Operations Management Suite

SUNET INKUBATOR WORKSHOP

Jakob Knutsson
IT Architect and Senior Consultant
jakob.knutsson@addlevel.se
@kntsn

addlevel

Provide out of the box application and workload insights

Hyper-scale machine data analytics platform

Robust hybrid monitoring solution

Jakob Knutsson
www.addlevel.se

addlevel


addlevel

OMS - Hybrid cloud management solution

Analytics & Monitoring

Security & Compliance

Backup & Disaster recovery

Configuration & Automation

Jakob Knutsson
www.addlevel.se

addlevel

Bakgrund

System Center Advisor

Jan 2012

Operational Insights

Maj 2014

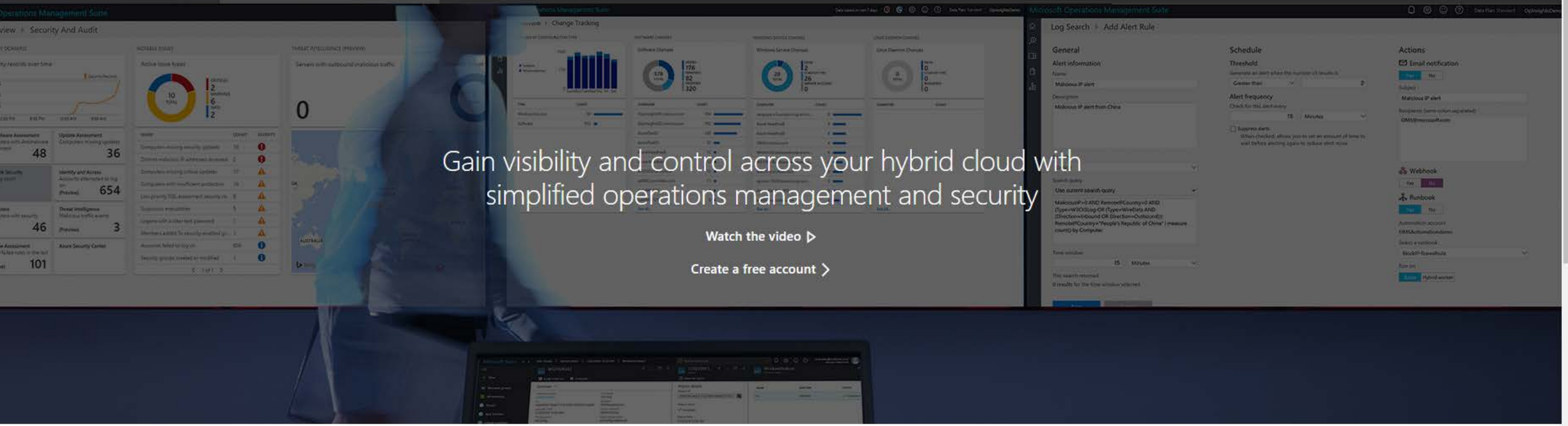
Operations Management Suite

Maj 2015

Sept 2016

Jakob Knutsson
www.addlevel.se

addlevel



Gain immediate insights across workloads

Tap into operational intelligence when it matters to explore, analyze, and take action faster.

Learn more about Insight & Analytics

Respond faster to security threats

Identify emerging threats to protect your critical data and workloads.

Learn more about Security & Compliance

Enable consistent control and compliance

Deliver continuous IT services and remediate issues quickly at scale.

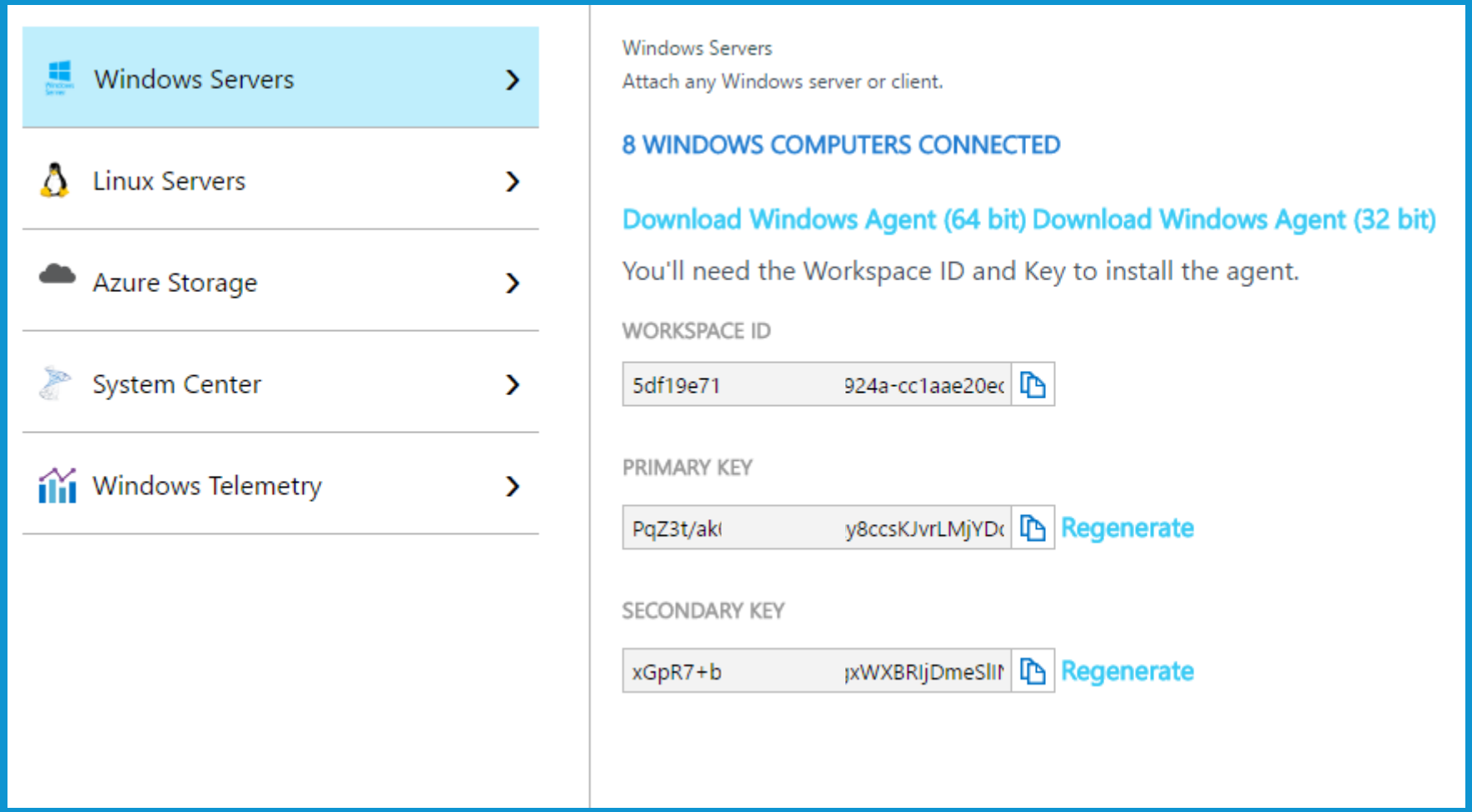
Learn more about Automation & Control

Ensure availability of apps and data

Simple, automated data protection and disaster recovery in the cloud.

Learn more about Protection & Recovery

Onboarding



Jakob Knutsson
www.addlevel.se

addlevel

OMS Query Language

filterExpression | command1 | command2 ...

String Literals
Date/Time:
Numbers
Type
Logical Operators
Sort
Wildcards
Top/Limit
Select
Avg

http://bit.ly/2bKMVFc

Jakob Knutsson
www.addlevel.se

addlevel

Log search

*

Type=Event
EventLevelName=Error

Jakob Knutsson
www.addlevel.se

addlevel

DEMO

Jakob Knutsson
www.addlevel.se

addlevel

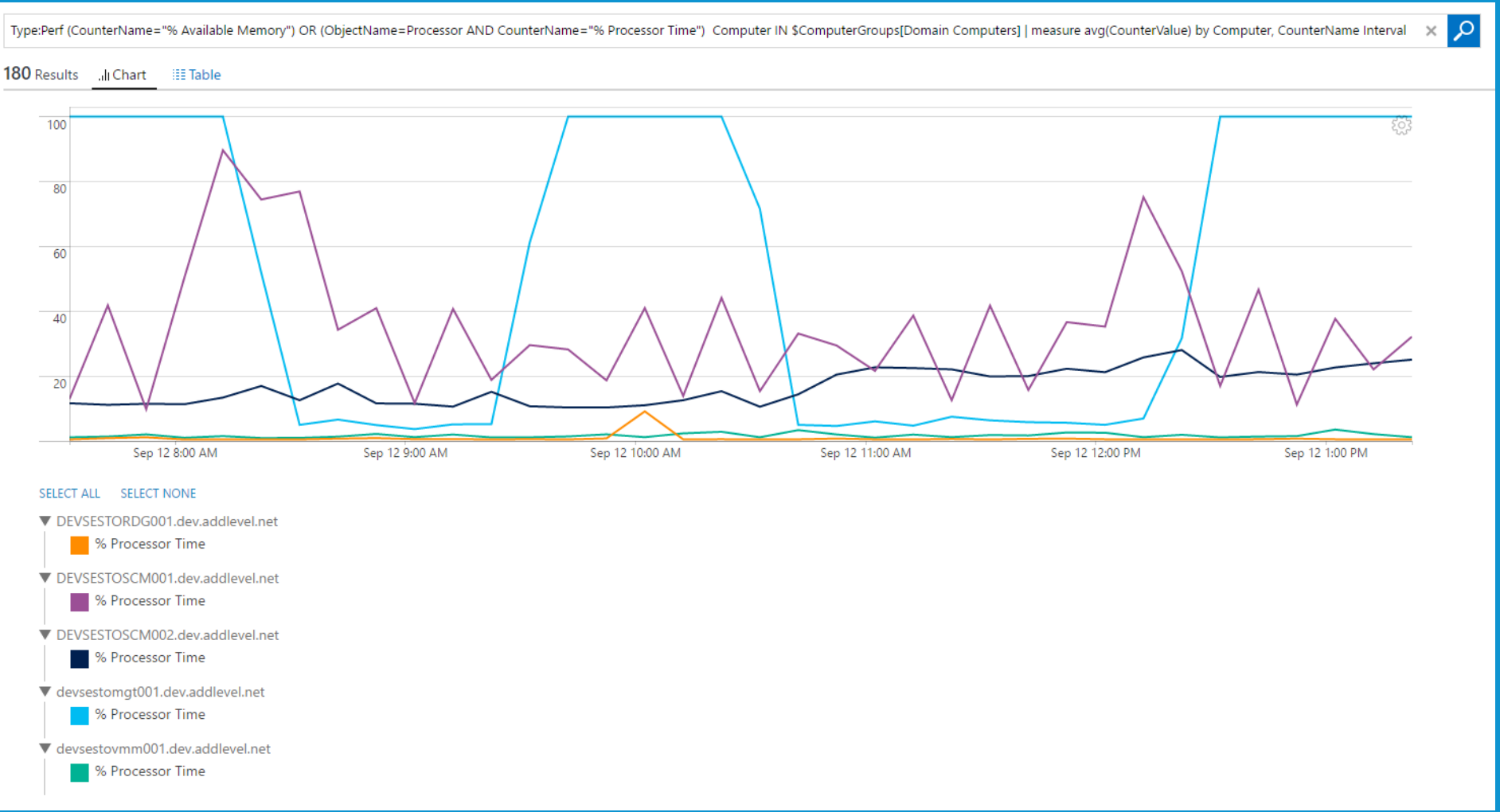
Egna Alerts

Skapa
Hantera

Jakob Knutsson
www.addlevel.se

addlevel

Performance Counters

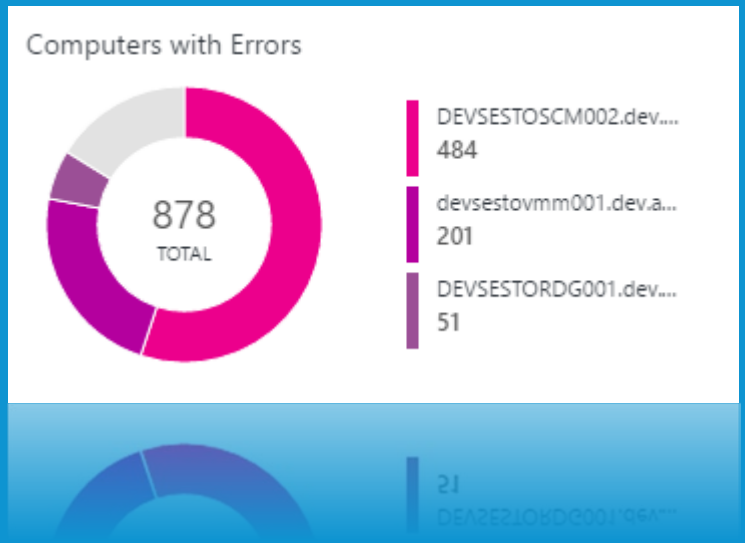


Jakob Knutsson
www.addlevel.se

addlevel

Skapa egna Views

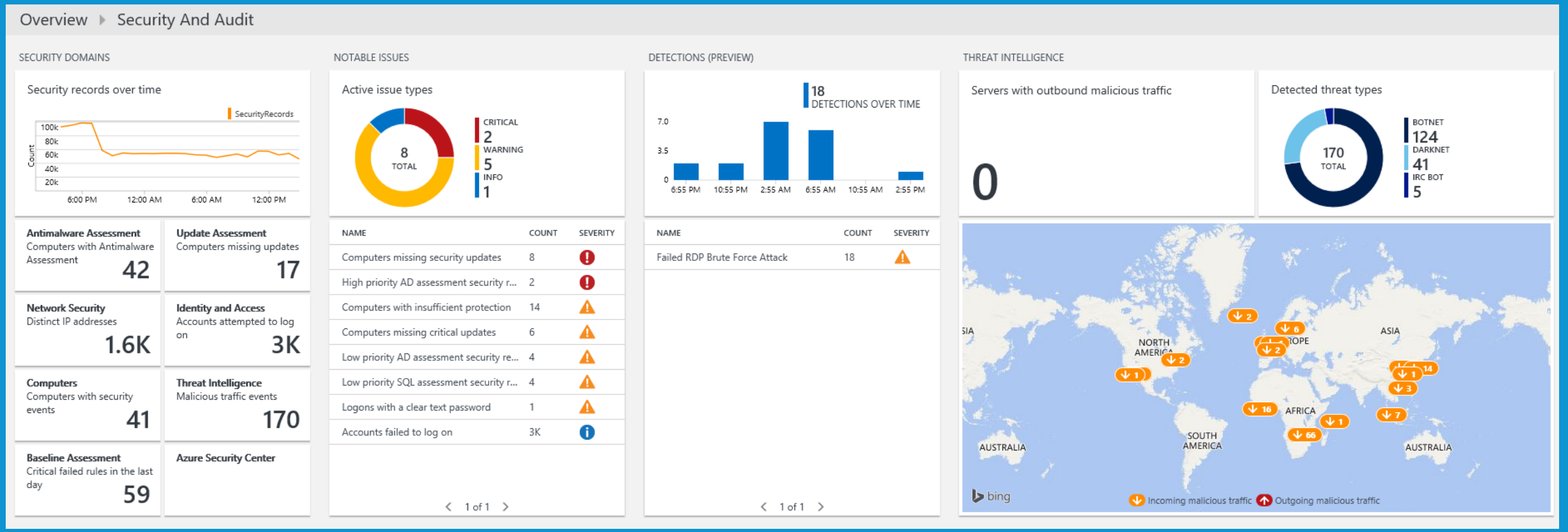
Dashboard och View Designer



Jakob Knutsson
www.addlevel.se

addlevel

Security and Audit



Jakob Knutsson
www.addlevel.se

addlevel

Security and Audit

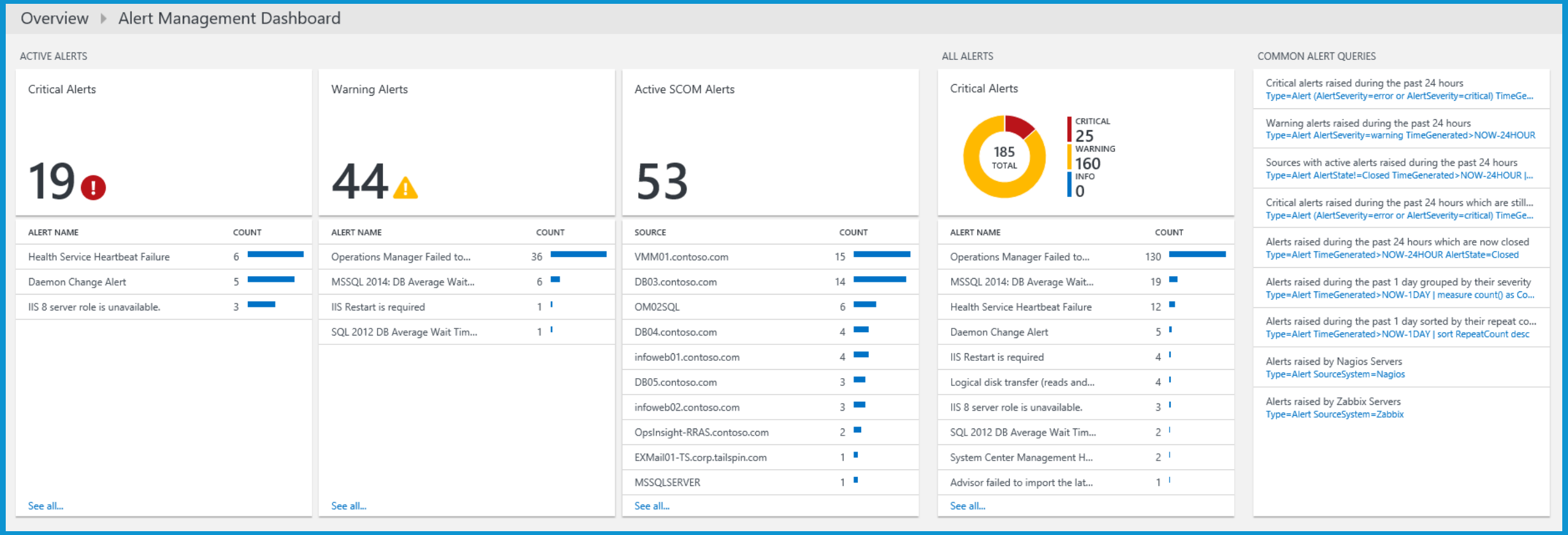
Type=SecurityEvent

Exempel query (failed logon):
Type=SecurityEvent EventID=4625 | measure count() by TargetAccount

Jakob Knutsson
www.addlevel.se

addlevel

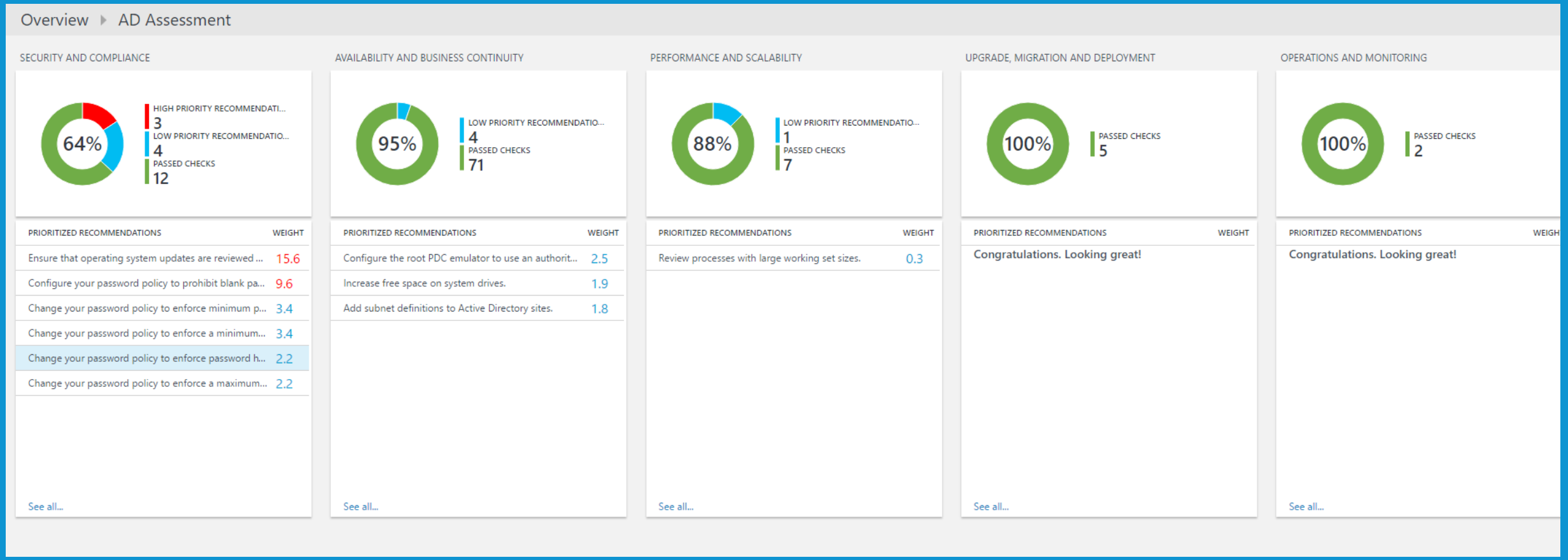
Alert Management



Jakob Knutsson
www.addlevel.se

addlevel

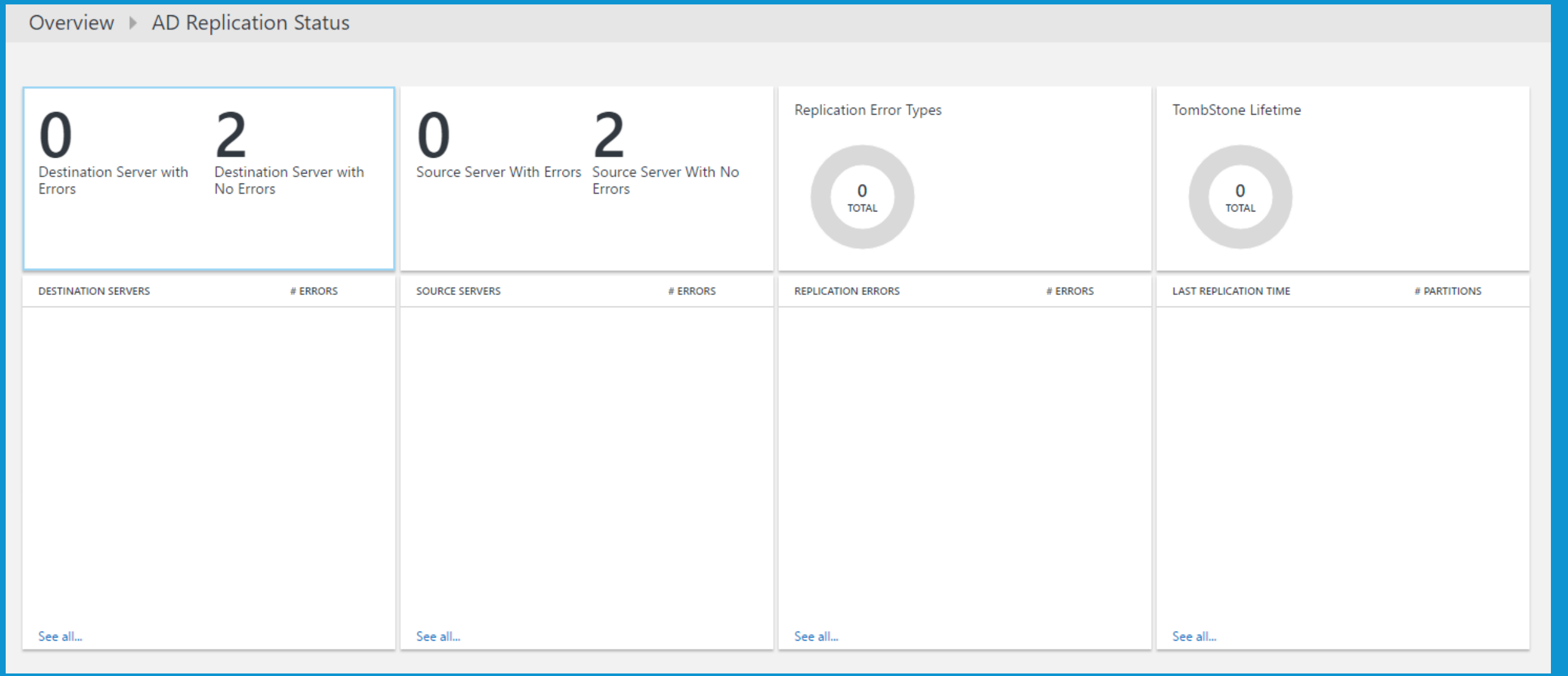
AD Assessments



Jakob Knutsson
www.addlevel.se

Microsoft addlevel

AD Replication Status



Jakob Knutsson
www.addlevel.se

Microsoft addlevel

Antimalware Assessments

Log Analytics rapporterar antimalware status för:

- Computers running Windows Defender on Windows 8, Windows 8.1, Windows 10, and Windows Server 2016 TP4 or later
- Windows Security Center (WSC) on Windows 8, Windows 8.1, Windows 10, Windows Server 2016 TP4 or later
- Servers running System Center Endpoint Protection (v4.5.216 or later), Azure virtual machines with the antimalware extension, and Windows Malicious Software Removal Tool (MSRT)
- Servers with Windows Management Framework 3 (or later) WMF 3.0, WMF 4.0

Jakob Knutsson
www.addlevel.se

addlevel

Antimalware Assessments

Antimalware assessment rapporterar inte på:

- Servers running Windows Server 2008 and earlier
- Web and Worker roles in Microsoft Azure
- 3rd party antimalware products

Refer to Reporting antimalware status for servers not supported by the antimalware solution for details on how to build a dashboard to report on all computers.

Jakob Knutsson
www.addlevel.se

addlevel

System Update

System Update Assessment samlar metadata och “state data” via OMS-agenten.

Type=Update

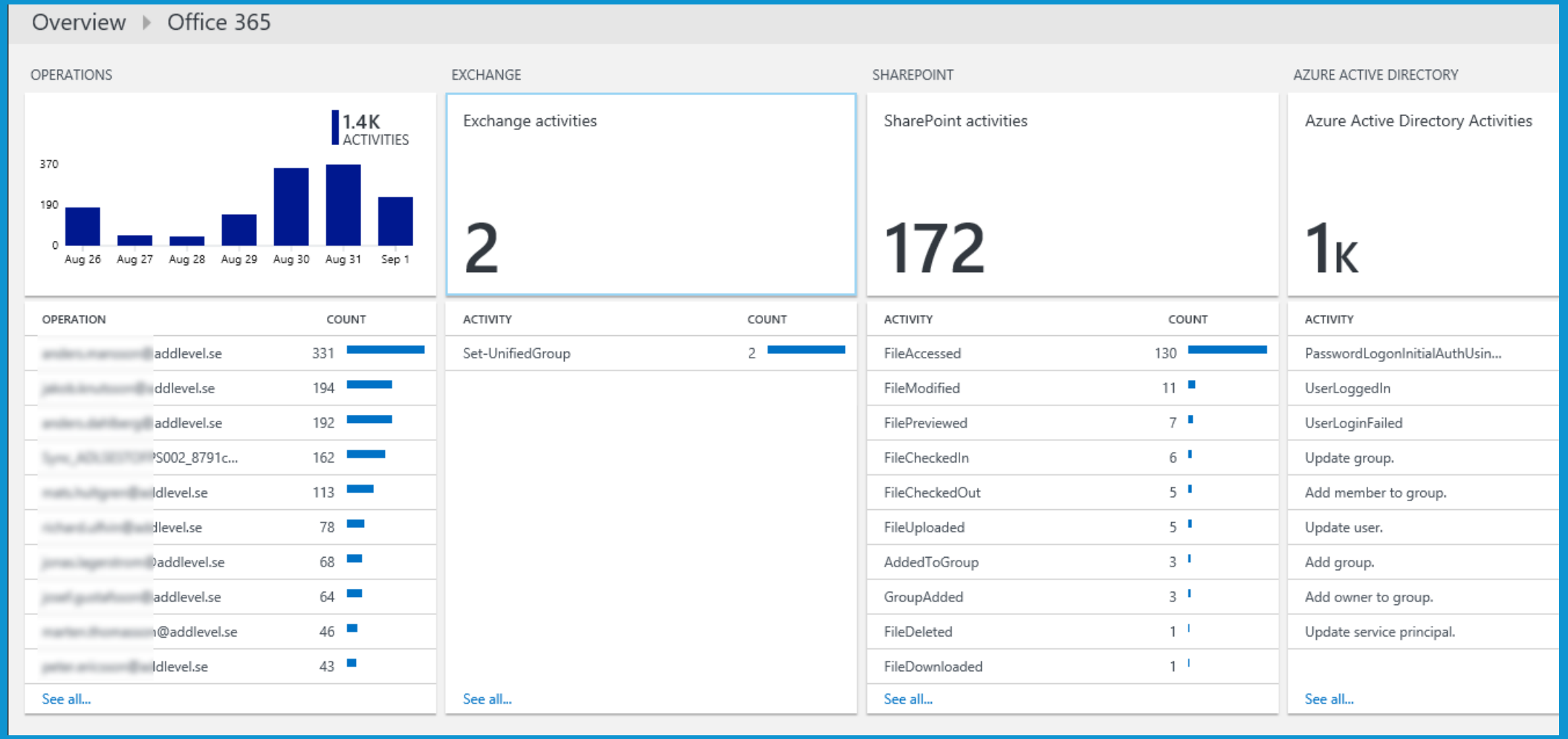
Insamlingsmetoderna:

platform	Direct Agent	SCOM agent	Azure Storage	SCOM required?	SCOM agent data sent via management group	collection frequency
Windows	✓	✓	✗	✗	✓	At least 2 times per day and 15 minutes after installing an update

Jakob Knutsson
www.addlevel.se

addlevel

Office 365



Jakob Knutsson
www.addlevel.se

addlevel

Upgrade Analytics

Add Upgrade Analytics to Operations Management Suite

Enable data sharing between your organization and Upgrade Analytics

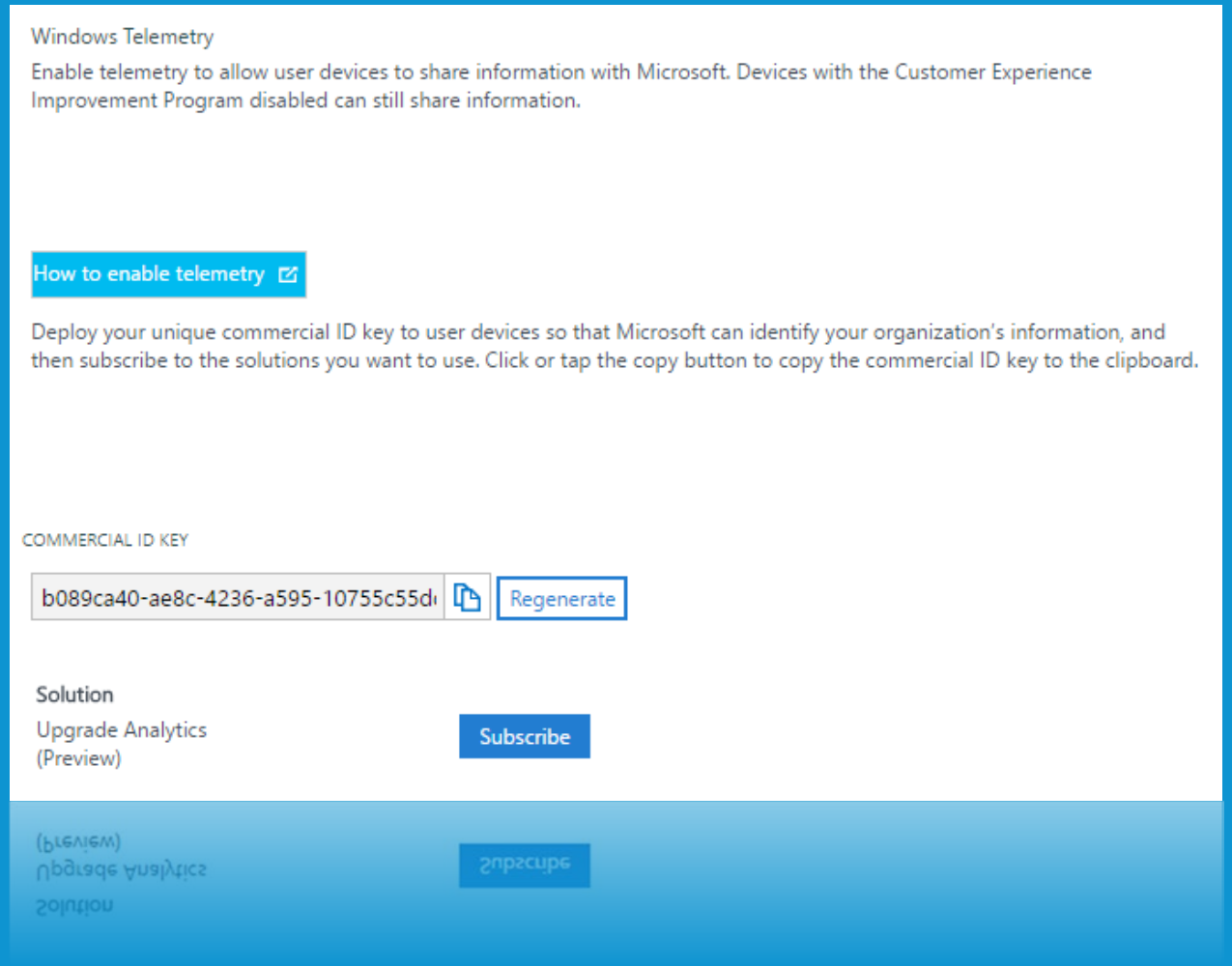
Generate your commercial ID key

Whitelist select endpoints

Deploy the compatibility update and related KBs

Download and run the Upgrade Analytics deployment script on clients.

https://technet.microsoft.com/itpro/windows/deploy/upgrade-analytics-get-started#enable-data-sharing-between-your-organization-and-upgrade-analytics

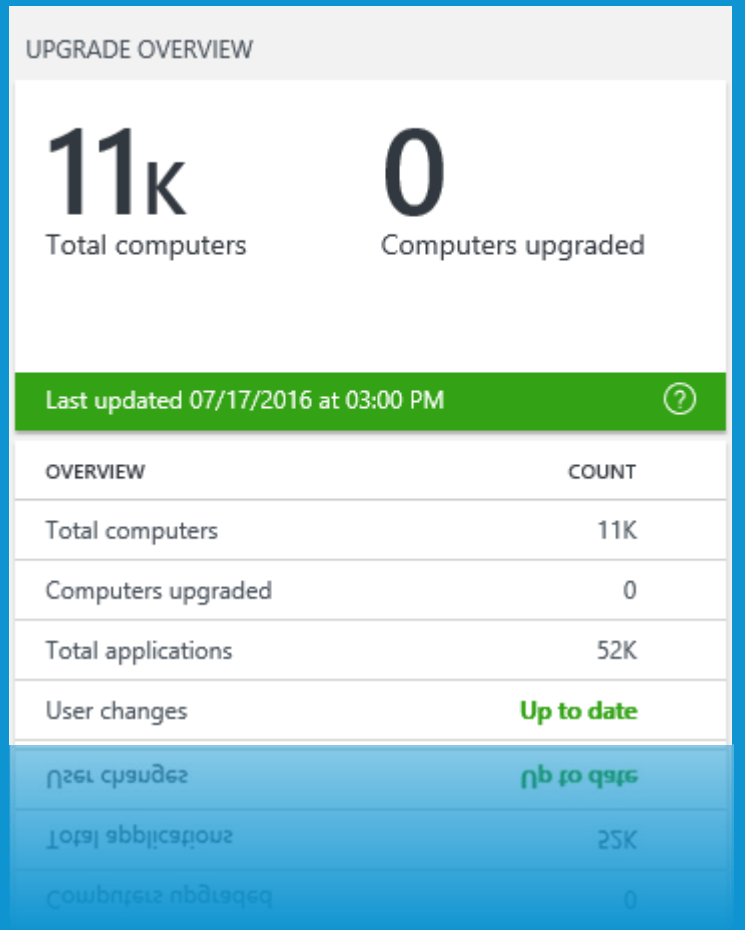


addlevel

Upgrade Analytics

Datorer

- Computer ID and computer name
- Computer manufacturer
- Computer model
- Operating system version and build
- Count of system requirement, application, and driver issues per computer
- Upgrade assessment based on analysis of computer telemetry data
- Upgrade decision status



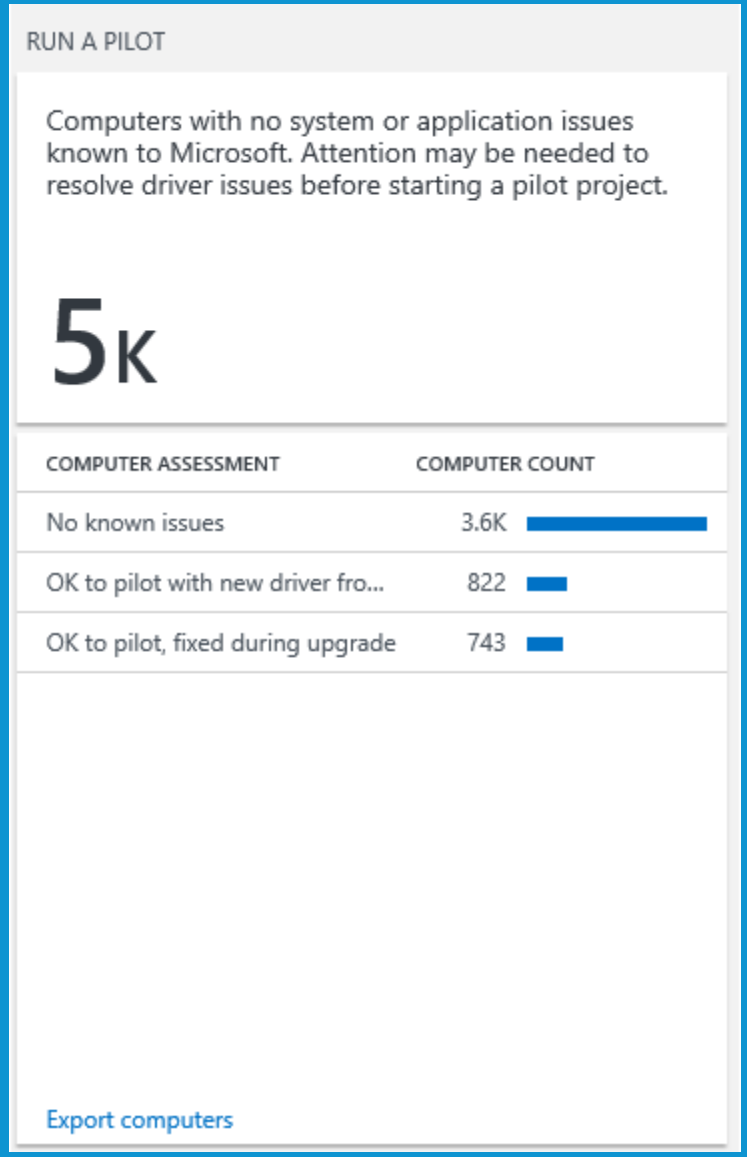
Jakob Knutsson
www.addlevel.se

addlevel

Upgrade Analytics

Applikationer

- Application vendor
- Application version
- Count of computers the application is installed on
- Count of computers that opened the application at least once in the past 30 days
- Percentage of computers in your total computer inventory that opened the application in the past 30 days
- Issues detected, if any
- Upgrade assessment based on analysis of application data
- Roll up level



Jakob Knutsson
www.addlevel.se

addlevel

PowerBI

1. Skapa upp ett PowerBI konto (finns Free Plan på 1GB).
   https://powerbi.microsoft.com/en-us/

2. Slå på PowerBI i OMS. Settings > Preview Features >

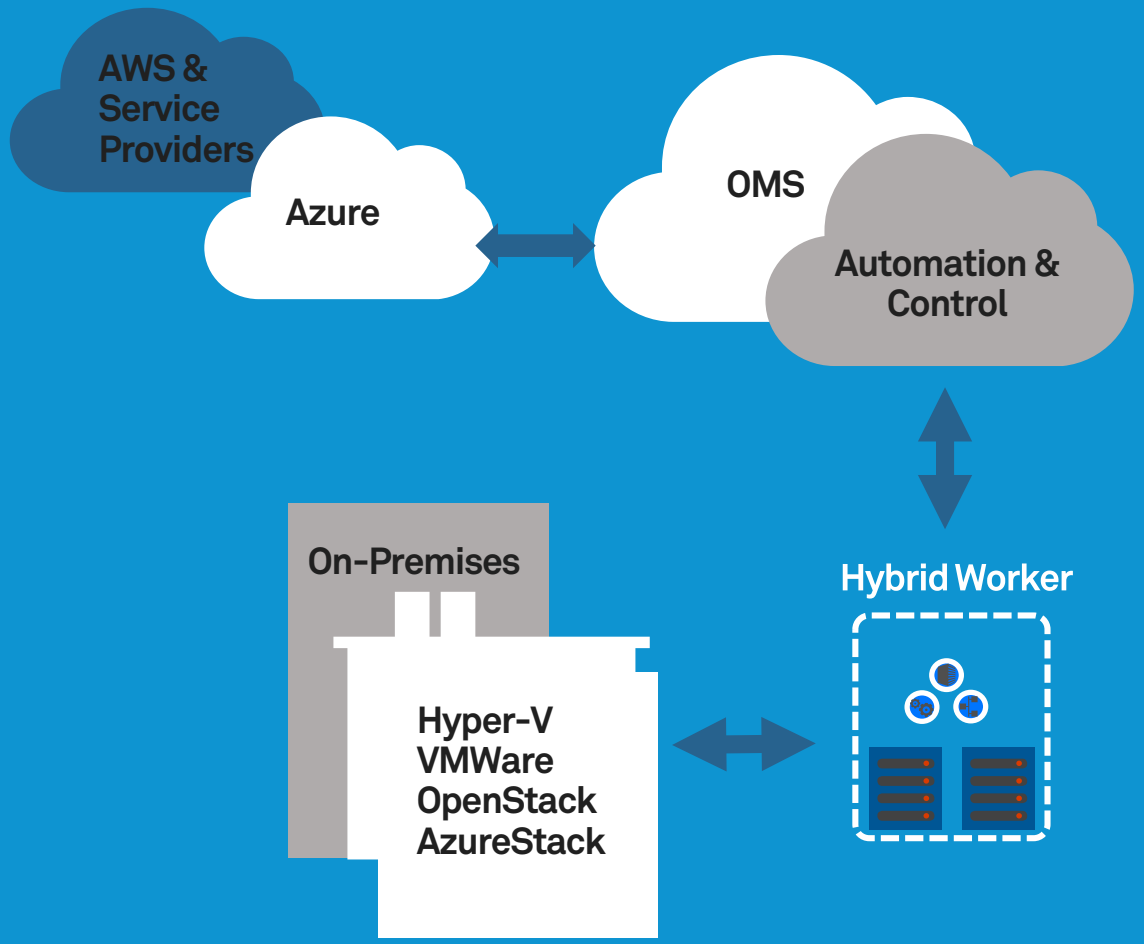
3. Koppla ihop PowerBi konto med OMS. Settings > Accounts > Workspace Information

4. Skapa searches för att få ut ”Datasets”. Klicka på PowerBi.
   Det din query får ut blir ditt dataset som du sedan kan arbeta med i PowerBi.

Jakob Knutsson
www.addlevel.se

addlevel

Automation & Control



- ✓ Process Automation (Runbooks, PowerShell, Gallery)
- ✓ Configuration Management (DSC, Change Tracking)
- ✓ Update Management
- ✓ Manage any cloud & on premises
- ✓ Windows & Linux

Jakob Knutsson
www.addlevel.se

addlevel

Azure Backup och Site Recovery

Simple & Cost Effective

Public cloud as DR site

Designed for public cloud with no Infrastructure components

Simple getting started experience

Heterogeneous

VMWare, Hyper-V, Physical

Windows, Linux (RHEL, Cent OS, SUSE, OEL etc.)

Application Aware

Application and Multi-VM consistent replication

Automate App failovers through Recovery Plans and Azure automation

Client routing through Azure Traffic Manager

Convergence

Across data and Application Availability

Jakob Knutsson
www.addlevel.se

addlevel


När en applikation går ner, finns det alltid
någon som har en värre dag på jobbet.
RE.VA
MONRC.VIA
msc
addlevel

Service Map

Tidigare kallad Application Dependency Monitor

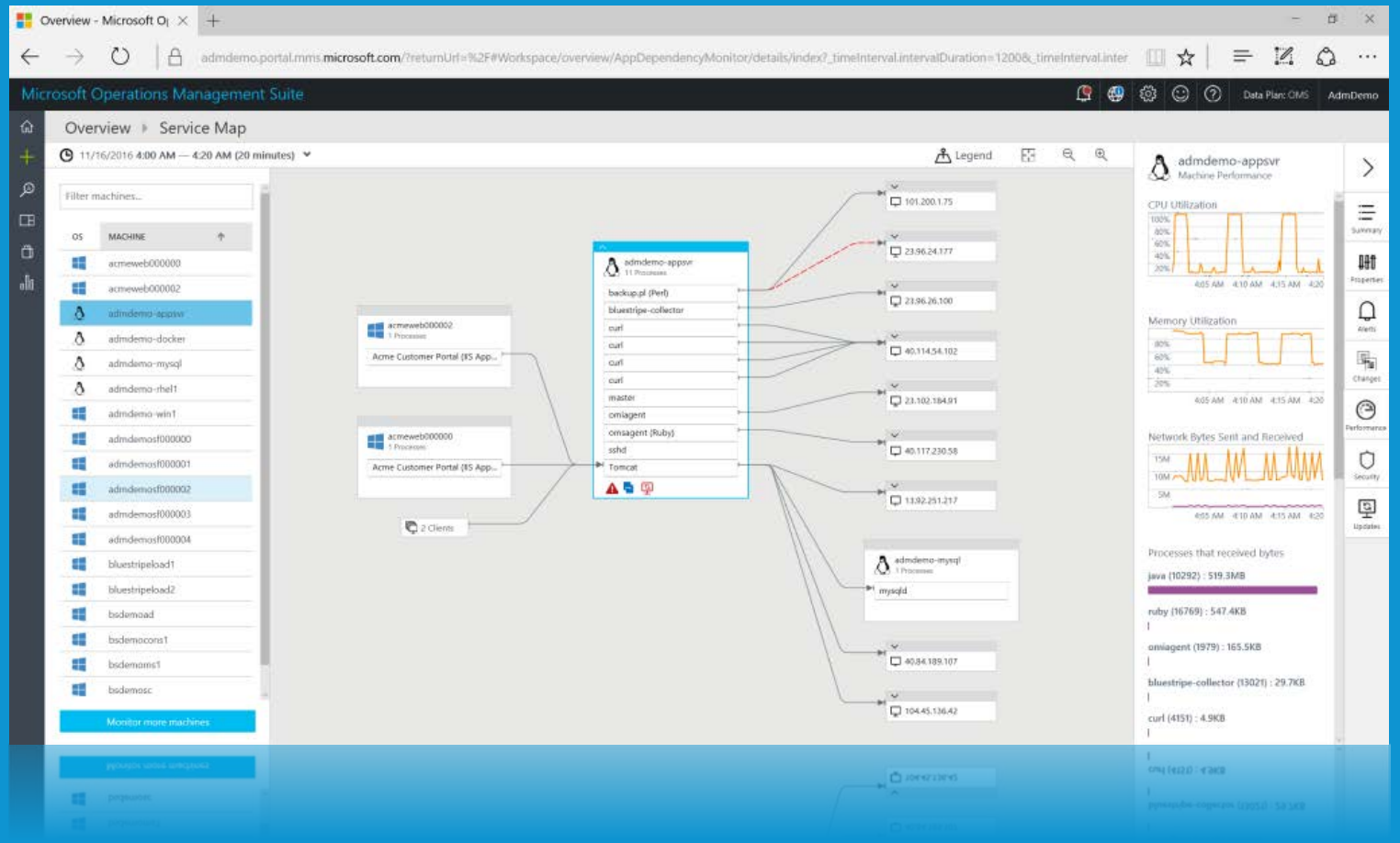
Bygger på FactFinder från BlueStripe

Automatically discover all dependencies for any Windows or Linux system

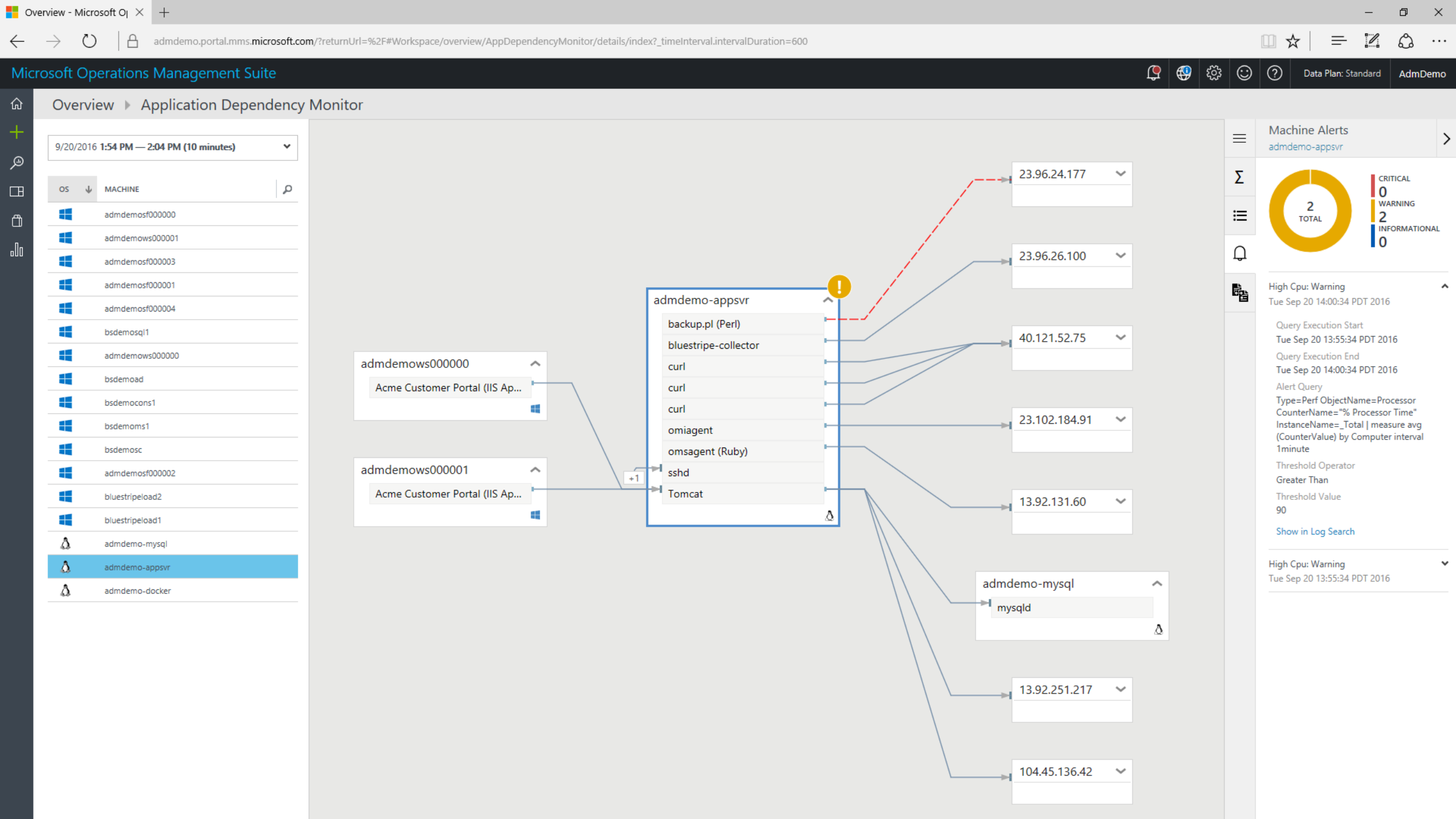
View all TCP-connected processes, their bound ports and connections

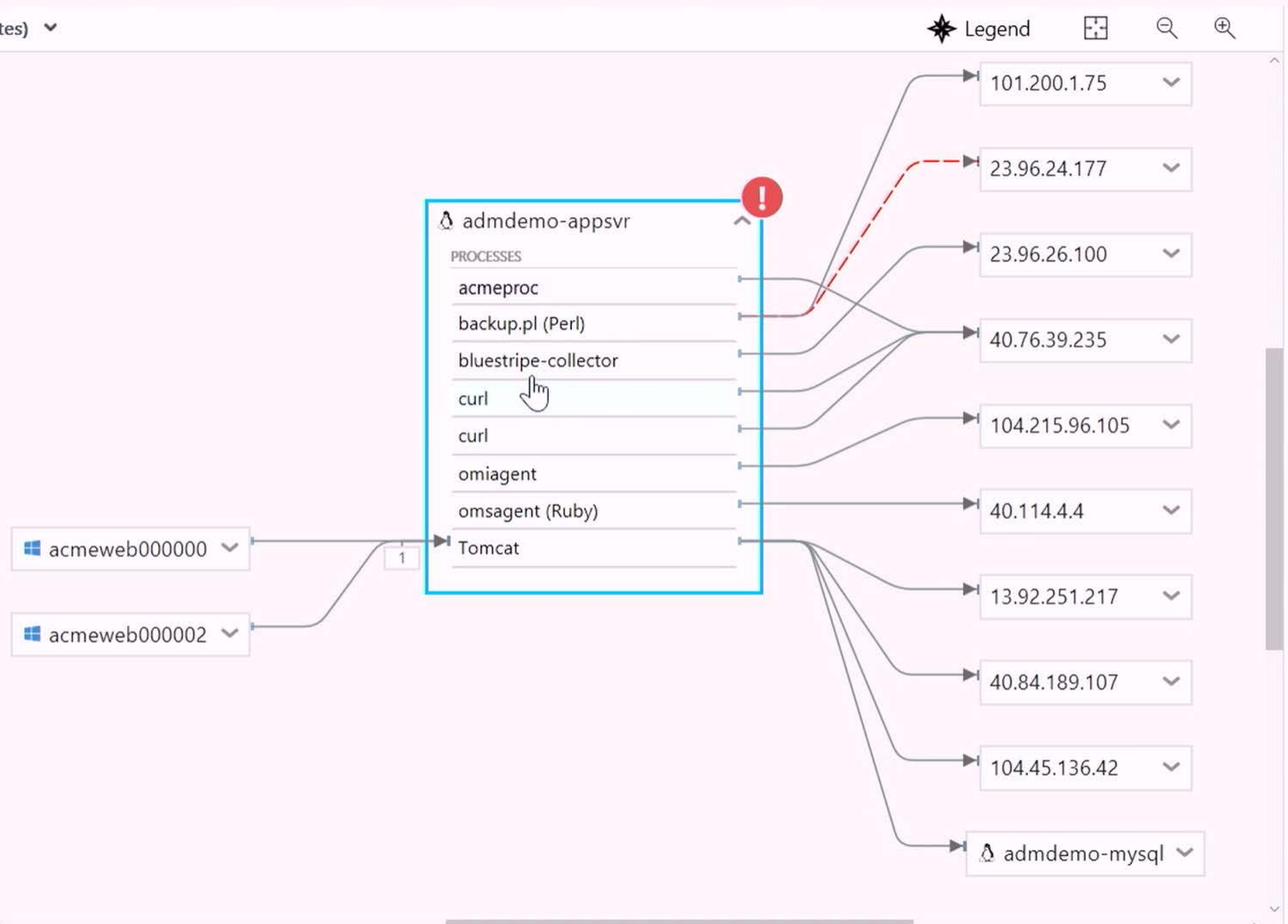
View dynamic maps of your system topology, live and historical

Visualize any alerts or change events across all dependencies for a given VM



addlevel


Overview - Microsoft O
admdemo.portal.mms.microsoft.com/?returnUrl=%2F#Workspace/overview/AppDependencyMonitor/details/index?_timeInterval.intervalDuration=600
Microsoft Operations Management Suite
Data Plan: Standard
AdmDemo
Overview
Application Dependency Monitor
9/20/2016 1:54 PM — 2:04 PM (10 minutes)
OS
MACHINE
admdemosf000000
admdemows000001
admdemosf000003
admdemosf000001
admdemosf000004
bsdemosql1
admdemows000000
bsdemoad
bsdemocons1
bsdemoms1
bsdemosc
admdemosf000002
bluestripeload2
bluestripeload1
admdemo-mysql
admdemo-appsvr
admdemo-docker
admdemows000000
Acme Customer Portal (IIS Ap...
admdemows000001
Acme Customer Portal (IIS Ap...
+1
admdemo-appsvr
backup.pl (Perl)
bluestripe-collector
curl
curl
curl
omiagent
omsagent (Ruby)
sshd
Tomcat
23.96.24.177
23.96.26.100
40.121.52.75
23.102.184.91
13.92.131.60
admdemo-mysql
mysqld
13.92.251.217
104.45.136.42
Machine Alerts
admdemo-appsvr
2
TOTAL
CRITICAL
0
WARNING
2
INFORMATIONAL
0
High Cpu: Warning
Tue Sep 20 14:00:34 PDT 2016
Query Execution Start
Tue Sep 20 13:55:34 PDT 2016
Query Execution End
Tue Sep 20 14:00:34 PDT 2016
Alert Query
Type=Perf ObjectName=Processor CounterName="% Processor Time" InstanceName=_Total | measure avg (CounterValue) by Computer interval 1minute
Threshold Operator
Greater Than
Threshold Value
90
Show in Log Search
High Cpu: Warning
Tue Sep 20 13:55:34 PDT 2016



admdemo-appsvr
Machine Summary

Linux 3.10.0-327.28.3.el7.x86_64,
CentOS Linux release 7.2.1511 (Core)

View More Properties...

Machine Dependencies

3	Connected Client Machines
10	Connected Server Machines

TCP Connections

4	Inbound Connections
12	Outbound Connections
1	Failed Connections

Alerts

2	Critical
0	Warning
0	Informational

Change Tracking

0	Windows Service
0	Software
0	Daemon

På väg

DDI Analytics (DNS, DHCP och IP infrastructure analys)
Windows File Tracking
Windows Registry Tracking
Flytt in i Azure-portalen

Nyligen släppta:
Service Map (tidigare kallad Application Dependency Monitor).
SCOM Assessment
Service Fabric
Wire Data 2.0

Jakob Knutsson
www.addlevel.se

Microsoft addlevel

Konkurrenter

Splunk

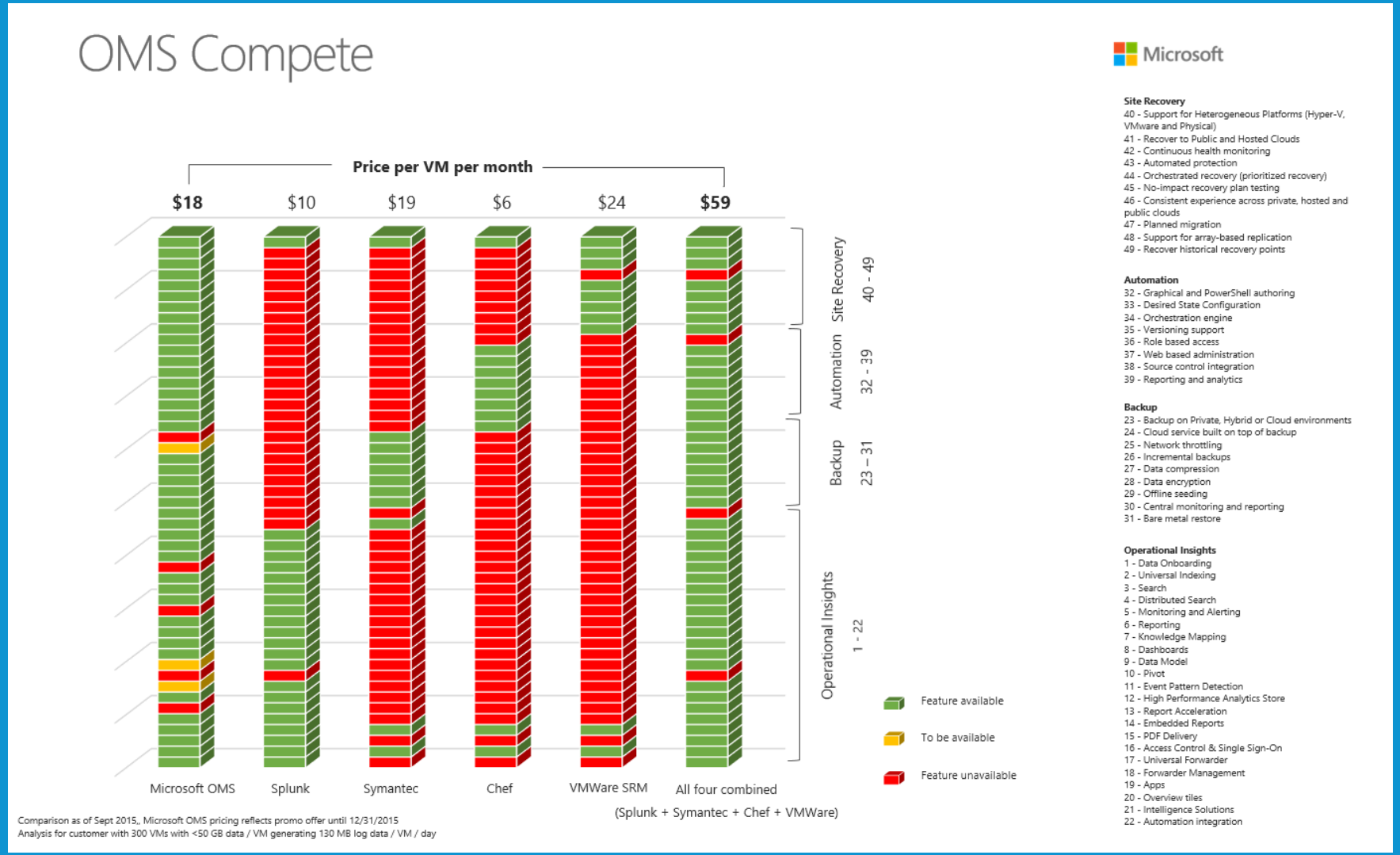
Elastic Search + Kibana

Traditionella övervakningsverktyg

Jakob Knutsson
www.addlevel.se

addlevel

Konkurrenter



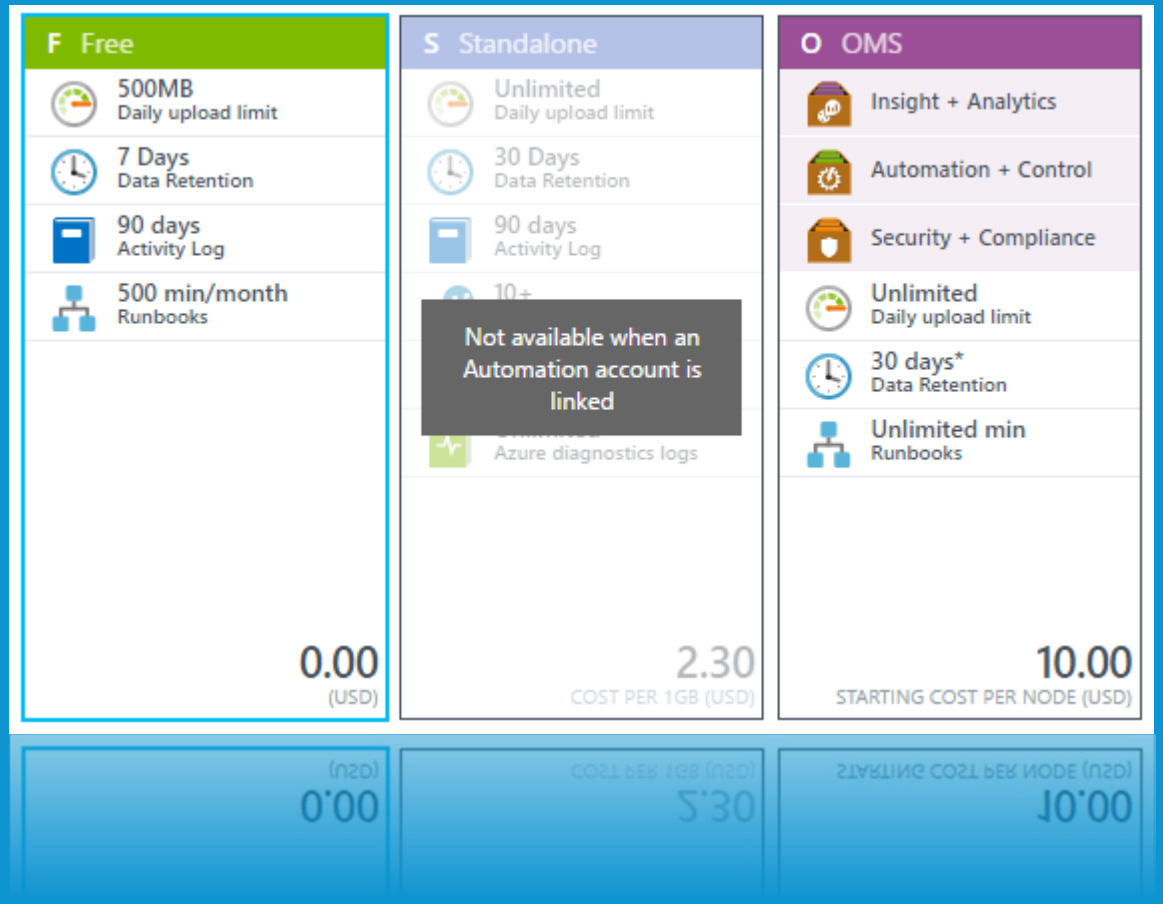
Jakob Knutsson
www.addlevel.se

addlevel

Priser

aka.ms/omscalculator

www.microsoft.com/en-us/cloud-platform/operations-management-suite-pricing



Jakob Knutsson
www.addlevel.se

addlevel

Priser

aka.ms/omscalculator

www.microsoft.com/en-us/cloud-platform/operations-management-suite-pricing

	E2	E1
Insight & Analytics	●	●
Automation & Control	●	●
Security & Compliance	●	
Backup	●	
Site Recovery	●	
System Center: Configuration Manager, Operations Manager, Orchestrator, Data Protection Manager, Virtual Machine Manager, Service Manager	●	●
Estimated Retail Price:	**$35 per node per month***	**$20 per node per month***

Jakob Knutsson
www.addlevel.se

addlevel

Bra länkar

OMS Experience
https://experience.mms.microsoft.com/

OMS Teamet
https://blogs.technet.microsoft.com/msoms/

Dokumentation
https://docs.microsoft.com/sv-se/azure/log-analytics/

https://www.microsoft.com/en-us/cloud-platform/operations-management-suite-resources

Twitter
@kntsn

Jakob Knutsson
www.addlevel.se

addlevel


50k+ kundkonton
20PB sökbar data
188 miljoner queries per vecka
addlevel

Tack!

Frågor?

Jakob Knutsson
www.addlevel.se

addlevel