#NVSummit2021

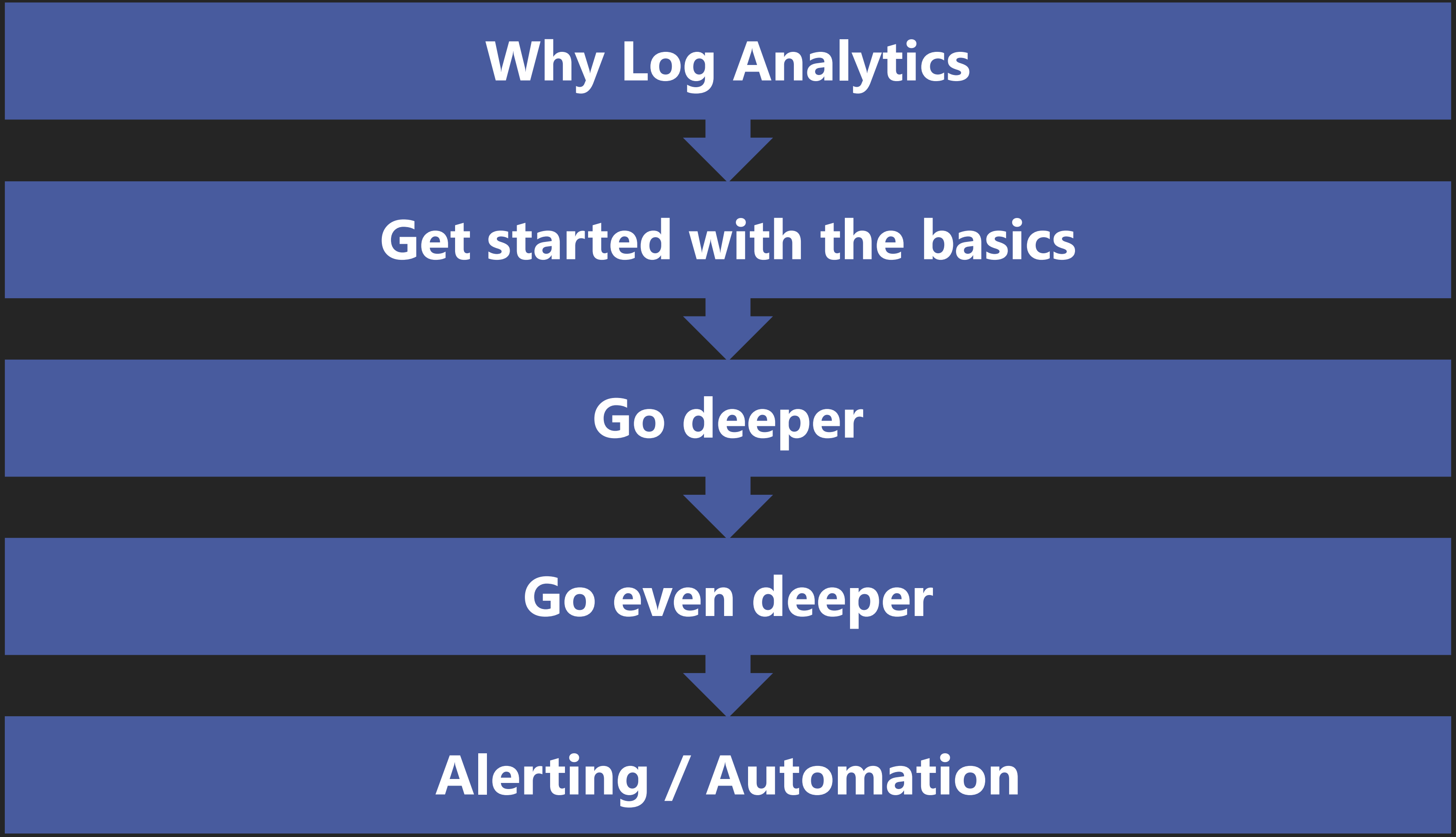
Log Analytics of MEM

- **Jan Ketil Skanke**
- Principal Cloud Architect at CloudWay
- Twitter @JankeSkanke
- MVP / MCT

- **Sandy Zeng**
- Senior Consultant at Sulava
- Twitter @sandy_tsang
- MVP

NORDIC – VIRTUAL SUMMIT –

Agenda



Why Log Analytics

Get started with the basics

Go deeper

Go even deeper

Alerting / Automation

Why Log Analytics

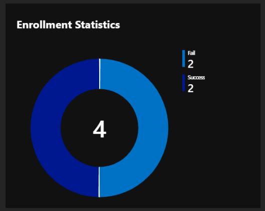
Log Analytics

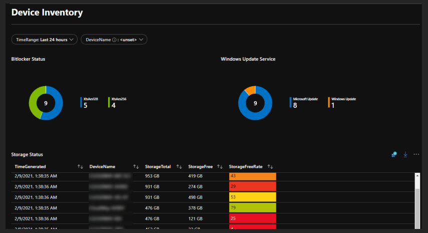
Traditional

- Typically reactive
- Manually or 3rd Party
- Hard to find the correct data
- Hard to get context

Modern

- Proactive
- Automated
- Query across datasources
- Cloud Delivered




Device Inventory

TimeRange: Last 24 hours
DeviceName: <unset>

Storage Status

TimeGenerated	DeviceName	StorageTotal	StorageFree	StorageFreeRate
2/9/2021, 1:38:35 AM	[redacted]	953 GB	419 GB	43
2/9/2021, 1:38:36 AM	[redacted]	931 GB	274 GB	29
2/9/2021, 1:38:36 AM	[redacted]	931 GB	498 GB	53
2/9/2021, 1:38:35 AM	[redacted]	476 GB	378 GB	79
2/9/2021, 1:38:36 AM	[redacted]	476 GB	121 GB	25

Log Analytics

- **What is it?**
  - Azure based log service
  - Collects/Inject logs from multiple locations, on-premises and in-cloud
- **Why use it?**
  - Get insights into your environment by merging data sources
  - Analyze metrics
  - Filter, sort, and group data as you see fit
  - Leverage built in reporting
  - Or.. Build your own reporting destiny
  - Can be used for monitoring and alerting

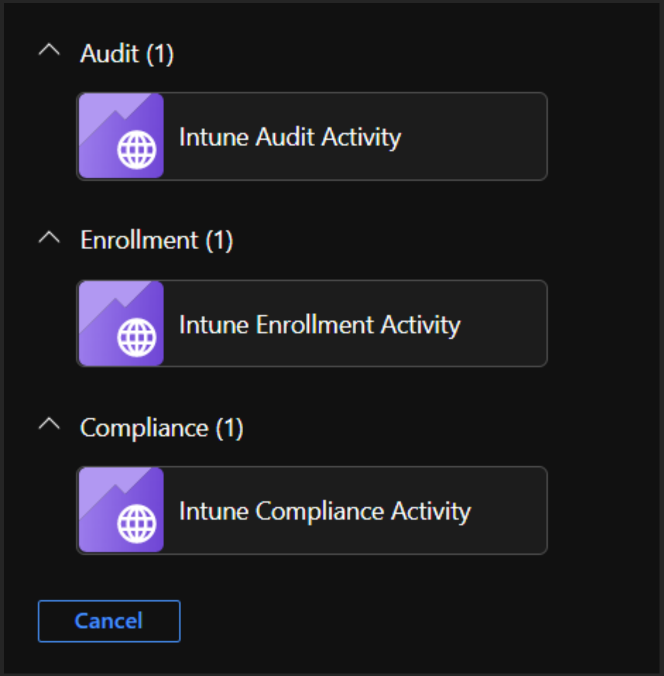
Get started with the basics

Collect Diagnostics Data

Use the Built-in Reports

Basic setup

- Collect diagnotics data from Intune and other sources
- Built-in Workbooks
- Data visualized



^ Audit (1)

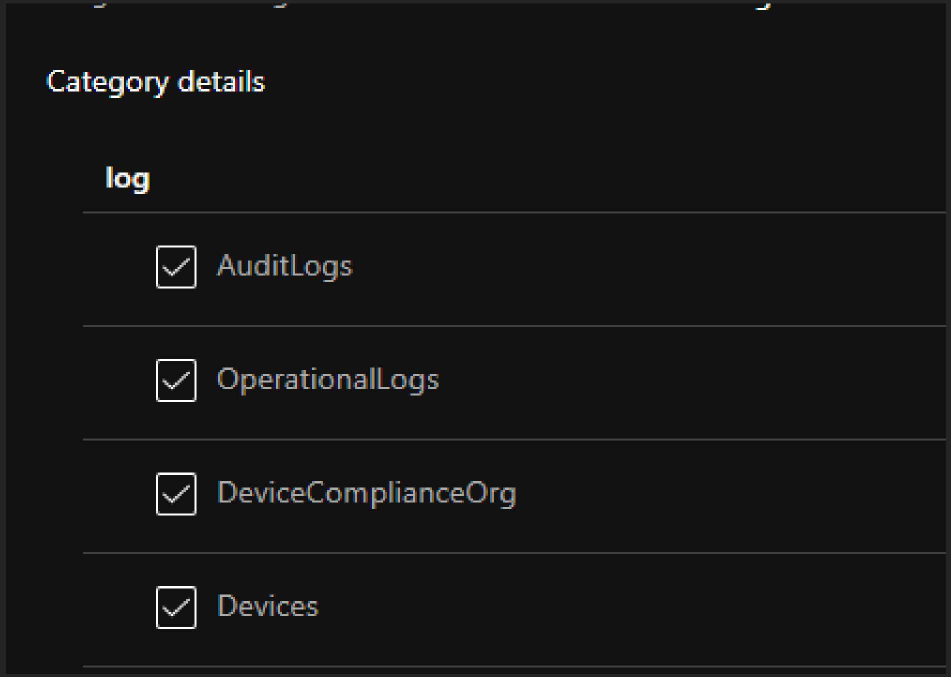
Intune Audit Activity

^ Enrollment (1)

Intune Enrollment Activity

^ Compliance (1)

Intune Compliance Activity



Category details

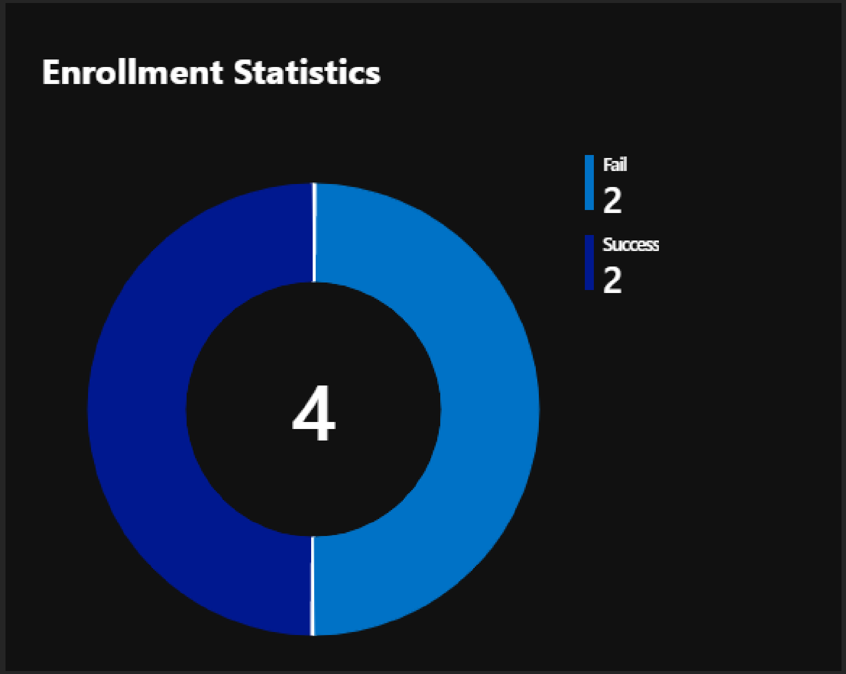
log

☑ AuditLogs

☑ OperationalLogs

☑ DeviceComplianceOrg

☑ Devices



Demo

Setup Intune Diagnostics
Built-in Reports
Workbooks

NORDIC
— VIRTUAL SUMMIT —

Demo

Setup Update Compliance

Update Compliance built-in reports

Go deeper

Build your own queries

Write your own queries (KQL)

- Ask logs for what YOU need to know!
- Combine datasources (Intune/AzureAD++)

Demo

Query data

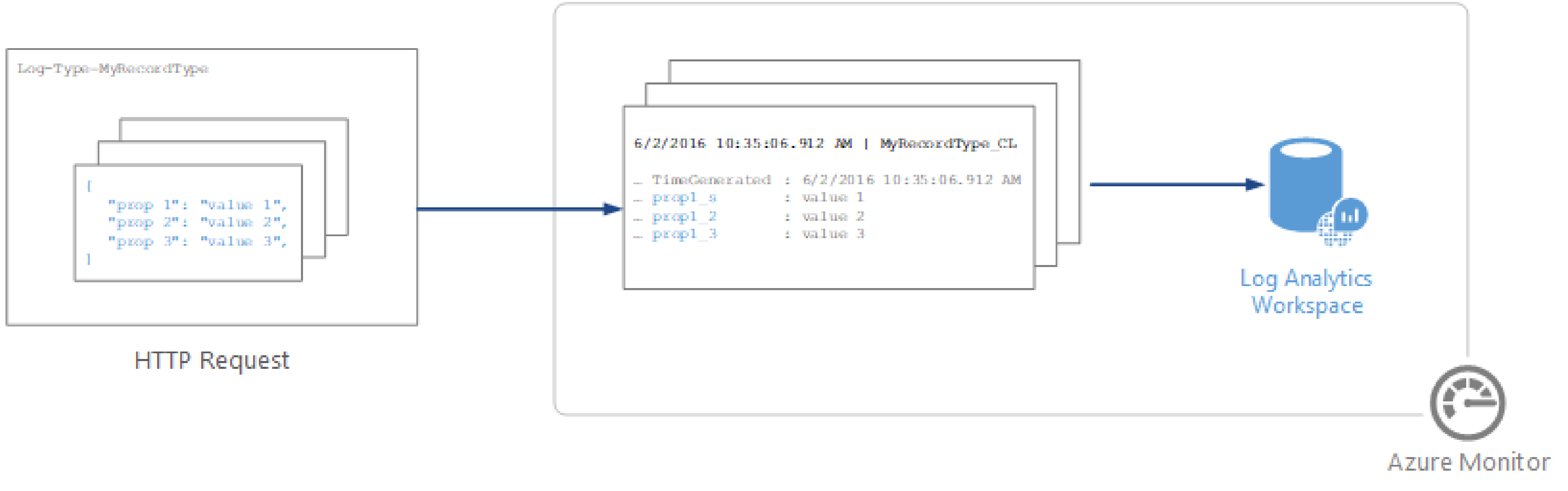
Go even deeper

Inject your own data

Build your own workbooks

HTTP Data Collector API

Authorize – SharedKey + WorkspaceID
Post via Rest API

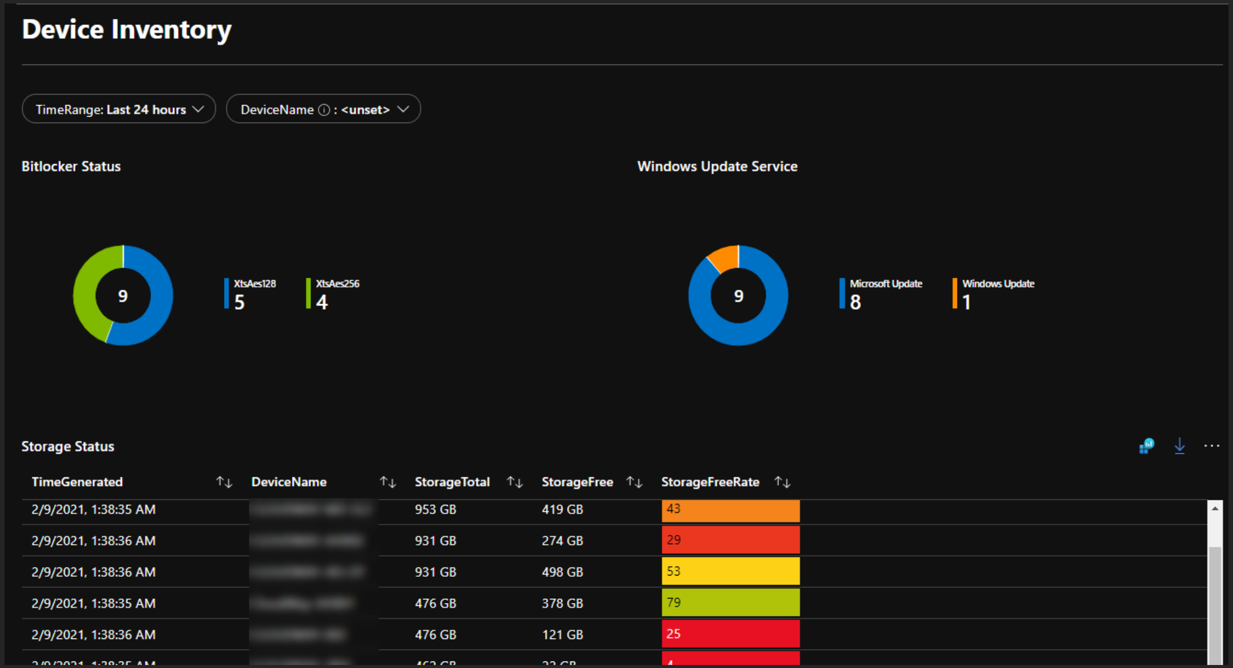


```
Log-Type-MyRecordType

[
  "prop 1": "value 1",
  "prop 2": "value 2",
  "prop 3": "value 3",
]
```

```
6/2/2016 10:35:06.912 AM | MyRecordType_CL

… TimeGenerated  : 6/2/2016 10:35:06.912 AM
… prop1_s        : value 1
… prop1_2        : value 2
… prop1_3        : value 3
```

https://docs.microsoft.com/en-us/azure/azure-monitor/platform/data-collector-api

Workbooks



Device Inventory

TimeRange: Last 24 hours

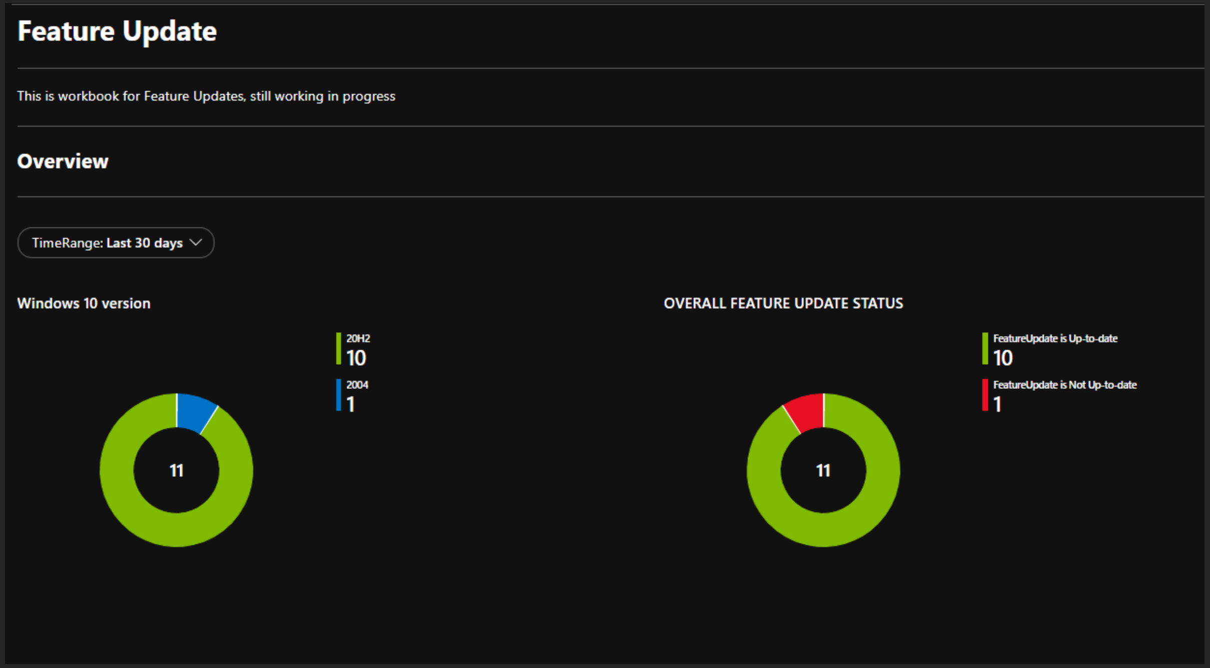
DeviceName ⓘ : <unset>

Bitlocker Status

Windows Update Service

Storage Status

TimeGenerated	DeviceName	StorageTotal	StorageFree	StorageFreeRate
2/9/2021, 1:38:35 AM	[redacted]	953 GB	419 GB	43
2/9/2021, 1:38:36 AM	[redacted]	931 GB	274 GB	29
2/9/2021, 1:38:36 AM	[redacted]	931 GB	498 GB	53
2/9/2021, 1:38:35 AM	[redacted]	476 GB	378 GB	79
2/9/2021, 1:38:36 AM	[redacted]	476 GB	121 GB	25
2/9/2021, 1:38:35 AM	[redacted]	462 GB	22 GB	4



Feature Update

This is workbook for Feature Updates, still working in progress

Overview

TimeRange: Last 30 days

Windows 10 version

OVERALL FEATURE UPDATE STATUS

Demo

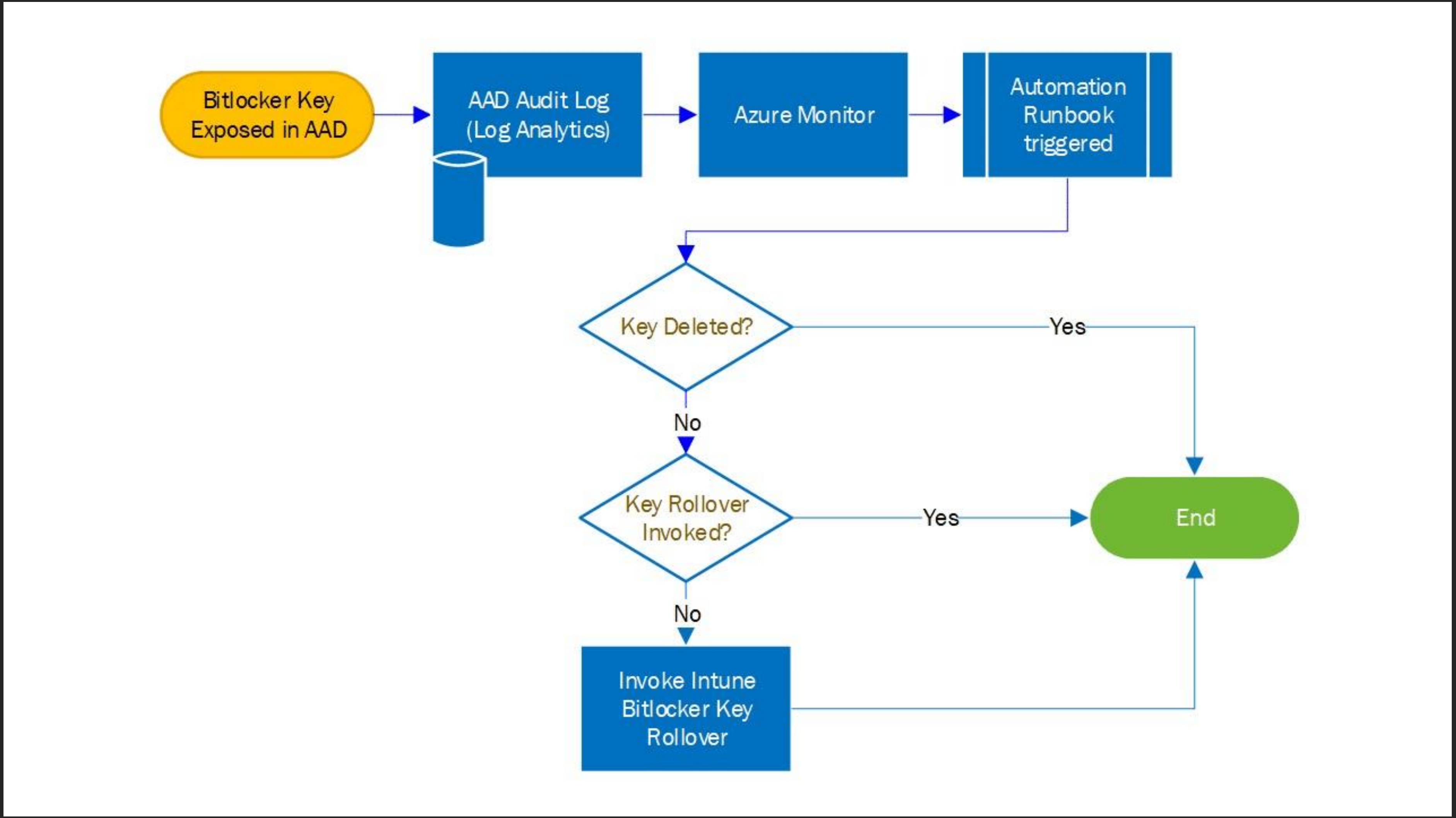
Inject custom logs
Workbooks

NORDIC
– VIRTUAL SUMMIT –

Azure Monitor + Automation

Bitlocker Scenario

Bitlocker Remedy


Bitlocker Key Exposed in AAD
AAD Audit Log (Log Analytics)
Azure Monitor
Automation Runbook triggered
Key Deleted?
Yes
No
Key Rollover Invoked?
Yes
No
End
Invoke Intune Bitlocker Key Rollover

https://msendpointmgr.com/2020/10/05/true-bitlocker-one-time-recovery-key-with-intune/

Demo

Automation - Bitlocker Remedy

Thank you!

NORDIC
– VIRTUAL SUMMIT –

MSEndPointMgr.com
#MSEndPointMgr

System Center User Group
Finland
#SCUGFI

System Center User Group
Denmark

#SCUGDK

System Center User Group
Sweden
#SCUGSE

Modern Management User Group
Norway
#MMUGNO