABLED | CLIENTS | COUNT
log-management-client-demo1-t (@ 3/19 4:16 PM)
0

INCOMPLIANT UPDATE CHANNEL O365 OFFICE | CLIENTS | CO...
log-management-client-demo1-t (@ 3/19 4:16 PM)
0

O365 OFFICE | CLIENTS | COUNT
log-management-client-demo1-t (@ 3/19 4:16 PM)
3

STANDALONE OFFICE 2016 | CLIENTS | COUNT
log-management-client-demo1-t (@ 3/19 4:16 PM)
0

LEGACY OFFICE | CLIENTS | COUNT
log-management-client-demo1-t (@ 3/19 4:16 PM)
0

O365 OFFICE | CLIENTS | LIST
log-management-client-demo1-t (@ 3/19 4:16 PM)

Computer	CollectionTime	UserLoggedOn	ProductReleaseIds	VersionToReport	OfficeMgmtCO...	Platform	ClientCulture	ClientFolder	CDNBaseUrl	OneDriveClientAddon	Tea
STRV-ACW-DT-01	3/19/2023, 3:44:23 PM	2LINKIT\Anne	O365ProPlusRetail	16.0.16130.20306	True	x64	da-dk	C:\Program Files\Common Files\Microsoft Shared\ClickTo...	http://officecdn.microsoft.com/pr/64256afe-f5d9-4f86-89...	INSTALLED	INS
STRV-MOK-DT-02	3/19/2023, 3:41:06 PM	2LINKIT\mok	O365ProPlusRetail,ProjectProRetail,VisioProRetail	16.0.16130.20306	True	x64	en-us	C:\Program Files\Common Files\Microsoft Shared\ClickTo...	http://officecdn.microsoft.com/pr/64256afe-f5d9-4f86-89...	INSTALLED	INS
STRV-MOK-LT-02	3/19/2023, 12:51:39 PM	2LINKIT\mok	O365ProPlusRetail,ProjectProRetail,VisioProRetail	16.0.16130.20218		x64	en-us	C:\Program Files\Common Files\Microsoft Shared\ClickTo...	http://officecdn.microsoft.com/pr/64256afe-f5d9-4f86-89...	INSTALLED	INS

Meet the PMs in charge of Azure Workbooks & Azure Dashboards – John & Shikha

(Seattle, USA)

DEFENDER ANTIVIRUS | CLIENTS | ...

Shared dashboard

Create | Upload | Refresh | Full screen | Edit | Manage sharing | Export | Clone | Assign tags | Delete | Feedback

Auto refresh : **Off** | UTC Time : **Past 24 hours**

COMPLIANT DEFENDER AV | CLIENTS | COUNT
log-management-client-demo1-t (@ 3/23 7:24 PM)
8

INCOMPLIANT DEFENDER AV | CLIENTS | COUNT
log-management-client-demo1-t (@ 3/23 7:24 PM)
1

DEFENDER AV NOT INSTALED OR ENABLED | CLIENTS | COUNT
log-management-client-demo1-t (@ 3/23 7:24 PM)
0

SIGNATURE TOO OLD DEFENDER AV | CLIENTS | COUNT
log-management-client-demo1-t (@ 3/23 7:24 PM)
0

AM SERVICE NOT RUNNING DEFENDER AV | CLIENTS | COUNT
log-management-client-demo1-t (@ 3/23 7:24 PM)
0

AM VERSION TOO OLD DEFENDER AV | CLIENTS | COUNT
log-management-client-demo1-t (@ 3/23 7:24 PM)
0

REALTIME PROTECTION NOT RUNNING DEFENDER AV | CLIEN...
log-management-client-demo1-t (@ 3/23 7:24 PM)
0

ANTISPYWARE TOO OLD DEFENDER AV | CLIENTS | COUNT
log-management-client-demo1-t (@ 3/23 7:24 PM)
0

PASSIVE / EDB BLOCK MODE DEFENDER AV | CLIENTS | COUNT
log-management-client-demo1-t (@ 3/23 7:24 PM)
0

ANTISPYWARE NOT ENABLED DEFENDER AV | CLIENTS | COUNT
log-management-client-demo1-t (@ 3/23 7:24 PM)
0

TAMPERPROTECTION NOT ENABLED DEFENDER AV | CLIENTS |...
log-management-client-demo1-t (@ 3/23 7:24 PM)
1

ONACCESSPROTECTION DISABLED DEFENDER AV | CLIENTS | C...
log-management-client-demo1-t (@ 3/23 7:24 PM)
0

GROUP POLICY LAST REFRESH | CLIENTS | LIST

log-management-client-demo1-t (@ 3/19 4:16 PM)

Search

Computer	UserLoggedOn	CollectionTime	GPLastRefreshDays	GPLastRefresh
STRV-MOK-DT-02	2LINKIT\mok	3/19/2023, 3:42:29 PM	0	3/19/2023, 3:28:11 PM
STRV-ACW-DT-01	2LINKIT\Anne	3/19/2023, 3:45:53 PM	0	3/19/2023, 3:26:35 PM
STRV-MOK-LT-02	2LINKIT\mok	3/19/2023, 12:52:53 PM	0	3/19/2023, 12:36:01 PM

COMPLIANT WINDOWS FIREWALL | CLIENTS | LIST

log-management-client-demo1-t (@ 3/19 4:17 PM)

Search

Computer	Profile	TimeGenerated	TimeGenerated1	AllowInboundRules	AllowLocalFirewallRules	AllowLocalIPsecRules	AllowUnicastResponseToMulticast	Allo
STRV-ACW-DT-01	Domain	3/19/2023, 3:45:52 PM	3/19/2023, 3:45:53 PM	1	1	1	1	
STRV-ACW-DT-01	Private	3/19/2023, 3:45:52 PM	3/19/2023, 3:45:53 PM	1	1	1	1	
STRV-ACW-DT-01	Public	3/19/2023, 3:45:52 PM	3/19/2023, 3:45:53 PM	1	1	1	1	
STRV-MOK-DT-02	Domain	3/19/2023, 3:42:29 PM	3/19/2023, 3:42:30 PM	1	0	0	1	
STRV-MOK-DT-02	Private	3/19/2023, 3:42:29 PM	3/19/2023, 3:42:30 PM	1	0	0	1	
STRV-MOK-DT-02	Public	3/19/2023, 3:42:29 PM	3/19/2023, 3:42:30 PM	1	0	0	1	
STRV-MOK-LT-02	Domain	3/19/2023, 12:52:52 PM	3/19/2023, 12:52:52 PM	1	0	0	1	
STRV-MOK-LT-02	Private	3/19/2023, 12:52:52 PM	3/19/2023, 12:52:52 PM	1	0	0	1	
STRV-MOK-LT-02	Public	3/19/2023, 12:52:52 PM	3/19/2023, 12:52:52 PM	1	0	0	1	

NETWORK INFORMATION | CLIEN...

Shared dashboard

Create | Upload | Refresh | Full screen | Edit | Manage sharing | Export | Clone | Assign tags | Delete | Feedback

Auto refresh : **Off** | UTC Time : **Past 24 hours**

NETWORK ADAPTERS | CLIENTS | LIST

log-management-client-demo1-t (@ 3/23 7:23 PM)

Search

Computer	UserLoggedOn	CollectionTime	Name	InterfaceDescription	InterfaceAlias	TimeGenerated
HEIM-NEW-DT-01	2LINKIT\Niels.Waltorp	3/23/2023, 6:38:32 PM	Ethernet	Realtek PCIe GBE Family Controller	Ethernet	3/23/2023, 6:38:36 PM
STRV-ACW-DT-01	2LINKIT\Anne	3/23/2023, 6:52:41 PM	Ethernet	Intel(R) Ethernet Connection (7) I219-LM	Ethernet	3/23/2023, 6:52:44 PM
STRV-ACW-DT-01	2LINKIT\Anne	3/23/2023, 6:52:41 PM	Wi-Fi	Intel(R) Wireless-AC 9560 160MHz	Wi-Fi	3/23/2023, 6:52:44 PM
STRV-ACW-DT-01	2LINKIT\Anne	3/23/2023, 6:52:41 PM	Bluetooth-netværksforbindelse	Bluetooth Device (Personal Area Network)	Bluetooth-netværksforbindelse	3/23/2023, 6:52:44 PM
STRV-ACW-LT-01	2LINKIT\Anne	3/22/2023, 12:15:54 PM	Wi-Fi	Intel(R) Wireless-AC 9560 160MHz	Wi-Fi	3/22/2023, 12:15:53 PM
STRV-CEW-LT-03	2LINKIT\Caroline	3/23/2023, 2:05:06 PM	Wi-Fi	Realtek RTL8852BE WiFi 6 802.11ax PCIe Adapter	Wi-Fi	3/23/2023, 2:05:08 PM
STRV-CEW-LT-03	2LINKIT\Caroline	3/23/2023, 2:05:06 PM	Bluetooth Network Connection	Bluetooth Device (Personal Area Network)	Bluetooth Network Connection	3/23/2023, 2:05:08 PM
STRV-MEW-DT-02	2LINKIT\magnus	3/22/2023, 9:35:42 PM	Ethernet	Realtek PCIe GbE Family Controller	Ethernet	3/22/2023, 9:35:45 PM
STRV-MEW-DT-02	2LINKIT\magnus	3/22/2023, 9:35:42 PM	LAN-forbindelse	TAP-Windows Adapter V9	LAN-forbindelse	3/22/2023, 9:35:45 PM
STRV-MEW-LT-02	2LINKIT\magnus	3/23/2023, 1:02:48 PM	Bluetooth Network Connection	Bluetooth Device (Personal Area Network)	Bluetooth Network Connection	3/23/2023, 1:02:52 PM

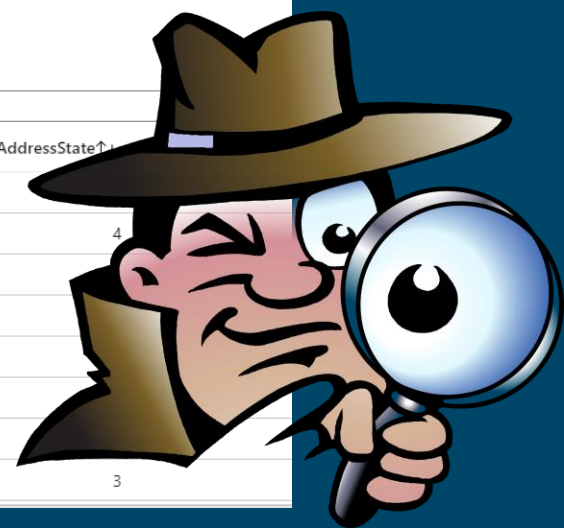
⚠ Columns were limited to the first 100

IP INFORMATION | CLIENTS | LIST

log-management-client-demo1-t (@ 3/23 7:23 PM)

Search

Computer	UserLoggedOn	CollectionTime	InterfaceAlias	TimeGenerated	Address	AddressFamily	AddressOrigin	AddressState
HEIM-NEW-DT-01	2LINKIT\Niels.Waltorp	3/23/2023, 6:38:37 PM	Loopback Pseudo-Interface 1	3/23/2023, 6:38:40 PM		2	0	
HEIM-NEW-DT-01	2LINKIT\Niels.Waltorp	3/23/2023, 6:38:37 PM	Ethernet	3/23/2023, 6:38:40 PM		2	0	4
STRV-ACW-DT-01	2LINKIT\Anne	3/23/2023, 6:52:44 PM	Ethernet	3/23/2023, 6:52:46 PM		2	0	
STRV-ACW-DT-01	2LINKIT\Anne	3/23/2023, 6:52:44 PM	LAN-forbindelse* 1	3/23/2023, 6:52:46 PM		2	0	
STRV-ACW-DT-01	2LINKIT\Anne	3/23/2023, 6:52:44 PM	Bluetooth-netværksforbindelse	3/23/2023, 6:52:46 PM		2	0	
STRV-ACW-DT-01	2LINKIT\Anne	3/23/2023, 6:52:44 PM	LAN-forbindelse* 12	3/23/2023, 6:52:46 PM		2	0	
STRV-ACW-DT-01	2LINKIT\Anne	3/23/2023, 6:52:44 PM	Loopback Pseudo-Interface 1	3/23/2023, 6:52:46 PM		2	0	
STRV-ACW-DT-01	2LINKIT\Anne	3/23/2023, 6:52:44 PM	Wi-Fi	3/23/2023, 6:52:46 PM		2	0	3

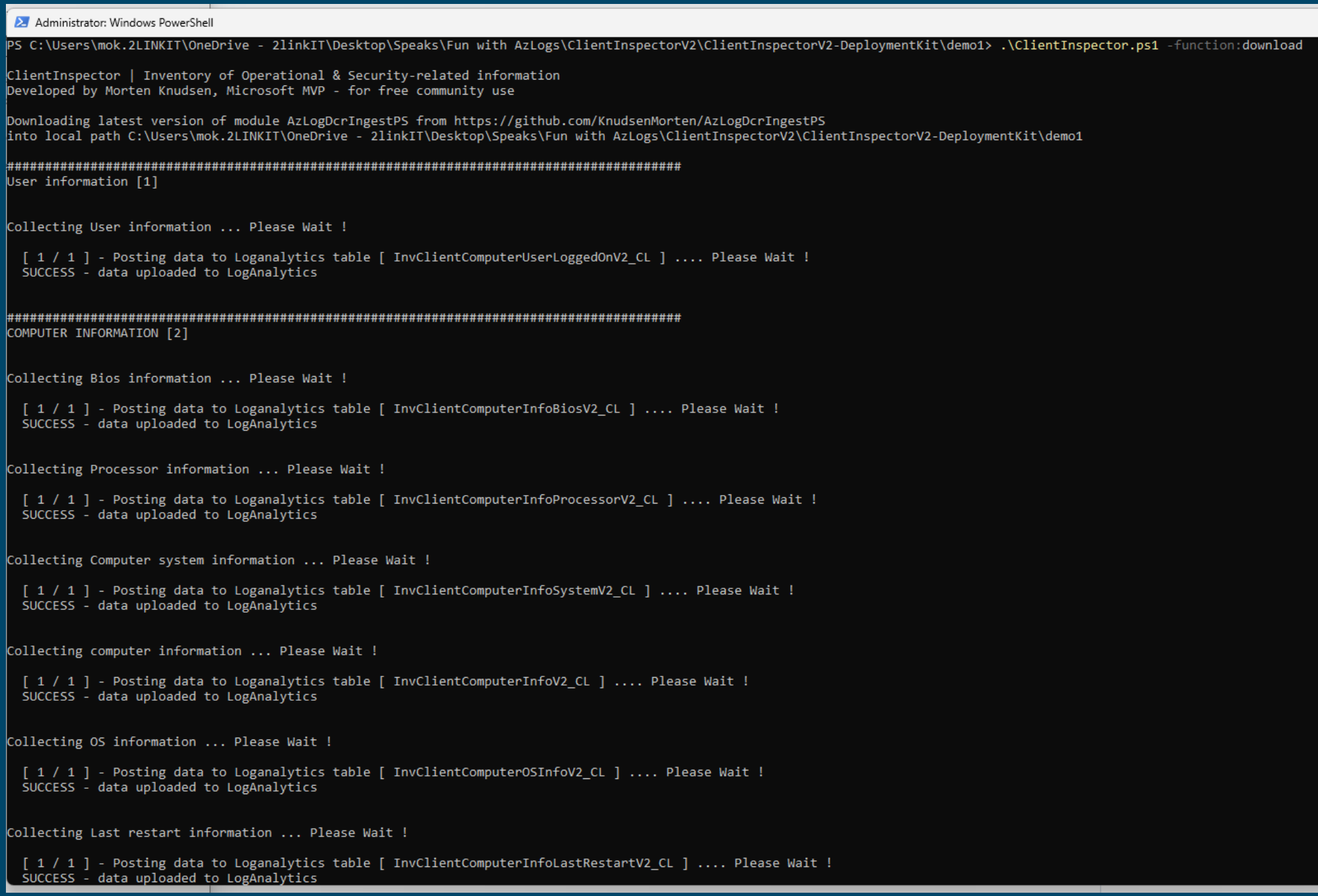


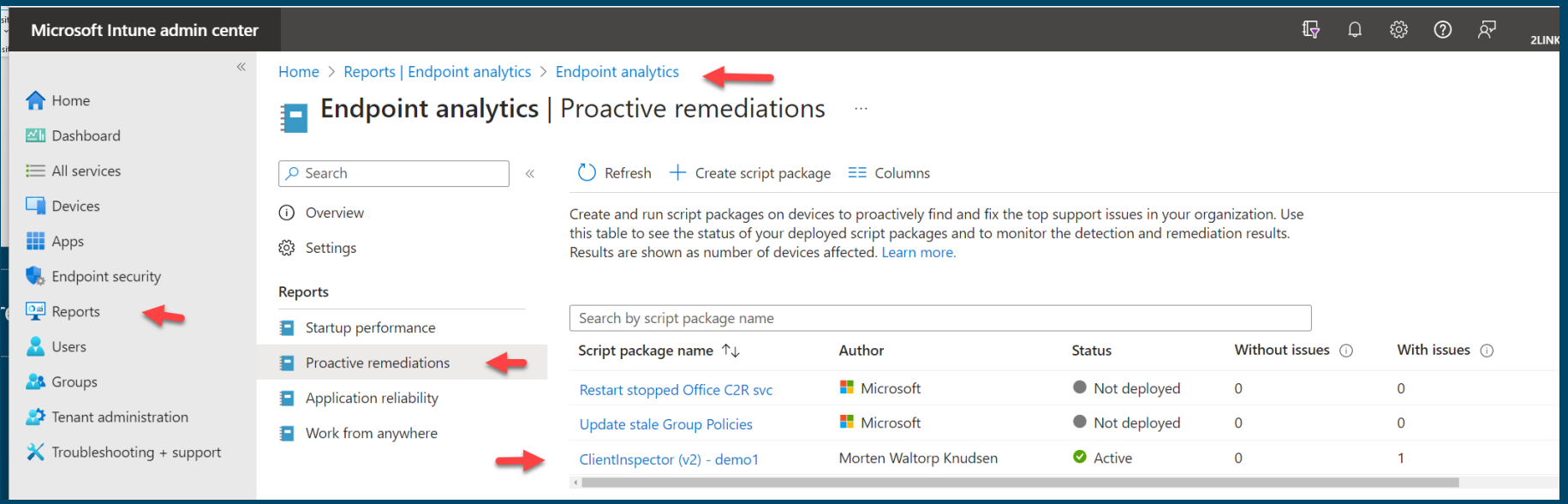
Warranty lookup Lenovo – via collected data (online)

Run with

ConfigMgr
Intune
any deployment-tool

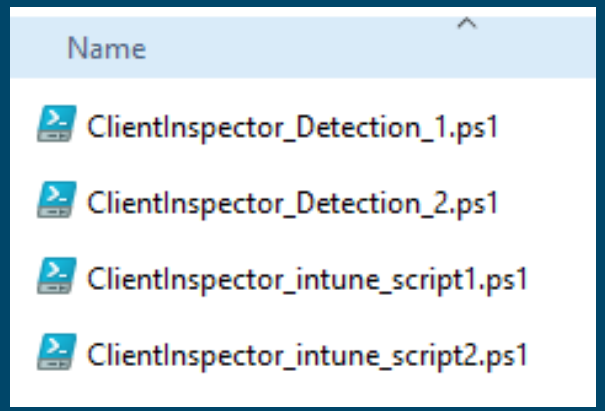
Servers:
RemotePS
CustomScript Extension

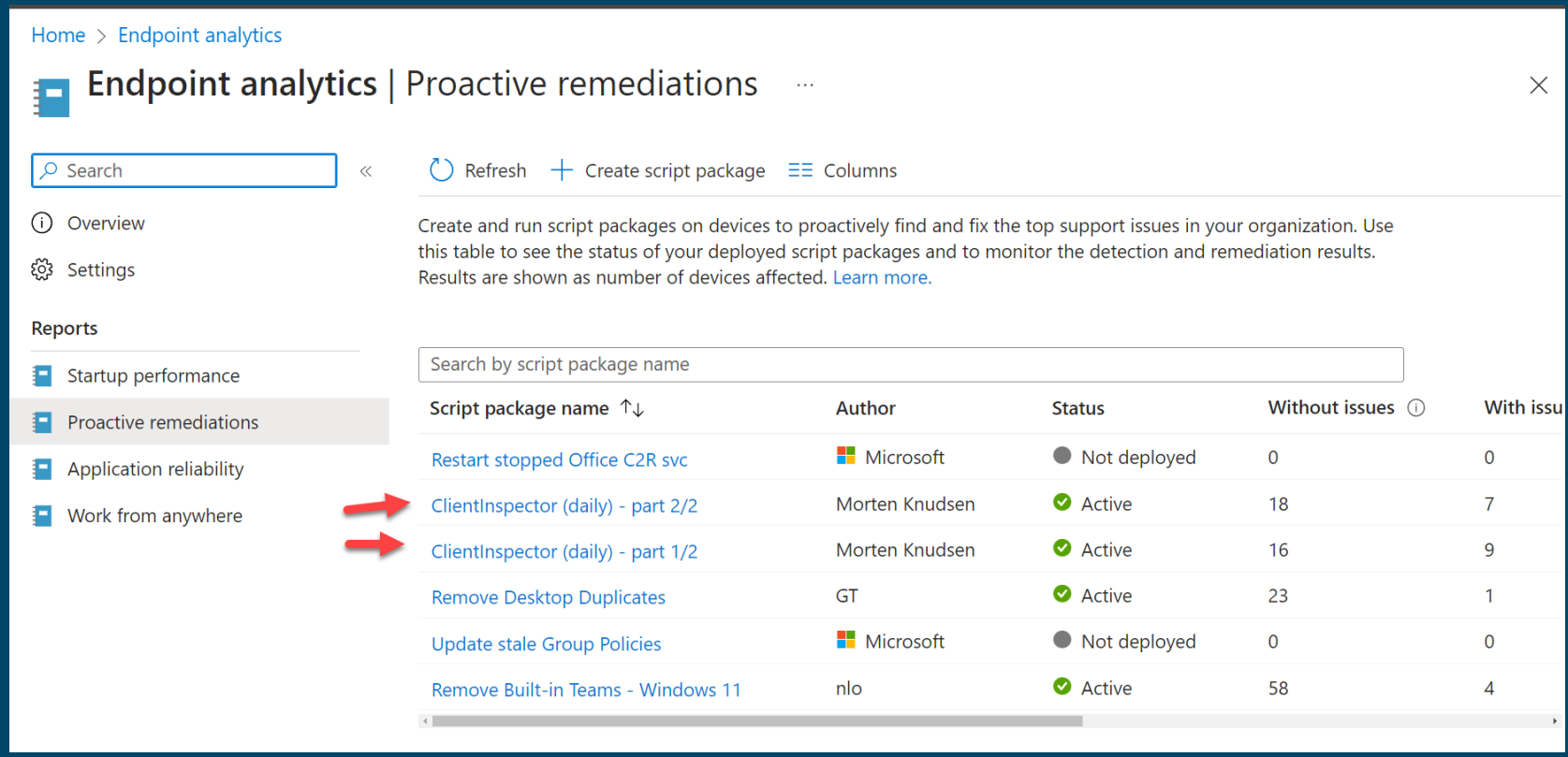




Intune deployment (<200 Kb in size)

Intune deployment >200 Kb size, split

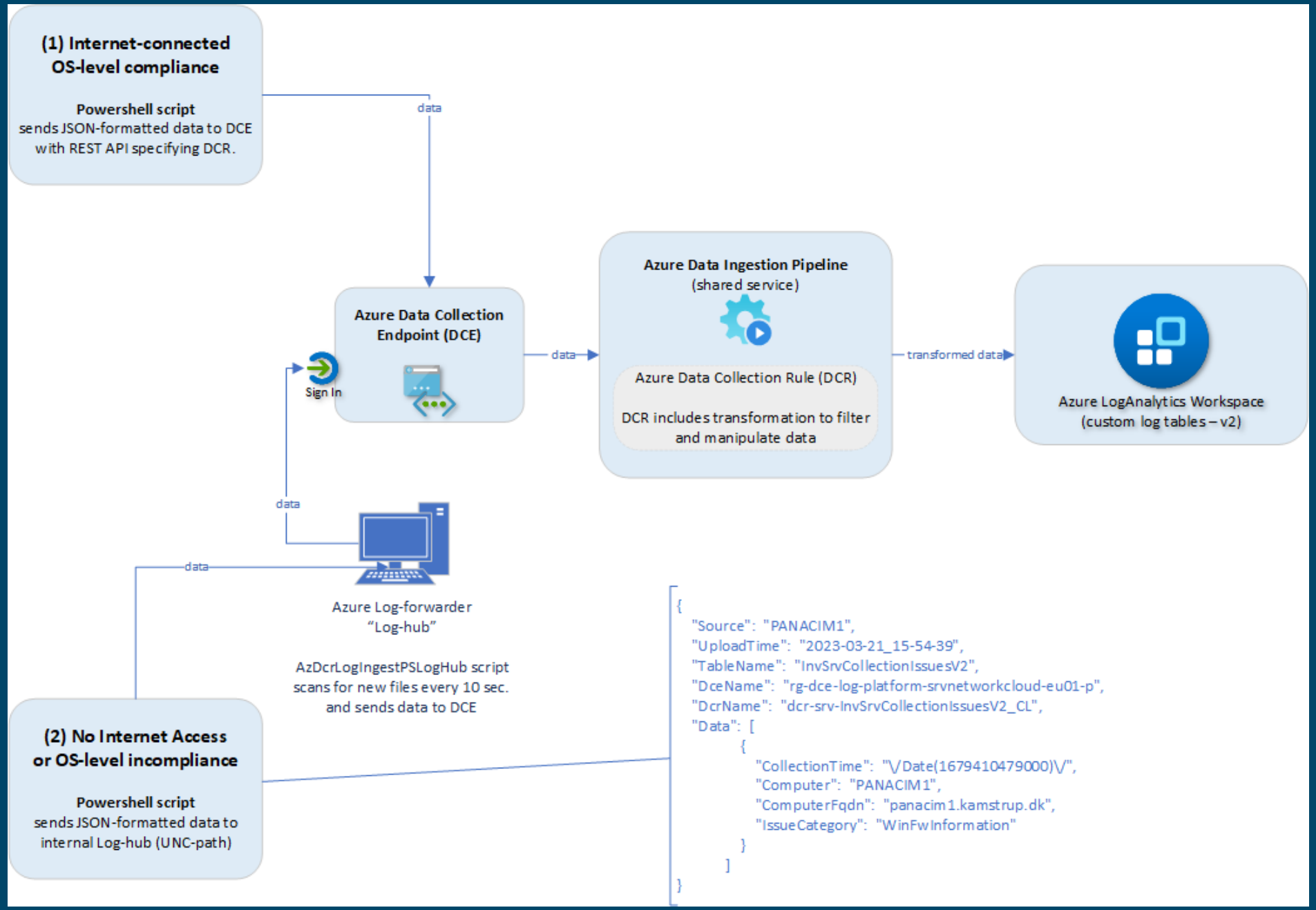


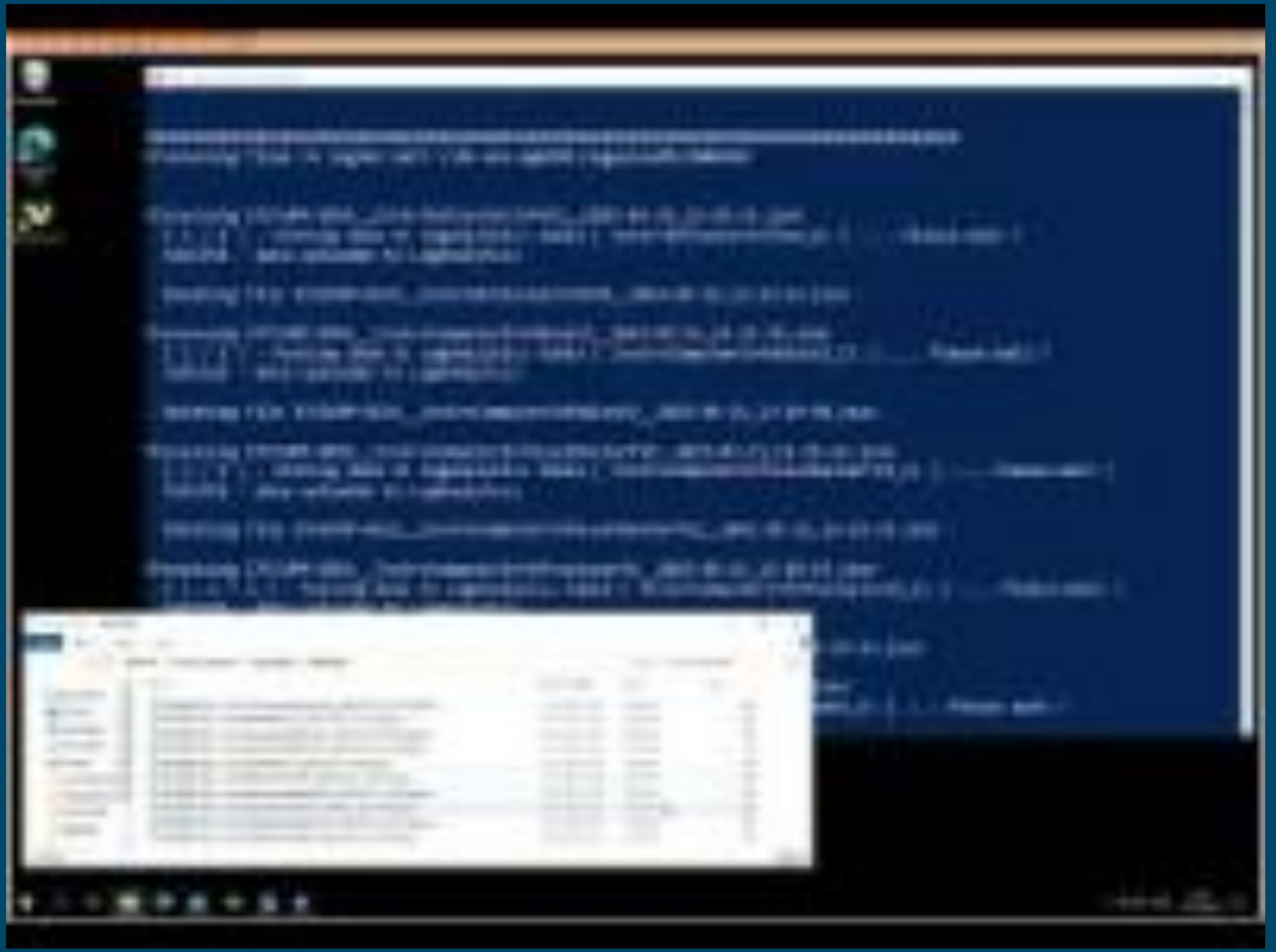


LogHub

Available on Github

Free





Query

Workbooks & Dashboards

“AnyConnector” | AzLogDcrIngestPS

Variables (1/4)

naming - where to send the data

```
#--------------------------------------------------------------------
# Variables
#--------------------------------------------------------------------

    $TableName   = 'InvClientDefenderAvV2'    # must not contain _CL
    $DcrName     = "dcr-" + $AzDcrPrefix + "-" + $TableName + "_CL"
```

Data Collection (2/4)

```powershell
#-----------------------------------------------------------------
# Collecting data (in)
#-----------------------------------------------------------------

    Write-Output ""
    Write-Output "Collecting Bios information ... Please Wait !"

    $DataVariable = Get-CimInstance -ClassName Win32_BIOS
```

```powershell
#-----------------------------------------------------------------
# Collecting data (in)
#-----------------------------------------------------------------

    Write-Output ""
    Write-Output "Collecting Microsoft Defender Antivirus information ... Please Wait !"

    $MPComputerStatus = Get-MpComputerStatus
    $MPPreference = Get-MpPreference
```

Data Manipulation (3/4)

ensure data is in correct format and any "noice" was removed and relevant information has been added

```powershell
# removing apps without DisplayName fx KBs
$DataVariable = $DataVariable | Where-Object { $_.DisplayName -ne $null }

# convert PS object and remove PS class information
$DataVariable = Convert-PSArrayToObjectFixStructure -Data $DataVariable -Verbose:$Verbose

# add CollectionTime to existing array
$DataVariable = Add-CollectionTimeToAllEntriesInArray -Data $DataVariable -Verbose:$Verbose

# add Computer, ComputerFqdn & UserLoggedOn info to existing array
$DataVariable = Add-ColumnDataToAllEntriesInArray -Data $DataVariable -Column1Name Computer -Column1Data $Env:ComputerName -Column2Name ComputerFqdn -Column2

# Get insight about the schema structure of an object BEFORE changes. Command is only needed to verify columns in schema
# $SchemaBefore = Get-ObjectSchemaAsArray -Data $DataVariable

# Remove unnecessary columns in schema
$DataVariable = Filter-ObjectExcludeProperty -Data $DataVariable -ExcludeProperty Memento*,Inno*,'(default)',1033 -Verbose:$Verbose

# Validating/fixing schema data structure of source data
$DataVariable = ValidateFix-AzLogAnalyticsTableSchemaColumnNames -Data $DataVariable -Verbose:$Verbose

# Aligning data structure with schema (requirement for DCR)
$DataVariable = Build-DataArrayToAlignWithSchema -Data $DataVariable -Verbose:$Verbose
```

Data Out (4/4)

send to LogAnalytics - combined functions

```
#-------------------------------------------------------------------------------------------
# Create/Update Schema for LogAnalytics Table & Data Collection Rule schema
#-------------------------------------------------------------------------------------------

    CheckCreateUpdate-TableDcr-Structure -AzLogWorkspaceResourceId $LogAnalyticsWorkspaceResourceId `
                                         -AzAppId $LogIngestAppId -AzAppSecret $LogIngestAppSecret -TenantId $TenantId -Verbose:$Verbose `
                                         -DceName $DceName -DcrName $DcrName -TableName $TableName -Data $DataVariable `
                                         -LogIngestServicePricipleObjectId $AzDcrLogIngestServicePrincipalObjectId `
                                         -AzDcrSetLogIngestApiAppPermissionsDcrLevel $AzDcrSetLogIngestApiAppPermissionsDcrLevel `
                                         -AzLogDcrTableCreateFromAnyMachine $AzLogDcrTableCreateFromAnyMachine `
                                         -AzLogDcrTableCreateFromReferenceMachine $AzLogDcrTableCreateFromReferenceMachine

#-------------------------------------------------------------------------------------------
# Upload data to LogAnalytics using DCR / DCE / Log Ingestion API
#-------------------------------------------------------------------------------------------

    Post-AzLogAnalyticsLogIngestCustomLogDcrDce-Output -DceName $DceName -DcrName $DcrName -Data $DataVariable -TableName $TableName `
                                                       -AzAppId $LogIngestAppId -AzAppSecret $LogIngestAppSecret -TenantId $TenantId -Verbose:$Verbose
```

Detailed Documentation

https://github.com/KnudsenMorten/AzLogDcrIngestPS

Videos

I have provided 4 demos for you to try, but if you want to see it first using video, check out these videos:

Video 3m 19s - Running ClientInspector using commandline (normal mode)
Video 1m 40s - Automatic creation of 2 tables & DCRs (verbose mode)
Video 1m 37s - Automatic creation of 2 tables & DCRs (normal mode)
Video 1m 34s - See schema of DCR and table)
Video 2m 19s - Data manipulation
Video 1m 58s - Kusto queries against data
Video 3m 01s - Dashboards
Video 0m 48s - Sample usage of data - lookup against Ler
Video 7m 25s - Deployment via ClientInspector Deployme

Download latest version

You can download latest version of AzLogDcrIngestPS here

Install AzLogDcrIngestPS from Powershell Gallery

```
install-module AzLogDcrIngestPS
```

Download AzLogDcrIngestPS module from this Github rep

Quick links for more information

How to get started in your own environment (demo)
Background for building this Powershell module
Deep-dive about Azure Data Collection Rules (DCRs)
Deep-dive about Log Ingestion API
Architecture, Schema & Networking
Security
Source data - what data can I use ?
Example of how to use the functions
How can I modify the schema of LogAnalytics table & Data
How to enable verbose-mode & get more help ?
Integration of AzLogDcrIngest in your scripts
Function synopsis
Detailed - Data Manipulation
Detailed - Table/DCR/Schema/Transformation managemer
Detailed - Data Out (upload to Azure LogAnalytics) Detaile
Contact me

```
PS C:\Users\mok.2LINKIT> get-command -module azlogdcringestps

CommandType     Name                                               Version    Source
-----------     ----                                               -------    ------
Function        Add-CollectionTimeToAllEntriesInArray              1.2.36     azlogdcringestps
Function        Add-ColumnDataToAllEntriesInArray                  1.2.36     azlogdcringestps
Function        Build-DataArrayToAlignWithSchema                   1.2.36     azlogdcringestps
Function        CheckCreateUpdate-TableDcr-Structure               1.2.36     azlogdcringestps
Function        Convert-CimArrayToObjectFixStructure               1.2.36     azlogdcringestps
Function        Convert-PSArrayToObjectFixStructure                1.2.36     azlogdcringestps
Function        CreateUpdate-AzDataCollectionRuleLogIngestCusto... 1.2.36     azlogdcringestps
Function        CreateUpdate-AzLogAnalyticsCustomLogTableDcr       1.2.36     azlogdcringestps
Function        Delete-AzDataCollectionRules                       1.2.36     azlogdcringestps
Function        Delete-AzLogAnalyticsCustomLogTables               1.2.36     azlogdcringestps
Function        Filter-ObjectExcludeProperty                       1.2.36     azlogdcringestps
Function        Get-AzAccessTokenManagement                        1.2.36     azlogdcringestps
Function        Get-AzDataCollectionRuleTransformKql               1.2.36     azlogdcringestps
Function        Get-AzDceListAll                                   1.2.36     azlogdcringestps
```

```
PS C:\Users\mok.2LINKIT> get-help Add-CollectionTimeToAllEntriesInArray -full

NAME
    Add-CollectionTimeToAllEntriesInArray

SYNOPSIS
    Add property CollectionTime (based on current time) to all entries on the object


SYNTAX
    Add-CollectionTimeToAllEntriesInArray [-Data] <Array> [<CommonParameters>]


DESCRIPTION
    Gives capability to do proper searching in queries to find latest set of records with same collection ti
    Time Generated cannot be used when you are sending data in batches, as TimeGenerated will change
    An example where this is important is a complete list of applications for a computer. We want all applic
    ions to
    show up when queriying for the latest data


PARAMETERS
    -Data <Array>
        Object to modify

        Required?                    true
        Position?                    1
        Default value
        Accept pipeline input?       false
        Accept wildcard characters?  false

    <CommonParameters>
        This cmdlet supports the common parameters: Verbose, Debug,
        ErrorAction, ErrorVariable, WarningAction, WarningVariable,
        OutBuffer, PipelineVariable, and OutVariable. For more information, see
        about_CommonParameters (https:/go.microsoft.com/fwlink/?LinkID=113216).

INPUTS
    None. You cannot pipe objects


OUTPUTS
    Updated object with CollectionTime
```

KnudsenMorten / AzLogDcrIngestPS Public

Notifications | Fork 0 | Star 0

Code | Issues | Pull requests | Discussions | Actions | Projects | Security

main | AzLogDcrIngestPS / RELEASENOTES | Go to file

KnudsenMorten def — Latest commit bc2916f 2 days ago — History

1 contributor

29 lines (18 sloc) | 1.35 KB | Raw | Blame

```
RELEASE NOTES
v1.2.38  Changed the logic around SchemaMode = Merge, so the schema in DCR will be based on LogAnalytics tabl

v1.2.37  Adding another check to SchemaMode = Merge, so it will support existing properties are changing type

v1.2.36  Bugfix

v1.2.35  Changing so $AzDcrLogIngestServicePrincipalObjectId is not a mandatory parameter

v1.2.34  Bugfix - schemamode = merge wasn't updating table correctly

v1.2.33  Bugfix - signature was by mistake in source file (removed)

v1.2.32  Bugfix - skip TimeGenerated in DCR table schema when doing a merge. TimeGenerated only exist in tabl

v1.2.31  Added parameter SchemaMode = Merge/Overwrite for functions CheckCreateUpdate-TableDcr-Structure, Cre
                    SchemaMode = Merge (default)
                    It will do a merge/union of new properties and existing schema properties. DCR will i

                    SchemaMode = Overwrite
                    It will overwrite existing schema in DCR/table - based on source object schema
```

Step 1 - Get demo environment up and running.

Download the Powershell script Step1-Deployment-DemoEnvironment

Modify the SubscriptionId and TenantId in the header before running the deployment

The deployment-script will setup the following tasks:

- create Azure Resource Group for Azure LogAnalytics Workspace
- create Azure LogAnalytics Workspace
- create Azure App registration used for upload of data by demo-upload script
- create Azure service principal on Azure App
- create needed secret on Azure app
- create the Azure Resource Group for Azure Data Collection Endpoint (DCE) in same region as Azure LogAnalytics Workspace
- create the Azure Resource Group for Azure Data Collection Rules (DCR) in same region as Azure LogAnalytics Workspace
- create Azure Data Collection Endpoint (DCE) in same region as Azure LogAnalytics Workspace
- delegate permissions for Azure App on LogAnalytics workspace
- delegate permissions for Azure App on Azure Resource Group for Azure Data Collection Rules (DCR)
- delegate permissions for Azure App on Azure Resource Group for Azure Data Collection Endpoints (DCE)

Step 2 - Adjust the demo-script with the needed variables (sample below).

Demo-script can also be found here

```
########################################
# VARIABLES
########################################

<# ----- onboarding lines ----- BEGIN #>

$TenantId                                   = "xxxxxxxxxxxxf63-9a77-ec94786b7c9e"
$LogIngestAppId                             = "xxxxxxxxxxxx-b45b-fe5e78392285"
$LogIngestAppSecret                         = "xxxxxxxxxxxx_NJFrBH_o-QdNR1Ga.T"

$LogAnalyticsWorkspaceResourceId            = "/subscriptions/xxxxxx/resourceGroups/rg-logworkspaces-client

$DceName                                    = "dce-log-management-client-demo1-t"
$AzDcrResourceGroup                         = "rg-dcr-log-management-client-demo1-t"
$AzDcrSetLogIngestApiAppPermissionsDcrLevel = $false

$AzDcrPrefix                                = "clt" # used to make it easy to find the DCRs when searching

# Used so schema changes will only happen on reference machines and not from other machines, if AzLogDcrInges
$AzLogDcrTableCreateFromReferenceMachine    = @()   # you will add your machine like @("MyDeviceName")
$AzLogDcrTableCreateFromAnyMachine          = $true # should be $false when you are ready for production. I

$global:Verbose                             = $true   # can be removed from script and added as parameter (

<# ----- onboarding lines ----- END  #>
```

How to get started ? (demo)

Step 3 - Run demos

You can now run the different sections in the script and see the demos. The demos will use most functions in AzLogDcrIngestPS

Start by running lines 1-275, which will load the initial header and build variables

Demo #1 will demonstrate data manipulation + show schema content

Demo #2 will demonstrate collection data + create LogAnalytics table + DCR + send data

Demo #3 will demonstrate collection of data, remove unnecessary data-properties, create schema with modified structure

Demo #4 will demonstrate schema change of existing table

NOTE:
Have patience :-)

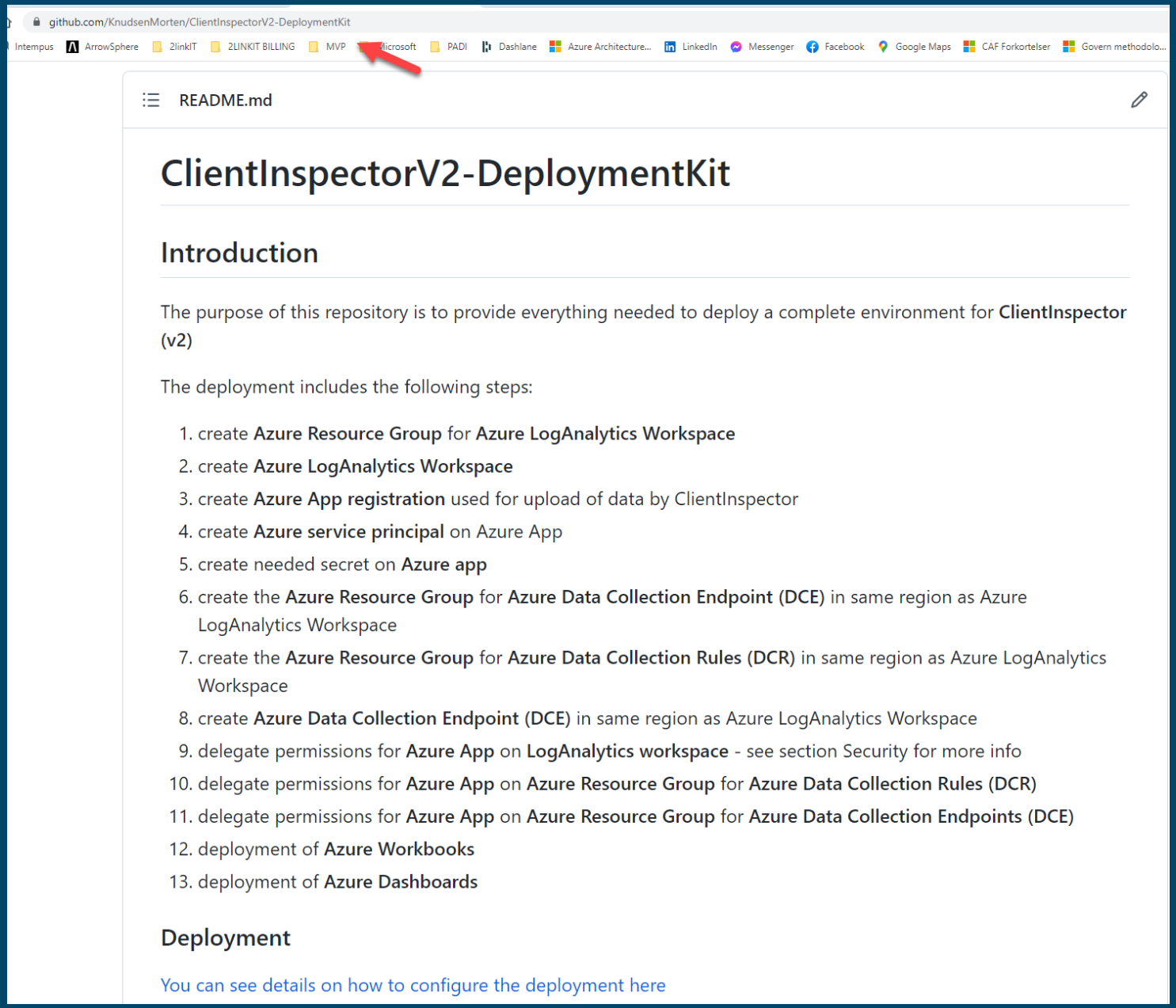
Making schema changes + creating new pipelines will require 10-15 min delays right now. Data WILL come - have patience.

When the DCR + table + schema is in place, normal upload of data will happen very fast afterwords.

I have outlined the things to notice during the demos - run the lines one by one (sample below)

https://github.com/KnudsenMorten/ClientInspectorV2-DeploymentKit

You can get started today
for free (only pay for Azure consumption)



Thank You for today ☺

- Blog: https://mortenknudsen.net/
- Mail: mok@mortenknudsen.net | mok@2linkit.net
- Linkedin: https://www.linkedin.com/in/mortenwaltorpknudsen/
- Github: https://github.com/KnudsenMorten
- Twitter: https://twitter.com/knudsenmortendk

Topic	Link
ClientInspector	https://github.com/KnudsenMorten/ClientInspectorV2
ClientInspector DeploymentKit	https://github.com/KnudsenMorten/ClientInspectorV2-DeploymentKit
Powershell module AzLogDcrIngestPS	https://github.com/KnudsenMorten/AzLogDcrIngestPS
LogHub (AzLogDcrIngestPSLogHub)	https://github.com/KnudsenMorten/AzLogDcrIngestPSLogHub
Deep-dive about Azure Data Collection Rules (DCRs)	https://github.com/KnudsenMorten/AzLogDcrIngestPS#deep-dive-about-azure-data-collection-rules-dcrs
Deep-dive about Log Ingestion API	https://github.com/KnudsenMorten/AzLogDcrIngestPS#deep-dive-about-log-ingestion-api

2LINKIT

More deep-dive information, if people are interested

(not part of main presentation)

What is collected ?

- User Logged On to Client
- Computer information
  - bios, processor, hardware info, Windows OS info, OS information, last restart
- Installed applications
  - both using WMI and registry
- Antivirus Security Center from Windows
  - default antivirus, state, configuration
- Microsoft Defender Antivirus
  - all settings including ASR, exclusions, realtime protection, etc
- Office - version, update channel config, SKUs
- VPN client - version, product
- LAPS – version
- Admin By Request (3rd party) – version
- Bitlocker - configuration
- Windows Update
  - last result (when), windows update source information (where), pending updates, last installations (what)
- Eventlog
  - look for specific events including logon events, blue screens, etc.
- Network adapters - configuration, installed adapters
- IP information for all adapters
- Local administrators group membership
- Windows firewall
  - settings for all 3 modes
- Group Policy - last refresh
- TPM information
  - relevant to detect machines with/without TPM

```
PS  get-command -module AzLogDcrIngestPS

CommandType     Name                                               Version    Source
-----------     ----                                               -------    ------
Function        Add-CollectionTimeToAllEntriesInArray              1.1.17     AzLogDcrIngestPS
Function        Add-ColumnDataToAllEntriesInArray                  1.1.17     AzLogDcrIngestPS
Function        Build-DataArrayToAlignWithSchema                   1.1.17     AzLogDcrIngestPS
Function        CheckCreateUpdate-TableDcr-Structure               1.1.17     AzLogDcrIngestPS
Function        Convert-CimArrayToObjectFixStructure               1.1.17     AzLogDcrIngestPS
Function        Convert-PSArrayToObjectFixStructure                1.1.17     AzLogDcrIngestPS
Function        CreateUpdate-AzDataCollectionRuleLogIngestCusto... 1.1.17     AzLogDcrIngestPS
Function        CreateUpdate-AzLogAnalyticsCustomLogTableDcr       1.1.17     AzLogDcrIngestPS
Function        Delete-AzDataCollectionRules                       1.1.17     AzLogDcrIngestPS
Function        Delete-AzLogAnalyticsCustomLogTables               1.1.17     AzLogDcrIngestPS
Function        Filter-ObjectExcludeProperty                       1.1.17     AzLogDcrIngestPS
Function        Get-AzAccessTokenManagement                        1.1.17     AzLogDcrIngestPS
Function        Get-AzDceListAll                                   1.1.17     AzLogDcrIngestPS
Function        Get-AzDcrDceDetails                                1.1.17     AzLogDcrIngestPS
Function        Get-AzDcrListAll                                   1.1.17     AzLogDcrIngestPS
Function        Get-AzLogAnalyticsTableAzDataCollectionRuleStatus  1.1.17     AzLogDcrIngestPS
Function        Get-ObjectSchemaAsArray                            1.1.17     AzLogDcrIngestPS
Function        Get-ObjectSchemaAsHash                             1.1.17     AzLogDcrIngestPS
Function        Post-AzLogAnalyticsLogIngestCustomLogDcrDce        1.1.17     AzLogDcrIngestPS
Function        Post-AzLogAnalyticsLogIngestCustomLogDcrDce-Output 1.1.17     AzLogDcrIngestPS
Function        Update-AzDataCollectionRuleDceEndpoint             1.1.17     AzLogDcrIngestPS
Function        Update-AzDataCollectionRuleResetTransformKqlDef... 1.1.17     AzLogDcrIngestPS
Function        Update-AzDataCollectionRuleTransformKql            1.1.17     AzLogDcrIngestPS
Function        ValidateFix-AzLogAnalyticsTableSchemaColumnNames   1.1.17     AzLogDcrIngestPS
```

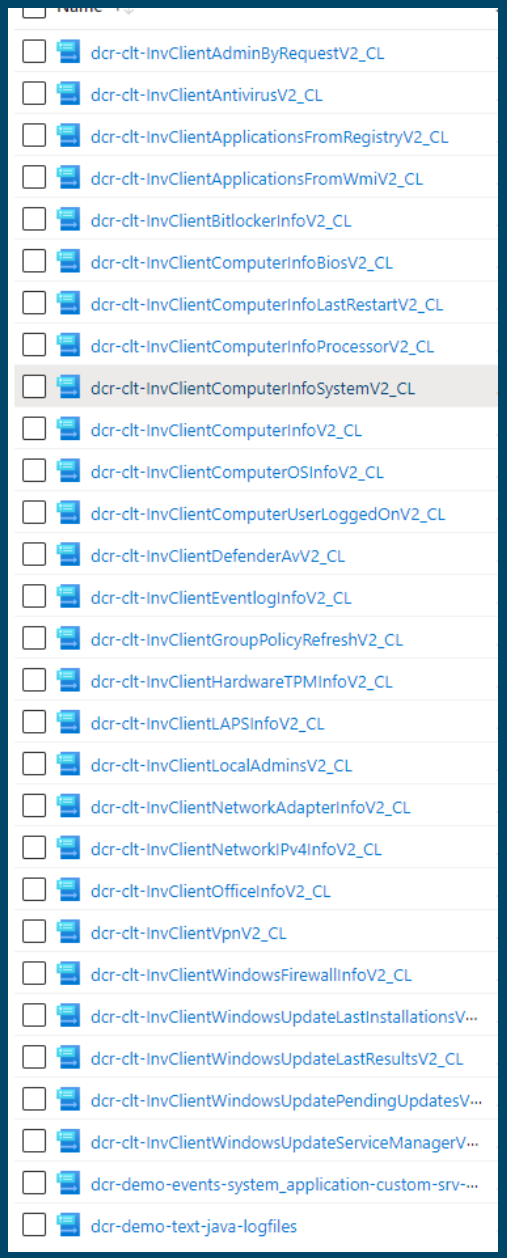
```
get-help Add-CollectionTimeToAllEntriesInArray -full

NAME
    Add-CollectionTimeToAllEntriesInArray

SYNOPSIS
    Add property CollectionTime (based on current time) to all entries on the object


SYNTAX
    Add-CollectionTimeToAllEntriesInArray [-Data] <Array> [<CommonParameters>]


DESCRIPTION
    Gives capability to do proper searching in queries to find latest set of records with same collection tim
    Time Generated cannot be used when you are sending data in batches, as TimeGenerated will change
    An example where this is important is a complete list of applications for a computer. We want all applica
    show up when queriying for the latest data


PARAMETERS
    -Data <Array>
        Object to modify

        Required?                    true
        Position?                    1
        Default value
        Accept pipeline input?       false
        Accept wildcard characters?  false

    <CommonParameters>
        This cmdlet supports the common parameters: Verbose, Debug,
        ErrorAction, ErrorVariable, WarningAction, WarningVariable,
        OutBuffer, PipelineVariable, and OutVariable. For more information, see
        about_CommonParameters (https:/go.microsoft.com/fwlink/?LinkID=113216).

INPUTS
    None. You cannot pipe objects


OUTPUTS
    Updated object with CollectionTime


    -------------------------- EXAMPLE 1 --------------------------

    PS C:\>#-------------------------------------------------------------------------------------------------

    # Variables
    #-------------------------------------------------------------------------------------------------
    $Verbose                  = $true  # $true or $false

    #-------------------------------------------------------------------------------------------------
    # Collecting data (in)
    #-------------------------------------------------------------------------------------------------
    $DNSName                  = (Get-CimInstance win32_computersystem).DNSHostName +"." + (Get-CimInstance w
    $ComputerName             = (Get-CimInstance win32_computersystem).DNSHostName
```

```
.\ClientInspector.ps1 -verbose:$false -function:download

ClientInspector | Inventory of Operational & Security-related information
Developed by Morten Knudsen, Microsoft MVP - for free community use

Downloading latest version of module AzLogDcrIngestPS from https://github.com/KnudsenMorten/CientInspectorV2
into local path D:\scripts\ClientInspectorV2
```

```
.\ClientInspector.ps1 -verbose:$false -function:localpath

ClientInspector | Inventory of Operational & Security-related information
Developed by Morten Knudsen, Microsoft MVP - for free community use

Using AzLogDcrIngestPS module from local path D:\scripts\ClientInspectorV2
```

```
.\ClientInspector.ps1 -verbose:$false -function:PSGallery -scope:CurrentUser

ClientInspector | Inventory of Operational & Security-related information
Developed by Morten Knudsen, Microsoft MVP - for free community use

Powershell module was not found !
Installing in scope currentuser .... Please Wait !
```

```
.\ClientInspector.ps1 -verbose:$false -function:PsGallery -scope:currentuser

ClientInspector | Inventory of Operational & Security-related information
Developed by Morten Knudsen, Microsoft MVP - for free community use

Checking latest version at PsGallery for AzLogDcrIngestPS module
OK - Running latest version
```



Home > Monitor | Data Collection Rules >

dcr-clt-InvClientComputerInfoSystemV2_CL

Data collection rule | Directory: 2linkIT

Search

Delete

- Overview
- Activity log
- Access control (IAM)
- Tags

Settings

- Locks

Configuration

- Data sources
- Resources

Automation

- Tasks (preview)
- Export template

Support + troubleshooting

- New Support Request

Essentials

Resource group (move)	: rg-dcr-log-management-client
Status	: Provisioned
Location	: West Europe
Subscription (move)	: 2LINKIT CLOUD (MS SPONSOF
Subscription ID	: fce4f282-fcc6-43fb-94d8-bf17
Tags (edit)	: Click here to add tags

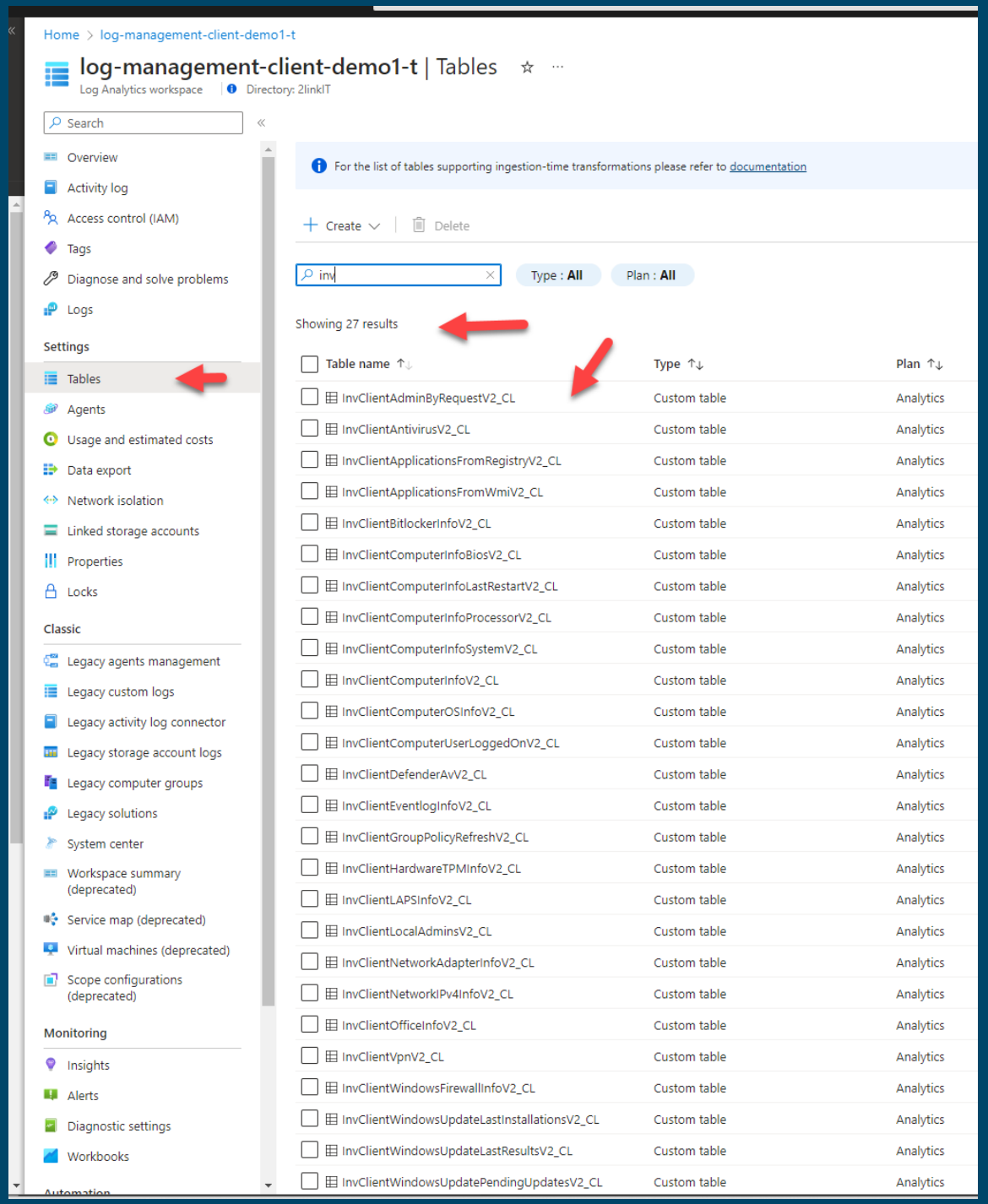
Resource JSON

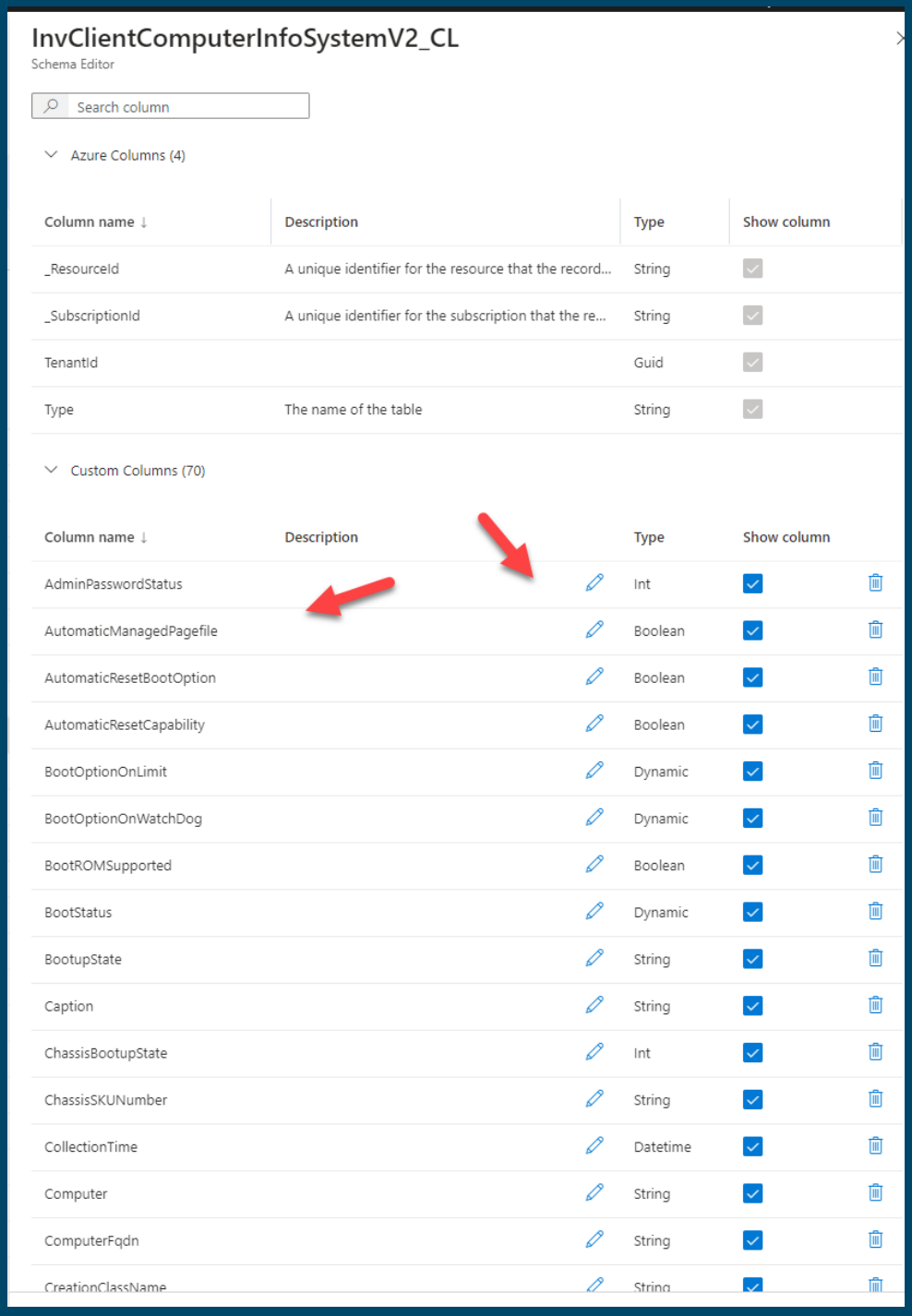
dcr-clt-InvClientComputerInfoSystemV2_CL

Resource ID: /subscriptions/fce4f282-fcc6-43fb-94d8-bf1701b862c3/resourceGroups/rg-dcr-log-management-client-demo1-t/providers/microsoft.insights/dataCol...

API version: 2022-06-01

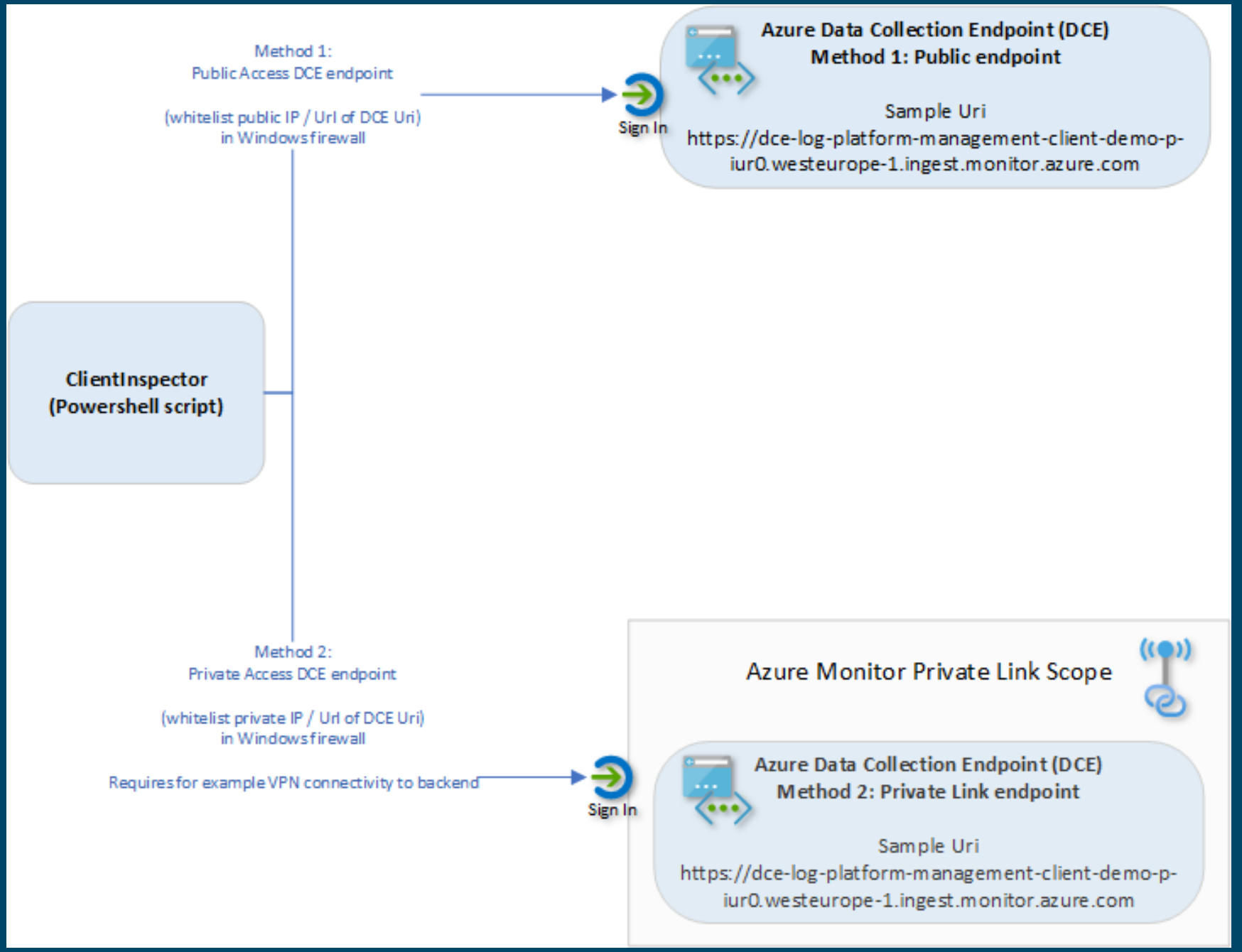

```
{
    "properties": {
        "immutableId": "dcr-857e7b752da1400bac1e302c194bf1f3",
        "dataCollectionEndpointId": "/subscriptions/fce4f282-fcc6-43fb-94d8-bf1701b862c3/resourceGroups/rg-dce-log-management-client
        "streamDeclarations": {
            "Custom-InvClientComputerInfoSystemV2_CL": {
                "columns": [
                    {
                        "name": "AdminPasswordStatus",
                        "type": "int"
                    },
                    {
                        "name": "AutomaticManagedPagefile",
                        "type": "boolean"
                    },
                    {
                        "name": "AutomaticResetBootOption",
                        "type": "boolean"
                    },
                    {
                        "name": "AutomaticResetCapability",
                        "type": "boolean"
                    },
                    {
                        "name": "BootOptionOnLimit",
                        "type": "dynamic"
                    },
                    {
                        "name": "BootOptionOnWatchDog",
                        "type": "dynamic"
                    },
                    {
                        "name": "BootROMSupported",
                        "type": "boolean"
                    },
                    {
                        "name": "BootStatus",
                        "type": "dynamic"
                    },
                    {
                        "name": "BootupState",
                        "type": "string"
                    },
                    {
                        "name": "Caption",
                        "type": "string"
                    },
                    {
                        "name": "ChassisBootupState",
                        "type": "int"
                    },
                    {
                        "name": "ChassisSKUNumber",
                        "type": "string"
                    },
                    {
```

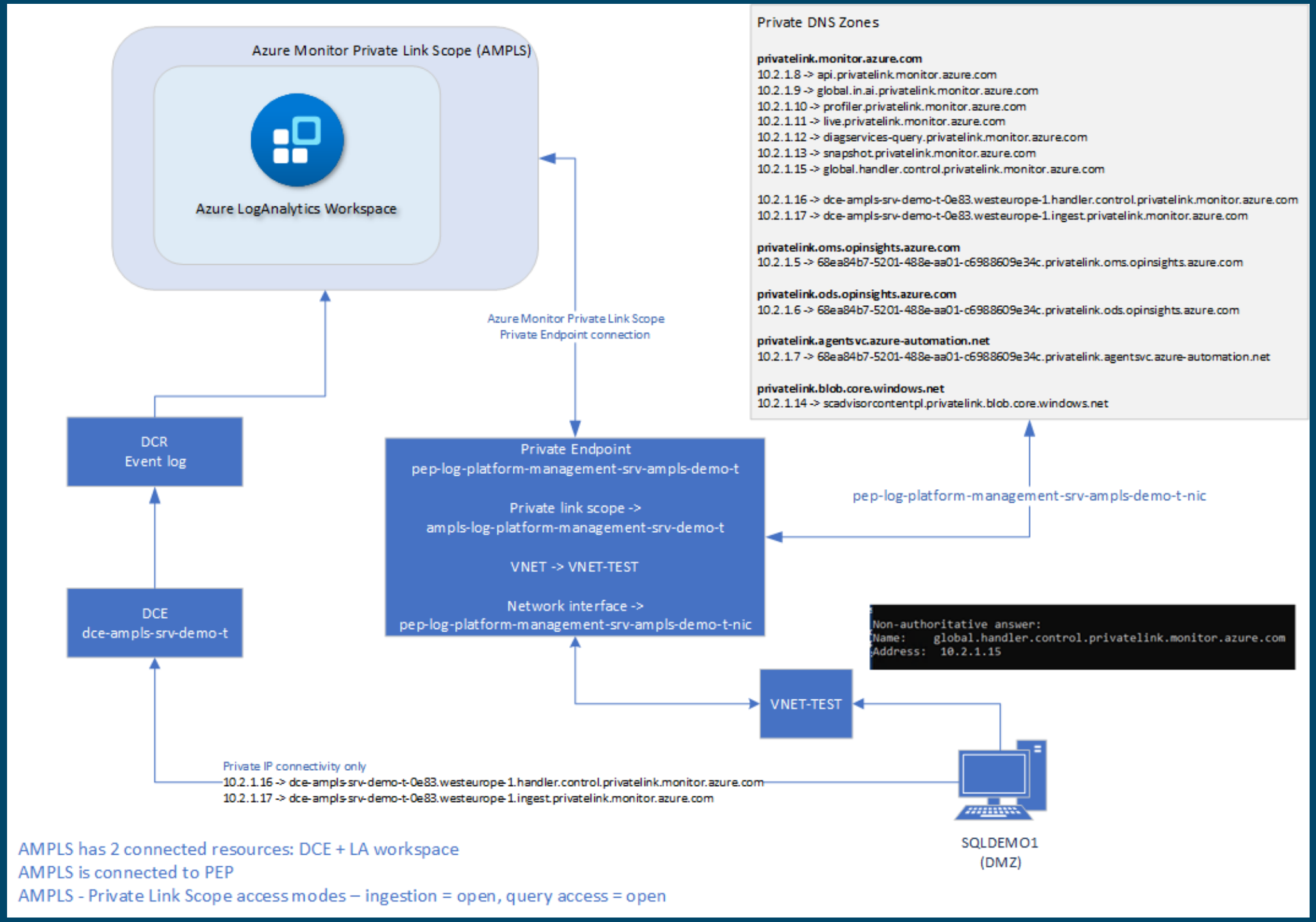

Home > log-management-client-demo1-t
log-management-client-demo1-t | Tables
Log Analytics workspace | Directory: 2linkIT
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Logs
Settings
Tables
Agents
Usage and estimated costs
Data export
Network isolation
Linked storage accounts
Properties
Locks
Classic
Legacy agents management
Legacy custom logs
Legacy activity log connector
Legacy storage account logs
Legacy computer groups
Legacy solutions
System center
Workspace summary (deprecated)
Service map (deprecated)
Virtual machines (deprecated)
Scope configurations (deprecated)
Monitoring
Insights
Alerts
Diagnostic settings
Workbooks
For the list of tables supporting ingestion-time transformations please refer to documentation
Create
Delete
inv
Type : All
Plan : All
Showing 27 results
Table name
Type
Plan
InvClientAdminByRequestV2_CL Custom table Analytics
InvClientAntivirusV2_CL Custom table Analytics
InvClientApplicationsFromRegistryV2_CL Custom table Analytics
InvClientApplicationsFromWmiV2_CL Custom table Analytics
InvClientBitlockerInfoV2_CL Custom table Analytics
InvClientComputerInfoBiosV2_CL Custom table Analytics
InvClientComputerInfoLastRestartV2_CL Custom table Analytics
InvClientComputerInfoProcessorV2_CL Custom table Analytics
InvClientComputerInfoSystemV2_CL Custom table Analytics
InvClientComputerInfoV2_CL Custom table Analytics
InvClientComputerOSInfoV2_CL Custom table Analytics
InvClientComputerUserLoggedOnV2_CL Custom table Analytics
InvClientDefenderAvV2_CL Custom table Analytics
InvClientEventlogInfoV2_CL Custom table Analytics
InvClientGroupPolicyRefreshV2_CL Custom table Analytics
InvClientHardwareTPMInfoV2_CL Custom table Analytics
InvClientLAPSInfoV2_CL Custom table Analytics
InvClientLocalAdminsV2_CL Custom table Analytics
InvClientNetworkAdapterInfoV2_CL Custom table Analytics
InvClientNetworkIPv4InfoV2_CL Custom table Analytics
InvClientOfficeInfoV2_CL Custom table Analytics
InvClientVpnV2_CL Custom table Analytics
InvClientWindowsFirewallInfoV2_CL Custom table Analytics
InvClientWindowsUpdateLastInstallationsV2_CL Custom table Analytics
InvClientWindowsUpdateLastResultsV2_CL Custom table Analytics
InvClientWindowsUpdatePendingUpdatesV2_CL Custom table Analytics


InvClientComputerInfoSystemV2_CL
Schema Editor
Search column
Azure Columns (4)
Column name
Description
Type
Show column
_ResourceId A unique identifier for the resource that the record... String
_SubscriptionId A unique identifier for the subscription that the re... String
TenantId Guid
Type The name of the table String
Custom Columns (70)
Column name
Description
Type
Show column
AdminPasswordStatus Int
AutomaticManagedPagefile Boolean
AutomaticResetBootOption Boolean
AutomaticResetCapability Boolean
BootOptionOnLimit Dynamic
BootOptionOnWatchDog Dynamic
BootROMSupported Boolean
BootStatus Dynamic
BootupState String
Caption String
ChassisBootupState Int
ChassisSKUNumber String
CollectionTime Datetime
Computer String
ComputerFqdn String
CreationClassName String

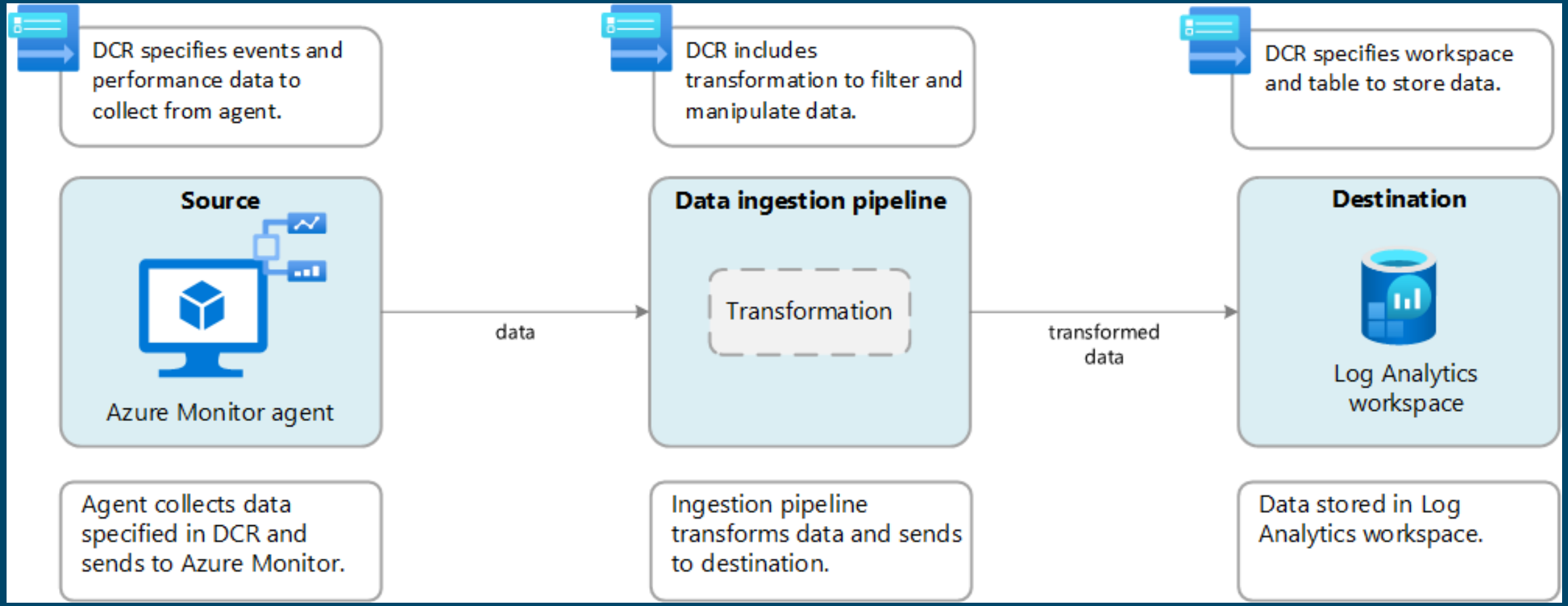
Networking

Client endpoint (REST api) sends data to DCE

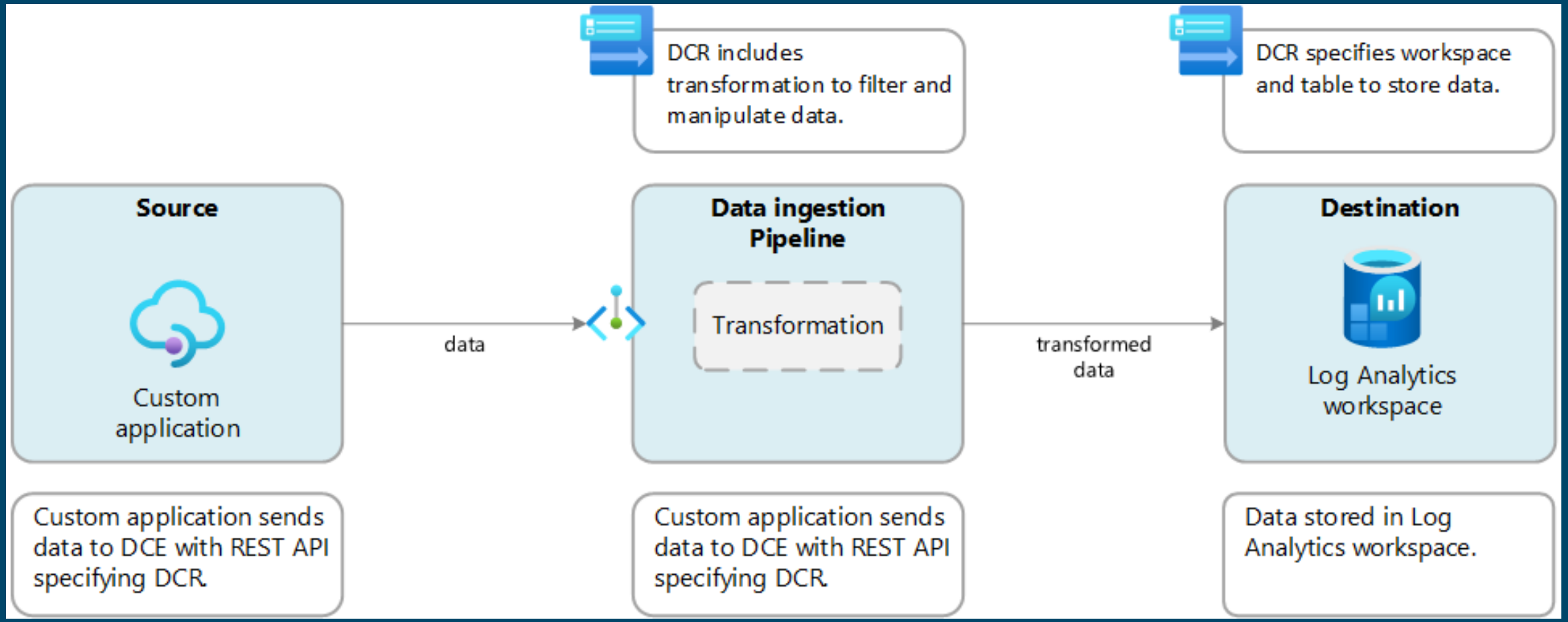



Azure Monitor Private Link Scope (AMPLS)
Azure LogAnalytics Workspace
Azure Monitor Private Link Scope
Private Endpoint connection
Private DNS Zones
privatelink.monitor.azure.com
10.2.1.8 -> api.privatelink.monitor.azure.com
10.2.1.9 -> global.in.ai.privatelink.monitor.azure.com
10.2.1.10 -> profiler.privatelink.monitor.azure.com
10.2.1.11 -> live.privatelink.monitor.azure.com
10.2.1.12 -> diagservices-query.privatelink.monitor.azure.com
10.2.1.13 -> snapshot.privatelink.monitor.azure.com
10.2.1.15 -> global.handler.control.privatelink.monitor.azure.com
10.2.1.16 -> dce-ampls-srv-demo-t-0e83.westeurope-1.handler.control.privatelink.monitor.azure.com
10.2.1.17 -> dce-ampls-srv-demo-t-0e83.westeurope-1.ingest.privatelink.monitor.azure.com
privatelink.oms.opinsights.azure.com
10.2.1.5 -> 68ea84b7-5201-488e-aa01-c6988609e34c.privatelink.oms.opinsights.azure.com
privatelink.ods.opinsights.azure.com
10.2.1.6 -> 68ea84b7-5201-488e-aa01-c6988609e34c.privatelink.ods.opinsights.azure.com
privatelink.agentsvc.azure-automation.net
10.2.1.7 -> 68ea84b7-5201-488e-aa01-c6988609e34c.privatelink.agentsvc.azure-automation.net
privatelink.blob.core.windows.net
10.2.1.14 -> scadvisorcontentpl.privatelink.blob.core.windows.net
DCR
Event log
DCE
dce-ampls-srv-demo-t
Private Endpoint
pep-log-platform-management-srv-ampls-demo-t
Private link scope ->
ampls-log-platform-management-srv-demo-t
VNET -> VNET-TEST
Network interface ->
pep-log-platform-management-srv-ampls-demo-t-nic
pep-log-platform-management-srv-ampls-demo-t-nic
Non-authoritative answer:
Name: global.handler.control.privatelink.monitor.azure.com
Address: 10.2.1.15
VNET-TEST
Private IP connectivity only
10.2.1.16 -> dce-ampls-srv-demo-t-0e83.westeurope-1.handler.control.privatelink.monitor.azure.com
10.2.1.17 -> dce-ampls-srv-demo-t-0e83.westeurope-1.ingest.privatelink.monitor.azure.com
SQLDEMO1
(DMZ)
AMPLS has 2 connected resources: DCE + LA workspace
AMPLS is connected to PEP
AMPLS - Private Link Scope access modes – ingestion = open, query access = open

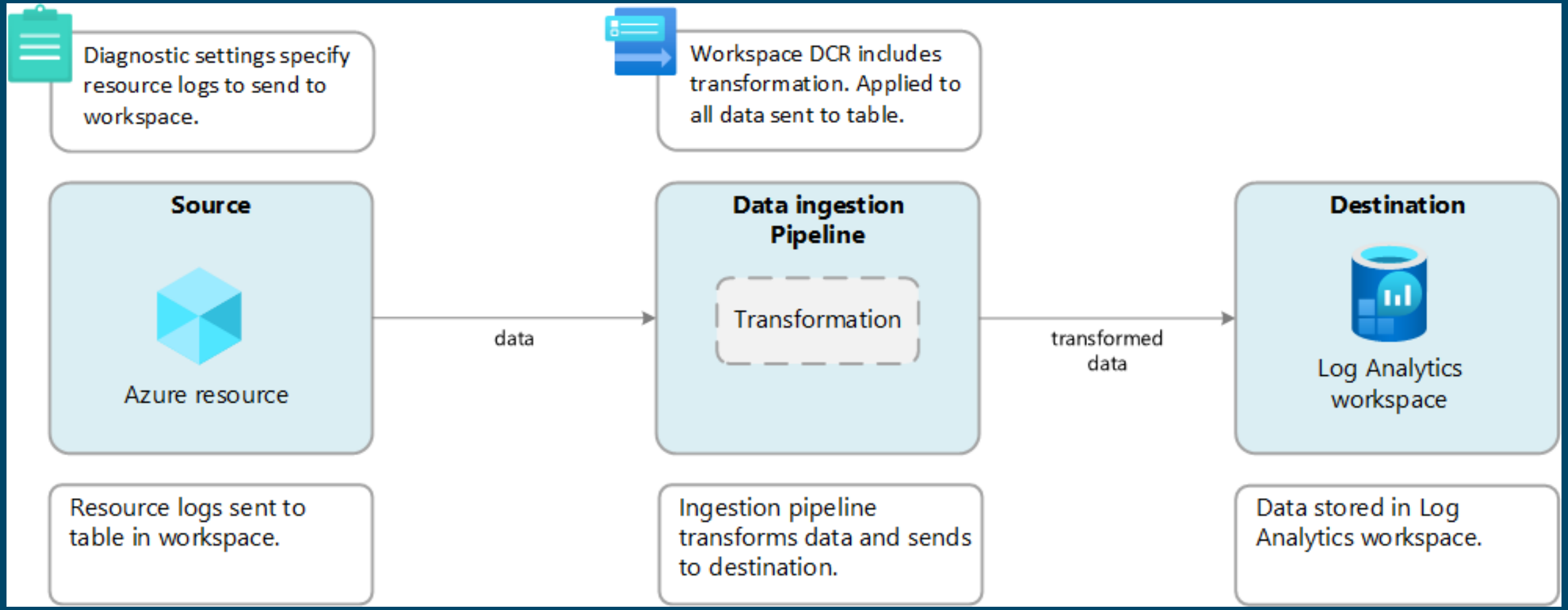
Transformation using AMA & DCR



Transformation using Log ingestion API, DCR & DCE



Workspace Transformation DCR



Collection Source	Technologies needed	Resource Association	Target (today)
Performance Eventlog Syslog	AMA / DCR	Required (DCR)	Standard table (LogAnalytics)
Text logs IIS logs Windows Firewall logs (preview)	AMA / DCR / DCE	Required (DCR)	Custom Log table (LogAnalytics)
SNMP traps	Linux with SNMP trap receiver -and- AMA (syslog file) / DCR - or - AMA (syslog stream) / DCR	Required (DCR)	???? (LogAnalytics)
Change Tracking (legacy	Change Tracking extension (FIM) / DCR	Required (DCR)	Standard table (LogAnalytics)
Custom logs (Log Ingest API)	DCR / DCE	N/A	Custom Log table (LogAnalytics)
Standard logs (Log Ingest API) (*)	DCR / DCE	N/A	Standard table (LogAnalytics)
Standard/Platform Metrics/Telemetry (Azure Paas)	DCR (built-in, non-manageable, hidden)	N/A	Azure Monitor Metrics
Custom Metrics/Telemetry (custom app)	AMA / DCR -or – Azure Diagnostics extension -or- Azure Monitor REST API -or- Linux: InfluxData Telegraf agent (Linux) + Azure Monitor output plugin	Required (DCR)	Azure Monitor Metrics
Platform Logs (diagnostics per resource) • AllMetrics (don't send to LA – you already have data via Azure Monitor Metrics) • Resource logs (alllogs, audit)	Azure Policy (Diagnostics) DCR (built-in, non-manageable, hidden)	Required (Policy)	Standard table (LogAnalytics)
Activity logs (audit per subscription)	Azure Policy (Diagnostics) DCR (built-in, non-manageable, hidden)		Standard table (LogAnalytics)

Collection Source	Technologies needed	Flow
Performance Eventlog Syslog	AMA / DCR	AMA -> DCR Ingestion Pipeline (backend) → LA
Text logs IIS logs Windows Firewall logs (preview)	AMA / DCR / DCE	AMA -> DCE -> DCR Ingestion Pipeline (backend) → LA
SNMP traps	Linux with SNMP trap receiver -and- AMA (syslog file) / DCR - or - AMA (syslog stream) / DCR	AMA-> DCR Ingestion Pipeline (backend) → LA
Change Tracking (legacy	Change Tracking extension (FIM) / DCR	FIM -> DCR Ingestion Pipeline (backend) → LA
Custom logs (Log Ingest API)	DCR / DCE	REST EndPoint -> DCE -> DCR Ingestion Pipeline (backend) → LA
Standard logs (Log Ingest API) (*)	DCR / DCE	REST EndPoint -> DCE -> DCR Ingestion Pipeline (backend) → LA
Platform (Standard) Metrics/Telemetry (Azure Paas)	DCR (built-in, non-manageable)	Azure Resource -> DCR Ingestion Pipeline (backend) -> Azure Monitor Metrics
Custom Metrics/Telemetry (custom app)	AMA / DCR -or – Azure Diagnostics extension -or- Azure Monitor REST API -or- Linux: InfluxData Telegraf agent (Linux) + Azure Monitor output plugin	AMA -> DCR Ingestion Pipeline (backend) → LA AzDiag Ext -> LA REST EndPoint -> DCE -> DCR Ingestion Pipeline (backend) → LA InfuxData Telegraf -> Azure Monitor output plugin -> LA
Platform Logs (diagnostics per resource) • AllMetrics • Resource logs (alllogs, audit)	Azure Policy (Diagnostics) DCR	Azure Resource -> DCR -> LA
Activity logs (audit per subscription)	Azure Policy (Diagnostics) DCR	Azure Resource -> DCR -> LA