Sentinel log ingest with Azure Monitor Agent deep dive

Markus Lintuala

www.wpninjas.eu
#WPNinjaS

Platinum Sponsor

PATCH MY PC

Microsoft Security

Gold Sponsor

glueckkanja gab

LIQUIT

baseVISION
SECURE & MODERN WORKPLACE

Lenovo

RECAST SOFTWARE

Snapdragon

Silver and Special Sponsors

SD:>_ SwissDev Jobs

LUZERN
DIE STADT. DER SEE. DIE BERGE.

sepago®

EPIC FUSION

SCAPPMAN

AppManagEvent.com
2022
October 7
Netherlands

dinext.

About Markus

Focus

Public cloud architectures and solutions with a focus on security

From

Finland

My Blog

Bloggerz.cloud

Certifications

Hobbies

- IT
- Aviation
- Cooking

Contact

LinkedIn: lintuala

Twitter: @MarkusLintuala

E-mail: markus@lintuala.fi

Agenda

Brief history and agents

Summary of history and agent comparison

How does Azure Monitor Agent work

Azure Monitor Agent, Extensions, Arc for servers

Applying monitoring

Installing agent and Data collection rules and Data collection endpoints

Sentinel use cases

Different use cases for Azure Monitor Agent

Troubleshooting

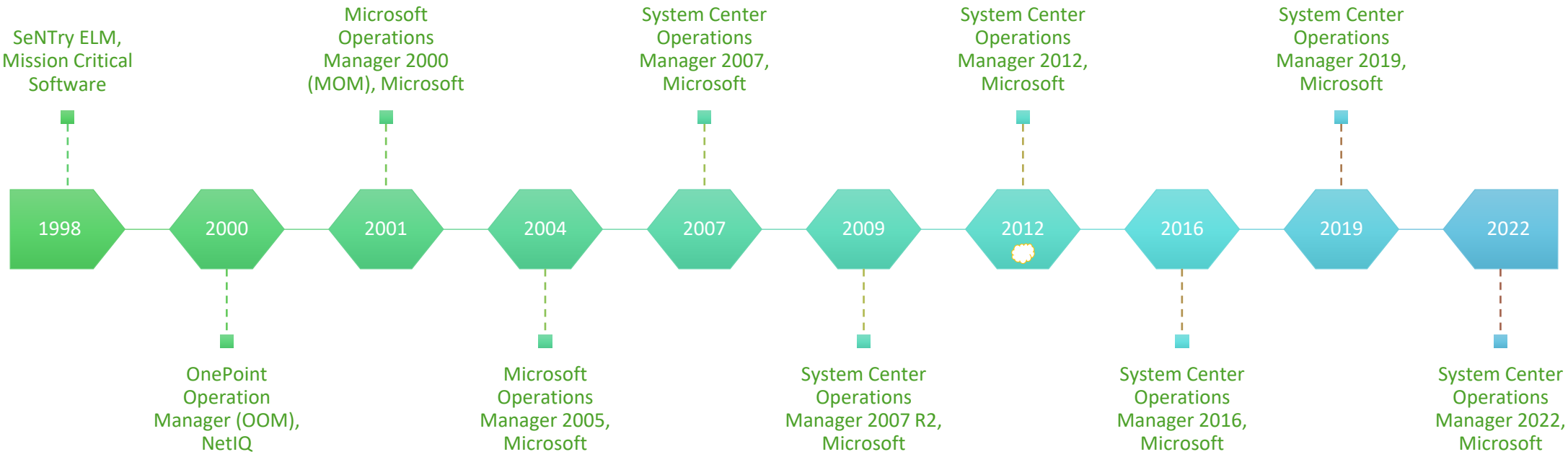
What happens and when and where are logs

Key takeaways:

- **Use Azure Monitor Agent when possible**
- **Old agents are going to be retire in 2024**

History of Microsoft’s monitoring

History of Microsoft's monitoring



History of Microsoft's Cloud monitoring

2012	2014	2015	2016	2016	2017	2017	2017	2018	2018	2021
System Center Advisor	Azure Operational Insights	Operations Management Suite	Service Map Public Preview	Operational Insights to Log Analytics	Service Map GA	Security & Audit and Antimalware	Part of Azure Security Center	ASC started to use OMS agent and Log Analytics workspace	Alerts to Azure Monitor	Azure Monitor Agent

Compare current Windows agents

	Diagnostics extension (WAD)	Log Analytics agent	Dependency agent
Environments supported	Azure	Azure Other cloud On-premises	Azure Other cloud On-premises
Agent requirements	None	None	Requires Log Analytics agent
Data collected	Event Logs ETW events Performance File based logs IIS logs .NET app logs Crash dumps Agent diagnostics logs	Event Logs Performance File based logs IIS logs Insights and solutions Other services	Process dependencies Network connection metrics
Data sent to	Azure Storage Azure Monitor Metrics Event Hub	Azure Monitor Logs	Azure Monitor Logs (through Log Analytics agent)
Services and features supported	Metrics explorer	VM insights Log Analytics Azure Automation Microsoft Defender for Cloud Microsoft Sentinel	VM insights Service Map

Compare current Windows agents

	Agent Monitor Agent	Diagnostics extension (WAD)	Log Analytics agent	Dependency agent
Environments supported	Azure Other cloud (Azure Arc) On-premises (Azure Arc) Windows Client OS (preview)	Azure	Azure Other cloud On-premises	Azure Other cloud On-premises
Agent requirements	None	None	None	Requires Log Analytics agent
Data collected	Event Logs Performance File based logs (preview)	Event Logs ETW events Performa File based IIS logs .NET app l Crash dum Agent diag	Event Logs	ies metrics
Data sent to	Azure Monitor Logs Azure Monitor Metrics	Azure Storage Azure Monitor Metrics Event Hub	Azure Monitor Logs	Azure Monitor Logs (through Log Analytics agent)
Services and features supported	Log Analytics Metrics explorer Microsoft Sentinel	Metrics explorer	VM insights Log Analytics Azure Automation Microsoft Defender for Cloud Microsoft Sentinel	VM insights Service Map

Retires 31st Aug 2024

Compare current Linux agents

	Diagnostics extension (LAD)	Telegraf agent	Log Analytics agent	Dependency agent
Environments supported	Azure	Azure Other cloud On-premises	Azure Other cloud On-premises	Azure Other cloud On-premises
Agent requirements	None	None	None	Requires Log Analytics agent
Data collected	Syslog Performance	Performance	Syslog Performance	Process dependencies Network connection metrics
Data sent to	Azure Storage Event Hub	Azure Monitor Metrics	Azure Monitor Logs	Azure Monitor Logs (through Log Analytics agent)
Services and features supported		Metrics explorer	VM insights Log Analytics Azure Automation Microsoft Defender for Cloud Microsoft Sentinel	VM insights Service Map

Compare current Linux agents

	Azure Monitor Agent	Diagnostics extension (LAD)	Telegraf agent	Log Analytics agent	Dependency agent
Environments supported	Azure Other cloud (Azure Arc) On-premises (Azure Arc)	Azure	Azure Other cloud On-premises	Azure Other cloud On-premises	Azure Other cloud On-premises
Agent requirements	None	None	None	None	Requires Log Analytics agent
Data collected	Syslog Performance File based logs (preview)	Syslog Performance	Performance	Sysl…	…dencies …ection metrics
Data sent to	Azure Monitor Logs Azure Monitor Metrics	Azure Storage Event Hub			…e Monitor Logs (through Log Analytics agent)
Services and features supported	Log Analytics Metrics explorer Microsoft Sentinel		Metrics explorer	VM insights Log Analytics Azure Automation Microsoft Defender for Cloud Microsoft Sentinel	VM insights Service Map

Retires 31st Aug 2024

Managing Azure Monitor Agent

What is Azure Monitor Agent

- Agent that replaces all other agents (at the end)
- Managed through Azure’s extensions
- Enables hybrid capabilities via Azure Arc connectivity
- Engine for data collection rules
- Authentication towards Azure with System-Assigned Managed Identity

Azure Extensions

- Small wrapped applications hosted in Microsoft’s repository
- Used for VM configuration, monitoring, security, etc.
- Managed through Azure Resource Manger
- Contains Automatic Extension Upgrade option

What is Azure Arc for Servers

- Agent that connects non-Azure virtual machine (Windows or Linux) to Azure for Azure Resource Manager capabilities
- Establish extension management, update management, monitoring, CMDB, Defender for Cloud (and Defender for Endpoint), policies, Azure Automation capabilities, etc.
- Can authenticate to Azure with System-Assigned Managed Identity
- Called Azure Connected Machines or Azure Hybrid Machines

Installing Azure Monitor Agent

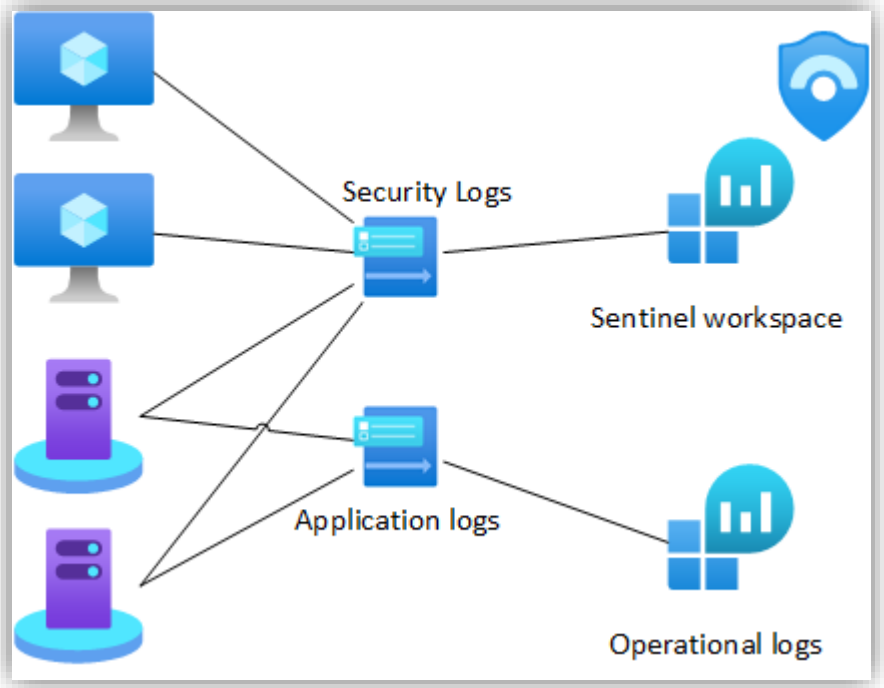
- Enable extension for Azure VM or Azure Arc Machine
- Enabling auto-provisioning from Microsoft Defender for Cloud
- Enable extension
  - From portal deploying Azure Monitor Agent extension for VM
  - With Azure Resource Manager Template
  - With PowerShell
  - With Azure CLI
  - With Policy

Demo

Installing Azure Monitor Agent

What is Data Collection Rule

- Select what to collect and where to forward it
- Rules that are run with Azure Monitor Agent
- Supports multiple sources and destinations
- Still limited features, more coming all the time



How does Data Collection Rule work?

- Data collection rule is ARM resource with own JSON-based configuration
- For Windows DCR includes simple selection (in portal) or X-Path filters what to collect depending on data source
- For Linux you filter by facility and severity level
- Streams is the schema and destination target table of logs

How does Data Collection Rule work?


```
{
    "properties": {
        "immutableId": "dcr-abcdefghijklmn123e4567890",
        "dataSources": {
            "syslog": [
                {
                    "streams": [
                        "Microsoft-CommonSecurityLog"
                    ],
                    "facilityNames": [
                         "auth",
                         "authpriv",
                         "user"
                        ],
                    "logLevels": [
                        "Debug"
                         ],
```

How does Data Collection Rule work?


```
        {
            "streams": [
                "Microsoft-CommonSecurityLog"
            ],
            "facilityNames": [
                 "auth",
                 "authpriv",
                 "user"
                 ],
            "logLevels": [
                "Debug"
                 ],
            "name": "sysLogsDataSource-123456789"
            }
        ]
    }
```

How does Data Collection Rule work?


```
"destinations": {
            "logAnalytics": [
                {
                    "workspaceResourceId": "/subscriptions/aaaaaaaa-bbbb-cccc-dddd-
eeeeeeeee/resourceGroups/rg-log/providers/Microsoft.OperationalInsights/workspaces/log-sentinel",
                    "workspaceId": ”1111111-2222-3333-4444-5555555555",
                    "name": "la-123456789"
                }
            ]
        },
        "dataFlows": [
            {
                "streams": [
                    "Microsoft-CommonSecurityLog"
                ],
                "destinations": [
                    " la-123456789 "
```

How does Data Collection Rule work?


```
                    "workspaceResourceId": "/subscriptions/aaaaaaaa-bbbb-cccc-dddd-
eeeeeeeee/resourceGroups/rg-log/providers/Microsoft.OperationalInsights/workspaces/log-sentinel",
                    "workspaceId": "1111111-2222-3333-4444-5555555555",
                    "name": "la-123456789"
                }
            ]
        },
        "dataFlows": [
            {
                "streams": [
                    "Microsoft-CommonSecurityLog"
                ],
                "destinations": [
                    "la-123456789"
                ]
            }
        ]
```

How to Enable Data Collection Rule?

- Associate DCR for Azure VM or Azure Arc VM
- For Azure VM’s enable System-Assigned Managed Identity
- Associate DCR
  - Manually from Azure Portal (enables MSI same time)
  - Azure Policy
  - Azure Resource Manager templates

Demo

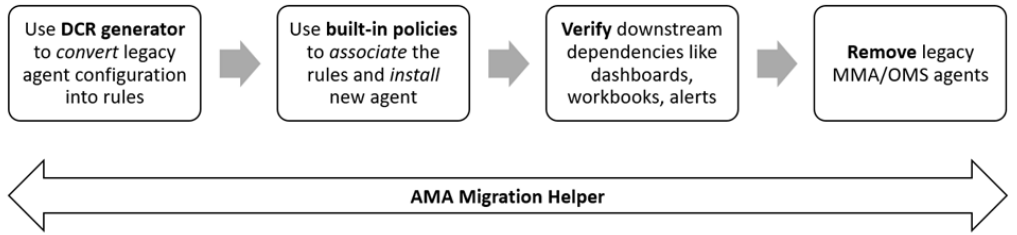
Enabling Data Collection Rule

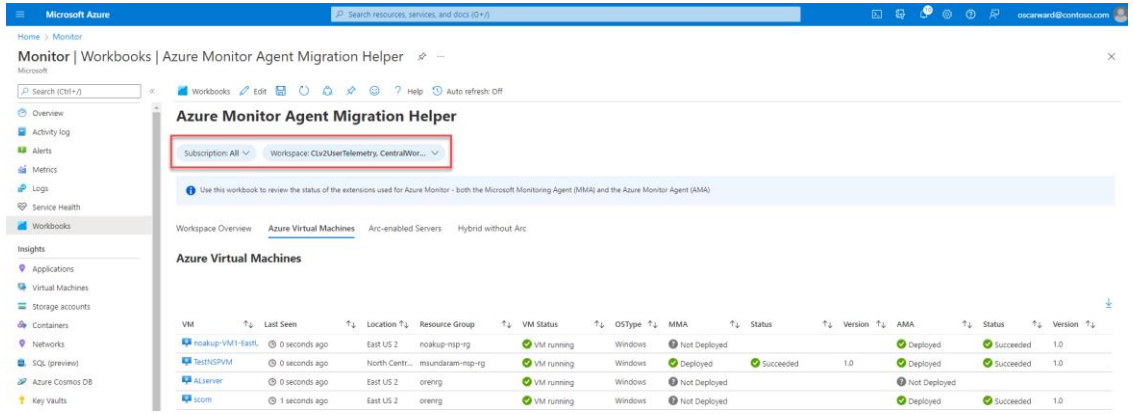
Data collection endpoints

- Use instead of public endpoints
- Can be restricted to own managed network with Azure Monitor Private Link Scopes (AMPLS)
- As private link and private endpoint concepts, also AMPLS relies heavily on DNS
- Shared between all your Log Analytics workspaces
- Resource must be in the same region as data collection endpoint

Migrating from legacy clients

- Microsoft provides a workbook-based tool and scripts to help in migration
- Discover what to migrate
- Track the migration process
- Powershell migrator tool that parses the Log Analytics Agent configuration and creates DCR based on findings





Sentinel Use Cases

Sentinel use cases

- Windows Event logs
- Syslogs
- Windows Event Forwarding
- Windows Security Events

- Announced previews
  - Custom Text Logs and Windows IIS logs
  - VM insights
  - Linux Syslog CEF collector
  - Windows DNS logs
  - Defender for Cloud
  - Change Tracking (File and registry integrity monitoring)
  - Network Watcher

Create Sentinel Data Collection Rule

- Create it through the Sentinel, IaC, or REST
- Same object as Data Collection Rule from Azure Monitor, but modifies the DCR automatically for Sentinel tables
- If using data Windows Security Events collector, check the destination table!!

Windows Security Event DCR


```
"properties": {
        "immutableId": "dcr-aaaaaaaaaaaaaaaaaaaaaaaaaa",
        "dataSources": {
            "windowsEventLogs": [
                {
                    "streams": [
                        "Microsoft-SecurityEvent"
                    ],
                    "xPathQueries": [
                        "Security!*",
                        "Microsoft-Windows-AppLocker/EXE and DLL!*",
                        "Microsoft-Windows-AppLocker/MSI and Script!*"
                    ],
                    "name": "eventLogsDataSource"
                }
            ]
```

Windows Security Event DCR


```
},
        "destinations": {
            "logAnalytics": [
                {
                    "workspaceResourceId": "/subscriptions/aaaaaaaa-bbbb-cccc-dddd-eeeeeeeee/resourceGroups/rg-
log/providers/Microsoft.OperationalInsights/workspaces/log-sentinel ",
                    "workspaceId": "1111111-2222-3333-4444-5555555555",
                    "name": "DataCollectionEvent"
                }
            ]
        },
        "dataFlows": [
            {
                "streams": [
                    "Microsoft-SecurityEvent"
                ],
                "destinations": [
                    "DataCollectionEvent"
                ]
            }
        ]
```

Troubleshooting Azure Monitor Agent

Troubleshooting Azure Monitor Agent

- Check heartbeat
- Check network connectivity
- Check that the Azure Monitor Agent is running
- Check that DCR is associated
- After this to logs…
  - Azure Monitor Agent overview - Azure Monitor | Microsoft Docs

Azure Monitor Agent logging

- Azure Monitor agent logs
  - C:\ProgramData\GuestConfig\extension_logs\Microsoft.Azure.Monitor.AzureMonitorWindowsAgent
- Create a zip file of logs to desktop
  - C:\Packages\Plugins\Microsoft.Azure.Monitor.AzureMonitorWindowsAgent\[version]\CollectAMALogs.ps1
- Linux logs
  - /var/log/azure/Microsoft.Azure.Monitor.AzureMonitorLinuxAgent/

Is extension installed successfully

- Check from portal or CLI or PowerShell or REST

- Logs available:

Azure Windows VM	Arc Windows	Linux
C:\WindowsAzure\Logs\Plugins\Microsoft.Azure.Monitor.AzureMonitorWindowsAgent	C:\ProgramData\GuestConfig\extension_logs\Microsoft.Azure.Monitor.AzureMonitorWindowsAgent	/var/log/azure/Microsoft.Azure.Monitor.AzureMonitorLinuxAgent/

Is Azure Monitor Agent running?

- MonAgentCore.exe
- systemctl status azuremonitoragent

- Logs available:

Azure Windows VM	Arc Windows	Linux
C:\WindowsAzure\Resources\AMADataStore.<virtual-machine-name>\Configuration	C:\Resources\Directory\AMADataStore\Configuration	/var/opt/microsoft/azuremonitoragent/log/mdsd.*

Is your DCR associated?

- DCR in same region than the resource?
- System-assigned managed identity enabled for Azure VMs?

- Logs available:

Azure Windows VM	Arc Windows	Linux
C:\WindowsAzure\Resources\AMADataStore.<virtual-machine-name>\mcs\mcsconfig.latest.xml OR C:\WindowsAzure\Resources\AMADataStore.<virtual-machine-name>\Tables\MAEventTable.tsf OR C:\WindowsAzure\Resources\AMADataStore.<virtual-machine-name>\mcs\configchunks	C:\Resources\Directory\AMADataStore\mcs\mcsconfig.latest.xml OR C:\Resources\Directory\AMADataStore\mcs\configchunks	/etc/opt/microsoft/azuremonitoragent/config-cache/configchunks/

Which client should I use?

- If your use case is supported by Azure Monitor Agent and Data collection rules, go with it
- Otherwise use legacy clients

Key takeaways

- DCEs, DCRs and Log Analytics workspace should be in same region
- Use Azure Monitor Agent if possible
- Azure Log Analytics agent retires 31st Aug 2024

Wednesday, September 14

16:30 CEST

Passwordless - Phishing proof identities?!
Markus Lintuala

Thank You