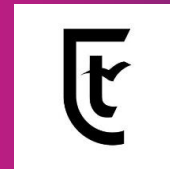


Insight 



Operation Management Suite (OMS) y Azure Security Center.

Juntos pero no revueltos

Roberto Tejero

@robtejero



Agenda

- ¿Quién soy yo?
- Predespliegue de Infraestructura
- OMS
 - ¿Que es OMS?
 - ¿Qué puede hacer OMS?
 - Arquitectura.
 - Despliegue de nuestro primer Workspace
 - Configuración inicial.
 - Despliegue de agentes.
 - OMS Gateway
 - Soluciones principales
 - Otras soluciones
 - Novedades
- Azure Security Center



¿Quien soy yo?

- Roberto Tejero
- @robtejero
- Solution Sales Specialist en **Insight Technology Solutions**.
- Blogs:
 - El camino de un ITPro <http://blogs.itpro.es/rtejero>
 - <https://masrobeznoquenunca.wordpress.com>
- Consultor desde hace He trabajado en Bolsas y Mercados (BME), Ministerio de Defensa, Zerkana, Capgemini, y, felizmente en Insight ... Especializado en Servicios de Infraestructura, Virtualización, Azure, Office 365, Power BI, contenedores, . Padre de los tres mosqueteros, esposo, y espíritu errante.



Pre-despliegue de Infraestructura.

Desde una suscripción de Azure despliegue de la siguiente Infraestructura:

- 3 IaaS
 - 2 Windows Server.
 - 1 Linux Server
- 1/2 WebApp (optativo)
 - Wordpress s/WebApp
- ¿?



Insight[®]



Operation Management Suite (OMS)

Roberto Tejero
@robtejero

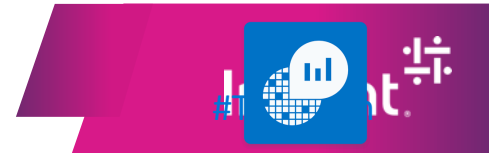
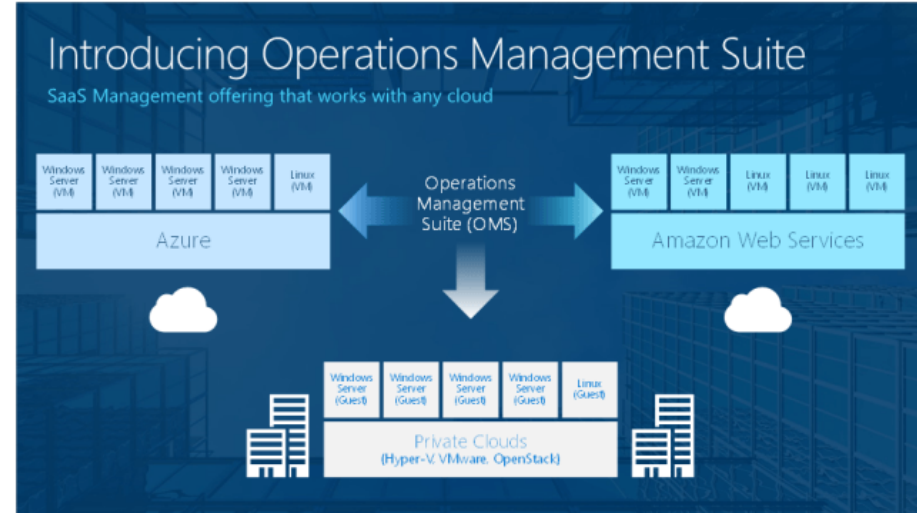


Qué es Operation Management Suite?

Microsoft Operation Management Suite (OMS), es un producto de Microsoft que sirve para gestionar nuestra infraestructura on-premise (Windows Server, Linux, Vmware, OpenStack, Dockers, etc) y nuestra nube pública (Azure, AWS, Google, ...). Nos permite asumir el control sobre cualquier nube híbrida.

¿Que nos proporciona OMS que no tengamos ya? OMS ayuda a simplificar la gestión de nuestros activos del centro de datos donde quiera que estén.

Es totalmente agnóstico a nuestro proveedor de servicio en la nube. Esto significa que cualquier instancia de cualquier nube, incluyendo nuestro centro de datos On-Premise, Azure, AWS, Windows Server, Linux, Google, VMware, OpenStack, etc. puede ser monitorizado, controlado, gestionado, auditado, securizado, etc., a un costo menor que la mayoría de las soluciones de la competencia.



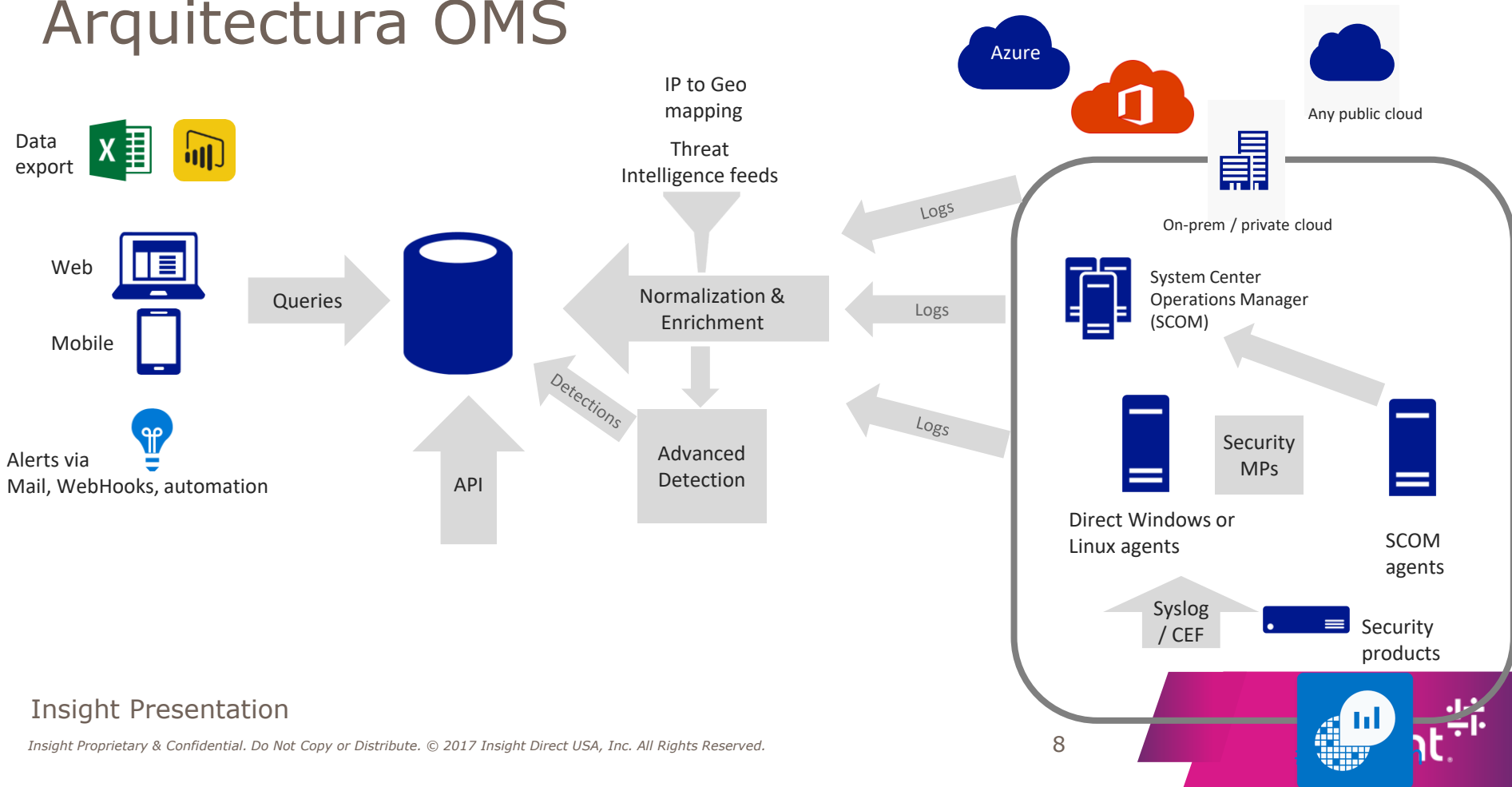
¿Qué puede hacer OMS?

- Múltiples orígenes de datos Cloud y On-Premise
- Correlación de datos
- Creación y configuración de alertas
- Creación de vistas customizadas.
- Controlar nuestros servidores y su uso.
- Centralizar todos los LOG de las máquinas, servicios, etc.
- Realizar una previsión de capacidad.
- Planificar las actualizaciones de nuestros servidores
- Alertas de Malware para proteger nuestros servidores
- Previsión de estado de nuestros SQL
- Trazabilidad y gestión de cambios de todos nuestros servicios.
- Gestión de alertas
- Seguridad y auditoria
- Automatización (despliegue, monitorización de recursos on-premise - public cloud)
- Backup
- Azure Site Recovery
- Wire Data: análisis de tráfico de nuestra red.

Insight Presentation



Arquitectura OMS

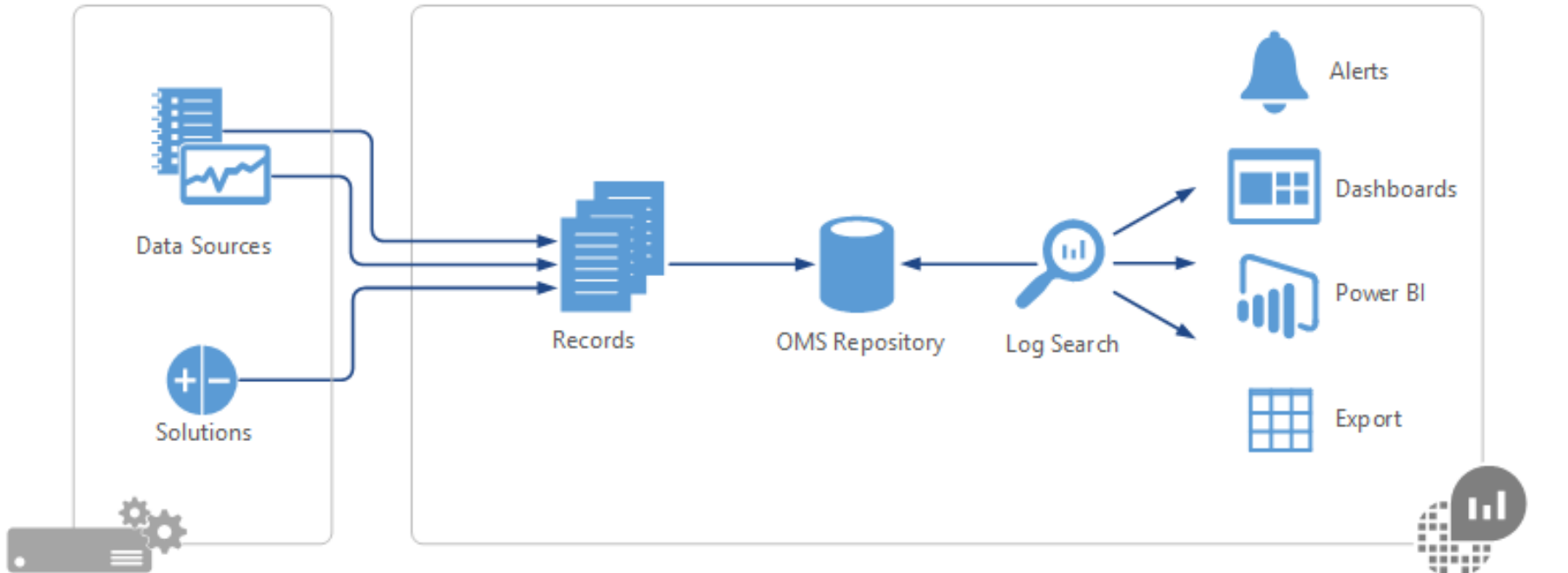


Insight Presentation

Insight Proprietary & Confidential. Do Not Copy or Distribute. © 2017 Insight Direct USA, Inc. All Rights Reserved.



Como funciona OMS Log Analytics?



Connected Sources

Insight Presentation

Insight Proprietary & Confidential. Do Not Copy or Distribute. © 2017 Insight Direct USA, Inc. All Rights Reserved.



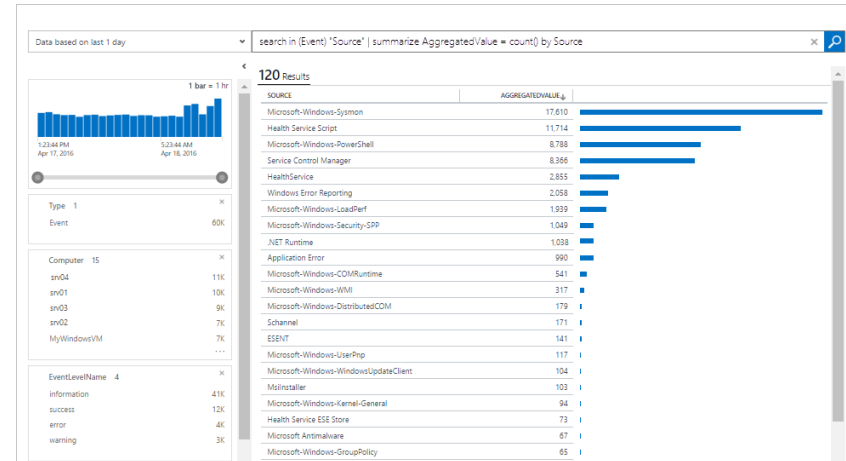
Conceptos básicos de OMS

- La forma de organizarse de Log Analytics es en base a un Espacio de Trabajo o Workspace

Workspace es un contenedor donde guardamos los datos recibidos por los agentes de OMS. Nos puede aportar:

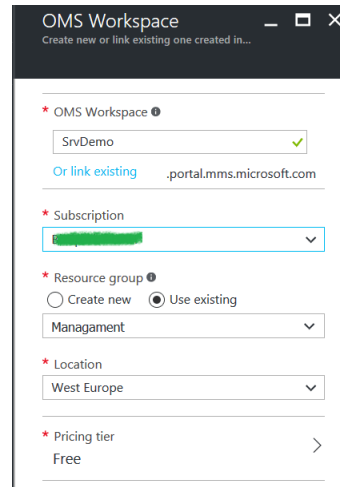
- Situación geográfica.- Cumplimiento GDPR, LOPD, etc.
- División departamental para facturación.
- Mantenimiento de datos aislados los unos de los otros.

- Log Analytics.- Es el Core de OMS.



Despliegue de nuestro primer cuadro de mando

- Nombre.
- Suscripción
- Grupo de Recursos
- Localización
- Plan de precios



OMS Workspace
Create new or link existing one created in...

* OMS Workspace

SrvDemo ✓

[Or link existing](#) .portal.mms.microsoft.com

* Subscription

[Redacted]

* Resource group

Create new Use existing

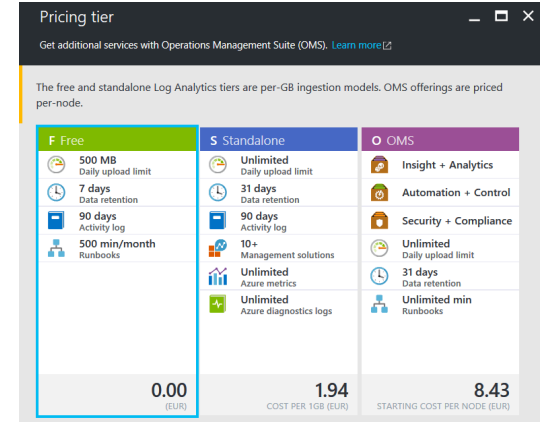
Management

* Location

West Europe

* Pricing tier

Free

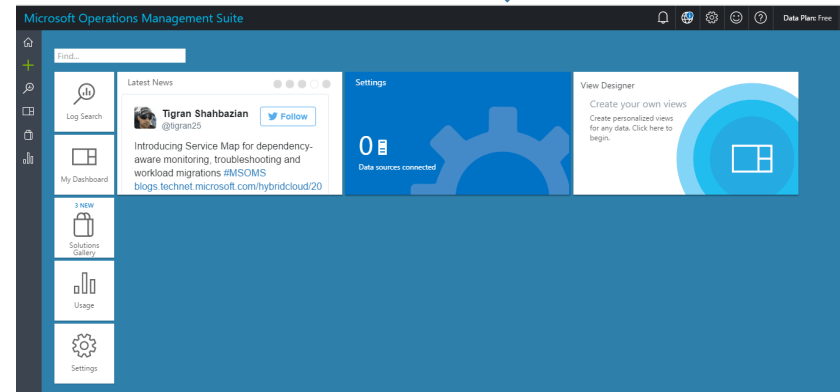


Pricing tier

Get additional services with Operations Management Suite (OMS). [Learn more](#)

The free and standalone Log Analytics tiers are per-GB ingestion models. OMS offerings are priced per-node.

F Free	S Standalone	O OMS
500 MB Daily upload limit	Unlimited Daily upload limit	Insight + Analytics
7 days Data retention	31 days Data retention	Automation + Control
90 days Activity log	90 days Activity log	Security + Compliance
500 min/month Runbooks	10+ Management solutions	Unlimited Daily upload limit
	Unlimited Azure metrics	31 days Data retention
	Unlimited Azure diagnostics logs	Unlimited min Runbooks
0.00 (EUR)	1.94 COST PER 1GB (EUR)	8.43 STARTING COST PER NODE (EUR)



Microsoft Operations Management Suite

Home | Log Search | My Dashboard | Solutions Gallery | Usage | Settings

Latest News

Tigran Shahbazian @tgran25

Introducing Service Map for dependency-aware monitoring, troubleshooting and workload migrations #MSOMS [blogs.technet.microsoft.com/hybridcloud/20](#)

Settings

0 Data sources connected

View Designer








Create your own views
Create personalized views for any data. Click here to begin.

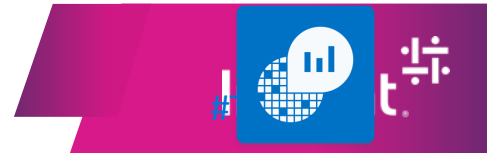
Data Plans Free

Insight Presentation

Insight Proprietary & Confidential. Do Not Copy or Distribute. © 2017 Insight Direct USA, Inc. All Rights Reserved.

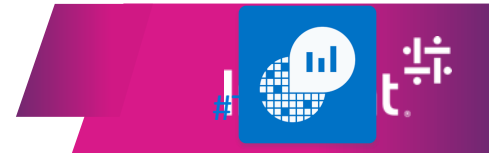
Configuración inicial.

 Solutions	>
 Connected Sources	>
 Data	>
 Computer Groups	>
 Accounts	>
 Alerts	>
 Preview Features	>



Origenes de datos.

Data Source	Event Type	Description
Custom logs	<LogName>_CL	Text files on Windows or Linux agents containing log information.
Windows Event logs	Event	Events collected from the event log on Windows computers.
Windows Performance counters	Perf	Performance counters collected from Windows computers.
Linux Performance counters	Perf	Performance counters collected from Linux computers.
IIS logs	W3CIISLog	Internet Information Services logs in W3C format.
Syslog	Syslog	Syslog events on Windows or Linux computers.



Despliegue de agentes...

Prerequisitos.

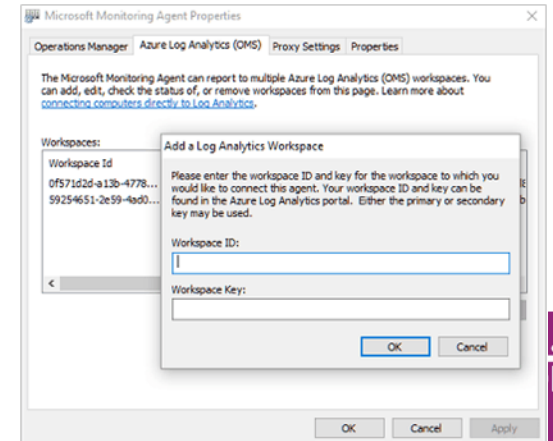
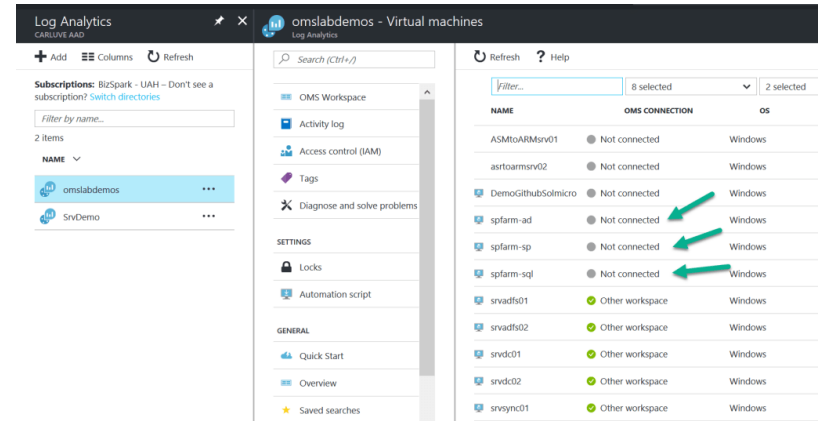
- Solo puede instalarse en equipos con Windows Server 2008 SP1 o en versiones posteriores y en equipos con Windows 7 SP1 o versiones superiores.
- Necesitaremos tener una suscripción de OMS.
- Todos los equipos necesitarán tener conexión a Internet a través de HTTPS (Puerto 443). Esta conexión puede ser directa, a través de un proxy o a través de la puerta de enlace (Gateway de OMS).
- Podemos instalar el agente de OMS en equipos independientes, servidores, máquinas físicas o virtuales.

Equipos:

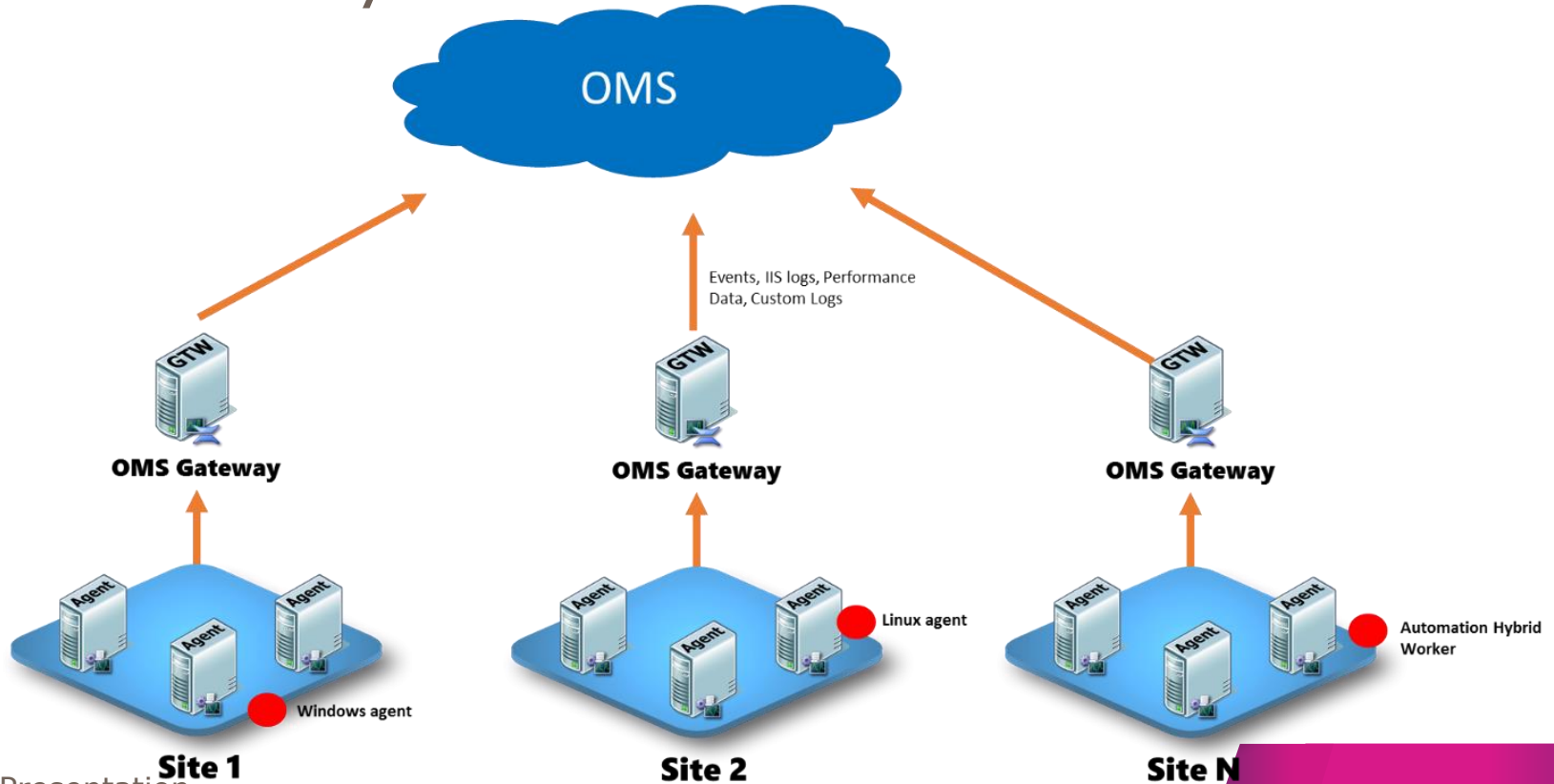
- Equipos que están en Azure.
- Equipos que no están en Azure.
 - Descargar el agente y la clave.
 - Instalar el agente manualmente
 - Instalar el agente por línea de comando

Insight Presentation

Insight Proprietary & Confidential. Do Not Copy or Distribute. © 2017 Insight Direct USA, Inc. All Rights Reserved.



OMS Gateway



Soluciones principales

Solution offers

Insight & Analytics

Microsoft

- Monitor and Troubleshoot Application and Infrastructure issues using Log Analytics.
- Includes 2 solutions



Automation & Control

Microsoft

- Increase control with automation and configuration management
- Includes 2 solutions



Security & Compliance

Microsoft

- Secure and audit your datacenter with full visibility to all security data and with advanced threat detection
- Includes 2 solutions



Protection & Recovery

Microsoft

- Ensure data protection with cloud backup and disaster recovery
- Includes 2 solutions



Insight Presentation

Insight Proprietary & Confidential. Do Not Copy or Dis



Soluciones principales

Log Analytics: Inteligencia operacional en tiempo real. Recopilar, almacenar y analizar los datos de cualquier registro de logging, de cualquier fuente.

- Recolectar datos en tiempo real.
- Transformación de los datos para su posterior tratamiento.
- Visualizar todos los eventos que estamos monitorizando.
- Posibilidad de actuación.

A purple graphic with a city skyline silhouette at the bottom. In the center, there are two overlapping circles, one containing a bar chart icon and the other a speech bubble icon. The text 'Insight & Analytics' is at the top, followed by 'Microsoft' and a bulleted list of features.

Insight & Analytics

Microsoft

- Monitor and Troubleshoot Application and Infrastructure issues using Log Analytics.
- Includes 2 solutions



Soluciones principales

Automation: Simplificar la gestión de nuestra nube o enterno Híbrido a través de la automatización de procesos. Lo que todos queremos, crear, monitorizar, administrar y desplegar recursos en nuestros entornos mientras reducimos errores y aumentamos la eficiencia, sin olvidarnos de la reducción de costes operativos.



Automation & Control

Microsoft

- Increase control with automation and configuration management
- Includes 2 solutions

The slide features a green background with a city skyline silhouette at the bottom. In the center, there is a large gear icon with a lightning bolt inside, surrounded by three white clouds. The text is positioned in the upper left quadrant of the slide.



Soluciones principales

Security: Control de seguridad centralizado. Identificar actualizaciones de los sistemas gestionados, estado del malware, recopilación de eventos relacionados con la seguridad y realización de análisis forenses.

A graphic with an orange background. At the top, it says "Security & Compliance" in white. Below that, "Microsoft" is written in white. There are two bullet points in white: "Secure and audit your datacenter with full visibility to all security data and with advanced threat detection" and "Includes 2 solutions". The bottom half of the graphic features a white shield icon in the center, surrounded by concentric circles, with a city skyline silhouette and white clouds in the background.

Security & Compliance

Microsoft

- Secure and audit your datacenter with full visibility to all security data and with advanced threat detection
- Includes 2 solutions



Soluciones principales

Availability: Solución de alta disponibilidad totalmente integrada incluyendo recuperación de desastres. Posibilidad de habilitar la copia de seguridad y la recuperación integrada para todos nuestros servicios y aplicaciones críticas.

A graphic with a blue background. At the top, the text 'Protection & Recovery' is written in white. Below it, 'Microsoft' is written in a smaller white font. Underneath, there is a bulleted list in white: '• Ensure data protection with cloud backup and disaster recovery' and '• Includes 2 solutions'. The bottom half of the graphic features a stylized city skyline in dark blue. In the center of the skyline is a large, light blue circular target icon with a white cloud in the middle. Several white clouds are scattered across the sky area.

Protection & Recovery

Microsoft

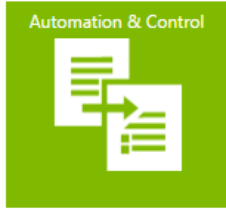
- Ensure data protection with cloud backup and disaster recovery
- Includes 2 solutions



Otras Soluciones



Backup
Available
Manage Azure IaaS VM backup and Windows Server backup status for your backup vault.



Change Tracking
Owned
Track configuration changes across your servers



Agent Health
Owned
The Agent Health solution gives customers insight into the health, performance and availability of their Windows and Linux agents



Configuration Monitor
Available
Automatically discover and monitor servers and their configurations in real-time.



AD Replication Status
Available
Identify Active Directory replication issues in your environment.



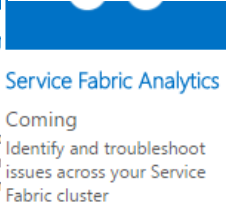
SQL Assessment
Owned
Assess the risk and health of your SQL Server environment



Antimalware Assessment
Owned
View status of antivirus and antimalware scans across your servers.



Azure Automation Analytics
Available
Create Hybrid Runbook Workers to run Automation runbooks on your on-premises servers.



Service Fabric Analytics
Coming
Identify and troubleshoot issues across your Service Fabric cluster



Assessment
Owned
Assess the risk and health of your Directory environments.



Surface Hub
Available
Provides the ability to monitor Microsoft Surface Hub devices.



Containers
Available
See Docker container performance metrics and logs from containers across your public or private cloud environments.



Azure Site Recovery
Available
Monitor virtual machine replication status for your Azure Site Recovery Vault.



Activity Log Analytics
Coming
Track all create, update and delete activities occurring in your Azure subscriptions.

Insight Presentation

Novedades

- ARM → Portal de Azure ;-)
- Actualizaciones constantes (SaaS).
- View Designer
- Service Map.
- Soluciones para:
 - Citrix
 - Surface Hub
 - Windows 10
 - DNS Analytics
 -

Insight Presentation

Insight Proprietary & Confidential. Do Not Copy or Distribute. © 2017 Insight Direct USA, Inc. All Rights Reserved.

What's new in this update

Powerful Search

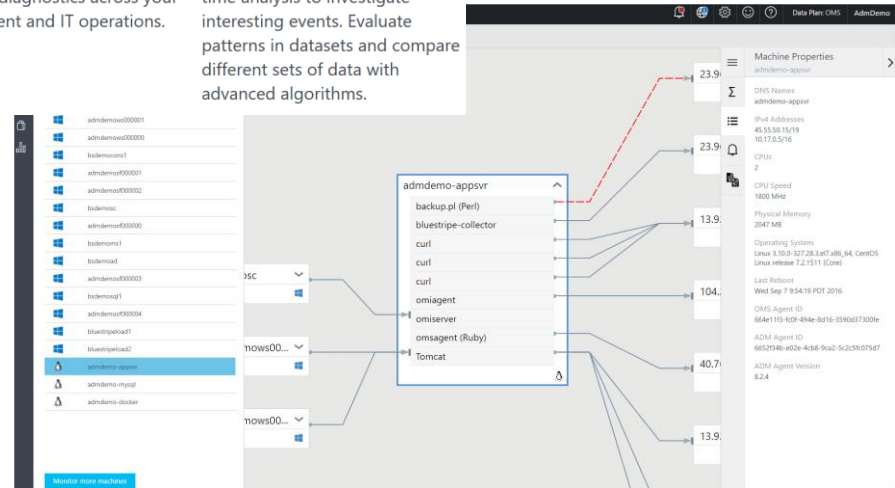
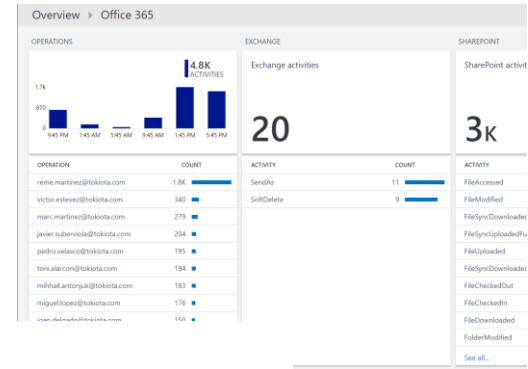
Easy to learn, simple yet powerful textual query syntax that is interactive, expressive and can scale complex scenarios. You can define custom fields using on-the-fly field extraction and rich built-in functions.

Smart Analytics

Advanced analytics portal that supports multiline editing of queries, new visualizations, and advanced diagnostics across your development and IT operations.

Deeper Insights

Correlate data with powerful joins to gain deeper insights and zoom in using advanced date-time analysis to investigate interesting events. Evaluate patterns in datasets and compare different sets of data with advanced algorithms.





Demos

Despliegue de soluciones
O365
AD

....

Despliegue de agentes
On-Premise vs On-Cloud

Queries
Alertas
Dashboards

.....

Demos

Actions

- Stop services: Print Spooler & ¿?
- Login fallidos.

Query

Type=Event Computer=srv01.contoso.com → Event | where Computer == "srv01.contoso.com"

Type=Event EventLog=System EventID=7036 → Stop Services.

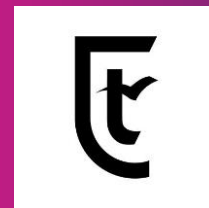
Type=SecurityEvent EventID = 4625 → Eventos fallidos de Login.

Type=Event | measure count() as Count by Computer → Event | summarize Count = count() by Computer

Type=Perf ObjectName=Processor CounterName="% Processor Time" | measure avg(CounterValue) by Computer interval 5minute → Perf | where ObjectName=="Processor" and CounterName=="% Processor Time" | summarize avg(CounterValue) by Computer, bin(TimeGenerated, 5min)



Insight 



Centro de Seguridad de Azure

Roberto Tejero
@robtejero

