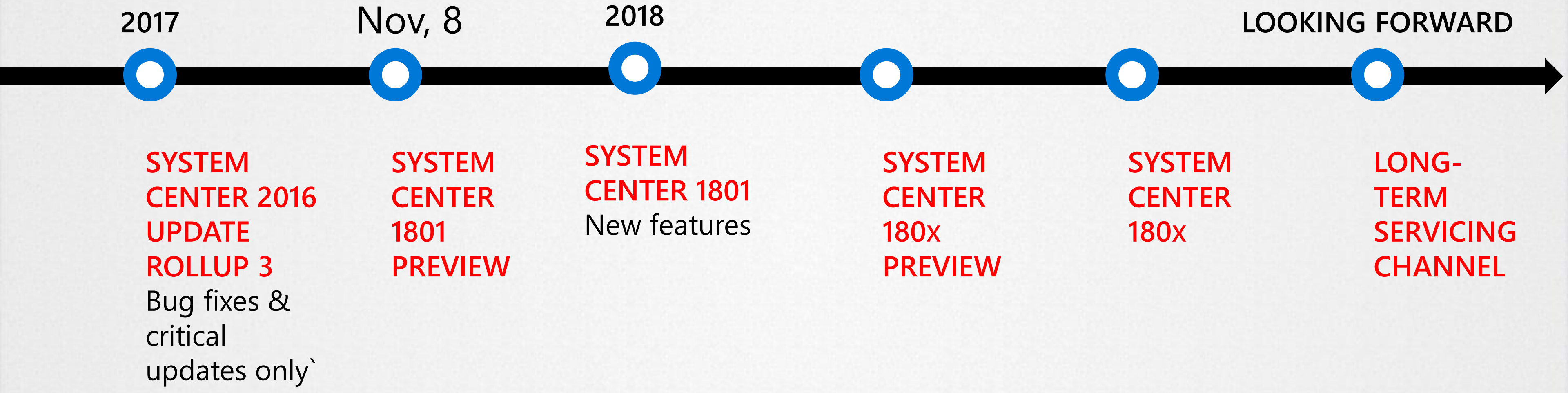
Best of Ignite 2017

Monitoring / Security / Management

Stefan Roth
Senior Systems Engineer
Microsoft MVP Cloud & Datacenter
@stefanroth_net
www.stefanroth.net

Experts Live Café

System Center Release Cadence



2017

SYSTEM CENTER 2016 UPDATE ROLLUP 3
Bug fixes & critical updates only`

Nov, 8

SYSTEM CENTER 1801 PREVIEW

2018

SYSTEM CENTER 1801
New features

SYSTEM CENTER 180x PREVIEW

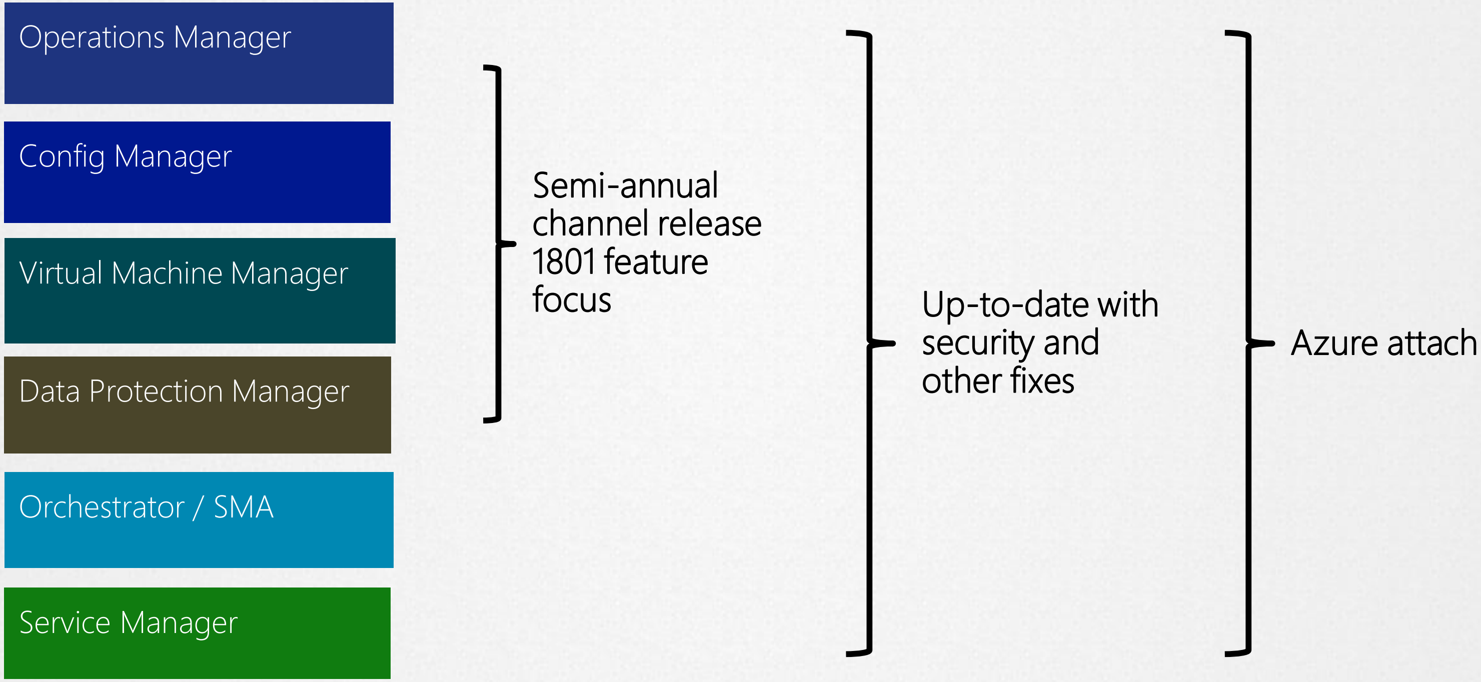
SYSTEM CENTER 180x

LOOKING FORWARD

LONG-TERM SERVICING CHANNEL

- Introducing semi-annual feature release cadence this fiscal year
- Semester planning
- Aligned with WS releases
- Access to semi-annual channel will require active Software Assurance

System Center 1801 Coverage



Operations Manager

Config Manager

Virtual Machine Manager

Data Protection Manager

Orchestrator / SMA

Service Manager

Semi-annual channel release 1801 feature focus

Up-to-date with security and other fixes

Azure attach

Investment Areas

Enhanced heterogeneity support

- Enhanced Windows Server, Linux and VMWare support

Focus on Fundamentals

- Improved user experience, performance, reliability and efficiency

Better with Azure

- SC attach to Azure management

EXPERTS LIVE
CAFÉ

System Center 1801

SCOM

- HTML 5 web console (finally no Silverlight, Edge/Firefox/Chrome support)
- New widgets
- Linux log file monitoring leveraging Fluentd
- MP updates and recommendations for 3rd party MPs
- Service Map integration MP
- VSAE 2017 support
- Improved UI responsiveness

SCCM

- Site Server high availability
- PXE network boot support for IPv6
- Server groups (cluster patching)

SCSM

- ITSM Connector Azure alerts action, create incidents

Orchestrator / SMA

- Migration Toolkit
- Not SMA = > Use Azure Automation ☺ Python Support

Integrating SCSM with Azure – ITSM Connector

Create incidents in SM automatically

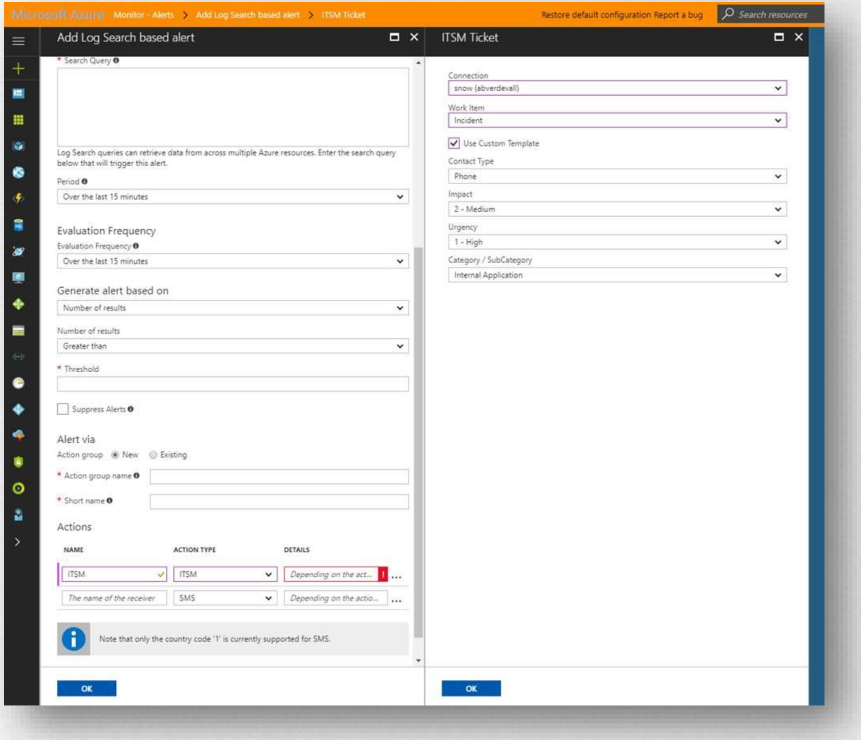
- Based on Alerts on Azure or on-prem resources

Resolve incidents faster

- Correlate relevant log data w/incidents
- Visualize related incidents in Service Map

Public preview

- SCSM
- ServiceNow
- Provance
- Cherwell


Microsoft Azure
Monitor - Alerts > Add Log Search based alert > ITSM Ticket
Restore default configuration
Report a bug
Search resources
OK
OK

Add Log Search based alert

* Search Query

Log Search queries can retrieve data from across multiple Azure resources. Enter the search query below that will trigger this alert.

Period: Over the last 15 minutes

Evaluation Frequency

Evaluation Frequency: Over the last 15 minutes

Generate alert based on: Number of results

Number of results: Greater than

* Threshold

□ Suppress Alerts

Alert via

Action group ● New ○ Existing

* Action group name

* Short name

Actions

NAME	ACTION TYPE	DETAILS
ITSM ✓	ITSM	Depending on the act... !
The name of the receiver	SMS	Depending on the actio...

Note that only the country code '1' is currently supported for SMS.

ITSM Ticket

Connection: snow (abverdevall)

Work Item: Incident

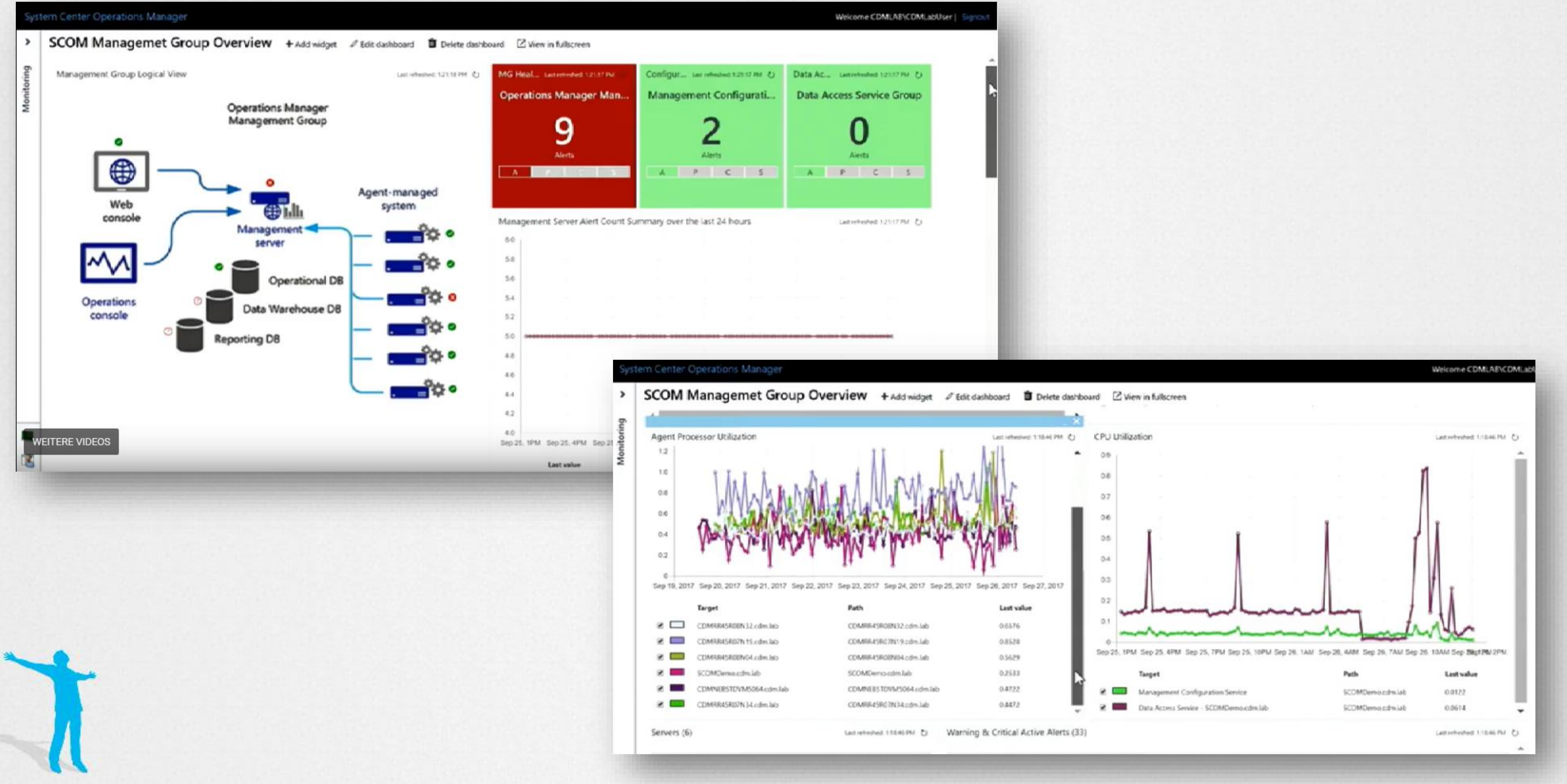
☑ Use Custom Template

Contact Type: Phone

Impact: 2 - Medium

Urgency: 1 - High

Category / SubCategory: Internal Application



System Center Operations Manager

Welcome CDMLAB\CDMLabUser | Signout

SCOM Managemet Group Overview

+ Add widget
Edit dashboard
Delete dashboard
View in fullscreen
Monitoring
Management Group Logical View
Last refreshed: 1:21:18 PM
Operations Manager Management Group
Web console
Operations console
Management server
Agent-managed system
Operational DB
Data Warehouse DB
Reporting DB
MG Heal... Last refreshed: 1:21:17 PM
Operations Manager Man...
9
Alerts
Configur... Last refreshed: 1:21:17 PM
Management Configurati...
2
Alerts
Data Ac... Last refreshed: 1:21:17 PM
Data Access Service Group
0
Alerts
A P C S
Management Server Alert Count Summary over the last 24 hours
6.0 5.8 5.6 5.4 5.2 5.0 4.8 4.6 4.4 4.2 4.0
Sep 25, 1PM Sep 25, 4PM
Last value
WEITERE VIDEOS
Agent Processor Utilization
Last refreshed: 1:18:46 PM
1.2 1.0 0.8 0.6 0.4 0.2 0
Sep 19, 2017 Sep 20, 2017 Sep 21, 2017 Sep 22, 2017 Sep 23, 2017 Sep 24, 2017 Sep 25, 2017 Sep 26, 2017 Sep 27, 2017
CPU Utilization
Last refreshed: 1:18:46 PM
0.9 0.8 0.7 0.6 0.5 0.4 0.3 0.2 0.1 0
Sep 25, 1PM Sep 25, 4PM Sep 25, 7PM Sep 25, 10PM Sep 26, 1AM Sep 26, 4AM Sep 26, 7AM Sep 26, 10AM Sep 26, 1PM 2PM

		Target	Path	Last value
☑	□	CDMRR45R08N32.cdm.lab	CDMRR45R08N32.cdm.lab	0.6576
☑	🟪	CDMRR45R07N19.cdm.lab	CDMRR45R07N19.cdm.lab	0.8528
☑	🟩	CDMRR45R08N04.cdm.lab	CDMRR45R08N04.cdm.lab	0.5629
☑	🟥	SCOMDemo.cdm.lab	SCOMDemo.cdm.lab	0.2533
☑	🟪	CDMNEBSTDVM5064.cdm.lab	CDMNEBSTDVM5064.cdm.lab	0.4722
☑	🟩	CDMRR45R07N34.cdm.lab	CDMRR45R07N34.cdm.lab	0.4472

		Target	Path	Last value
☑	🟩	Management Configuration Service	SCOMDemo.cdm.lab	0.0122
☑	🟪	Data Access Service - SCOMDemo.cdm.lab	SCOMDemo.cdm.lab	0.0614

Servers (6) Last refreshed: 1:18:46 PM

Warning & Critical Active Alerts (33) Last refreshed: 1:18:46 PM

EXPERTS LIVE
CAFÉ

VMM Summary

Enhanced Windows Server 2016 support

- Nested virtualization
- Migrate VMware UEFI VM to Hyper-V
- Configure SLB via Service Templates
- SLB Guest cluster floating IP support
- Storage QOS configured in VM template
- Storage QOS at VMM Cloud
- Storage QOS extended to SAN storage
- Remote to VMs in Enhanced Session mode
  - Copy / paste into VM via console session
- Seamless Update of non-domain host agent

Windows Server v1709 & Linux support

- Manage WS v1709 host at par with WS 2016
- Configure Encrypted SDN virtual network
- Manage Shielded Linux VMs on Hyper-V
- Support for fallback HGS for shielded VM
- VMM better together with in-box tools

Fundamentals

- Host Refresher up to 10X faster
- VMWare Migrate 50% faster

Better with Azure

- More Azure regions
- Azure AD support (add-in)
- Azure ARM VM Mgmt,
- VMM Analytics (OMS)

EXPERTS LIVE
CAFÉ

DPM Summary

Backup Windows and VMware efficiently

- Backup WS v1709 at par with WS 2016
- Store VMware backups efficiently using MBS

Fundamentals

- Upgrade with ease – No Production Server reboot

Better with Azure

- Generate custom reports using Power BI
- Recover files/folders of cloud recovery point in matter of minutes

SQL Server 2017

SQL Server 2017 GA

Docker

Linux

(Drawbridge)

Windows

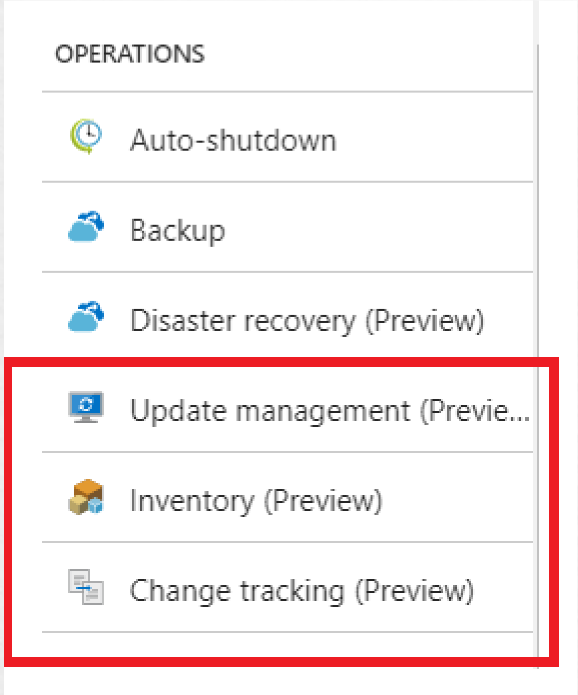
AI built-in, with R and Python analytics

Power BI Report Server

Run Power BI reports on-premises

Fully compatible with SSRS

Azure Monitoring

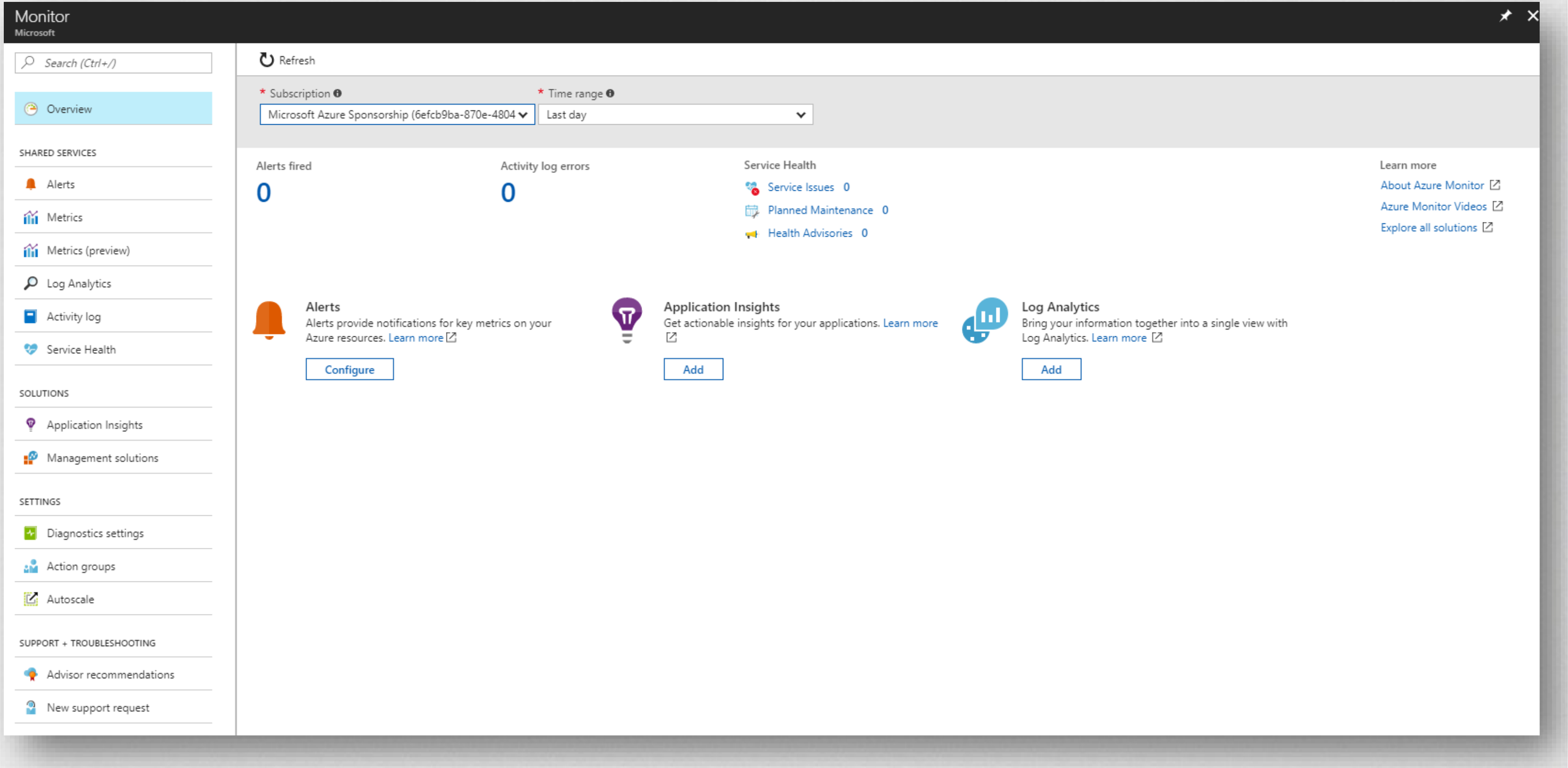


OPERATIONS

- Auto-shutdown
- Backup
- Disaster recovery (Preview)
- Update management (Previe...
- Inventory (Preview)
- Change tracking (Preview)

- New Operation Leaf in the Azure VM node
- Update Management solution is FREE
- Change Tracking solution for Azure resources is FREE
- Azure Log Analytics Container monitoring solution
  - Integration for Linux and Windows Kubernetes support
- Log Analytics Query Language cross workspace query (!)
- Azure Monitor facelift

EXPERTS LIVE
CAFÉ



* Subscription: Microsoft Azure Sponsorship (6efcb9ba-870e-4804

* Time range: Last day

Alerts fired: 0

Activity log errors: 0

Service Health
- Service Issues 0
- Planned Maintenance 0
- Health Advisories 0

Learn more
- About Azure Monitor
- Azure Monitor Videos
- Explore all solutions

Alerts
Alerts provide notifications for key metrics on your Azure resources. Learn more

Configure

Application Insights
Get actionable insights for your applications. Learn more

Add

Log Analytics
Bring your information together into a single view with Log Analytics. Learn more

Add

Azure Policy (Preview)

Azure Policy Center

IT governance

Management Group

Subscription

Resource group

Enforce rules & actions

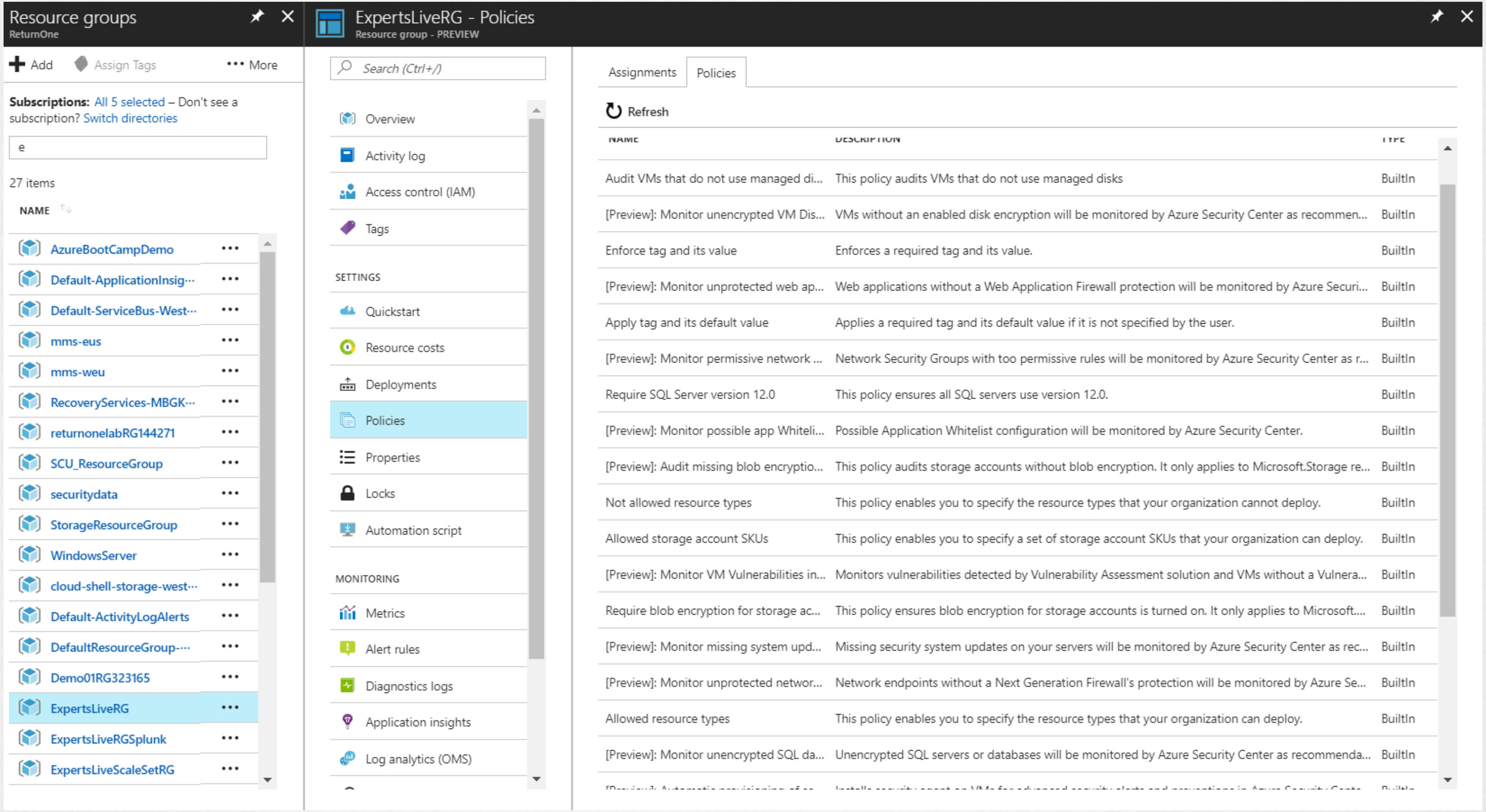
Built-in & custom

Naming conventions

Tags required

Require blob storage account encryption

EXPERTS LIVE
CAFÉ



Subscriptions: All 5 selected – Don't see a subscription? Switch directories

e

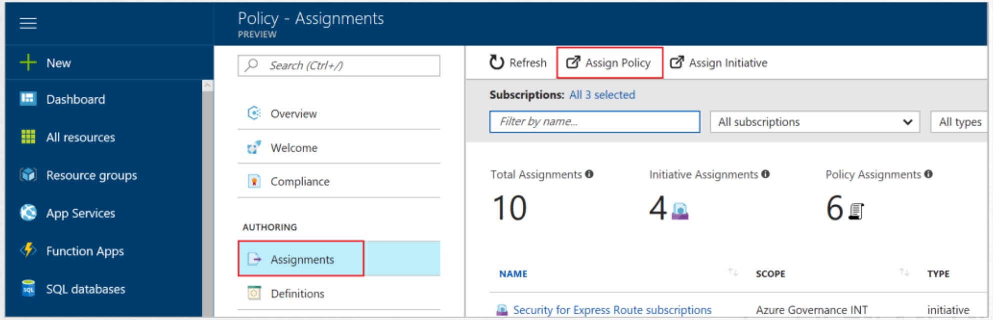
27 items

NAME

- AzureBootCampDemo
- Default-ApplicationInsig···
- Default-ServiceBus-West···
- mms-eus
- mms-weu
- RecoveryServices-MBGK···
- returnonelabRG144271
- SCU_ResourceGroup
- securitydata
- StorageResourceGroup
- WindowsServer
- cloud-shell-storage-west···
- Default-ActivityLogAlerts
- DefaultResourceGroup-···
- Demo01RG323165
- ExpertsLiveRG
- ExpertsLiveRGSplunk
- ExpertsLiveScaleSetRG

NAME	DESCRIPTION	TYPE
Audit VMs that do not use managed di...	This policy audits VMs that do not use managed disks	BuiltIn
[Preview]: Monitor unencrypted VM Dis...	VMs without an enabled disk encryption will be monitored by Azure Security Center as recommen...	BuiltIn
Enforce tag and its value	Enforces a required tag and its value.	BuiltIn
[Preview]: Monitor unprotected web ap...	Web applications without a Web Application Firewall protection will be monitored by Azure Securi...	BuiltIn
Apply tag and its default value	Applies a required tag and its default value if it is not specified by the user.	BuiltIn
[Preview]: Monitor permissive network ...	Network Security Groups with too permissive rules will be monitored by Azure Security Center as r...	BuiltIn
Require SQL Server version 12.0	This policy ensures all SQL servers use version 12.0.	BuiltIn
[Preview]: Monitor possible app Whiteli...	Possible Application Whitelist configuration will be monitored by Azure Security Center.	BuiltIn
[Preview]: Audit missing blob encryptio...	This policy audits storage accounts without blob encryption. It only applies to Microsoft.Storage re...	BuiltIn
Not allowed resource types	This policy enables you to specify the resource types that your organization cannot deploy.	BuiltIn
Allowed storage account SKUs	This policy enables you to specify a set of storage account SKUs that your organization can deploy.	BuiltIn
[Preview]: Monitor VM Vulnerabilities in...	Monitors vulnerabilities detected by Vulnerability Assessment solution and VMs without a Vulnera...	BuiltIn
Require blob encryption for storage ac...	This policy ensures blob encryption for storage accounts is turned on. It only applies to Microsoft....	BuiltIn
[Preview]: Monitor missing system upd...	Missing security system updates on your servers will be monitored by Azure Security Center as rec...	BuiltIn
[Preview]: Monitor unprotected networ...	Network endpoints without a Next Generation Firewall's protection will be monitored by Azure Se...	BuiltIn
Allowed resource types	This policy enables you to specify the resource types that your organization can deploy.	BuiltIn
[Preview]: Monitor unencrypted SQL da...	Unencrypted SQL servers or databases will be monitored by Azure Security Center as recommenda...	BuiltIn

EXPERTS LIVE
CAFÉ



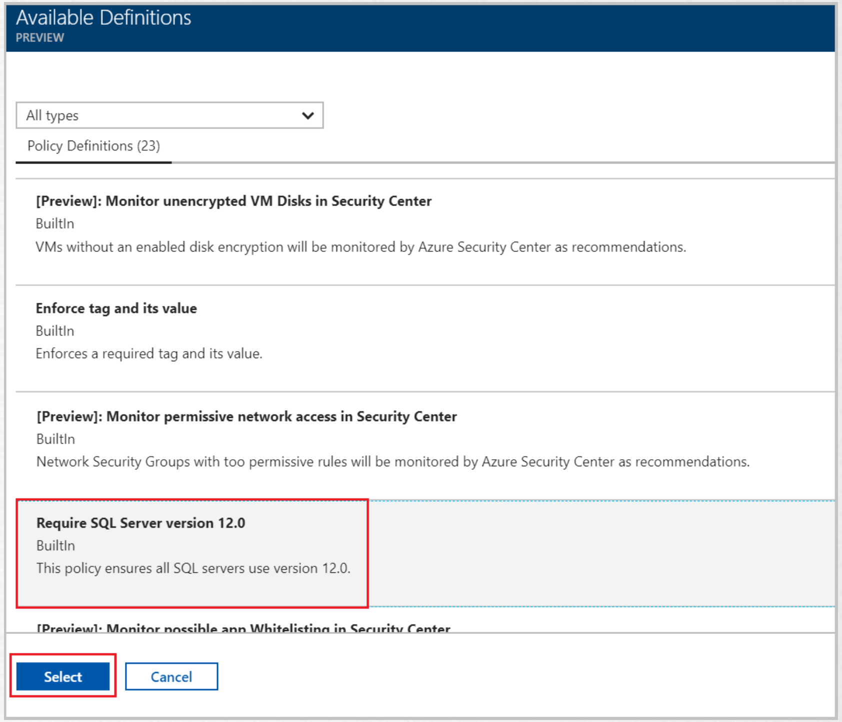
Subscriptions: All 3 selected

Total Assignments 10

Initiative Assignments 4

Policy Assignments 6

NAME	SCOPE	TYPE
Security for Express Route subscriptions	Azure Governance INT	initiative



[Preview]: Monitor unencrypted VM Disks in Security Center
BuiltIn
VMs without an enabled disk encryption will be monitored by Azure Security Center as recommendations.

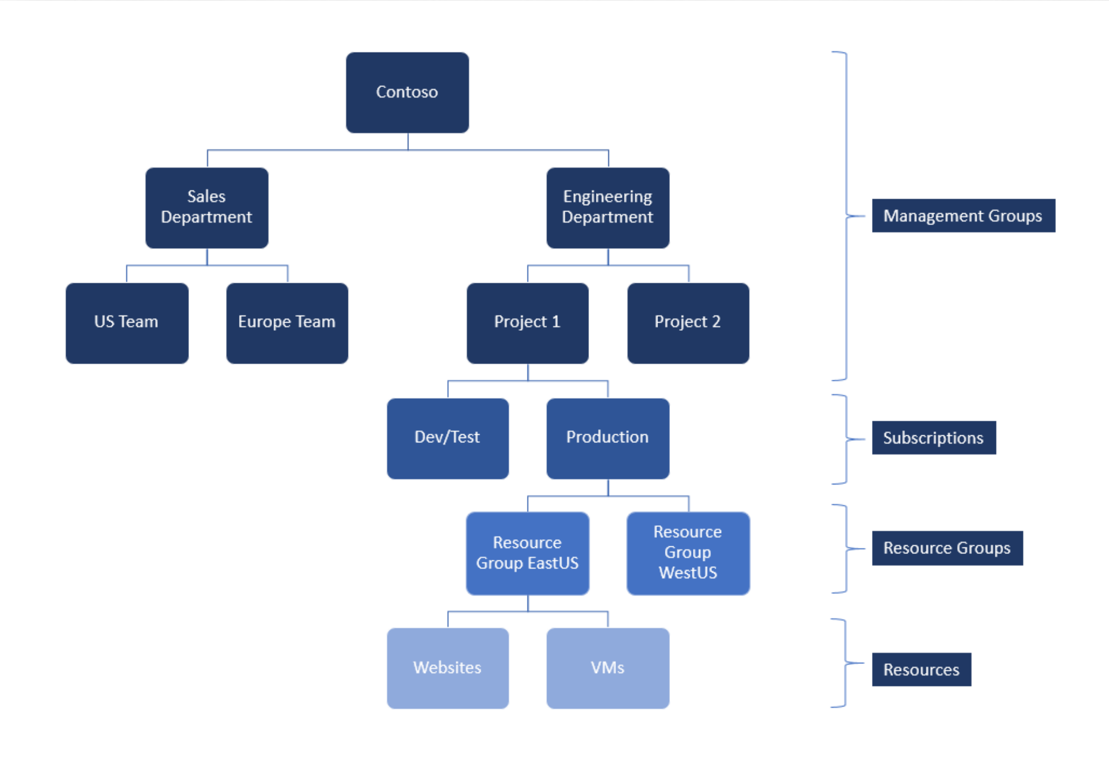
Enforce tag and its value
BuiltIn
Enforces a required tag and its value.

[Preview]: Monitor permissive network access in Security Center
BuiltIn
Network Security Groups with too permissive rules will be monitored by Azure Security Center as recommendations.

Require SQL Server version 12.0
BuiltIn
This policy ensures all SQL servers use version 12.0.

[Preview]: Monitor possible app Whitelisting in Security Center

Azure Management Groups



Contoso

Sales Department

Engineering Department

US Team

Europe Team

Project 1

Project 2

Dev/Test

Production

Resource Group EastUS

Resource Group WestUS

Websites

VMs

Management Groups

Subscriptions

Resource Groups

Resources

Azure Security Center

On-premises integration

(MMS Agent)

Playbooks

(Logic Apps)

Just In Time Access

Adaptive application controls

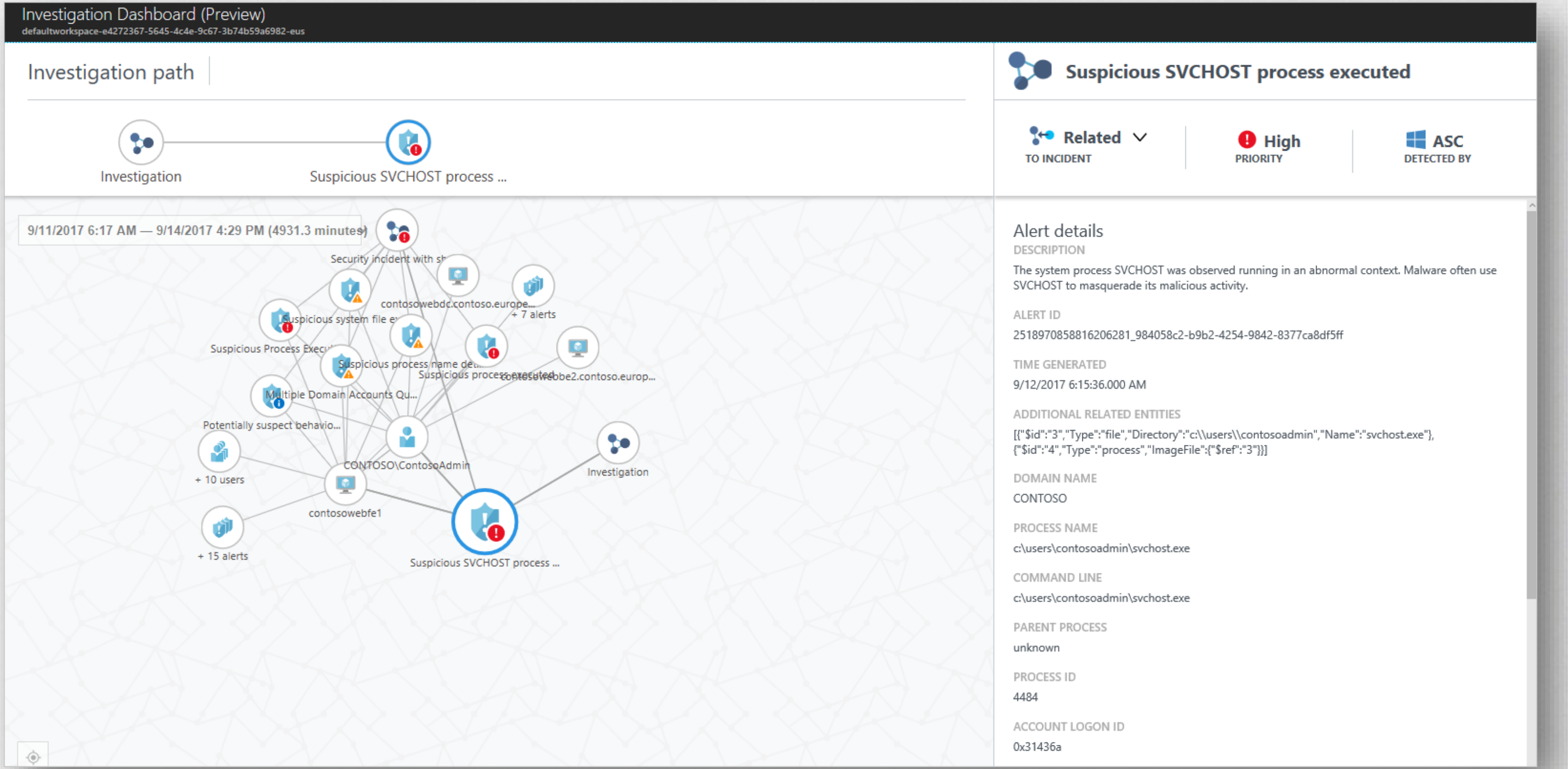
(Whitelisting Applications)

Alert & incident investigation

(Investigation Path)

Enterprise-wide security policy

(Preview)



Investigation Dashboard (Preview)
defaultworkspace-e4272367-5645-4c4e-9c67-3b74b59a6982-eus

Investigation path
Investigation
Suspicious SVCHOST process ...
9/11/2017 6:17 AM — 9/14/2017 4:29 PM (4931.3 minutes)
Security incident with sh
Suspicious system file e
contosowebdc.contoso.europe...
+ 7 alerts
Suspicious Process Execu
Suspicious process name de...
Suspicious process executed
contosowebbe2.contoso.europ...
Multiple Domain Accounts Qu...
Potentially suspect behavio...
+ 10 users
CONTOSO\ContosoAdmin
Investigation
contosowebfe1
+ 15 alerts
Suspicious SVCHOST process ...

Suspicious SVCHOST process executed

Related TO INCIDENT | High PRIORITY | ASC DETECTED BY

Alert details

DESCRIPTION
The system process SVCHOST was observed running in an abnormal context. Malware often use SVCHOST to masquerade its malicious activity.

ALERT ID
2518970858816206281_984058c2-b9b2-4254-9842-8377ca8df5ff

TIME GENERATED
9/12/2017 6:15:36.000 AM

ADDITIONAL RELATED ENTITIES
[{"$id":"3","Type":"file","Directory":"c:\\users\\contosoadmin","Name":"svchost.exe"},
{"$id":"4","Type":"process","ImageFile":{"$ref":"3"}}]

DOMAIN NAME
CONTOSO

PROCESS NAME
c:\users\contosoadmin\svchost.exe

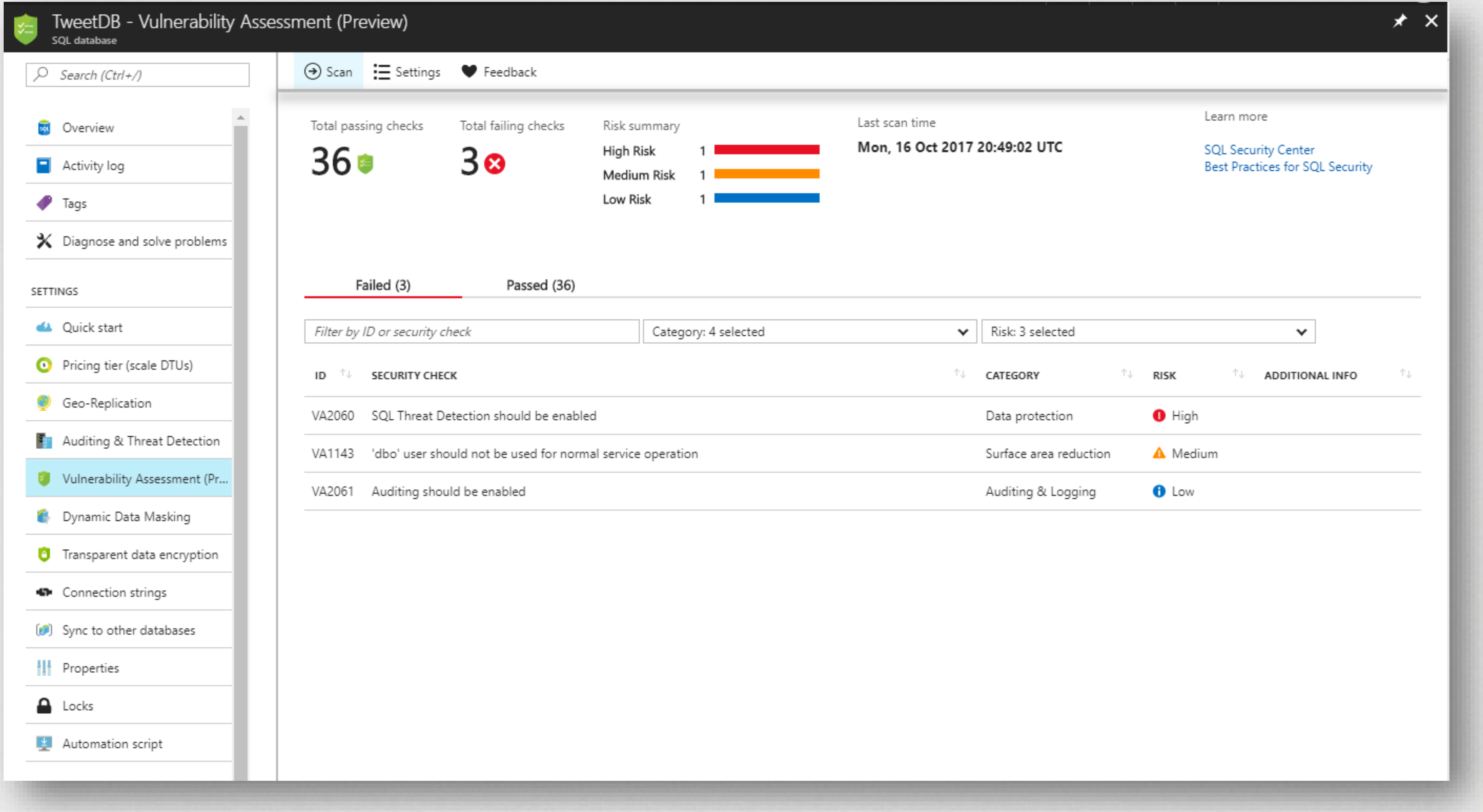
COMMAND LINE
c:\users\contosoadmin\svchost.exe

PARENT PROCESS
unknown

PROCESS ID
4484

ACCOUNT LOGON ID
0x31436a

EXPERTS LIVE
CAFÉ



TweetDB - Vulnerability Assessment (Preview)
SQL database

Total passing checks
36

Total failing checks
3

Risk summary

High Risk	1
Medium Risk	1
Low Risk	1

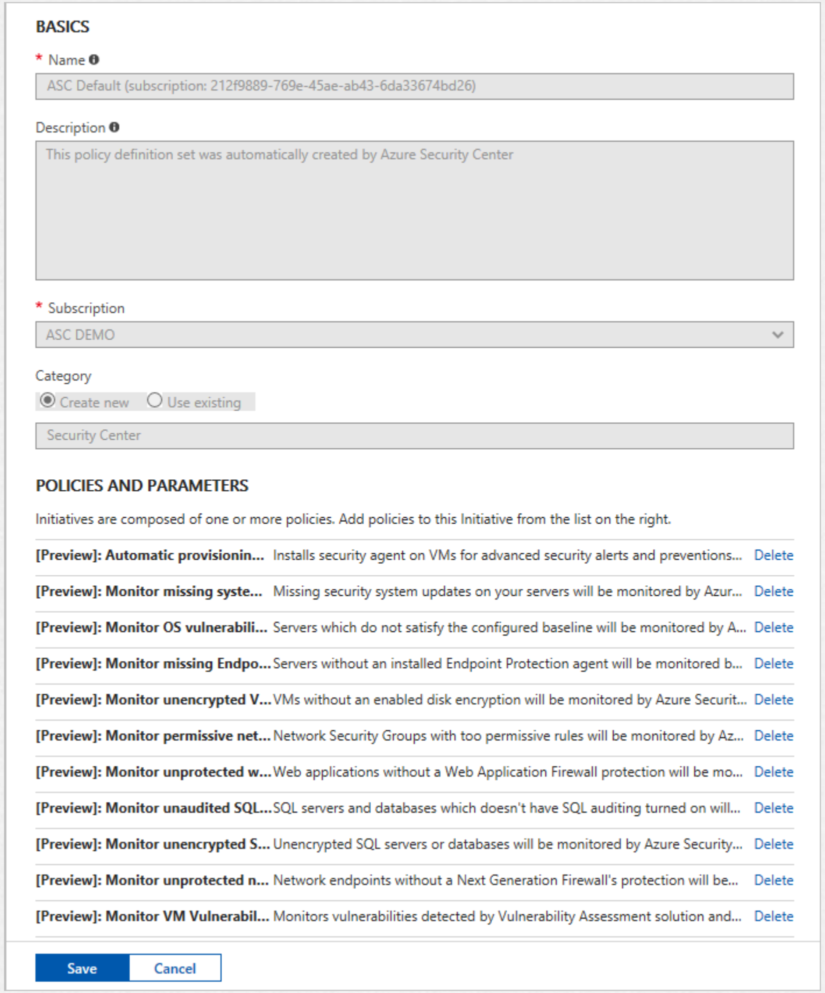
Last scan time
Mon, 16 Oct 2017 20:49:02 UTC

Learn more
SQL Security Center
Best Practices for SQL Security

Failed (3) | Passed (36)

Filter by ID or security check | Category: 4 selected | Risk: 3 selected

ID	SECURITY CHECK	CATEGORY	RISK	ADDITIONAL INFO
VA2060	SQL Threat Detection should be enabled	Data protection	High	
VA1143	'dbo' user should not be used for normal service operation	Surface area reduction	Medium	
VA2061	Auditing should be enabled	Auditing & Logging	Low	



BASICS

* Name ⓘ

ASC Default (subscription: 212f9889-769e-45ae-ab43-6da33674bd26)

Description ⓘ

This policy definition set was automatically created by Azure Security Center

* Subscription

ASC DEMO

Category

● Create new ○ Use existing

Security Center

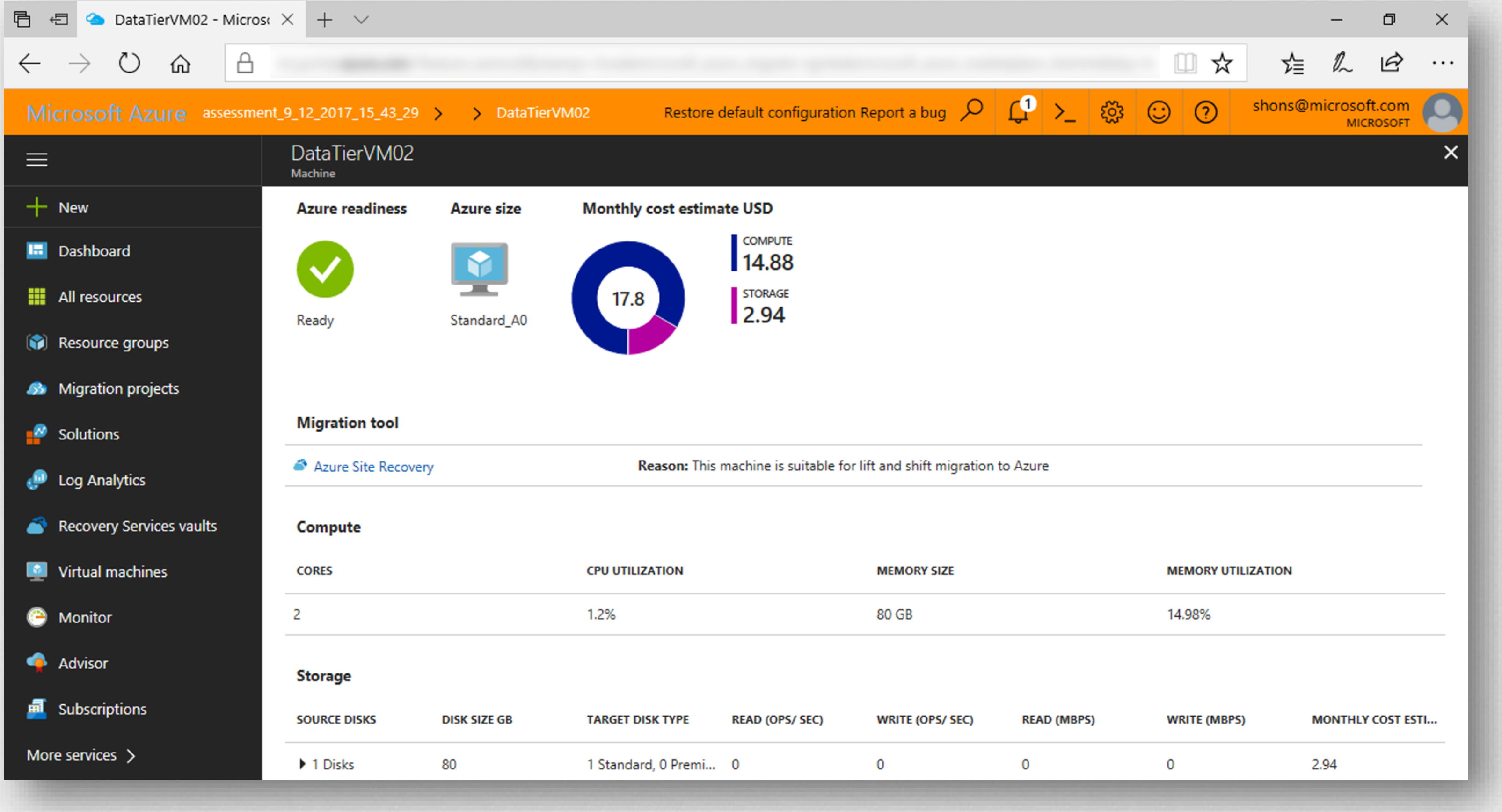
POLICIES AND PARAMETERS

Initiatives are composed of one or more policies. Add policies to this Initiative from the list on the right.

[Preview]: Automatic provisionin...	Installs security agent on VMs for advanced security alerts and preventions...	Delete
[Preview]: Monitor missing syste...	Missing security system updates on your servers will be monitored by Azur...	Delete
[Preview]: Monitor OS vulnerabili...	Servers which do not satisfy the configured baseline will be monitored by A...	Delete
[Preview]: Monitor missing Endpo...	Servers without an installed Endpoint Protection agent will be monitored b...	Delete
[Preview]: Monitor unencrypted V...	VMs without an enabled disk encryption will be monitored by Azure Securit...	Delete
[Preview]: Monitor permissive net...	Network Security Groups with too permissive rules will be monitored by Az...	Delete
[Preview]: Monitor unprotected w...	Web applications without a Web Application Firewall protection will be mo...	Delete
[Preview]: Monitor unaudited SQL...	SQL servers and databases which doesn't have SQL auditing turned on will...	Delete
[Preview]: Monitor unencrypted S...	Unencrypted SQL servers or databases will be monitored by Azure Security...	Delete
[Preview]: Monitor unprotected n...	Network endpoints without a Next Generation Firewall's protection will be...	Delete
[Preview]: Monitor VM Vulnerabil...	Monitors vulnerabilities detected by Vulnerability Assessment solution and...	Delete

Azure Migrate (Preview)

- Discovery and assessment for on-premises virtual machines
- Inbuilt dependency mapping for high-confidence discovery of multi-tier applications
- Based on “Service Map” technology
- Intelligent rightsizing to Azure virtual machines
- Compatibility reporting with guidelines for remediating potential issues
- Integration with Azure Database Management Service for database discovery and migration



DataTierVM02

Machine

Azure readiness

Ready

Azure size

Standard_A0

Monthly cost estimate USD

17.8

COMPUTE 14.88

STORAGE 2.94

Migration tool

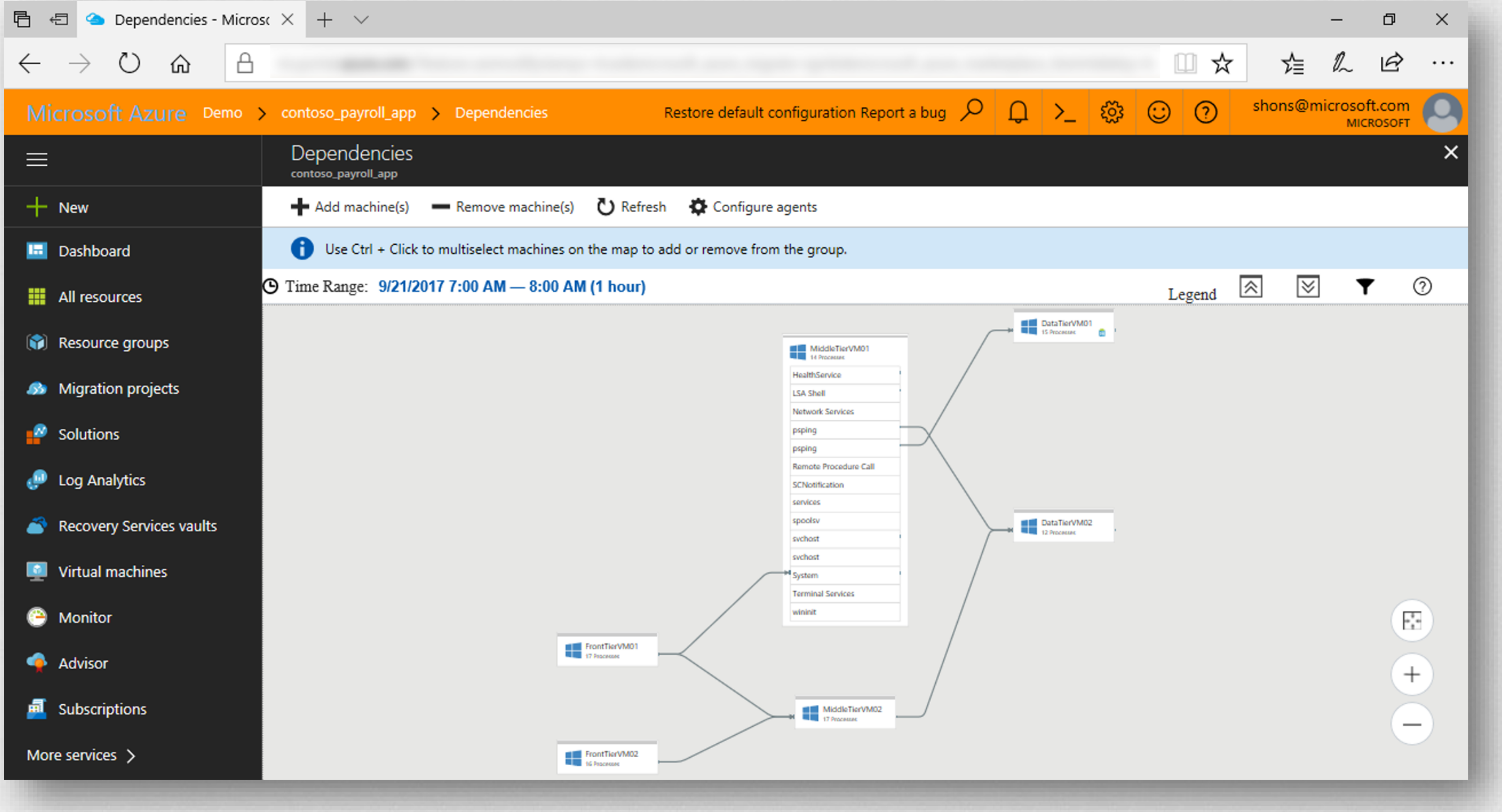
Azure Site Recovery — **Reason:** This machine is suitable for lift and shift migration to Azure

Compute

CORES	CPU UTILIZATION	MEMORY SIZE	MEMORY UTILIZATION
2	1.2%	80 GB	14.98%

Storage

SOURCE DISKS	DISK SIZE GB	TARGET DISK TYPE	READ (OPS/ SEC)	WRITE (OPS/ SEC)	READ (MBPS)	WRITE (MBPS)	MONTHLY COST ESTI...
▸ 1 Disks	80	1 Standard, 0 Premi...	0	0	0	0	2.94



Use Ctrl + Click to multiselect machines on the map to add or remove from the group.

Time Range: 9/21/2017 7:00 AM — 8:00 AM (1 hour)

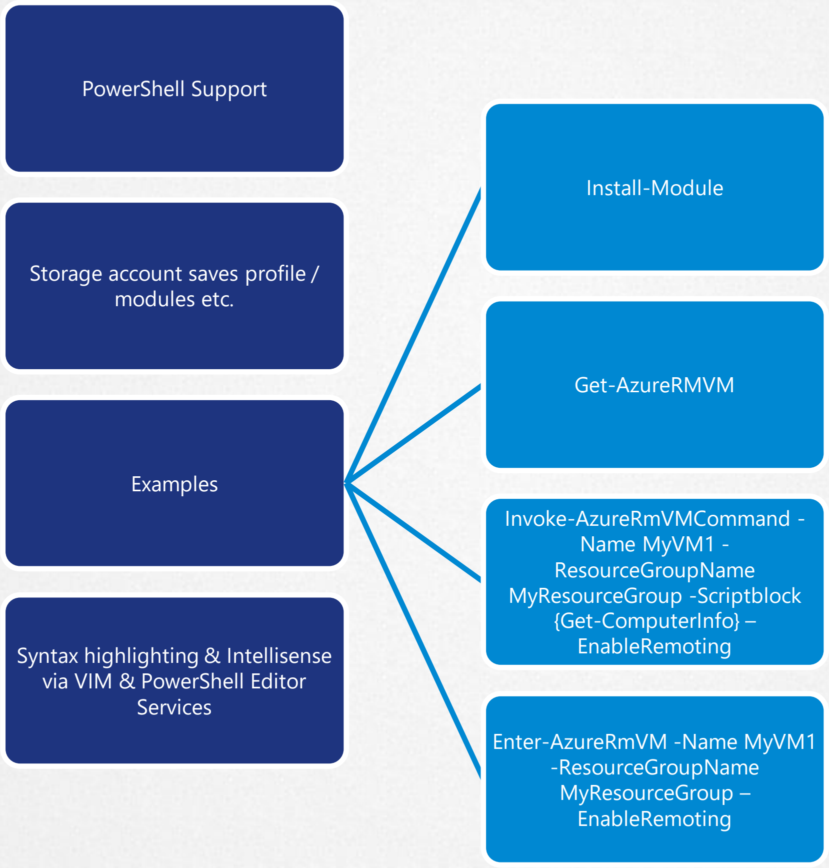
Azure Database Migration

- Azure Database Migration Service (Private Preview)
- Azure SQL Database – Managed Instance (Private Preview)

A new "Azure Database Migration service" will help you migrate existing on-premises SQL Server, Oracle, and MySQL databases to Azure SQL Database, Azure SQL Database Managed Instance or SQL Server on Azure virtual machines.

A new deployment option, "Azure SQL Database - Managed Instance" will bring increased compatibility with on-premises SQL Server instances, network isolation with full VNET and private IPs support, while keeping all the benefits of a fully managed PaaS.

Cloud Shell



PowerShell Support

Storage account saves profile / modules etc.

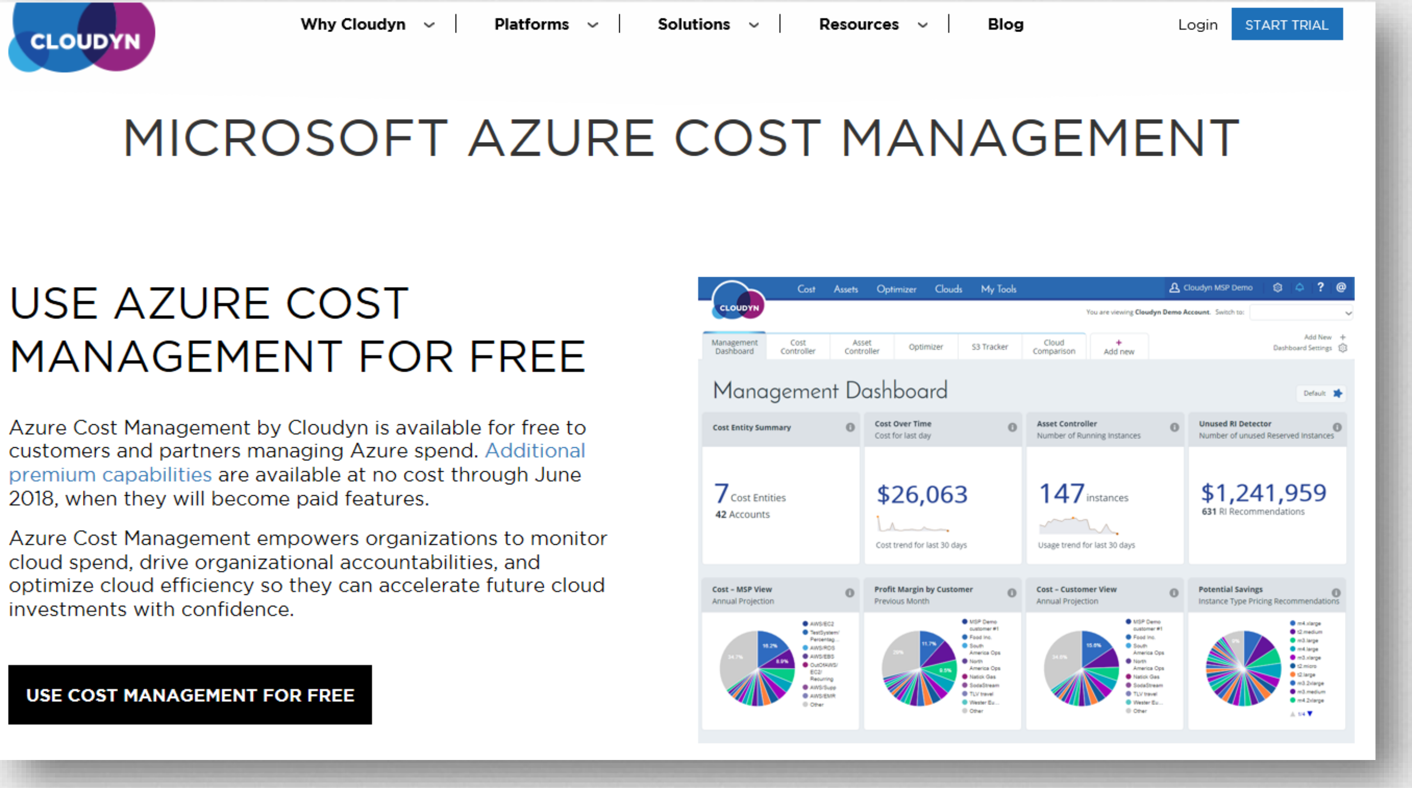
Examples

- Install-Module
- Get-AzureRMVM
- Invoke-AzureRmVMCommand -Name MyVM1 -ResourceGroupName MyResourceGroup -Scriptblock {Get-ComputerInfo} –EnableRemoting
- Enter-AzureRmVM -Name MyVM1 -ResourceGroupName MyResourceGroup –EnableRemoting

Syntax highlighting & Intellisense via VIM & PowerShell Editor Services

EXPERTS LIVE
CAFÉ

CLOUDYN



CLOUDYN Why Cloudyn | Platforms | Solutions | Resources | Blog Login START TRIAL

MICROSOFT AZURE COST MANAGEMENT

USE AZURE COST MANAGEMENT FOR FREE

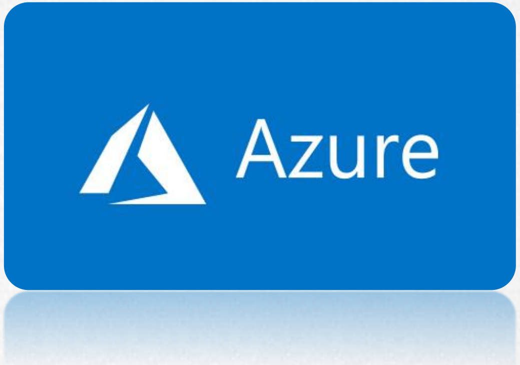
Azure Cost Management by Cloudyn is available for free to customers and partners managing Azure spend. Additional premium capabilities are available at no cost through June 2018, when they will become paid features.

Azure Cost Management empowers organizations to monitor cloud spend, drive organizational accountabilities, and optimize cloud efficiency so they can accelerate future cloud investments with confidence.

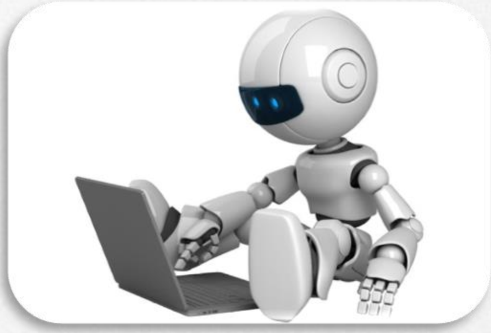
USE COST MANAGEMENT FOR FREE

...one more we have...

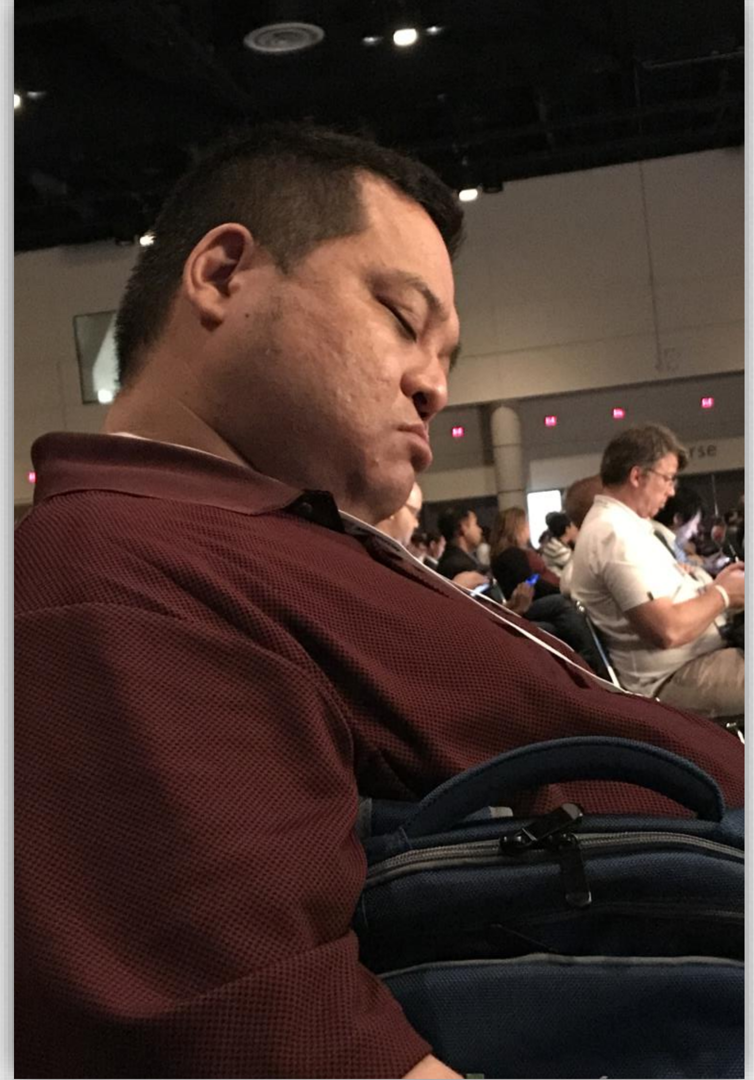
New Azure Logo...



Machine Learning...



EXPERTS LIVE
CAFÉ



Thank you for your attention!