

Operations Management Suite

SUNET INKUBATOR WORKSHOP

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

Provide out of the box application and workload insights

Hyper-scale machine data analytics platform

Robust hybrid monitoring solution



addlevel

OMS - Hybrid cloud management solution

Analytics & Monitoring



Security & Compliance



Backup & Disaster recovery



Configuration & Automation



Operations Management Suite



Bakgrund



**System Center
Advisor**

**Operational
Insights**

**Operations
Management Suite**



Jan 2012

Maj 2014

Maj 2015

Sept 2016



Gain visibility and control across your hybrid cloud with simplified operations management and security

[Watch the video ▶](#)

[Create a free account ▶](#)



Gain immediate insights across workloads

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

[Learn more about Insight & Analytics >](#)



Enable consistent control and compliance

Deliver continuous IT services and remediate issues quickly at scale.

[Learn more about Automation & Control >](#)



Respond faster to security threats

Identify emerging threats to protect your critical data and workloads.

[Learn more about Security & Compliance >](#)








Ensure availability of apps and data

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

[Learn more about Protection & Recovery >](#)

Onboarding

-  Windows Servers >
-  Linux Servers >
-  Azure Storage >
-  System Center >
-  Windows Telemetry >


Windows Servers
Attach any Windows server or client.

8 WINDOWS COMPUTERS CONNECTED


[Download Windows Agent \(64 bit\)](#) [Download Windows Agent \(32 bit\)](#)

You'll need the Workspace ID and Key to install the agent.


WORKSPACE ID

5df19e71	924a-cc1aae20ec	
----------	-----------------	---

PRIMARY KEY

PqZ3t/akl	y8ccsKJvrLMjYDc	 Regenerate
-----------	-----------------	--

SECONDARY KEY

xGpR7+b	ixWXBRIjDmeSIIt	 Regenerate
---------	-----------------	---

OMS Query Language

filterExpression | command1 | command2 ...

String Literals

Date/Time:

Numbers

Type

Logical Operators

Sort

Wildcards

Top/Limit

Select

Avg

<http://bit.ly/2bKMVFc>

Log search

*

Type=Event

EventLevelName=Error

A blue-tinted photograph of a desk. In the foreground, a silver laptop is open, with its lid propped up. A silver pen lies on the desk in front of the laptop. In the background, there are several sheets of paper and a blurred object, possibly a lamp or another device. The overall scene is dimly lit, creating a professional and focused atmosphere.

DEMO

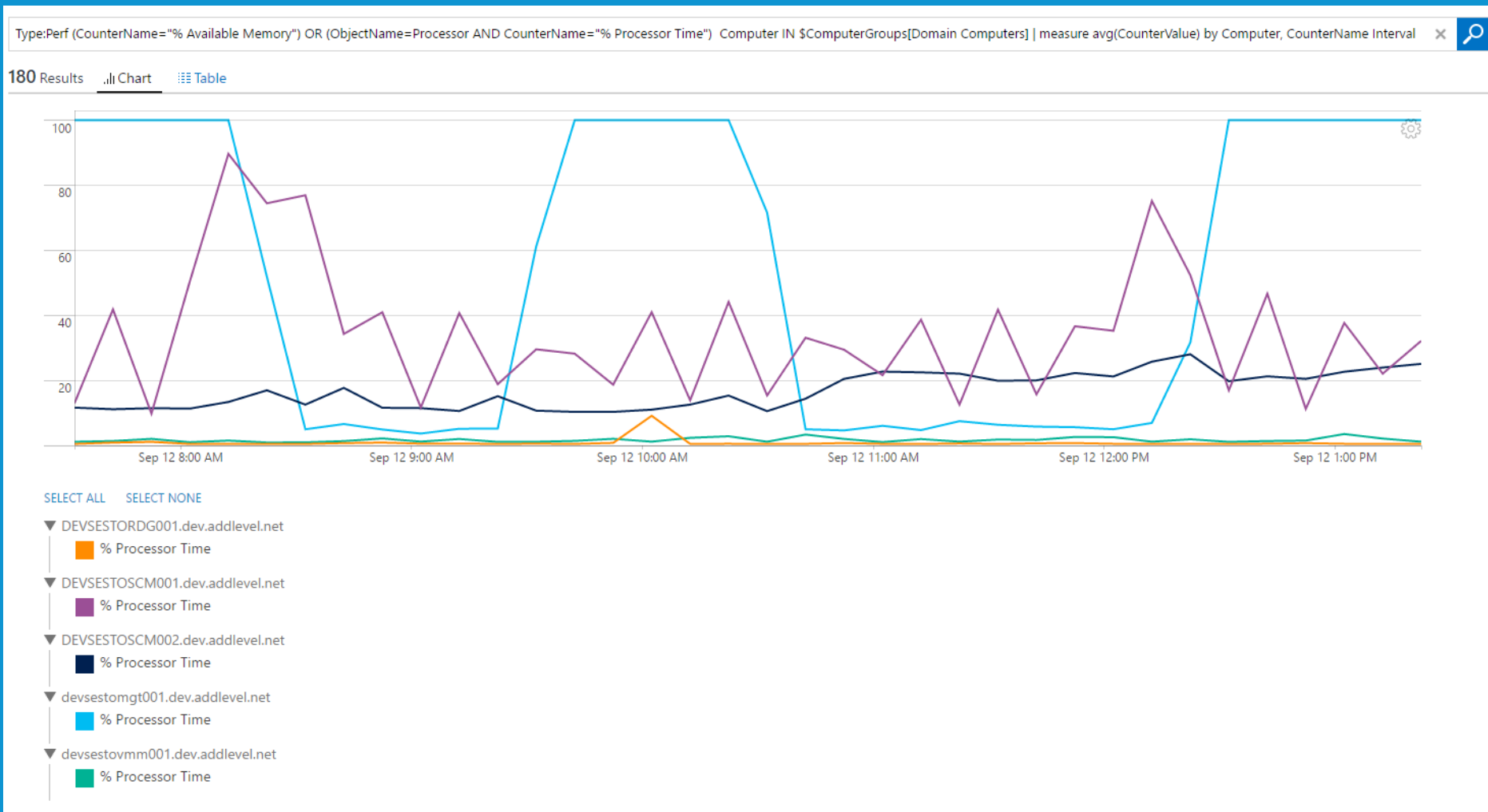
Jakob Knutsson
www.addlevel.se

addlevel

Egna Alerts

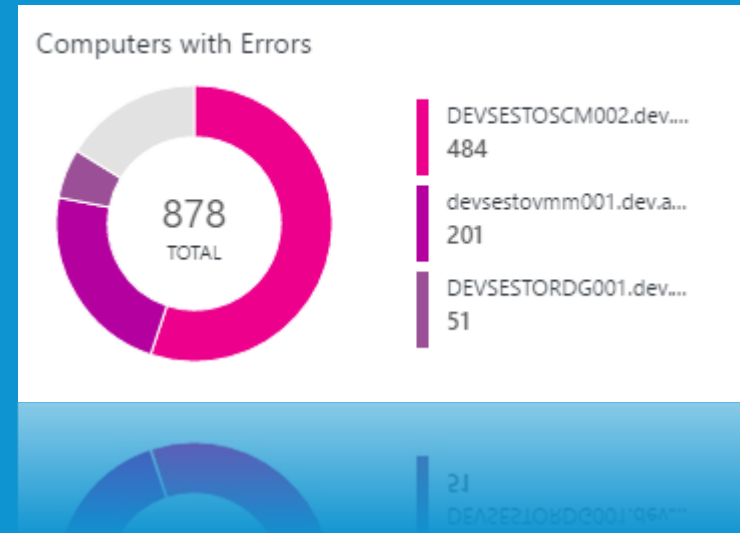
Skapa
Hantera

Performance Counters



Skapa egna Views

Dashboard och View Designer

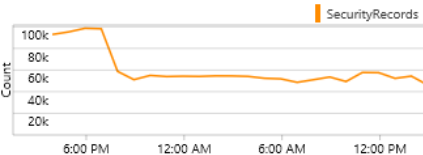


Security and Audit

Overview > Security And Audit

SECURITY DOMAINS

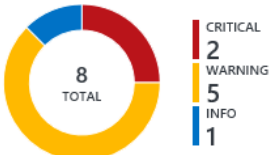
Security records over time



Antimalware Assessment Computers with Antimalware Assessment 42	Update Assessment Computers missing updates 17
Network Security Distinct IP addresses 1.6K	Identity and Access Accounts attempted to log on 3K
Computers Computers with security events 41	Threat Intelligence Malicious traffic events 170
Baseline Assessment Critical failed rules in the last day 59	Azure Security Center

NOTABLE ISSUES

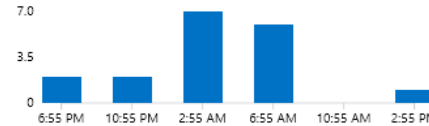
Active issue types



NAME	COUNT	SEVERITY
Computers missing security updates	8	CRITICAL
High priority AD assessment security r...	2	CRITICAL
Computers with insufficient protection	14	WARNING
Computers missing critical updates	6	WARNING
Low priority AD assessment security re...	4	WARNING
Low priority SQL assessment security r...	4	WARNING
Logons with a clear text password	1	WARNING
Accounts failed to log on	3K	INFO

DETECTIONS (PREVIEW)

18 DETECTIONS OVER TIME



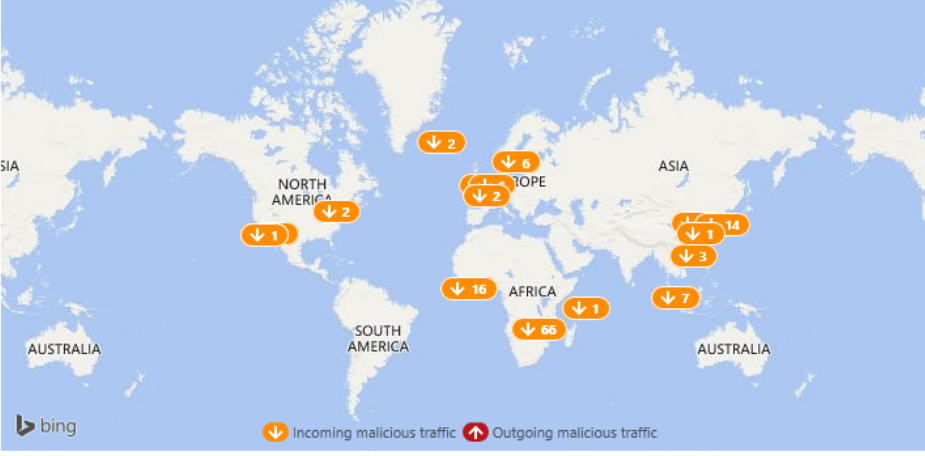
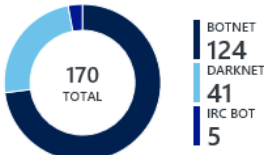
NAME	COUNT	SEVERITY
Failed RDP Brute Force Attack	18	WARNING

THREAT INTELLIGENCE

Servers with outbound malicious traffic

0

Detected threat types



Security and Audit

Type=SecurityEvent

Exempel query (failed logon):


Type=SecurityEvent EventID=4625 | measure count() by TargetAccount




Alert Management

Overview ▶ Alert Management Dashboard

ACTIVE ALERTS


Critical Alerts





19 

ALERT NAME	COUNT
Health Service Heartbeat Failure	6 
Daemon Change Alert	5 
IIS 8 server role is unavailable.	3 

[See all...](#)

Warning Alerts











44 

ALERT NAME	COUNT
Operations Manager Failed to...	36 
MSSQL 2014: DB Average Wait...	6 
IIS Restart is required	1 
SQL 2012 DB Average Wait Tim...	1 

[See all...](#)

Active SCOM Alerts

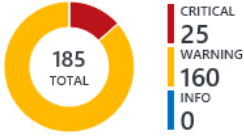
53

SOURCE	COUNT
VMM01.contoso.com	15 
DB03.contoso.com	14 
OM02SQL	6 
DB04.contoso.com	4 
infoweb01.contoso.com	4 
DB05.contoso.com	3 
infoweb02.contoso.com	3 
OpsInsight-RRAS.contoso.com	2 
EXMail01-TS.corp.tailspin.com	1 
MSSQLSERVER	1 











[See all...](#)

ALL ALERTS

Critical Alerts



185 TOTAL
25 CRITICAL
160 WARNING
0 INFO

ALERT NAME	COUNT
Operations Manager Failed to...	130 
MSSQL 2014: DB Average Wait...	19 
Health Service Heartbeat Failure	12 
Daemon Change Alert	5 
IIS Restart is required	4 
Logical disk transfer (reads and...	4 
IIS 8 server role is unavailable.	3 
SQL 2012 DB Average Wait Tim...	2 
System Center Management H...	2 
Advisor failed to import the lat...	1 

[See all...](#)

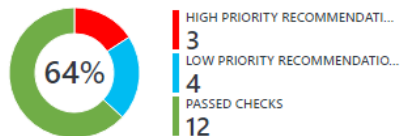
COMMON ALERT QUERIES

- [Critical alerts raised during the past 24 hours
Type=Alert \(AlertSeverity=error or AlertSeverity=critical\) TimeGe...](#)
- [Warning alerts raised during the past 24 hours
Type=Alert AlertSeverity=warning TimeGenerated>NOW-24HOUR](#)
- [Sources with active alerts raised during the past 24 hours
Type=Alert AlertState!=Closed TimeGenerated>NOW-24HOUR \[...](#)
- [Critical alerts raised during the past 24 hours which are still...
Type=Alert \(AlertSeverity=error or AlertSeverity=critical\) TimeGe...](#)
- [Alerts raised during the past 24 hours which are now closed
Type=Alert TimeGenerated>NOW-24HOUR AlertState=Closed](#)
- [Alerts raised during the past 1 day grouped by their severity
Type=Alert TimeGenerated>NOW-1DAY | measure count\(\) as Co...](#)
- [Alerts raised during the past 1 day sorted by their repeat co...
Type=Alert TimeGenerated>NOW-1DAY | sort RepeatCount desc](#)
- [Alerts raised by Nagios Servers
Type=Alert SourceSystem=Nagios](#)
- [Alerts raised by Zabbix Servers
Type=Alert SourceSystem=Zabbix](#)

AD Assessments

Overview ▶ AD Assessment

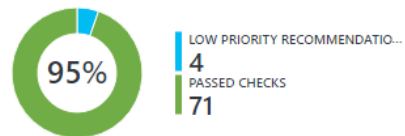
SECURITY AND COMPLIANCE



PRIORITIZED RECOMMENDATIONS	WEIGHT
Ensure that operating system updates are reviewed ...	15.6
Configure your password policy to prohibit blank pa...	9.6
Change your password policy to enforce minimum p...	3.4
Change your password policy to enforce a minimum...	3.4
Change your password policy to enforce password h...	2.2
Change your password policy to enforce a maximum...	2.2

See all...

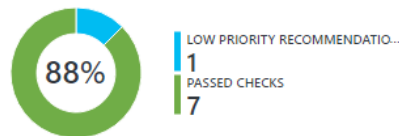
AVAILABILITY AND BUSINESS CONTINUITY



PRIORITIZED RECOMMENDATIONS	WEIGHT
Configure the root PDC emulator to use an authorit...	2.5
Increase free space on system drives.	1.9
Add subnet definitions to Active Directory sites.	1.8

See all...

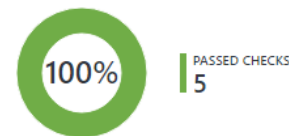
PERFORMANCE AND SCALABILITY



PRIORITIZED RECOMMENDATIONS	WEIGHT
Review processes with large working set sizes.	0.3

See all...

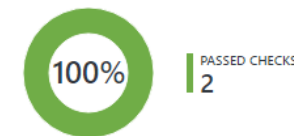
UPGRADE, MIGRATION AND DEPLOYMENT



PRIORITIZED RECOMMENDATIONS	WEIGHT
Congratulations. Looking great!	

See all...

OPERATIONS AND MONITORING

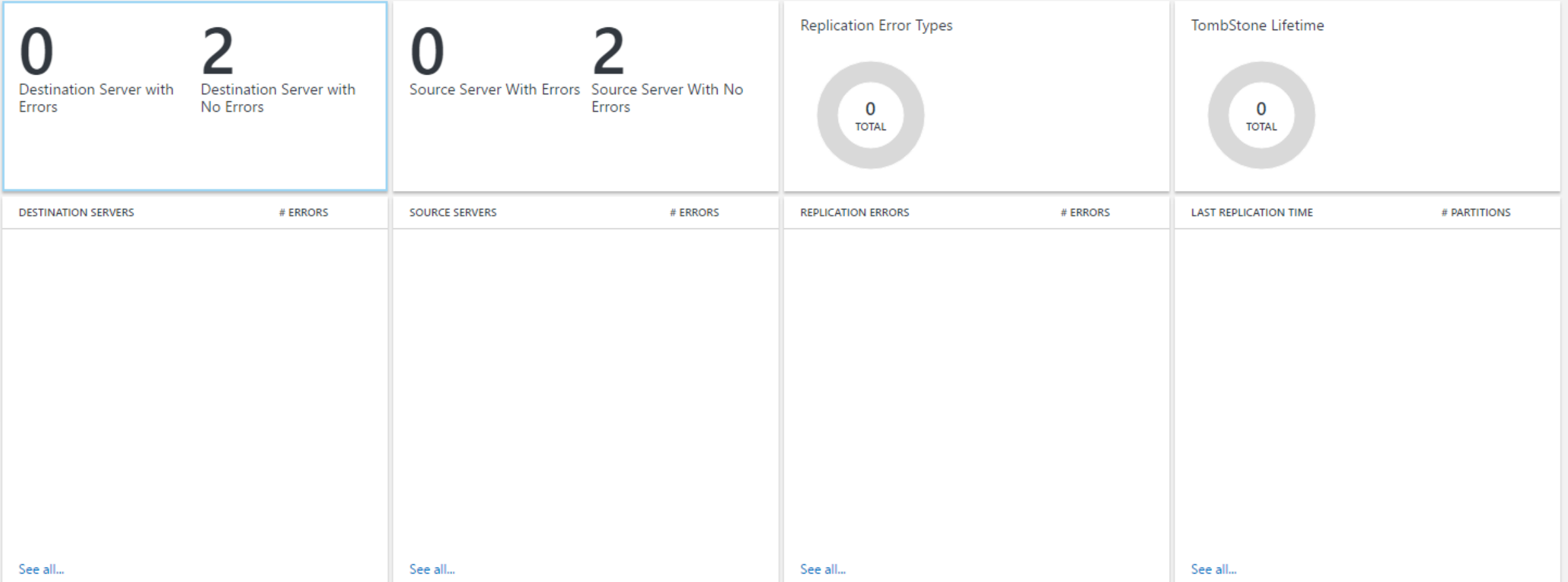


PRIORITIZED RECOMMENDATIONS	WEIGHT
Congratulations. Looking great!	

See all...

AD Replication Status

Overview ▶ AD Replication Status



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

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.

System Update

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

Type=Update

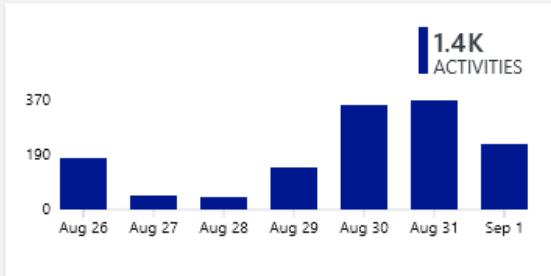
Insamlingsmetoderna:

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

Office 365

Overview ▶ Office 365

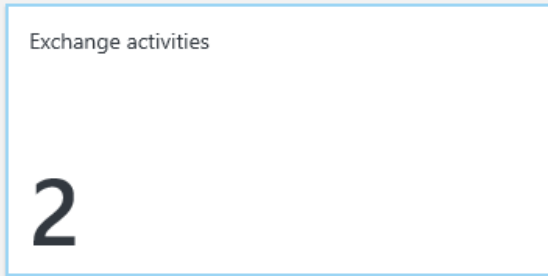
OPERATIONS



OPERATION	COUNT
admin@addlevel.se	331
jan@addlevel.se	194
admin@addlevel.se	192
jan@addlevel.se	162
admin@addlevel.se	113
jan@addlevel.se	78
jan@addlevel.se	68
jan@addlevel.se	64
jan@addlevel.se	46
jan@addlevel.se	43

[See all...](#)

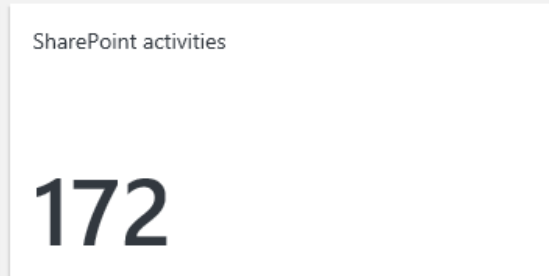
EXCHANGE



ACTIVITY	COUNT
Set-UnifiedGroup	2

[See all...](#)

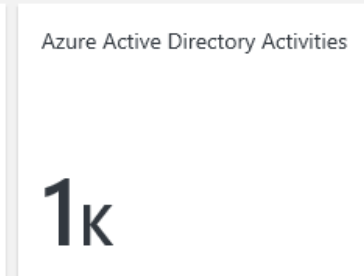
SHAREPOINT



ACTIVITY	COUNT
FileAccessed	130
FileModified	11
FilePreviewed	7
FileCheckedIn	6
FileCheckedOut	5
FileUploaded	5
AddedToGroup	3
GroupAdded	3
FileDeleted	1
FileDownloaded	1

[See all...](#)

AZURE ACTIVE DIRECTORY



ACTIVITY
PasswordLogonInitialAuthUsin...
UserLoggedIn
UserLoginFailed
Update group.
Add member to group.
Update user.
Add group.
Add owner to group.
Update service principal.

[See all...](#)

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>

Windows Telemetry

Enable telemetry to allow user devices to share information with Microsoft. Devices with the Customer Experience Improvement Program disabled can still share information.

[How to enable telemetry](#)

Deploy your unique commercial ID key to user devices so that Microsoft can identify your organization's information, and then subscribe to the solutions you want to use. Click or tap the copy button to copy the commercial ID key to the clipboard.

COMMERCIAL ID KEY

b089ca40-ae8c-4236-a595-10755c55d1



Regenerate

Solution

Upgrade Analytics
(Preview)

Subscribe

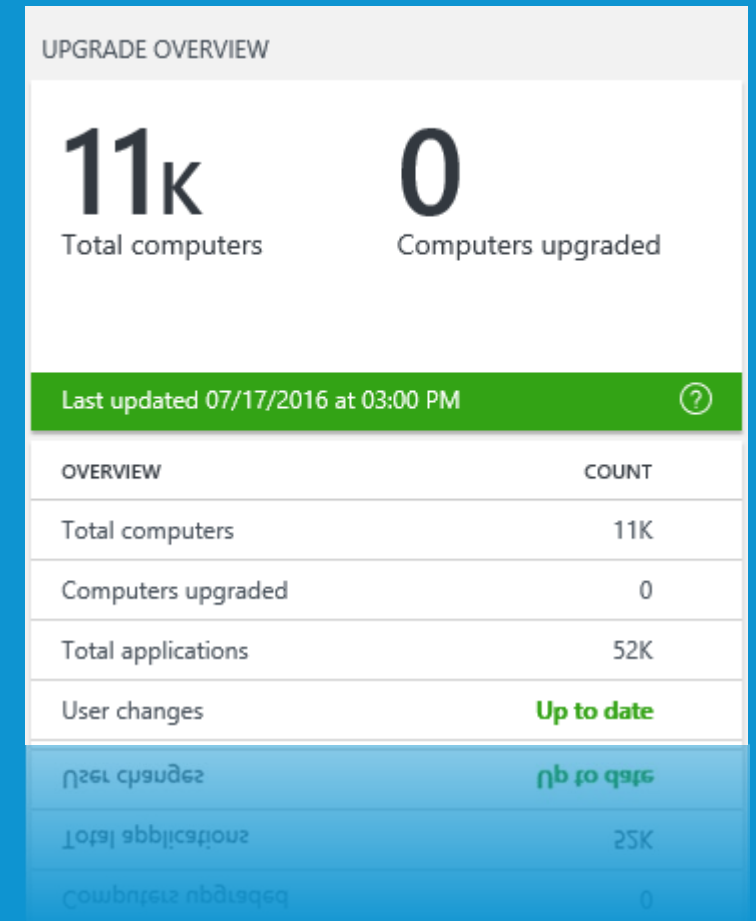
(Preview)
Upgrade Analytics
solution

Subscribe

Upgrade Analytics

Data

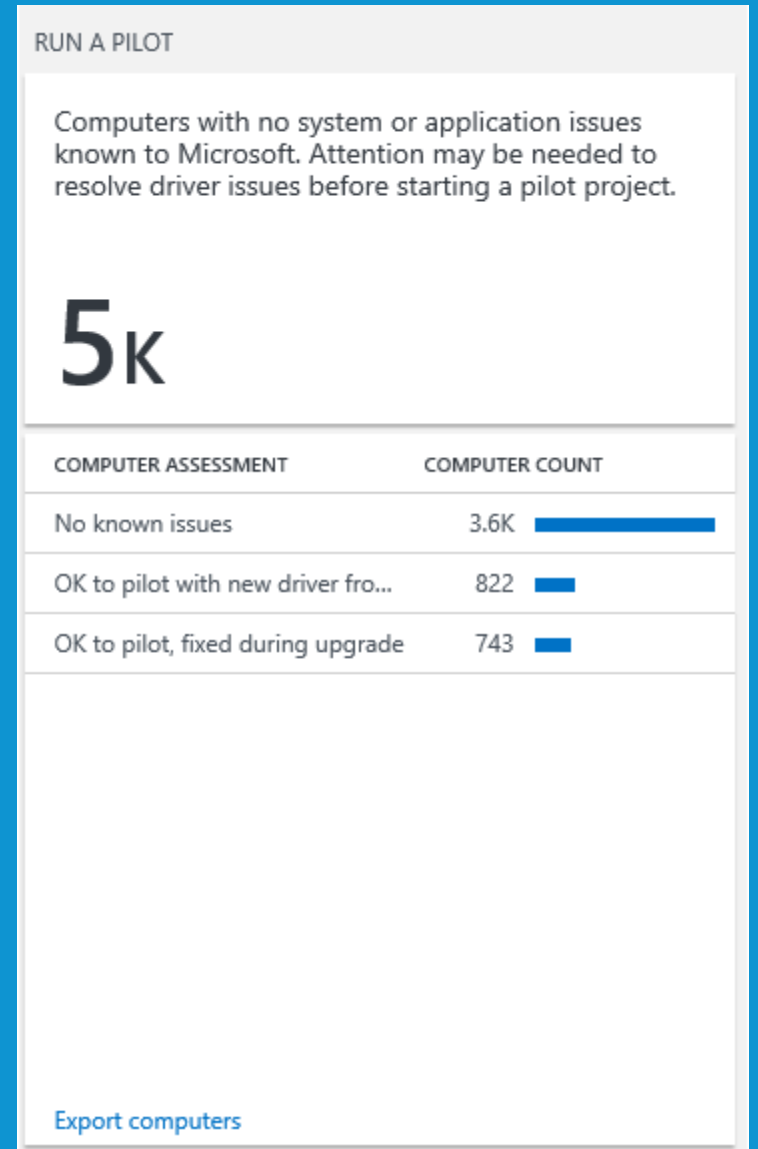
- Computer ID and computer name
- Computer manufacturer
- Computer model
- Operating system version and build
- Count of system requirement, application, and driver issues per computer
- Upgrade assessment based on analysis of computer telemetry data
- Upgrade decision status



Upgrade Analytics

Applikationer

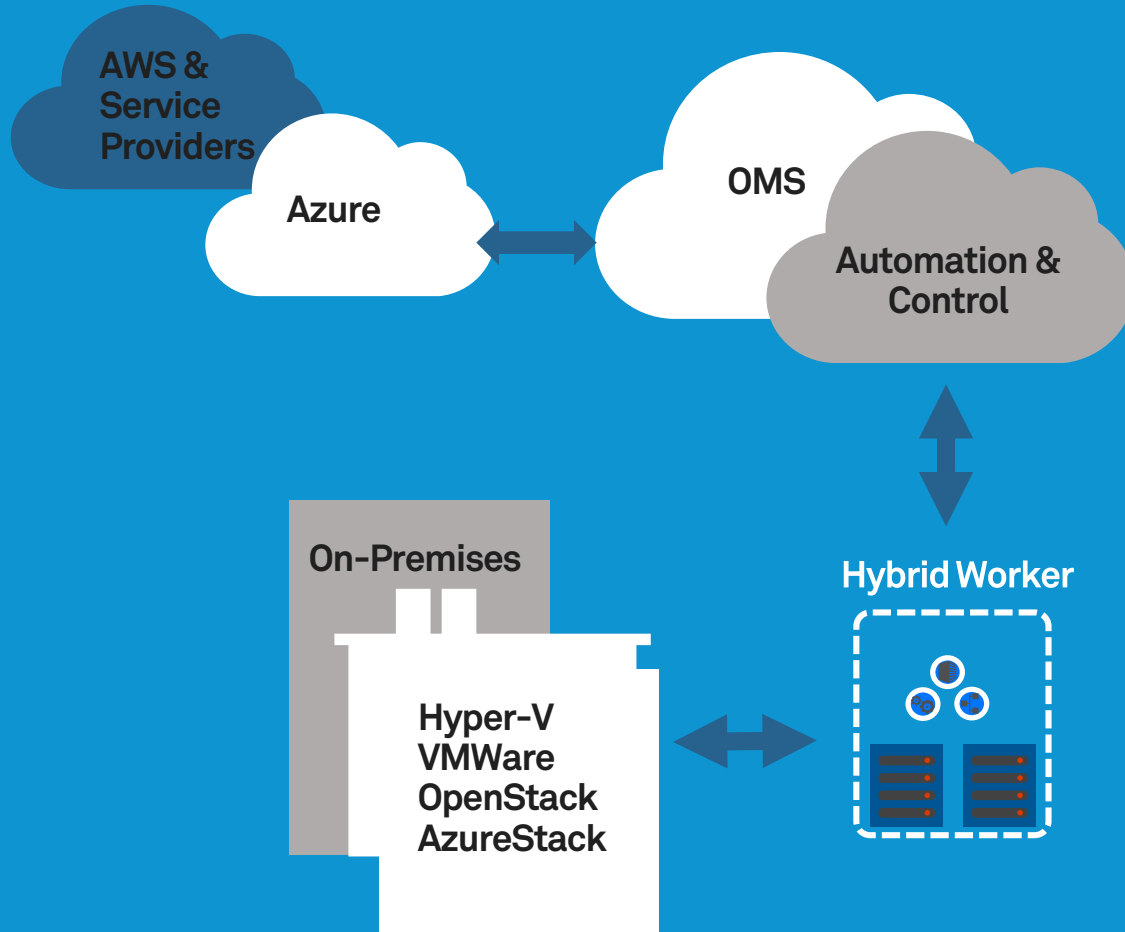
- Application vendor
- Application version
- Count of computers the application is installed on
- Count of computers that opened the application at least once in the past 30 days
- Percentage of computers in your total computer inventory that opened the application in the past 30 days
- Issues detected,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



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.

Automation & Control



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

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



När en applikation går ner, finns det alltid någon som har en värre dag på jobbet.

Service Map

Tidigare kallad Application Dependency Monitor

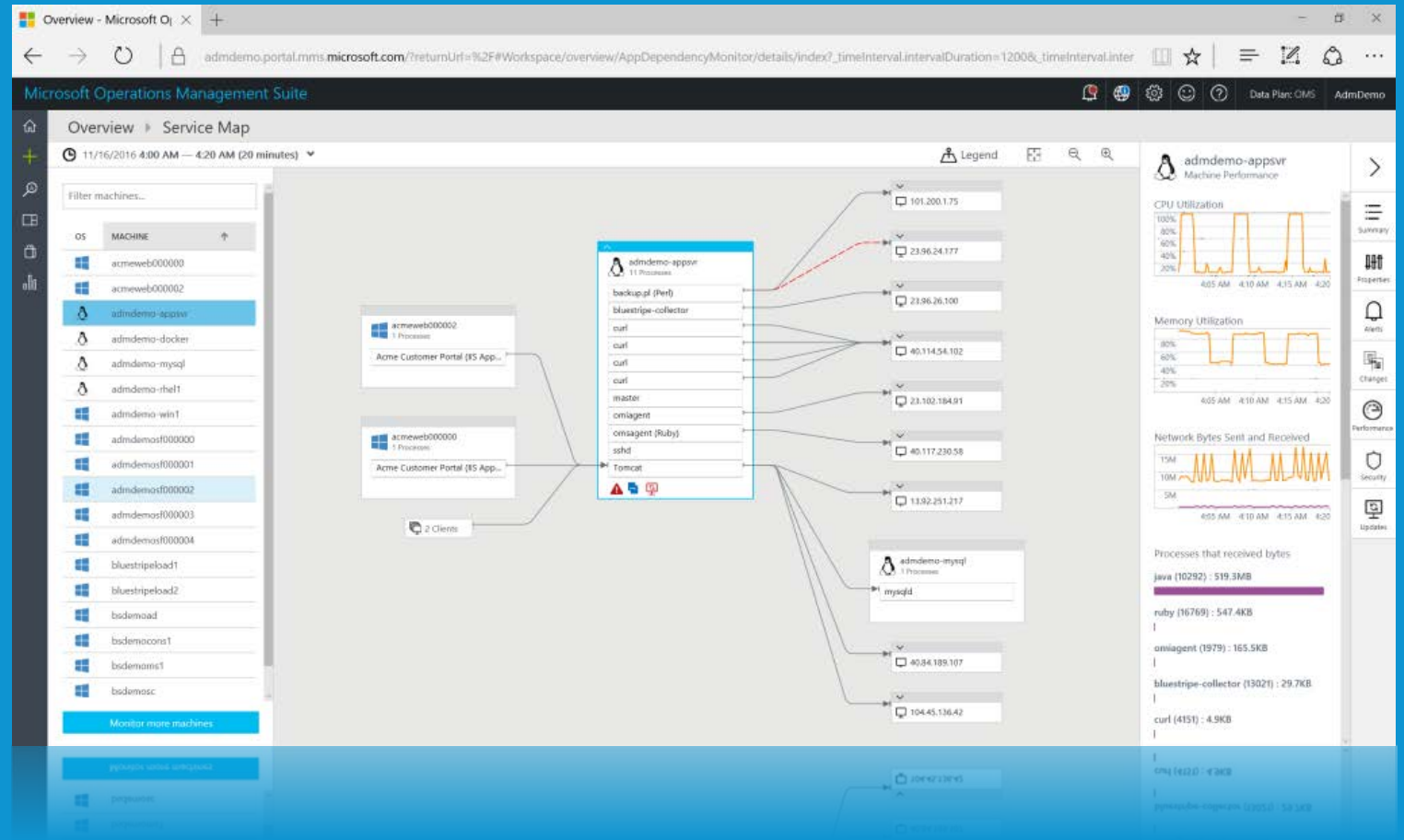
Bygger på FactFinder från BlueStripe

Automatically discover all dependencies for any Windows or Linux system

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

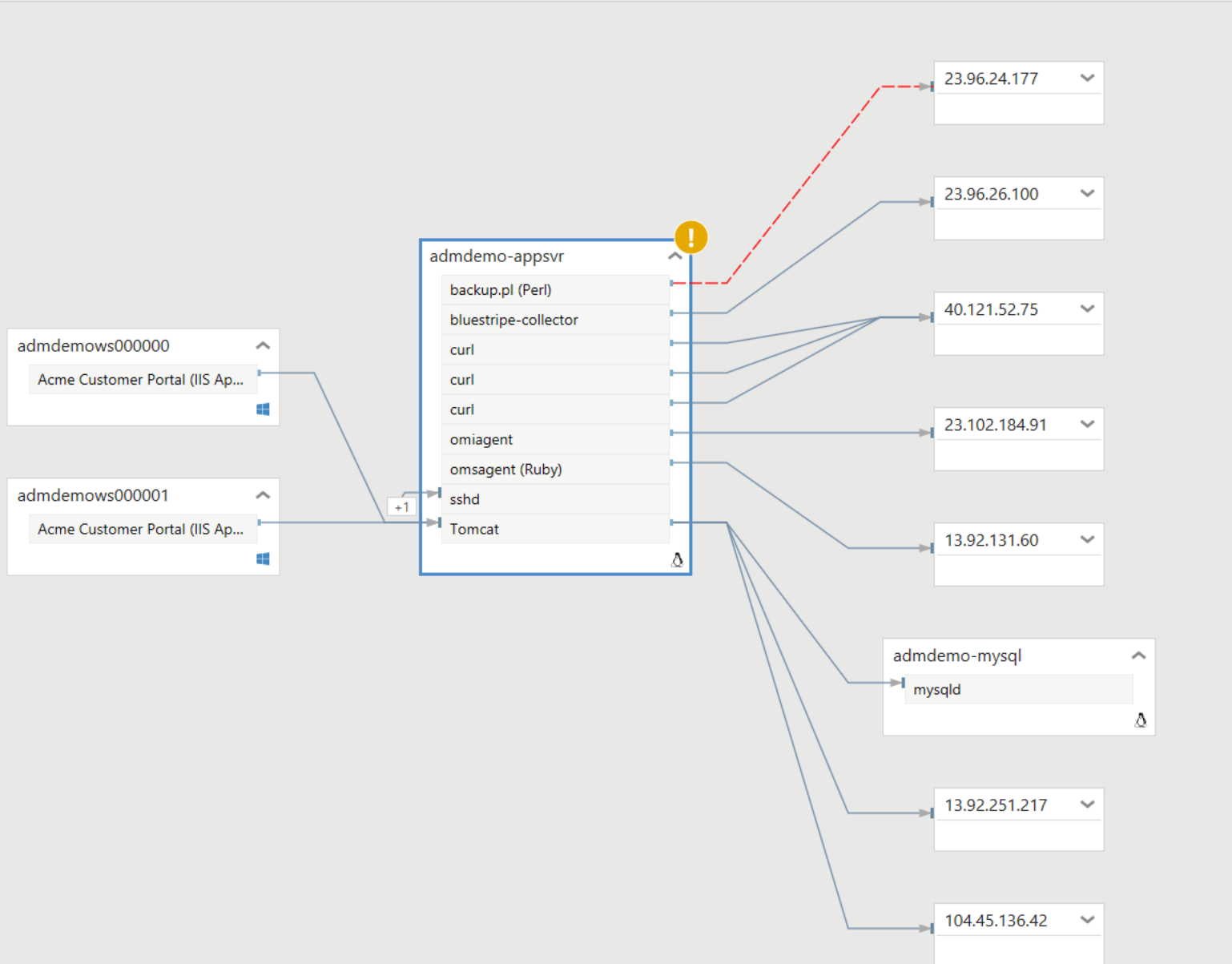
View dynamic maps of your system topology, live and historical

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



Overview Application Dependency Monitor

- 9/20/2016 1:54 PM — 2:04 PM (10 minutes)
- OS MACHINE
- admdemos000000
 - admdemos000001
 - admdemosf000003
 - admdemosf000001
 - admdemosf000004
 - bsdemosql1
 - admdemos000000
 - bsdemoad
 - bsdemocons1
 - bsdemos1
 - bsdemosc
 - admdemosf000002
 - bluestripeload2
 - bluestripeload1
 - admdemo-mysql
 - admdemo-appsvr**
 - admdemo-docker



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

[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

admdemo-appsvr

PROCESSES

- acmeproc
- backup.pl (Perl)
- bluestripe-collector
- curl
- curl
- omiagent
- omsagent (Ruby)
- Tomcat



101.200.1.75 ▾

23.96.24.177 ▾

23.96.26.100 ▾

40.76.39.235 ▾

104.215.96.105 ▾

40.114.4.4 ▾

13.92.251.217 ▾

40.84.189.107 ▾

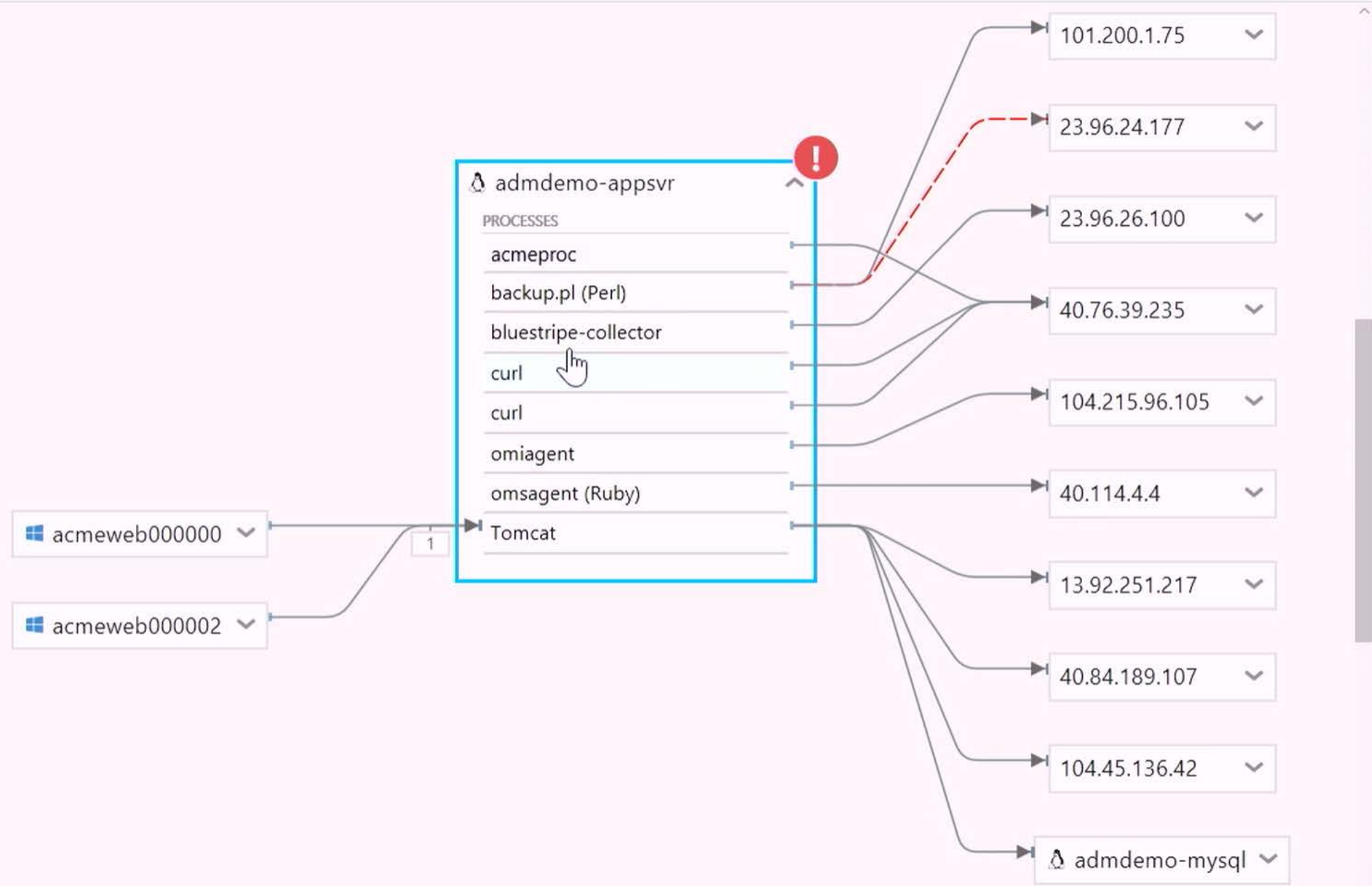
104.45.136.42 ▾

admdemo-mysql ▾

acmeweb000000 ▾

acmeweb000002 ▾

1



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

Konkurrenter

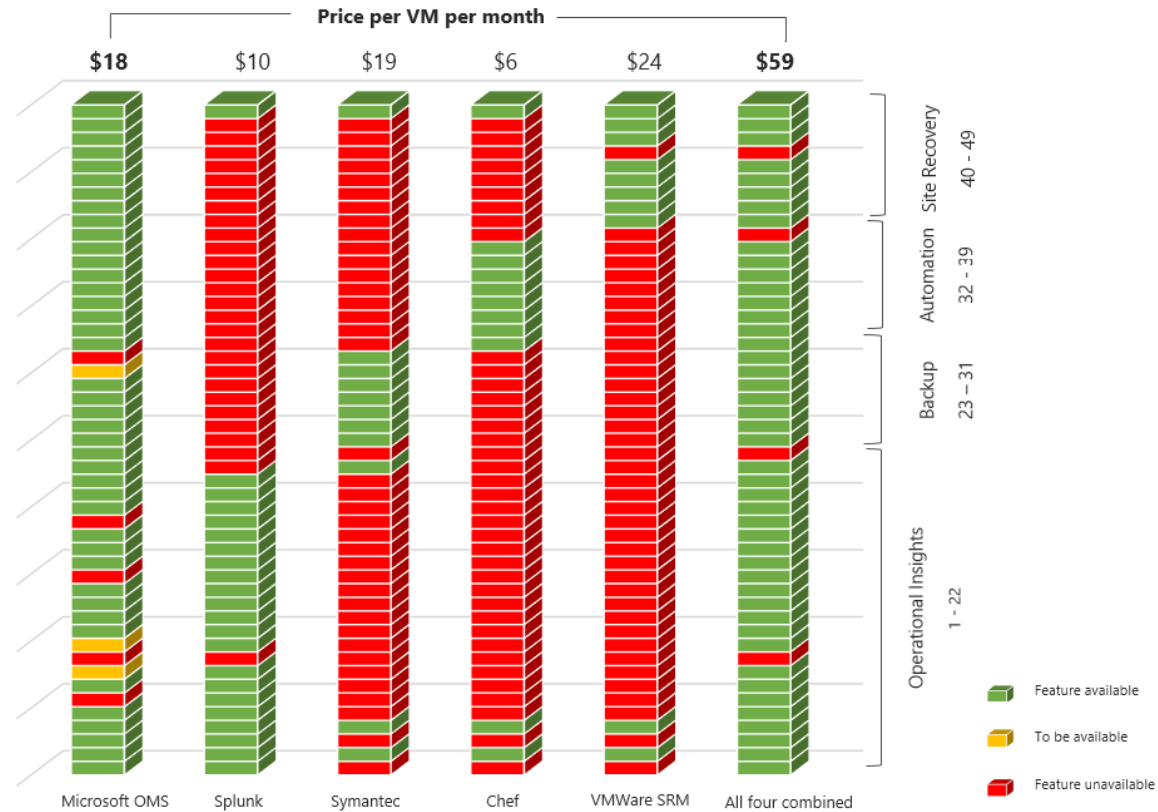
Splunk

Elastic Search + Kibana

Traditionella övervakningsverktyg

Konkurrenter

OMS Compete



Comparison as of Sept 2015. Microsoft OMS pricing reflects promo offer until 12/31/2015
 Analysis for customer with 300 VMs with <50 GB data / VM generating 130 MB log data / VM / day



- Site Recovery**
- 40 - Support for Heterogeneous Platforms (Hyper-V, VMware and Physical)
 - 41 - Recover to Public and Hosted Clouds
 - 42 - Continuous health monitoring
 - 43 - Automated protection
 - 44 - Orchestrated recovery (prioritized recovery)
 - 45 - No-impact recovery plan testing
 - 46 - Consistent experience across private, hosted and public clouds
 - 47 - Planned migration
 - 48 - Support for array-based replication
 - 49 - Recover historical recovery points

- Automation**
- 32 - Graphical and PowerShell authoring
 - 33 - Desired State Configuration
 - 34 - Orchestration engine
 - 35 - Versioning support
 - 36 - Role based access
 - 37 - Web based administration
 - 38 - Source control integration
 - 39 - Reporting and analytics

- Backup**
- 23 - Backup on Private, Hybrid or Cloud environments
 - 24 - Cloud service built on top of backup
 - 25 - Network throttling
 - 26 - Incremental backups
 - 27 - Data compression
 - 28 - Data encryption
 - 29 - Offline seeding
 - 30 - Central monitoring and reporting
 - 31 - Bare metal restore

- Operational Insights**
- 1 - Data Onboarding
 - 2 - Universal Indexing
 - 3 - Search
 - 4 - Distributed Search
 - 5 - Monitoring and Alerting
 - 6 - Reporting
 - 7 - Knowledge Mapping
 - 8 - Dashboards
 - 9 - Data Model
 - 10 - Pivot
 - 11 - Event Pattern Detection
 - 12 - High Performance Analytics Store
 - 13 - Report Acceleration
 - 14 - Embedded Reports
 - 15 - PDF Delivery
 - 16 - Access Control & Single Sign-On
 - 17 - Universal Forwarder
 - 18 - Forwarder Management
 - 19 - Apps
 - 20 - Overview tiles
 - 21 - Intelligence Solutions
 - 22 - Automation integration

Priser

aka.ms/omscalculator

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

F Free	S Standalone	O OMS
500MB Daily upload limit	Unlimited Daily upload limit	Insight + Analytics
7 Days Data Retention	30 Days Data Retention	Automation + Control
90 days Activity Log	90 days Activity Log	Security + Compliance
500 min/month Runbooks	10+ Runbooks	Unlimited Daily upload limit
	<div style="background-color: #333; color: white; padding: 5px; text-align: center;">Not available when an Automation account is linked</div>	30 days* Data Retention
	Azure diagnostics logs	Unlimited min Runbooks
0.00 (USD)	2.30 COST PER 1GB (USD)	10.00 STARTING COST PER NODE (USD)

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

	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*
Estimated Retail Price:	232 per node per month*	250 per node per month*
Managed Service Manager		

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

An iceberg floating in a dark blue sea under a cloudy sky. The visible tip of the iceberg is small, while the much larger submerged part is visible below the water line, illustrating the concept of hidden data.

50k+ kundkonton

20PB sökbar data

188 miljoner queries per vecka

addlevel

Tack!

Frågor?

Jakob Knutsson
www.addlevel.se

addlevel