

The Log Analytics of MEM!

Jan Ketil Skanke



Jan Ketil Skanke

COO & Principal Cloud Architect

CloudWay

«Geek on a Harley»

Twitter: @JankeSkanke

Blog: <https://msendpointmgr.com>

Community:

- Nordic Virtual Summit
- ExpertsLive Norway
- Microsoft Management User Group Norway (MMUGNO)

MVPDAGEN

En konferanse der
MVPer deler sin
kunnskap med deg

MVPdagen – 5 års jubileum
Fra oss til deg

 **CloudWay**

Why Log Analytics?

Inventory



Monitoring and Alerting



Intune Native

Intune Native Reporting Capabilities

- Data spread across many places in the portal
- Data is not rich enough for many customers needs
- Some critical data (based on needs) might be missing
- Reporting API exists, but hard to use (MSGraph)



Demo: Intune Native Reporting

MVPdagen – 5 års jubileum
Fra oss til deg

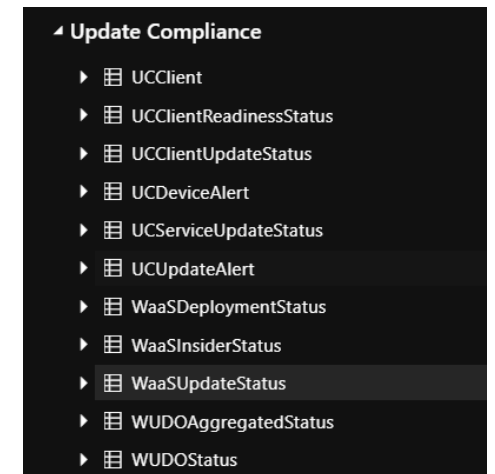
Windows Updates Reporting

Where is that Patch?

- Intune natively does not have enough information
- No history over time
- Update trends, rollout-times is missing

Update Compliance

- Update Compliance uses Windows diagnostic data for all its reporting
- It collects system data
 - Update deployment progress
 - Windows Update for Business configuration data
 - Delivery Optimization usage data
- Recently major update from MS with new tables



Update

- Update Co
- It collects s
 - Update d
 - Windows
 - Delivery
- Recently

Update Compliance

- ▶ UCClient
- ▶ UCClientReadinessStatus
- ▶ UCClientUpdateStatus
- ▶ UCDeviceAlert
- ▶ UCServiceUpdateStatus
- ▶ UCUpdateAlert
- ▶ WaaSDeploymentStatus
- ▶ WaaSInsiderStatus
- ▶ WaaSUpdateStatus
- ▶ WUDOAggregatedStatus
- ▶ WUDOSStatus

reporting

Onboarding to Update Compliance

- Log Analytics Workspace in Azure (Norway region not supported)
- Get your Commercial ID
- Enroll devices in Update Compliance
- Wait – up to 72 hours
- Build your Workbooks



Demo: Update Compliance Solution

MVPdagen – 5 års jubileum
Fra oss til deg

Enhance your Inventory

Device and App Inventory

- Device Inventory is missing data we need or want
 - Used to having rich data insights in ConfigMgr
 - Used to be able to enhance data via MOF files or similar
- App Inventory in Intune is not reliable enough
 - Apps Missing
 - Long delays in reporting

Custom Inventory via Proactive Remediations

- Collect our own data with PowerShell directly on the clients
- Send data to Azure Monitor logs via Rest API
 - Using Proactive Remediations
- Build our own reporting dashboards
 - Azure Workbooks
- V2: Secure the API connection with Azure Functions



Demo: Custom Inventory

MVPdagen – 5 års jubileum
Fra oss til deg




Demo: Other Use Cases

MVPdagen – 5 års jubileum
Fra oss til deg

Sep 2
9:46 AM

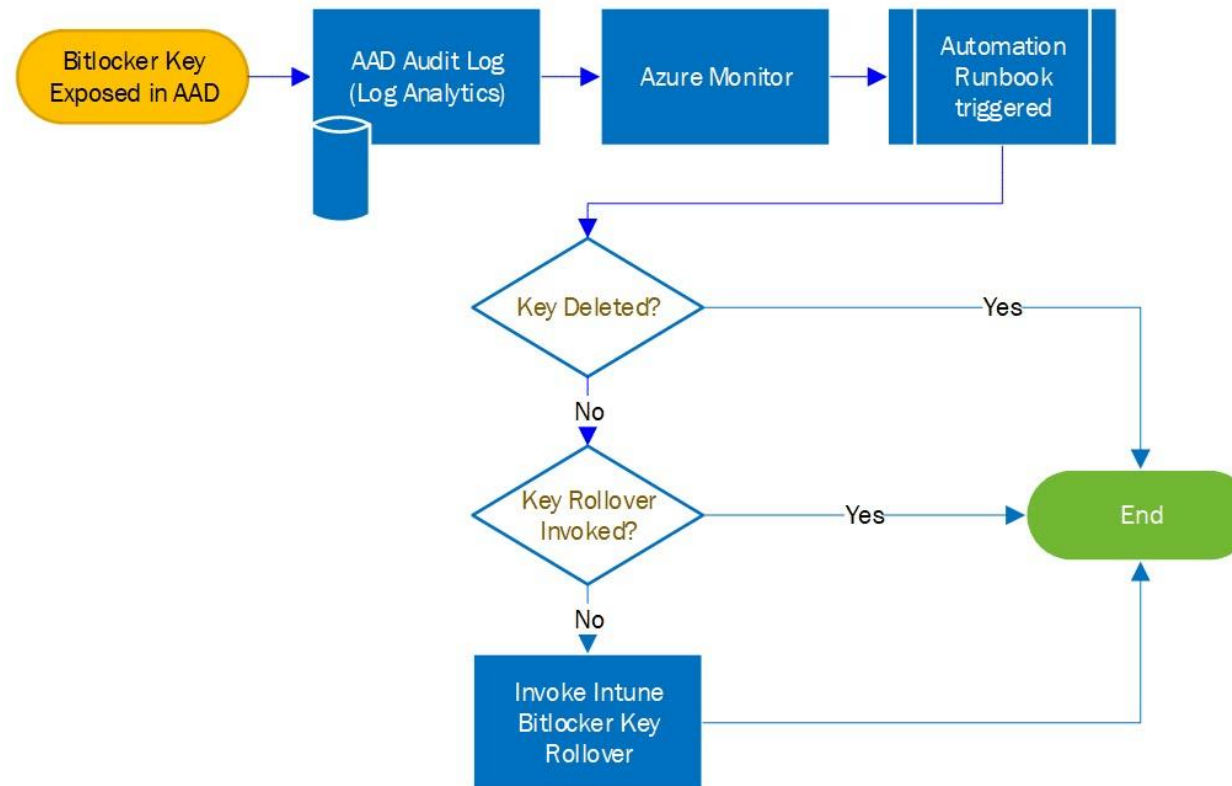


Bitlocker Key Exposed

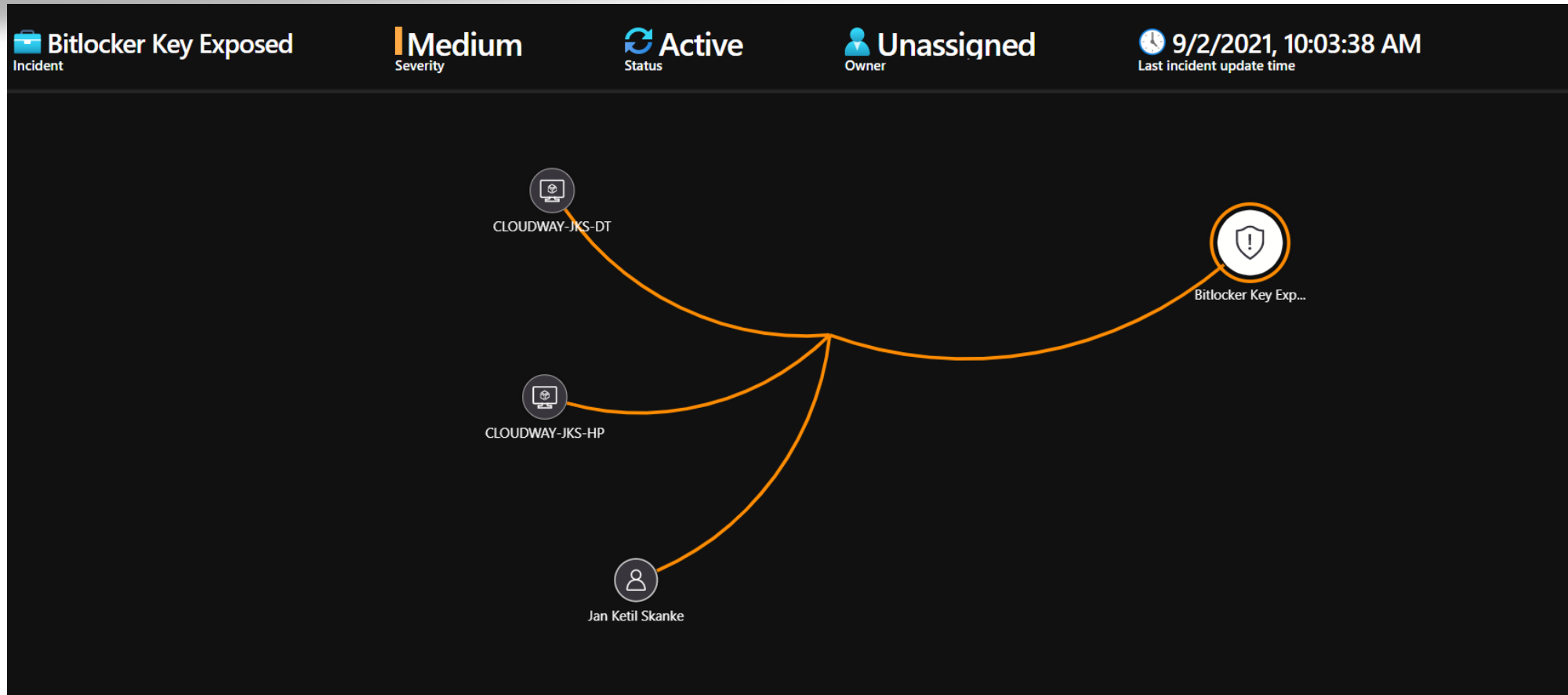
Medium | Detected by Azure Sentinel | Tactics:  Credential Access

11

Automate based on your data



Integrate your data with Azure Sentinel





Demo: Sentinel Integration

MVPdagen – 5 års jubileum
Fra oss til deg



Q&A

MVPdagen – 5 års jubileum
Fra oss til deg



Jan Ketil Skanke

COO & Principal Cloud Architect

CloudWay

«Geek on a Harley»

Twitter: @JankeSkanke

Blog: <https://msendpointmgr.com>

Community:

- Nordic Virtual Summit
- ExpertsLive Norway
- Microsoft Management User Group Norway (MMUGNO)

MVPDAGEN

En konferanse der
MVPer deler sin
kunnskap med deg

MVPdagen – 5 års jubileum
Fra oss til deg

 **CloudWay**