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

Insight

¿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.

Predespliegue 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
- ¿?

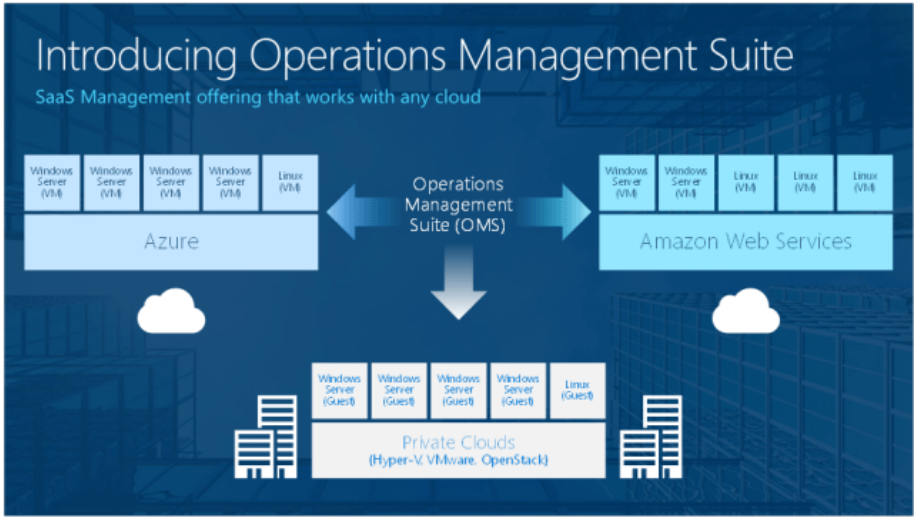
Insight

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.



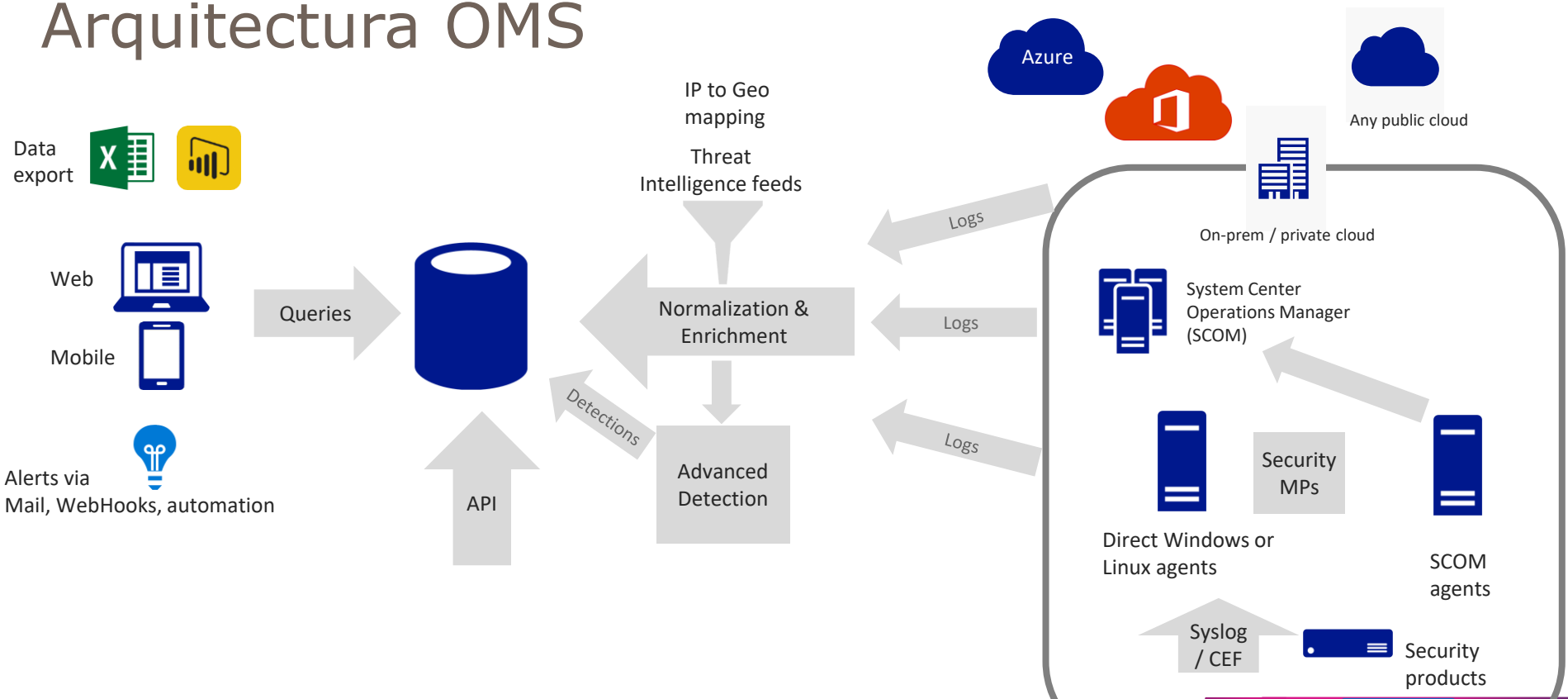
¿Que nos proporciona OMS que no tengamos ya? OMS ayuda a simplificar la gestión de nuestros activos del centro de datos donde quiera que estén.

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.

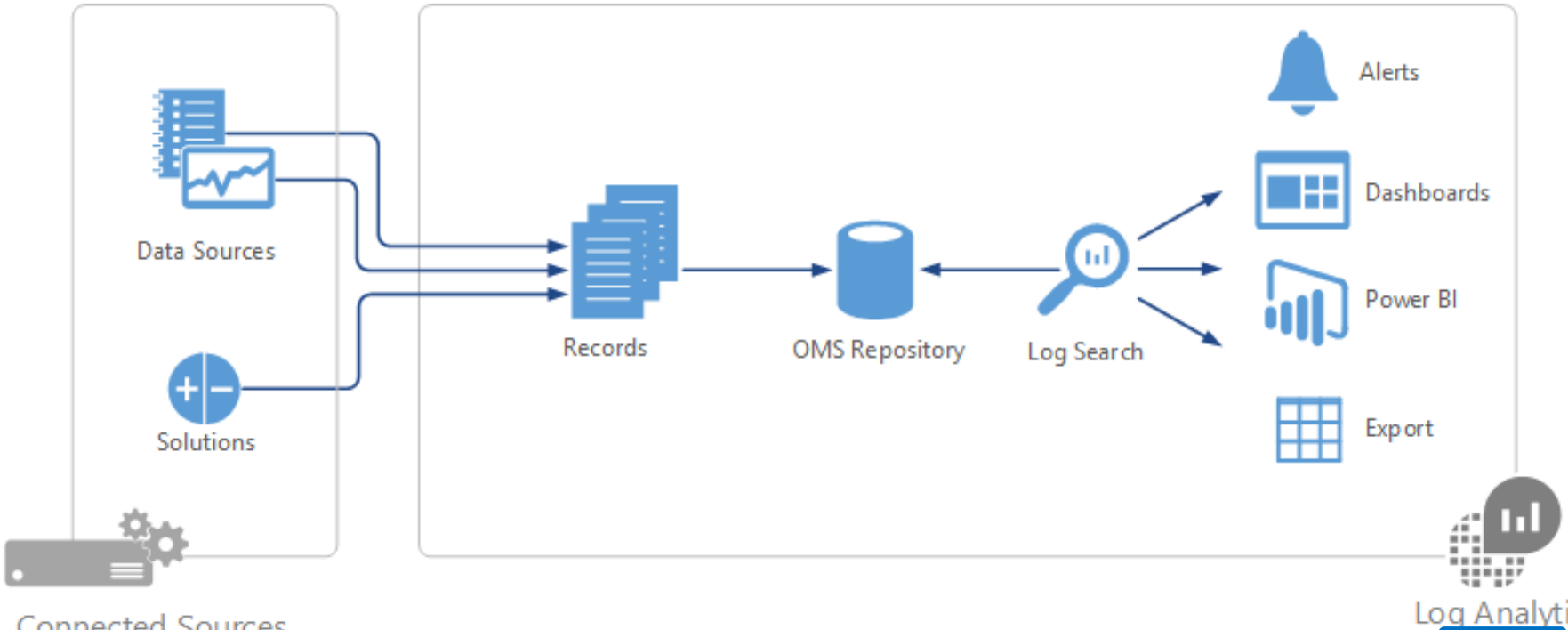
¿Qué puede hacer OMS?

- 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.

Arquitectura OMS



Como funciona OMS Log Analytics?

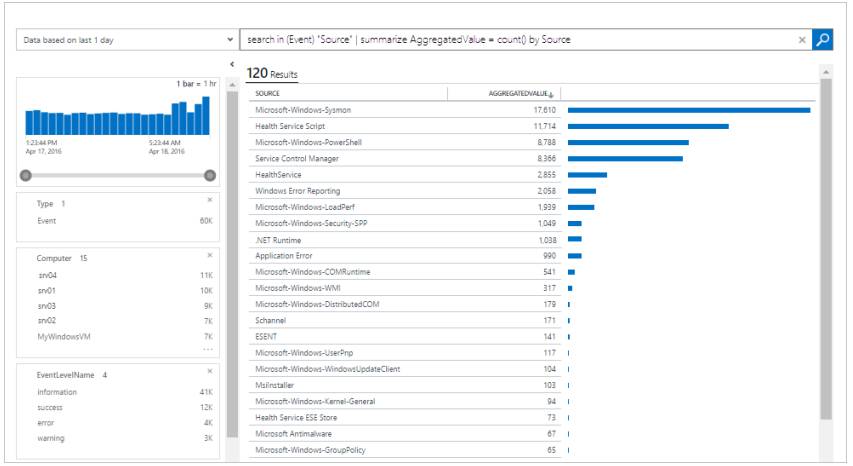


Conceptos básicos de OMS

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

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

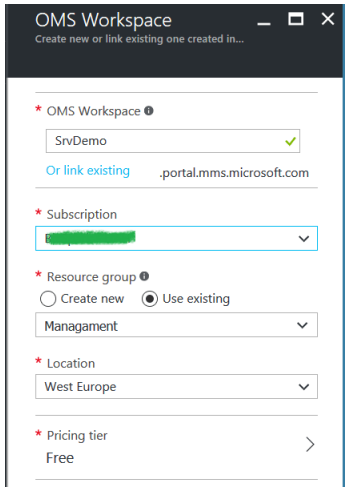
  - Situación geográfica.- Cumplimiento GDPR, LOPD, etc.
  - División departamental para facturación.
  - Mantenimiento de datos aislados los unos de los otros.

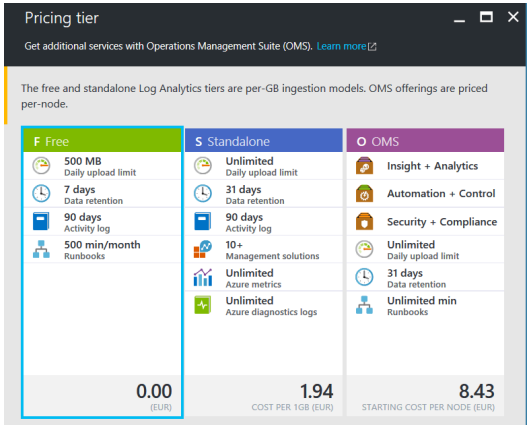


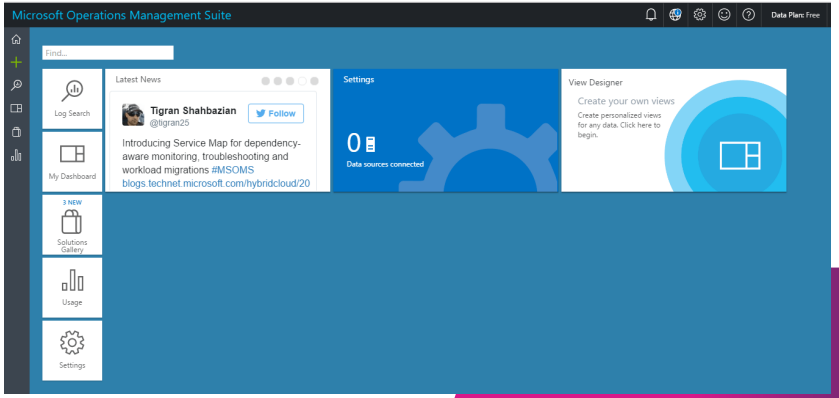
- Log Analytics.- Es el Core de OMS.

Despliegue de nuestro primer cuadro de mando

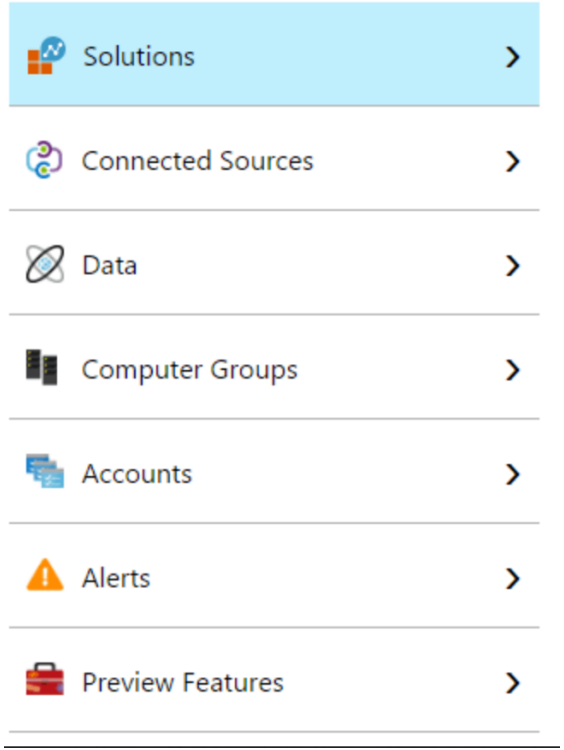
- Nombre.
- Suscripción
- Grupo de Recursos
- Localización
- Plan de precios







Configuración inicial.



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.

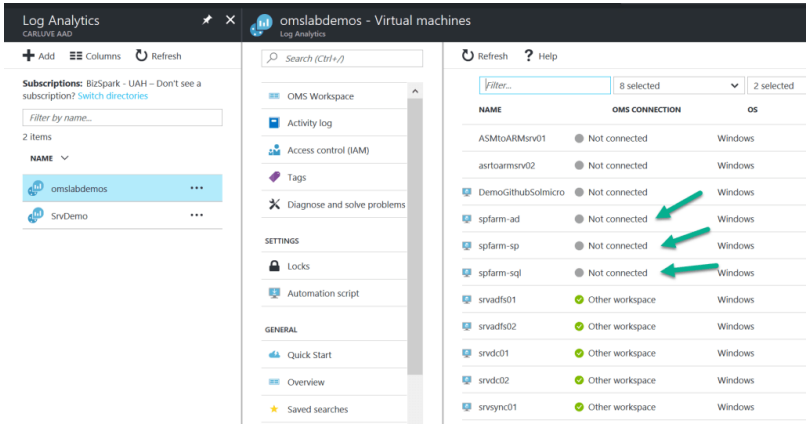
Despliegue de agentes…

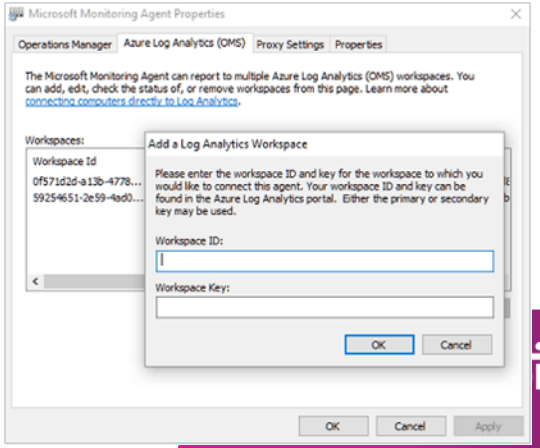
Prerequisitos.

- 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.

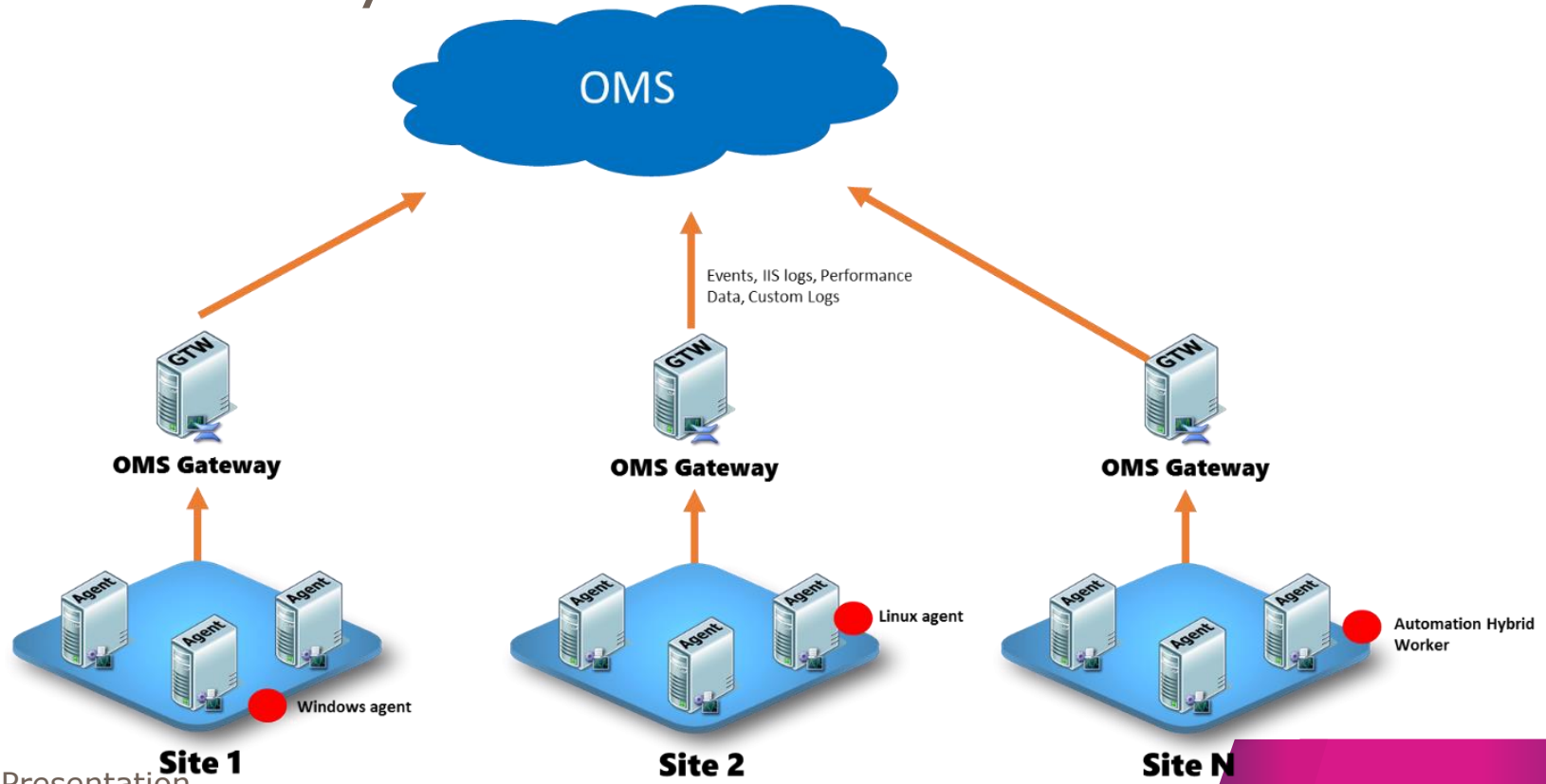
Equipos:

- 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





OMS Gateway



Soluciones principales

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.

Soluciones principales

Automation: Simplificar la gestión de nuestra nube o enterno Hibrido a traves 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.

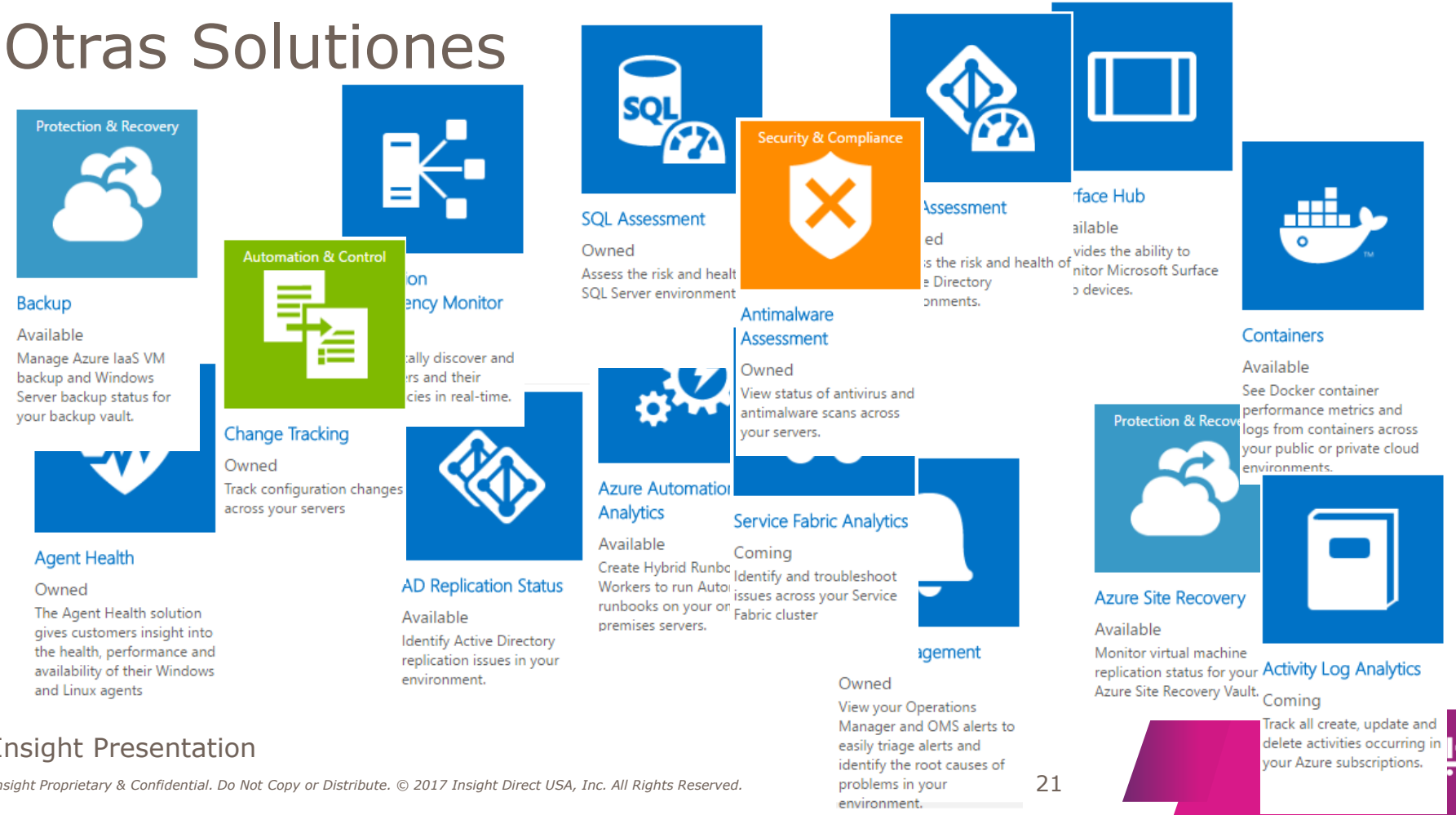
Soluciones principales

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

Soluciones principales

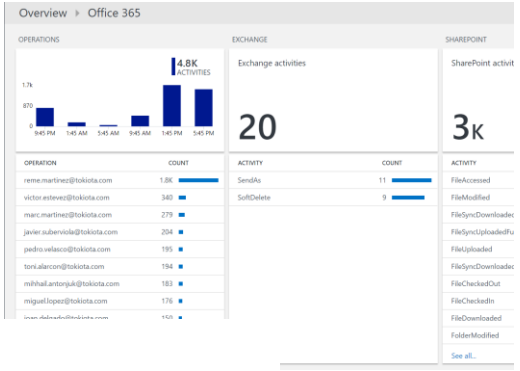
Availability: Solución de alta disponibilidad totalmente integrada incluyendo recuperación de desastres. Posibilidad de habilitar la copia de seguridad y la recuperación integrada para todos nuestros servicios y aplicaciones críticas.

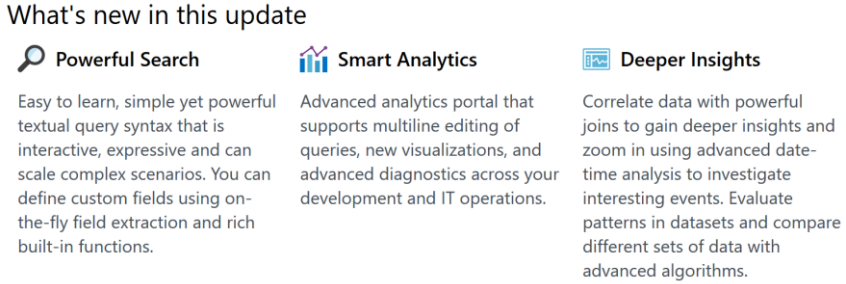
Otras Solutiones

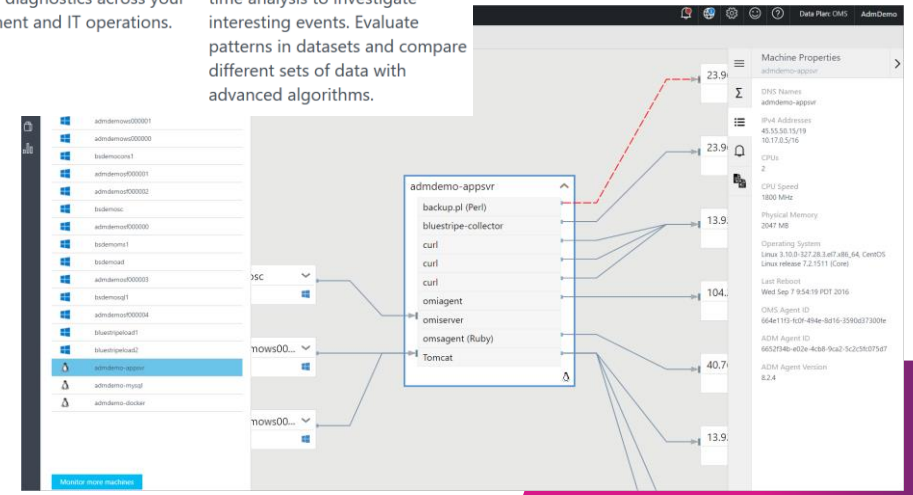


Novedades

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







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