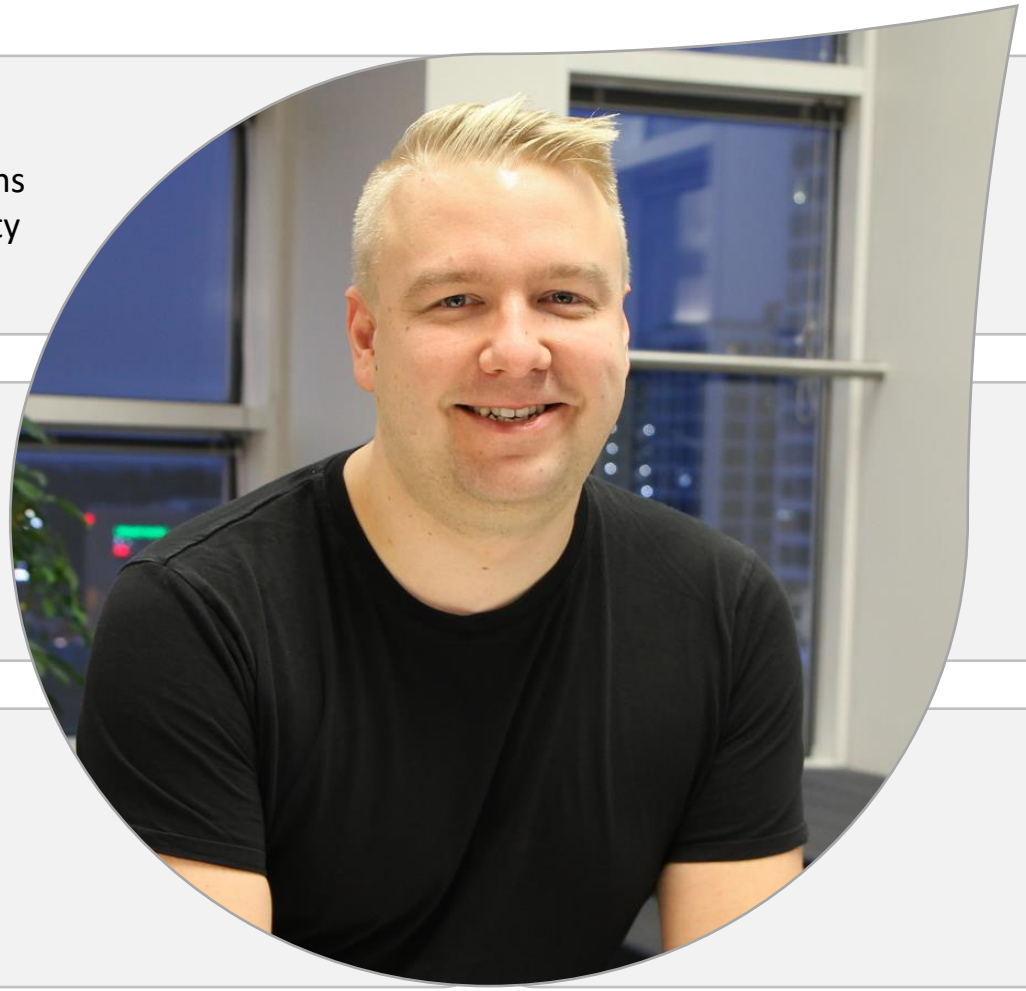
Microsoft

Azure Monitor Agent and Data Collection rule deep dive

Markus Lintuala, Elisa Oyj

Microsoft Kumppaniarkkitehtiseminaari 22.11.2022
aka.ms/kumppaniarkkitehtiseminaari

Markus Lintuala



Focus
Public and hybrid cloud solutions and architectures with a security aspect

Elisa Oyj
Senior Technical Consultant

Blog
https://bloggerz.cloud

Certifications
Security, Azure, DevOps, Microsoft 365 Expert, MCT
Rest here: those

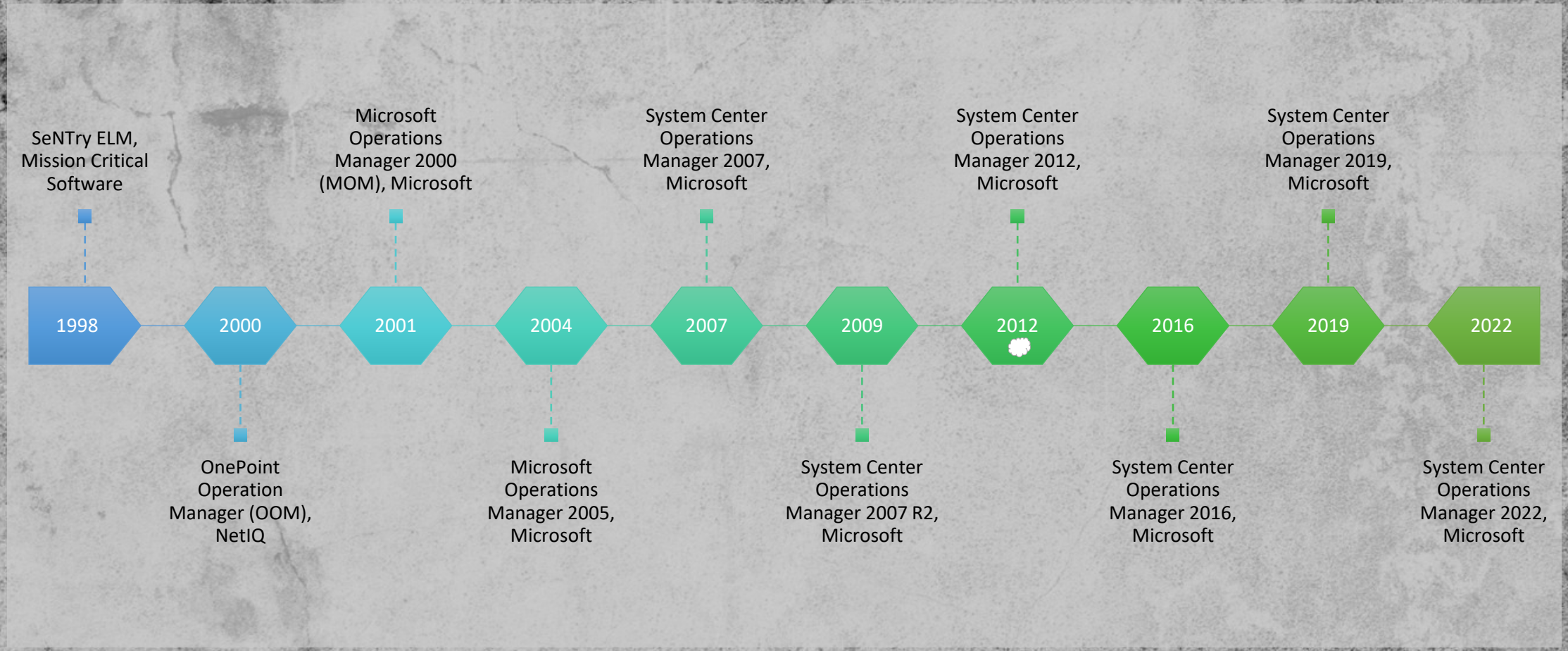
Hobbies
IT, Aviation, Food

Contact
LinkedIn: lintuala
Twitter: @MarkusLintuala
E-mail: markus@lintuala.fi

Agenda

- Brief history and agents
- How does Azure Monitor Agent work
- Applying monitoring
- Use cases
- Troubleshooting

History of Microsoft's monitoring



History of Microsoft's Cloud monitoring

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 diagn	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

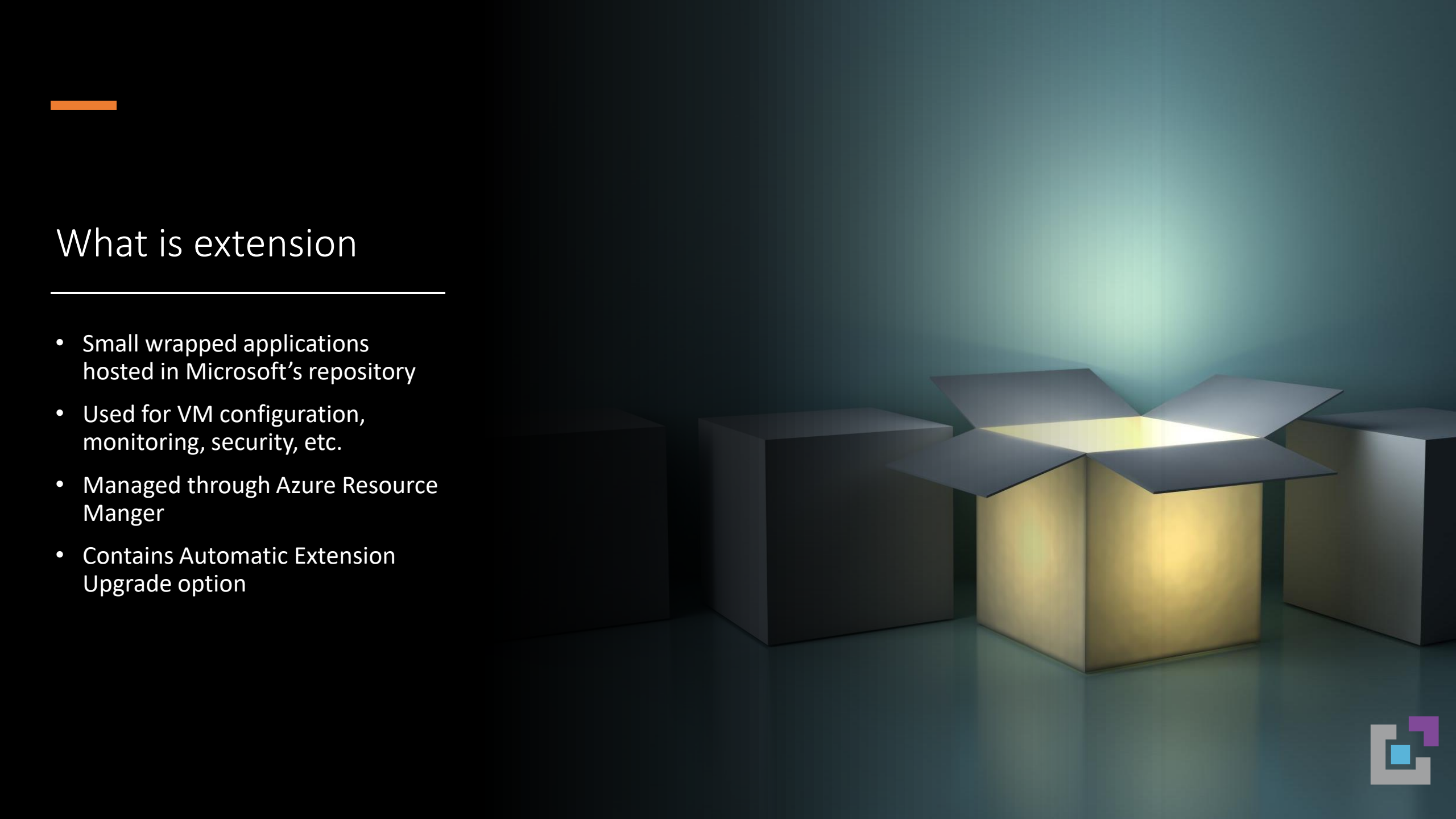
Managing Azure Monitor Agent

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

What is extension

- 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

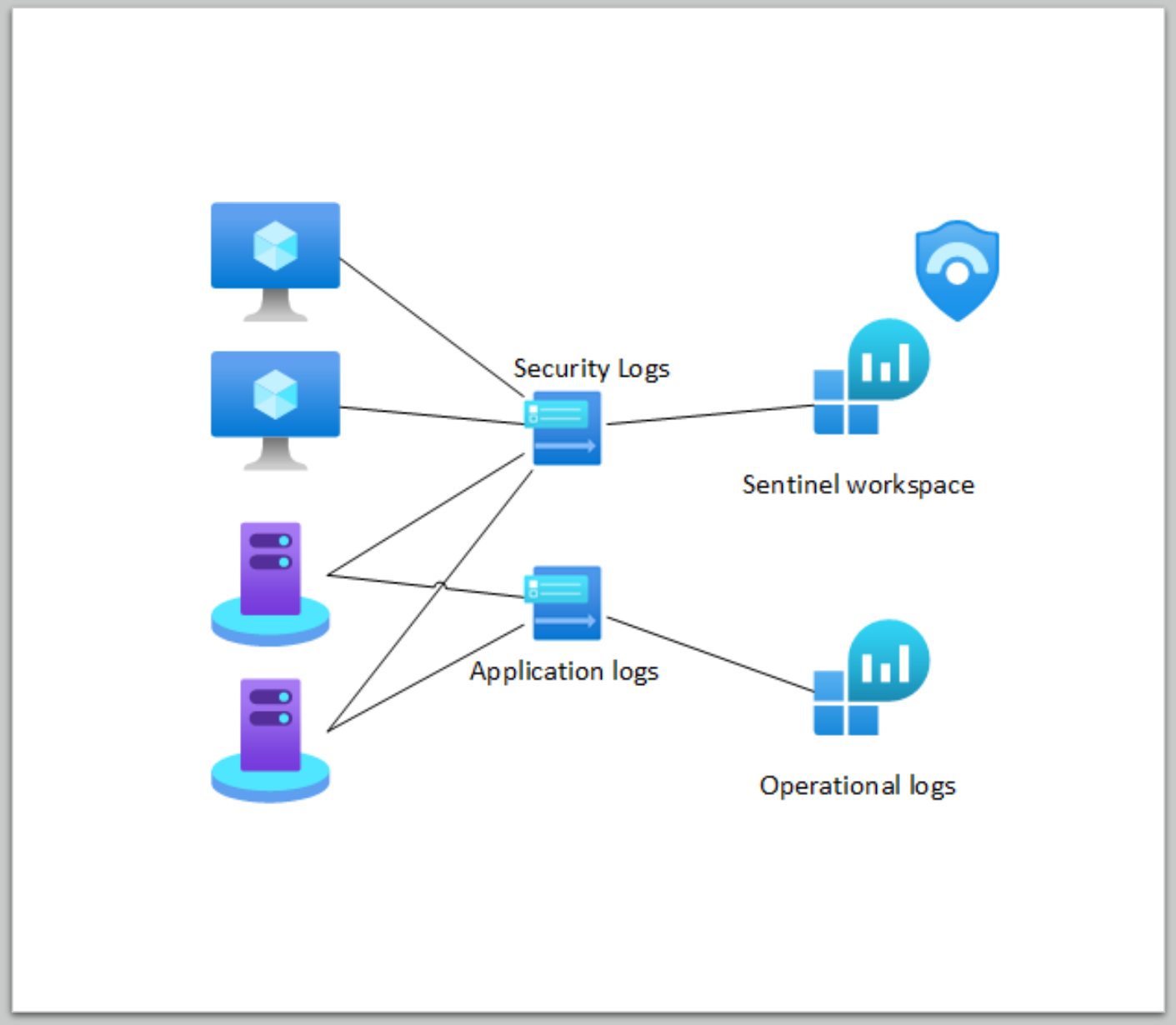
- Enable extension for Azure VM or Azure Arc Machine
- Enabling auto-provisioning from Microsoft Defender for Cloud
- Enable extension
  - From portal deploying Azure Monitor Agent extension for VM
  - With Azure Resource Manager Template
  - With PowerShell
  - With Azure CLI
  - With Policy

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



CommonEventFormat schema change 28.2.2023

Current Column Name	Column Data Type	New Column Name	New Column Data Type	Notes
ExternalID	System.Int32	ExtID	System.String	
DeviceCustomNumber1	System.Int32	FieldDeviceCustomNumber1	System.Int64	
DeviceCustomNumber2	System.Int32	FieldDeviceCustomNumber2	System.Int64	
DeviceCustomNumber3	System.Int32	FieldDeviceCustomNumber3	System.Int64	
		EventOutcome	System.String	Formerly located in AdditionalExtensions
		Reason	System.String	Formerly located in AdditionalExtensions
		DeviceEventCategory	System.String	Formerly located in AdditionalExtensions

This is already rolled out to all tenants. Test now your queries and update those before 27.2.2023

More info: [Upcoming changes to the CommonSecurityLog table - Microsoft Community Hub]

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 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

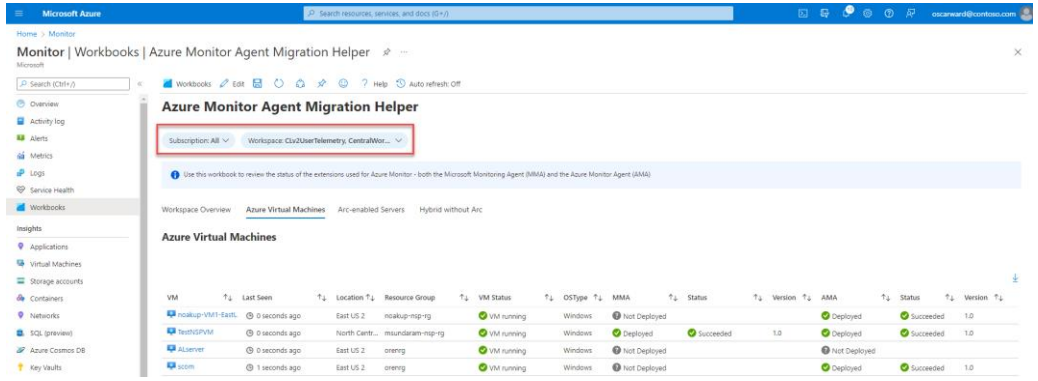
Data collection rule

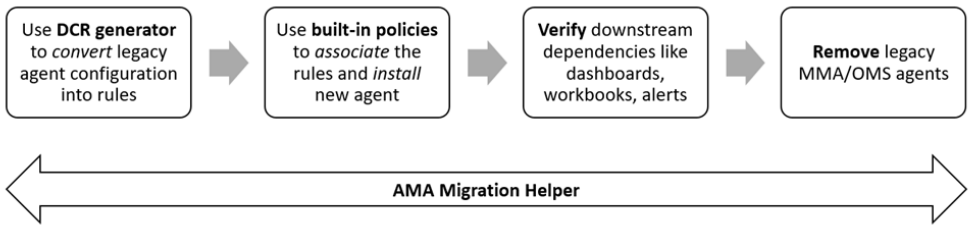
Data collection endpoints

- 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



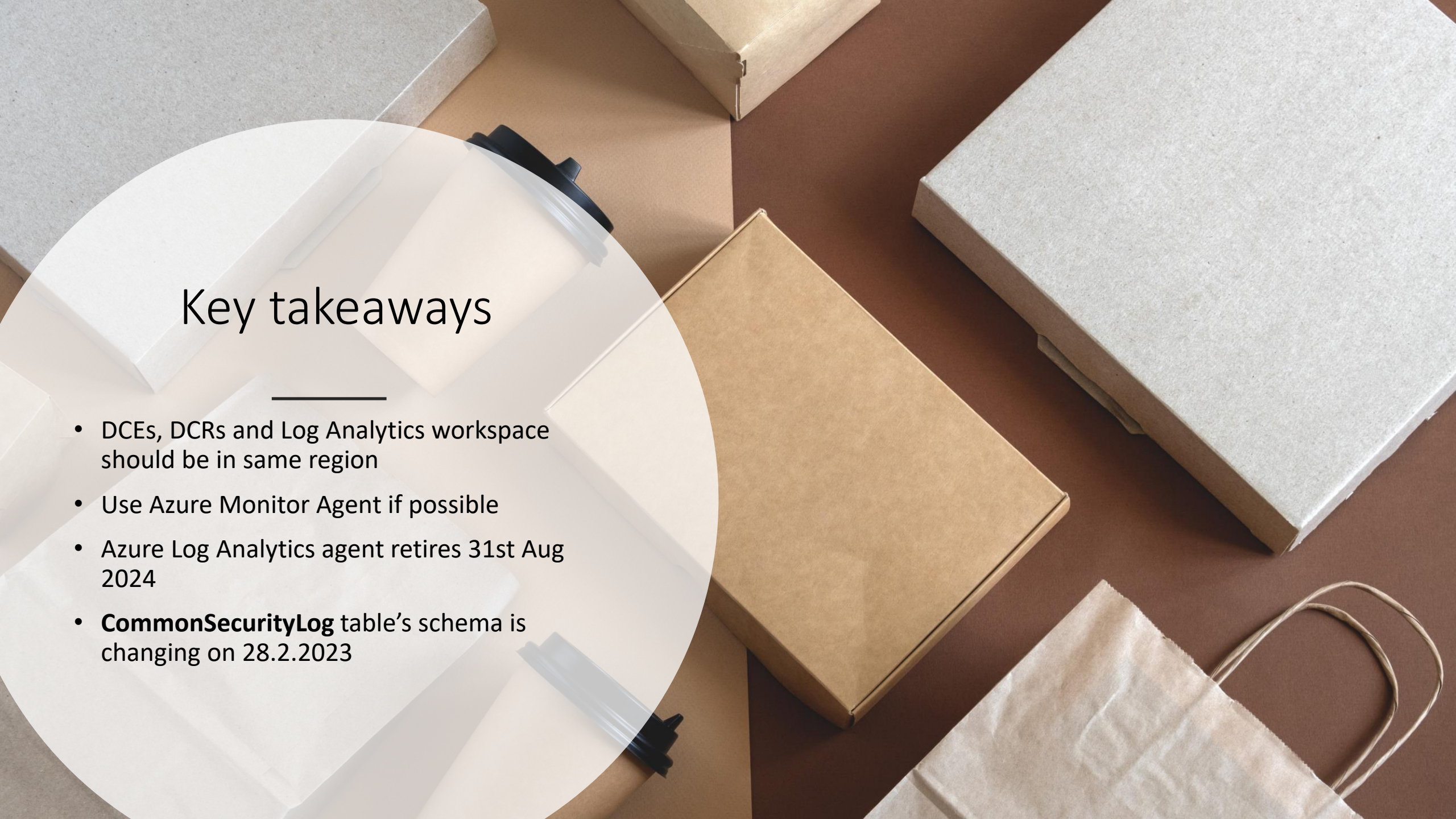


Use cases

- Sentinel data ingestion
- Operational VM data ingestion
- VM insights main agent for dependency agent

Troubleshooting

- 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



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
- **CommonSecurityLog** table’s schema is changing on 28.2.2023

Q & A

Markus Lintuala
+358 40 585 5531
markus.lintuala@elisa.fi