



Enhance Microsoft Intune data with Log Analytics

Peter van der Woude

10TH
ANNIVERSARY
EDITION

Experts Live Netherlands



MICROSOFT 365



Peter van der Woude

Principal Consultant @ InSpark

Enterprise Mobility MVP | Windows Insiders MVP

Family | Groningen | Basketball | Gaming



petervanderwoude.nl



@pvanderwoude



peterwoude



pvanderwoude@hotmail.com

Delta-N
Connecting the Cloud

 cegeka

 now

 LIQUIT

 INSPARK

 Microsoft



MICROSOFT 365

What about Microsoft Intune data and reporting?



Delta-N
Connecting the Cloud

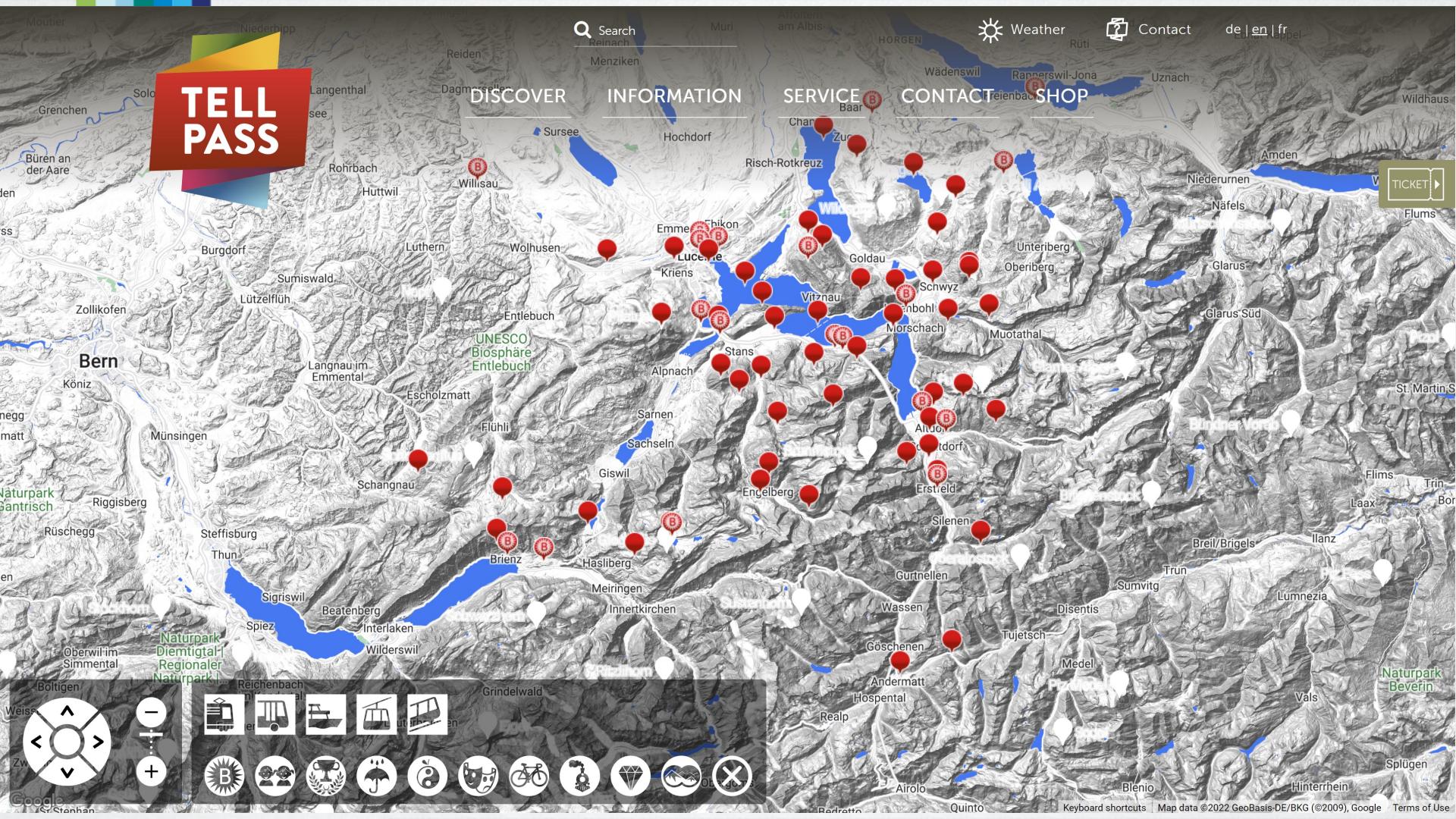
cegeka

MROW

LIQUIT

INSPARK

Microsoft



**TELL
PASS**

DISCOVER

INFORMATION

SERVICE
B

CONTACT Freienbach **SHOP**

 Search
Beinach

Search

Reinach



 Weather



 Contact

de | en | fr



Agenda



Collecting log data via a direct integration



Collecting update information via Update Compliance



Collecting custom inventory via the Azure Monitor HTTP Data Collector API



Collecting custom logs via the Azure Monitor Agent





MICROSOFT 365

Collecting log data via a direct integration

The screenshot shows the Microsoft Endpoint Manager admin center interface. The main title is "Diagnostic setting" under "Logs". On the left, there's a sidebar with icons for Home, Tenant admin, Diagnostics settings, and more. The right pane displays a form for configuring a diagnostic setting. It includes sections for "Logs" (with categories like AuditLogs, OperationalLogs, DeviceComplianceOrg, and Devices selected), "Destination details" (with "Send to Log Analytics workspace" checked and a subscription dropdown set to "Visual Studio Enterprise with MSDN"), and other optional checkboxes for "Archive to a storage account", "Stream to an event hub", and "Send to partner solution". A "JSON View" link is at the bottom right.



Microsoft Endpoint Manager admin center

Home > Tenant admin | Diagnostics settings >

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](#)

JSON View

Diagnostic setting name: Intune diagnostics

Logs

Categories:

- AuditLogs
- OperationalLogs
- DeviceComplianceOrg
- Devices

Destination details

Send to Log Analytics workspace

Subscription: Visual Studio Enterprise with MSDN

Log Analytics workspace: intuneauditlogging (westeurope)

Archive to a storage account

Stream to an event hub

Send to partner solution



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



The screenshot shows the Microsoft Azure WaaSUpdateInsights dashboard. At the top, it displays 'OVERVIEW: 5 DEVICES (2 ON INSIDER)' with a chart showing 3.0 Security Updates and 3.0 Feature Updates. A prominent red 'Need Attention!' box indicates 0 devices that need attention. Below this, sections include 'Security Update Status' (33.3% devices on latest security update), 'Feature Update Status' (0% devices on latest feature update), and 'Delivery Optimization Status' (0% bandwidth savings in Feature and Quality Updates over the last 18 days). On the right, a 'Device issues' section lists 'Out of support OS Version' (0) and 'Missing multiple security updates' (0). A sidebar on the far right shows navigation links for Home, Solutions, Log, Refresh, and Solution Settings.

Microsoft Azure Search resources, services, and docs (G+)

PETERVANDERWOUDE.NL (PVD...)

Home > desktopanalyticslogging | Solutions > WaaSUpdateInsights(desktopanalyticslogging) | Summary >

WaaSUpdateInsights(desktopanalyticslogging)

desktopanalyticslogging

Refresh Solution Settings Logs

OVERVIEW: 5 DEVICES (2 ON INSIDER)

UP-TO-DATE NOT UP-TO-DATE

4.0
3.0
2.0
1.0
0.0

Security Update Feature Update

Last updated on 09/22/2022 at 09:00 PM

⚠ Need Attention! # of devices that need attention 0 >

Security Update Status % of devices on latest security update 33.3% >

Feature Update Status % of devices on latest feature update 0% >

Delivery Optimization Status % bandwidth savings in Feature and Quality Updates over the last 28 days 0% >

Need Attention!

The AllowUpdateComplianceProcessing policy is required to continue using Update Compliance. If you have not previously configured this policy, please see <https://aka.ms/UCConfig> for more information

What follows is a breakdown of devices that need attention for problems specifically pertaining to errors encountered in the update process — divided into Update Issues and general Device Issues. Note: this section does not include Insider devices.

Device Issues

- Missing multiple security updates:** This issue occurs when a device is behind by two or more security updates. These devices may be more vulnerable and should be investigated and updated.
- Out of support OS Version:** This issue occurs when a

NEED ATTENTION!

Device issues 0

DEVICE ISSUES	COUNT
Out of support OS Version	0
Missing multiple security updates	0



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

Home > Devices | Configuration profiles > Windows - Settings Catalog - Update Compliance >

Edit profile - Windows - Settings Catalog - Update Compliance

Settings catalog

Configuration settings (1) **Review + save** (2)

+ Add settings (1)

Administrative Templates (1) Remove category

Windows Components > Data Collection and Preview Builds (1) Remove subcategory

Configure the Commercial ID (1) Enabled

Commercial Id: (Device)

System (1) Remove category

26 of 31 settings in this category are not configured (1)

Allow Commercial Data Pipeline (1) Enabled.

Allow device name to be sent in Windows diagnostic data (1) Allowed.

Allow Telemetry (1)

Allow Update Compliance Processing (1) Enabled

Configure Telemetry Opt in Settings Ux (1) Disable Telemetry opt-in Settings.

Review + save **Cancel**





Demo Update Compliance

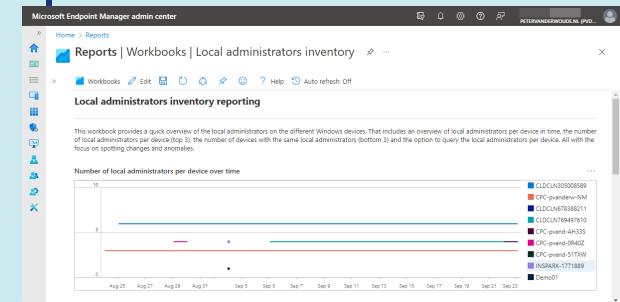
- Device configuration
- Log Analytics workspace
- New Microsoft workbook
- Custom workbook





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 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

Date	CLDCLN305008589	CPC-pvandew-NM	CLDCLN678388211	CLDCLN769497610	CPC-pvand-AH33S	CPC-pvand-0R40Z	CPC-pvand-51TXW	INSPARK-1771889	Demo01
Aug 25	5	4	1	1	1	1	1	1	1
Aug 27	5	4	1	1	1	1	1	1	1
Aug 29	5	4	1	1	1	1	1	1	1
Aug 31	5	4	1	1	1	1	1	1	1
Sep 3	5	4	1	1	1	1	1	1	1
Sep 5	5	4	1	1	1	1	1	1	1
Sep 7	5	4	1	1	1	1	1	1	1
Sep 9	5	4	1	1	1	1	1	1	1
Sep 11	5	4	1	1	1	1	1	1	1
Sep 13	5	4	1	1	1	1	1	1	1
Sep 15	5	4	1	1	1	1	1	1	1
Sep 17	5	4	1	1	1	1	1	1	1
Sep 19	5	4	1	1	1	1	1	1	1
Sep 21	5	4	1	1	1	1	1	1	1
Sep 23	5	4	1	1	1	1	1	1	1



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	<a href="https://<CustomerID>.ods.opinsights.azure.com<Resource>?api-version=<API Version>">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.



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 <code>TimeGenerated</code> , following the ISO 8601 format YYYY-MM-DDThh:mm:ssZ. When not specified, the default is the time that the data is ingested.





Microsoft Endpoint Manager admin center

Home > Reports | Endpoint analytics > Endpoint analytics | Proactive remediations > Windows 10 custom inventory | Properties >

Edit - Windows 10 custom inventory

Assignments (2) Review + save

Select one or more groups to assign the script package.

Included groups

Assign to

Selected groups	Schedule	Filter	Filter mode
All devices	Daily	None	None

Excluded groups

Selected groups

No groups selected

+ Select groups to exclude

Review + save **Cancel**





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



The screenshot shows the Microsoft Azure portal interface. The left sidebar includes links for Home, Monitor, Data Collection Rules, additionallogging, Data sources, Configuration, Automation, Tasks (preview), and Export template. The main content area is titled 'Add data source' under 'Data collection rule'. It asks to 'Select which data source type and the data to collect for your resources'. A dropdown menu shows 'Windows Event Logs' selected. Below this, the 'Event logs' section is visible, with a note: 'Choose Basic to enable collection of event logs. Choose Custom if you want more control over which event logs are collected.' There are 'None', 'Basic', and 'Custom' options, with 'Custom' being selected. An 'Event logs' input field contains 'Microsoft-Windows-DeviceManagement-Enterprise-Diagnostics-Provider/Admin'. At the bottom are 'Save', 'Next : Destination >', and 'Cancel' buttons.

Microsoft Azure Search resources, services, and docs (G+)

PETERVANDERWOUDE.NL (PVD...)

Home > Monitor | Data Collection Rules > additionallogging | Data source

Add data source

* Data source Destination

Select which data source type and the data to collect for your resource(s).

Data source type *

Windows Event Logs

Event logs

Choose Basic to enable collection of event logs. Choose Custom if you want more control over which event logs are collected.

None Basic Custom

Use XPath queries to filter event logs and limit data collection. [Learn More](#)

Add

Event logs

Microsoft-Windows-DeviceManagement-Enterprise-Diagnostics-Provider/Admin!*

Save Next : Destination > Cancel



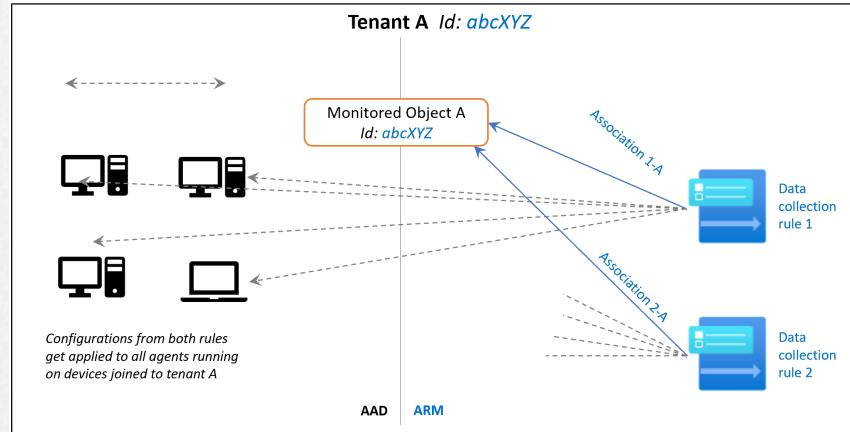
About the Azure Monitor Agent

- 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





MICROSOFT 365



Delta-N
Connecting the Cloud

 cegeka

 MARROW

 LIQUIT

 INSPARK

 Microsoft



Next session 15:30 – 16:20

Azure AD Conditional Access demystified

Kenneth van Surksum