Enhance Microsoft Intune data with Log Analytics

Peter van der Woude

10TH ANNIVERSARY EDITION
Experts Live Netherlands

Peter van der Woude

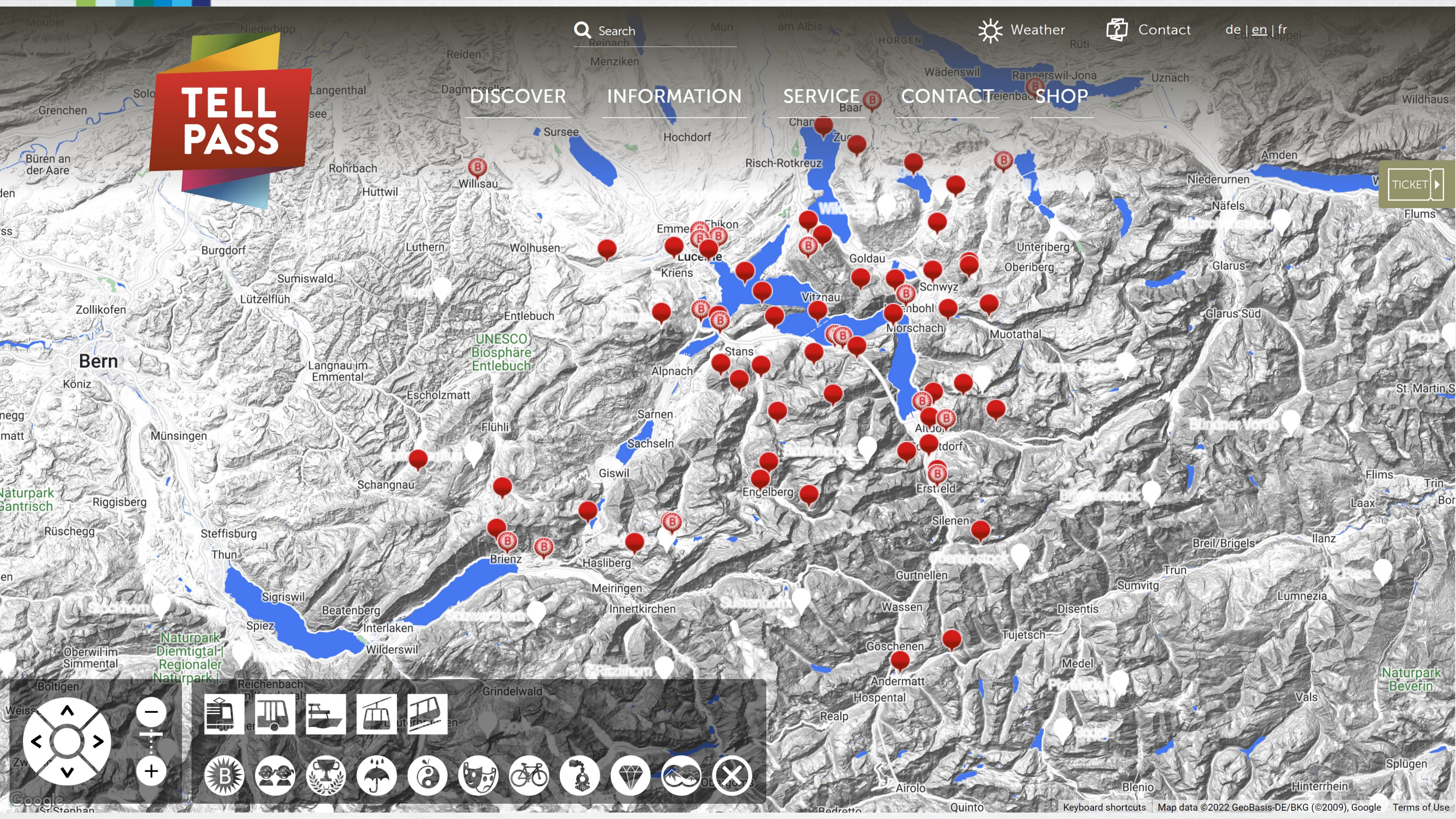
Principal Consultant @ InSpark

Enterprise Mobility MVP | Windows Insiders MVP

Family | Groningen | Basketball | Gaming

petervanderwoude.nl
@pvanderwoude
peterwoude
pvanderwoude@hotmail.com

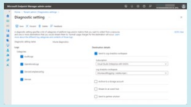
What about Microsoft Intune data and reporting?


Search
Weather
Contact
de | en | fr
TELL PASS
DISCOVER
INFORMATION
SERVICE
CONTACT
SHOP
TICKET
Grenchen
Büren an der Aare
Langenthal
Reiden
Menziken
Sursee
Hochdorf
Willisau
Huttwil
Rohrbach
Burgdorf
Luthern
Wolhusen
Emmen
Ebikon
Kriens
Risch-Rotkreuz
Baar
Goldau
Vitznau
Schwyz
Morschach
Muotathal
Unteriberg
Oberiberg
Wädenswil
Rapperswil-Jona
Uznach
Amden
Niederurnen
Näfels
Glarus
Glarus Süd
Flums
Sumiswald
Lützelflüh
Zollikofen
Bern
Köniz
Entlebuch
UNESCO Biosphäre Entlebuch
Langnau im Emmental
Escholzmatt
Flühli
Münsingen
Stans
Alpnach
Sarnen
Sachseln
Giswil
Engelberg
Erstfeld
Silenen
Schangnau
Riggisberg
Rüschegg
Steffisburg
Thun
Brienz
Hasliberg
Meiringen
Innertkirchen
Sigriswil
Beatenberg
Spiez
Interlaken
Wilderswil
Naturpark Diemtigtal | Regionaler Naturpark
Oberwil im Simmental
Boltigen
Reichenbach
Grindelwald
Gurtnellen
Wassen
Göschenen
Andermatt
Hospental
Realp
Airolo
Quinto
Disentis
Tujetsch
Medel
Sumvitg
Trun
Breil/Brigels
Ilanz
Lumnezia
Laax
Flims
St. Martin
Vals
Naturpark Beverin
Splügen
Hinterrhein
Blenio
Keyboard shortcuts
Map data ©2022 GeoBasis-DE/BKG (©2009), Google
Terms of Use

Agenda

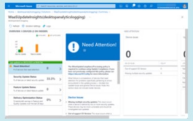
MICROSOFT 365

Collecting log data via a direct integration



MICROSOFT 365

Collecting update information via Update Compliance

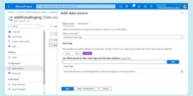


MICROSOFT 365

Collecting custom inventory via the Azure Monitor HTTP Data Collector API

MICROSOFT 365

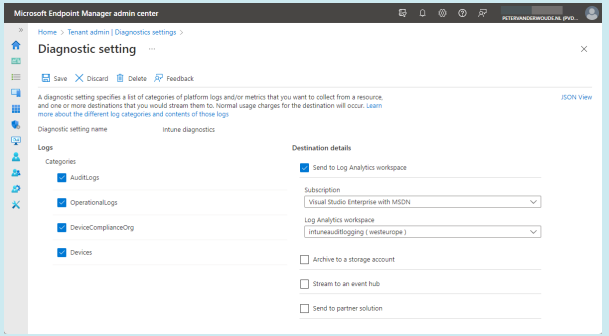
Collecting custom logs via the Azure Monitor Agent

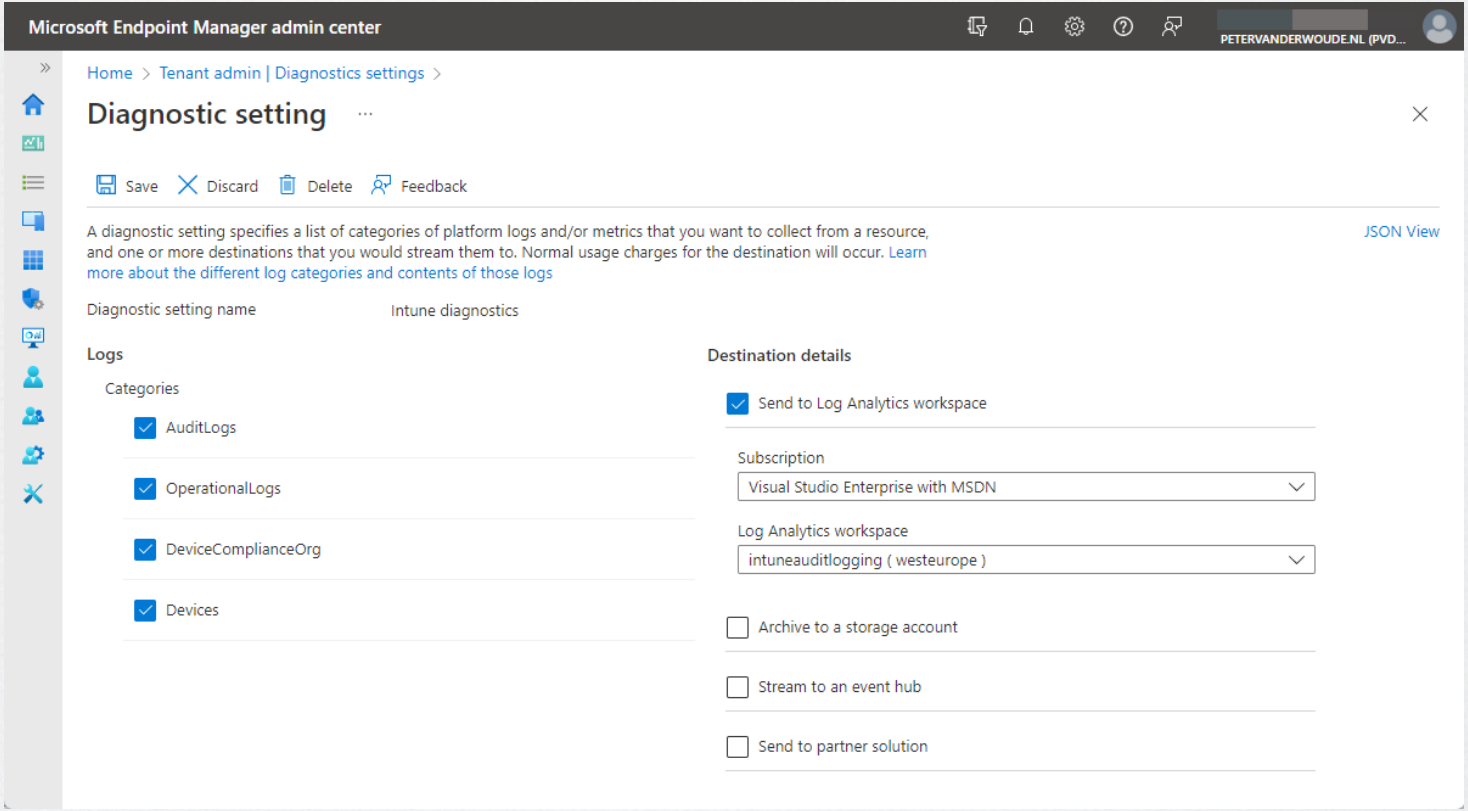


Delta-N Connecting the Cloud cegeka ARROW LIQUIT INSPARK Microsoft

MICROSOFT 365

Collecting log data via a direct integration





About log data in Microsoft Intune

Microsoft Intune includes built-in logs in the following categories that provide information about the environment

- **AuditLogs**: Contains a record of activities that generate a change Microsoft Intune (including create, update, delete, assign, and remote actions)
- **OperationalLogs**: Contains details about users and devices that successfully enrolled (or failed to), and details on non-compliant devices
- **DeviceComplianceOrg**: Contains an organizational report for device compliance in Microsoft Intune
- **Devices**: Contains device inventory and status information about Microsoft Intune enrolled and managed devices

Options with Azure Monitor services

Microsoft Intune includes the following built-in methods to sent log data to Azure Monitor services:

- **Send to Log Analytics workspace**: Send Intune logs to Log Analytics to enable rich visualizations, monitoring, and alerting on the connected data
- **Archive to a storage account**: Archive Intune logs to an Azure storage account to keep the data, or archive for a set time
- **Stream to an event hub**: Stream Intune logs to an Azure event hub for analytics using popular Security Information and Event Management (SIEM) tools, such as Splunk and QRadar
- **Send to partner solution**: Integrate Intune logs with a custom log solutions by streaming them to an event hub

Getting started with collecting log data in a Log Analytics workspace

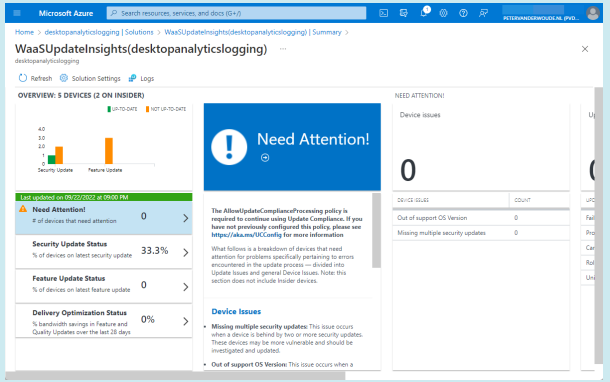
- An Azure subscription
- A Microsoft Intune tenant
- An Azure log analytics workspace
- A user with Global Administrator or Intune Service Administrator permissions
  - **To configure the log collection from Azure Storage, the Log Analytics Contributor role is required**
- Initially turn on diagnostics in Microsoft Intune

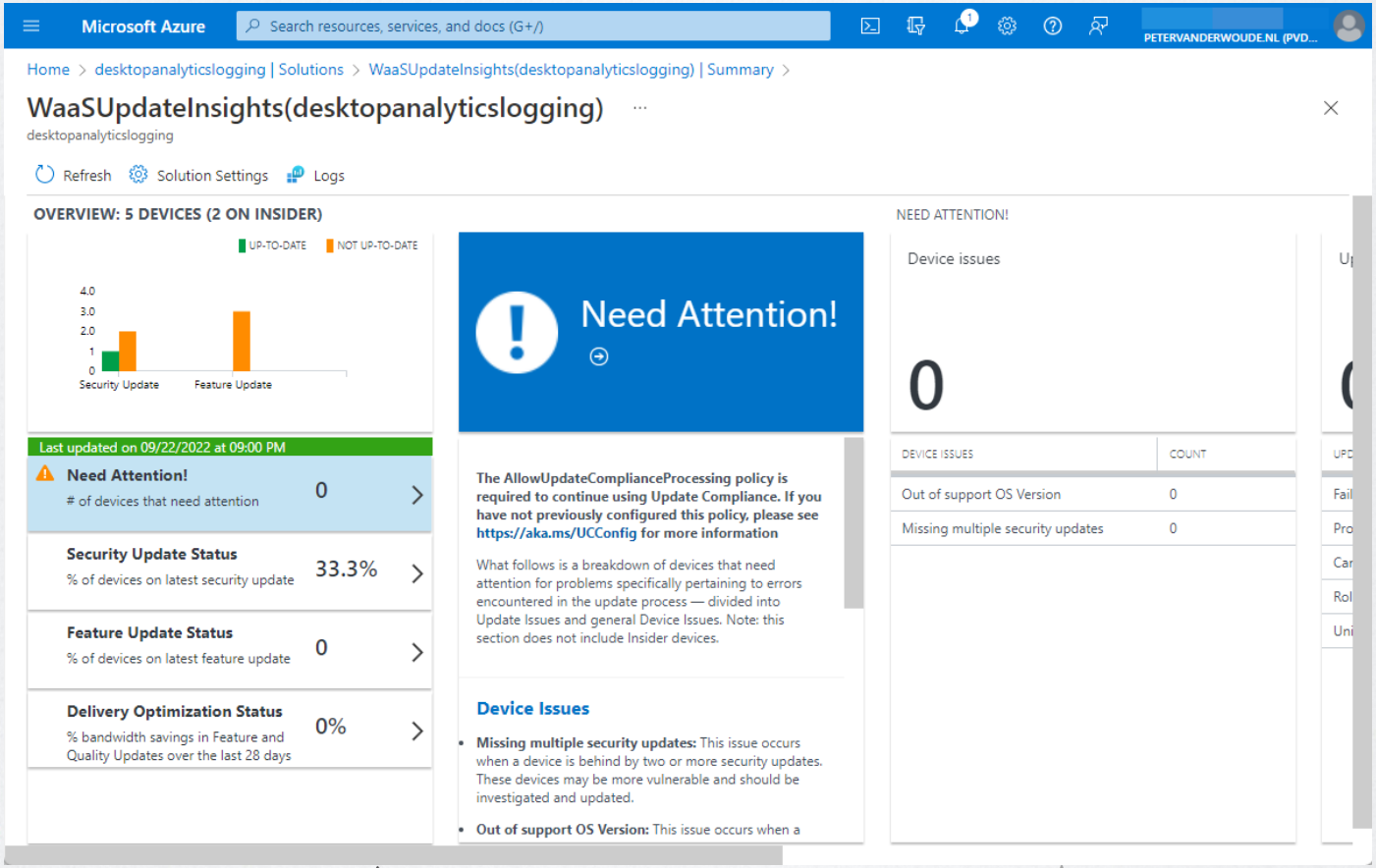
Demo log data

- Microsoft Intune configuration
- Log Analytics workspace

MICROSOFT 365

Collecting update information via Update Compliance





Delta-N Connecting the Cloud cegeka ARROW LIQUIT INSPARK Microsoft

About Update Compliance

Update Compliance is available within almost every Windows 10 and Windows 11 license and enables organizations to:

- Monitor security, quality, and feature updates for Windows 10 or Windows 11 Professional, Education, and Enterprise editions
- View reports of device and update issues related to compliance that need attention.
- Check bandwidth savings incurred across multiple content types by using Delivery Optimization.

Prerequisites for using Update Compliance

- **Supported operating systems and editions**: Windows 10 or Windows 11 Professional, Education, and Enterprise editions
- **Supported servicing channels**: General Availability Channel and the Long-term Servicing Channel (LTSC)
- **Diagnostic data requirements**: Optional level for Windows 11 devices and Enhanced level for Windows 10 devices
- **Data transmission requirements**: Devices must be able to contact the specific endpoints
- **Showing device names in Update Compliance**: Windows 10, version 1803 or later, device names will not appear by default
- **Azure AD device join or hybrid Azure AD join**

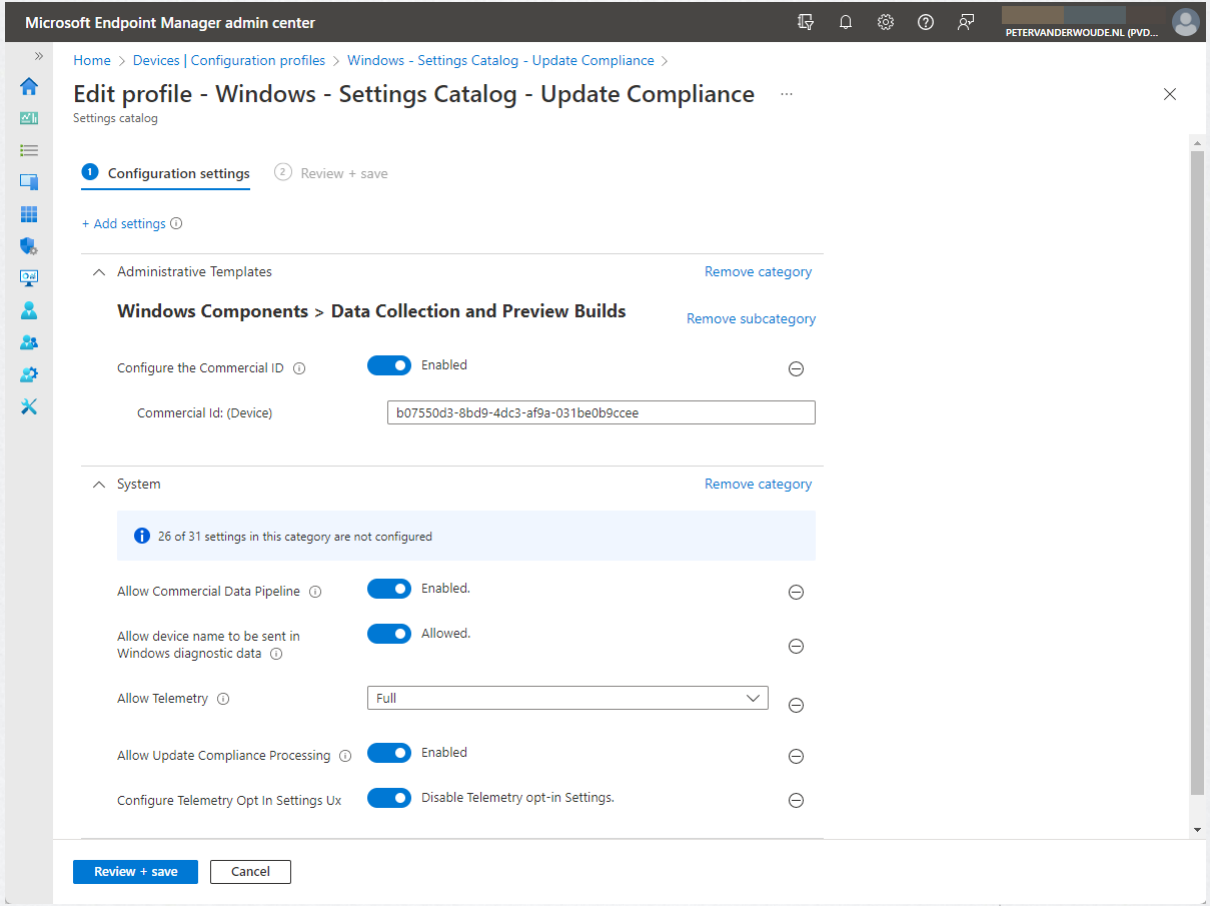
Getting started with collecting update data in Update Compliance

- An Azure subscription
- A Microsoft Intune tenant
- A Log Analytics workspace (at no charge)
- A user with Global Administrator or Intune Service Administrator permissions
  - **At least the Log Analytics Contributor role in the Log Analytics workspace**
- Get the Update Compliance application from the Azure Marketplace
- Get the CommercialID that belongs to the created solution (not required for current preview)

Configuring devices for sending update data to Update Compliance

Name (in Settings Catalog)	OMA-URI	Type	Value
Commercial ID	CommercialID[1]	String	{}
Allow Telemetry	AllowTelemetry[2]	Integer	3 - Optional
Configure Telemetry Opt In Settings Ux	*ConfigureTelemetryOptInSettingsUx*[2]	*Integer*	*1 - Disable*
Allow device name to be sent in Windows diagnostic data	AllowDeviceNameInDiagnosticData[2]	Integer	1 - Allowed
Allow Update Compliance Processing	AllowUpdateComplianceProcessing[2]	Integer	16 - Allowed
Allow Commercial Data Pipeline	AllowCommercialDataPipeline[2]	Integer	1 - Enabled

Nodes are [1]./Vendor/MSFT/DMClient/Provider/ProviderID and [2]./Vendor/MSFT/Policy/Config/System


Microsoft Endpoint Manager admin center
PETERVANDERWOUDE.NL (PVD...
Home > Devices | Configuration profiles > Windows - Settings Catalog - Update Compliance >
Edit profile - Windows - Settings Catalog - Update Compliance
Settings catalog
1 Configuration settings
2 Review + save
+ Add settings
Administrative Templates
Remove category
Windows Components > Data Collection and Preview Builds
Remove subcategory
Configure the Commercial ID
Enabled
Commercial Id: (Device)
b07550d3-8bd9-4dc3-af9a-031be0b9ccee
System
Remove category
26 of 31 settings in this category are not configured
Allow Commercial Data Pipeline
Enabled.
Allow device name to be sent in Windows diagnostic data
Allowed.
Allow Telemetry
Full
Allow Update Compliance Processing
Enabled
Configure Telemetry Opt In Settings Ux
Disable Telemetry opt-in Settings.
Review + save
Cancel

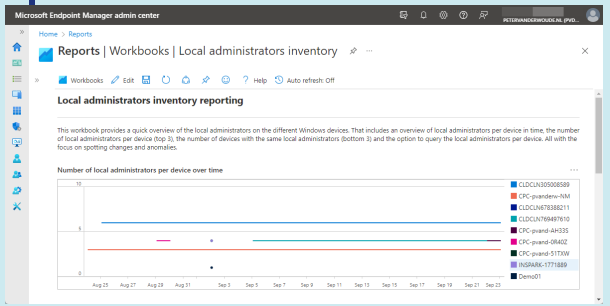
MICROSOFT 365

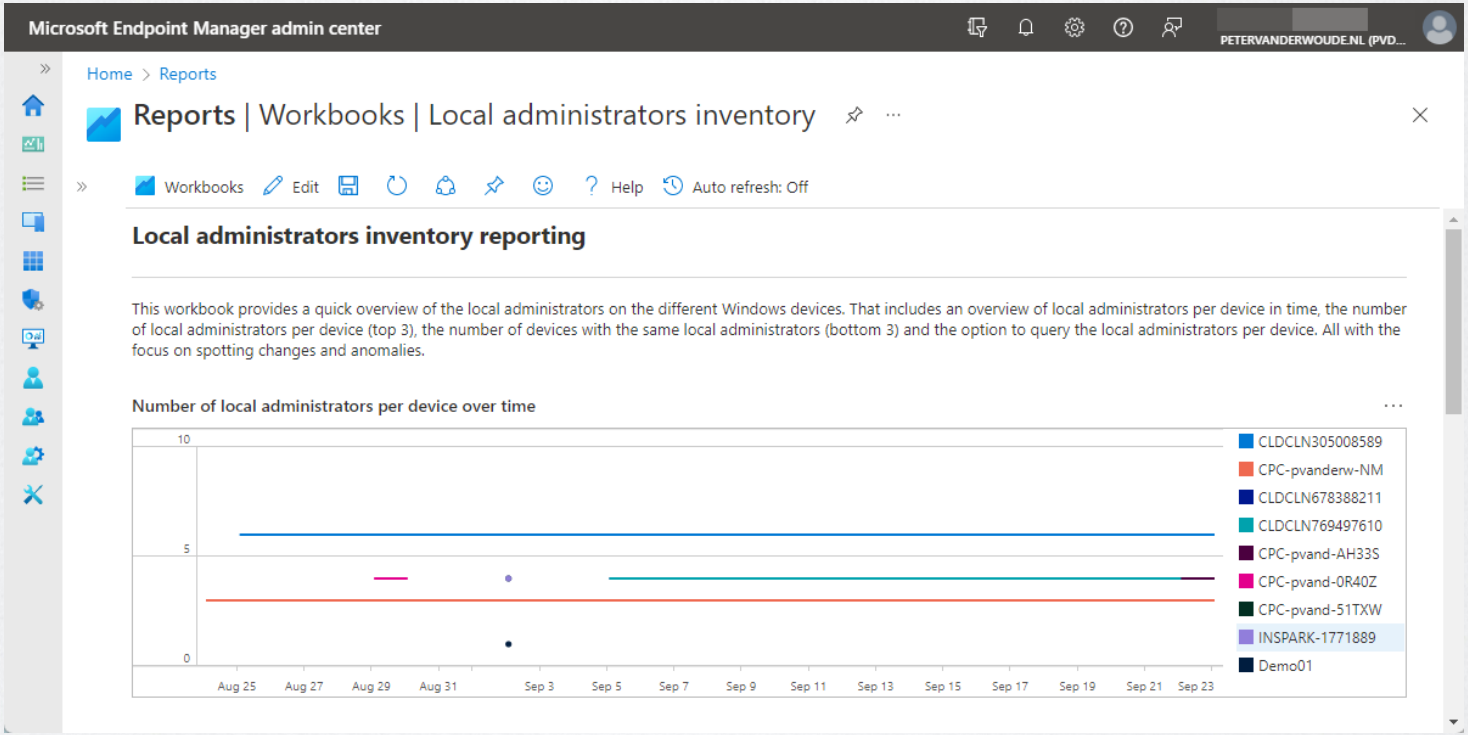
Demo Update Compliance

- Device configuration
- Log Analytics workspace
- New Microsoft workbook
- Custom workbook

MICROSOFT 365

Collecting custom inventory via the Azure Monitor HTTP Data Collector API




Microsoft Endpoint Manager admin center
PETERVANDERWOUDE.NL (PVD...
Home > Reports
Reports | Workbooks | Local administrators inventory
Workbooks
Edit
Help
Auto refresh: Off
Local administrators inventory reporting
This workbook provides a quick overview of the local administrators on the different Windows devices. That includes an overview of local administrators per device in time, the number of local administrators per device (top 3), the number of devices with the same local administrators (bottom 3) and the option to query the local administrators per device. All with the focus on spotting changes and anomalies.
Number of local administrators per device over time
10
5
0
Aug 25
Aug 27
Aug 29
Aug 31
Sep 3
Sep 5
Sep 7
Sep 9
Sep 11
Sep 13
Sep 15
Sep 17
Sep 19
Sep 21
Sep 23
CLDCLN305008589
CPC-pvanderw-NM
CLDCLN678388211
CLDCLN769497610
CPC-pvand-AH33S
CPC-pvand-0R40Z
CPC-pvand-51TXW
INSPARK-1771889
Demo01

About the Azure Monitor HTTP Data Collector API

- Azure Monitor HTTP Data Collector API can be used to send log data to a Log Analytics workspace in Azure Monitor from any client that can call a REST API
- All data in the Log Analytics workspace is stored as a record with a particular record type
- Format the data as multiple records in JSON
- An individual record is created in the repository for each record in the request payload

Getting started with collecting custom inventory via the Data Collector API

To use the HTTP Data Collector API, create a POST request that includes the data to send in JSON. The request being:

- Request URI
- Request URI parameters
- Request headers
- Request body

Getting started with collecting custom inventory via the Data Collector API

To use the HTTP Data Collector API, create a POST request that includes the data to send in JSON. The request being:

- Request URI

Attribute	Property
Method	POST
URI	https://<CustomerId>.ods.opinsights.azure.com<Resource>?api-version=<API Version>
Content type	application/json

Getting started with collecting custom inventory via the Data Collector API

To use the HTTP Data Collector API, create a POST request that includes the data to send in JSON. The request being:

- Request URI
- Request URI parameters

Parameter	Description
CustomerID	Specify the unique identifier for the Log Analytics workspace.
Resource	Specify the API resource name: /api/logs.
API Version	Specify the version of the API to use with this request: 2016-04-01.

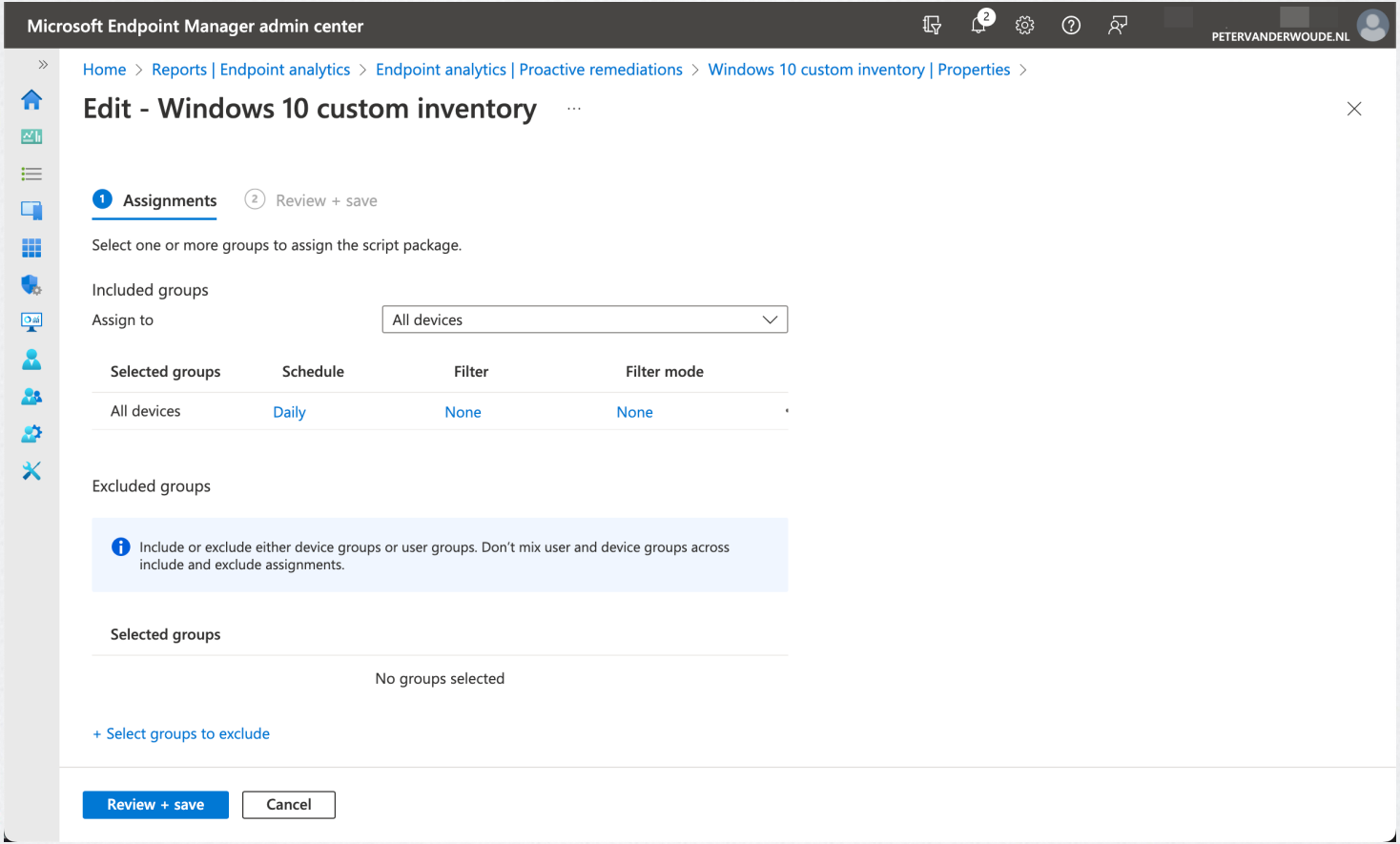
MICROSOFT 365

Getting started with collecting custom inventory via the Data Collector API

To use the HTTP Data Collector API, create a POST request that includes the data to send in JSON. The request being

- Request URI
- Request URI parameters
- Request headers

Header	Description
Authorization	Specify the authorization signature. To authenticate a request, sign the request with the primary key for the workspace. Pass that signature as part of the request.
Log-Type	Specify the name of the record type of the data that's being submitted. It can contain only letters, numbers, and the underscore (_) character, and it can't exceed 100 characters.
x-ms-date	Specify the date that the request was processed, in RFC 7234 format.
time-generated-field	Specify the timestamp of the data item that is used for **TimeGenerated**, following the ISO 8601 format YYYY-MM-DDThh:mm:ssZ. When not specified, the default is the time that the data is ingested.



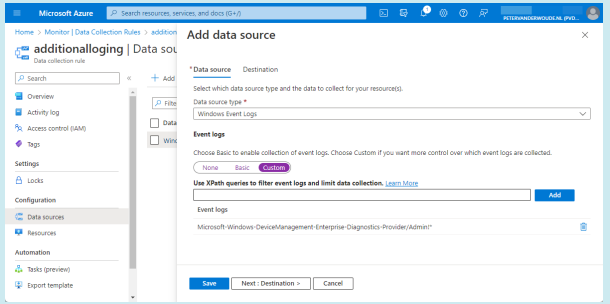
MICROSOFT 365

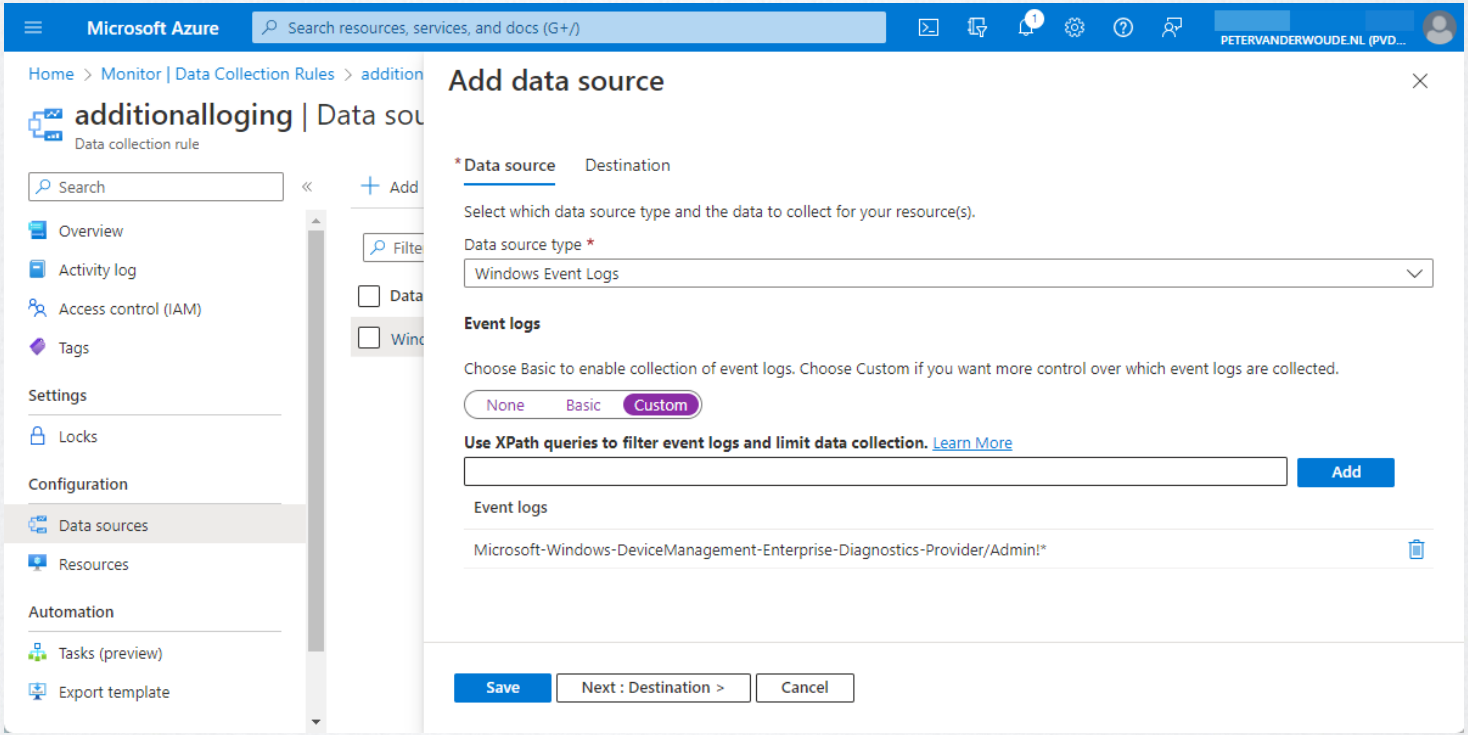
Demo custom inventory via the Data Collector API

- Custom PowerShell script
- Endpoint Analytics > Proactive remediations
- Log Analytics workspace
- Custom workbook

MICROSOFT 365

Collecting custom logs via the Azure Monitor Agent



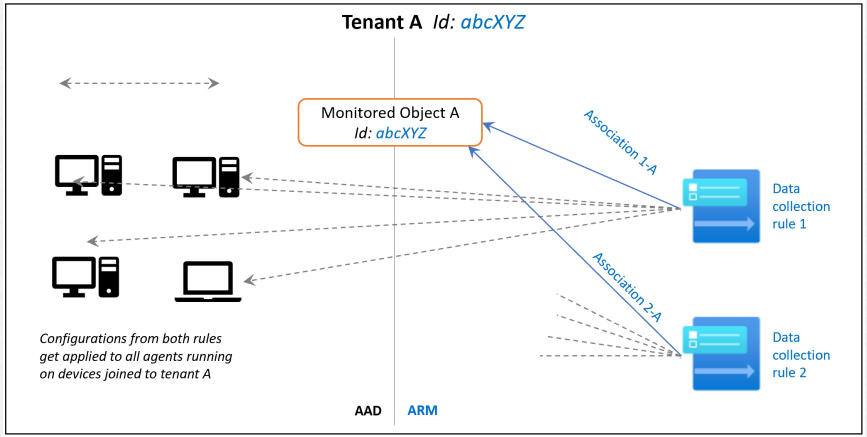


About the Azure Monitor Agent

- Collects monitoring data (like Event logs and Performance counters) from Windows client devices
- New client installer (MSI) available in preview
- Straight forward installation via Microsoft Intune
- Uses the Azure AD token to authenticate
- Relies on Data Collection rules to configure the agent
- Data Collection rules are associated to the agent via a Monitored Object that associates it to all devices within the tenant

Getting started with collecting custom inventory via the Azure Monitor Agent

- Create a Data Collection rule that defines the data that should be collected and the storage destination
- Create a Monitored Object
- Associate the Data Collection rule with the Monitored Object



Demo custom logs via the Azure Monitor Agent

- Azure Monitor Agent configuration
- Distribution of the Azure Monitor Agent
- Log Analytics workspace

Next session 15:30 – 16:20

Azure AD Conditional Access demystified

Kenneth van Surksum

10TH ANNIVERSARY EDITION

Experts Live Netherlands