

zMonitor

"Tu ojo de Sauron"



David Gomez - @dgomezm2
Roberto Tejero - @robtejero



#InsightIberia

¡Gracias!

Patrocinadores Locales



Colabora



David Gómez

Consultor Cloud en Insight

Más de 18 años brujuleando por los entornos más peculiares que os podáis imaginar.

- Especialista en entorno de comunicaciones unificadas y Modern Workplace
- Especialista en entornos de sistemas microsoft.
- DBA SQL Server
- Virtualización en entorno Microsoft (On-Premise, Hybrid y cloud)



Roberto Tejero

Solution Sales Specialist en Insight

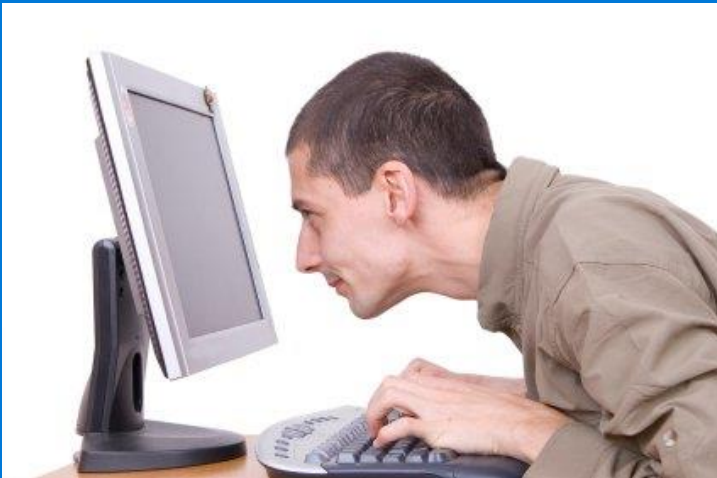
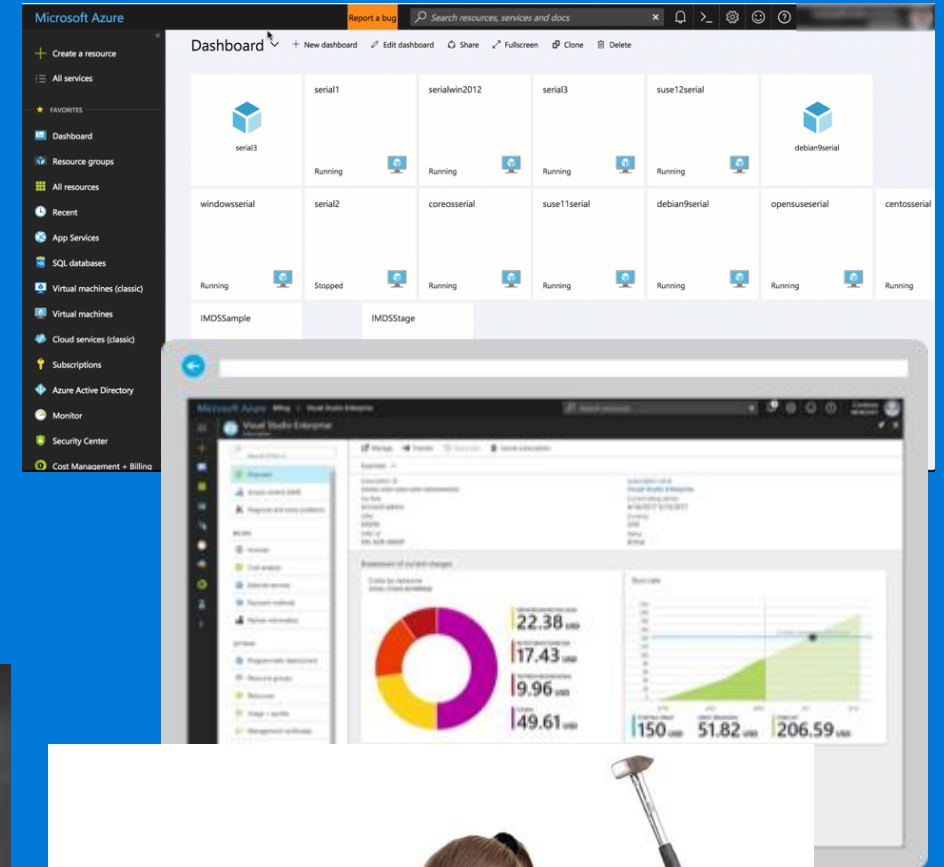
MVP Padrazo, Padre de los tres mosqueteros, esposo, y espíritu errante. Azure, Servicios de Infraestructura, Office 365.

MVP Cloud and Datacenter Management



Situación actual de un Cloud Admin

¿Que ocurre si queremos monitorizar múltiples suscripciones de Azure?
¿Y si además queremos añadir diversos Tenants?
¿Y si también queremos añadir diversos Dominios?
¿Y si tenemos múltiples herramientas y consolas para hacerlo?
¿Y si, para variar, tenemos 8 hora diarias para gestionarlo todo?



¿Qué hacemos?



 **ZMonitor Mobile 2**
Zone Soft Herramientas ★★★★★ 6
3 PEGI 3
Esta aplicación es compatible con todos tus dispositivos.
[Añadir a la lista de deseos](#) [Instalar](#)

ZMonitor Mobile v1.2
CENTRO DE PRODUCCIÓN DESBLOQUEAR PRODUCTOS LIMPIAR PEDIDOS DEFINICIONES

#20 00:00:02 B1	#21 00:00:32 B1	#22 00:00:47 B1
1 Salada de Chocos Sem tomate	1 Salada de Chocos Sem tempero Sem tomate	1 Salada de Chocos
1 Salada de Chocos	1 Salada de Chocos	1 Salada de Chocos
1 Salada de Chocos	1 Salada de Chocos	1 Salada de Chocos
1 Salada de Chocos	1 Salada de Chocos	1 Salada de Chocos
1 Salada de Chocos	1 Salada de Chocos	1 Salada de Chocos
1 Salada de Chocos	1 Salada de Chocos	1 Salada de Chocos
	1 Salada de Chocos	
	1 Salada de Chocos	
	1 Salada de Chocos	

Online (~71ms) zone

ZMonitor 2
Ligação ao Servidor SQL
Impressora
Aspecto e Personalização
Modo Take-Away
Configurações do modo Take-Away
Permitir recuperar pedidos
Permitir recuperar pedidos já completos, cancelar
Permitir limpar pedidos
Permitir limpar todos os pedidos dos centros visitados
Iniciar no arranque
Iniciar aplicação no arranque do dispositivo.




zMonitor



Microsoft / **zMonitor**

Watch 15 Unstar 24 Fork 11

<> Code Issues 2 Pull requests 1 Projects 0 Wiki Insights

Branch: master zMonitor / README.md Find file Copy path

 Springstone Grammar corrections 51502e0 on 31 May 2017

2 contributors  

93 lines (53 sloc) 5.07 KB Raw Blame History

zMonitor

An Azure platform native monitoring solution that enables Azure monitoring across multiple tenants or subscriptions.

Overview

Problem statement: A service provider with 50 tenants, each with Azure subscriptions provisioned through CSP (Cloud Solution Provider), needs to consolidate operational telemetry to optimize running costs, as well as deliver higher SLAs with a minimum amount of administrative overhead.

Enter zMonitor, a platform for reporting based on Log Analytics data collected, quickly gaining insights across tenants or subscriptions. Gain insights on disks capacity status, VM performance - over or under utilized CPU/Memory/Disk/etc, security vulnerabilities - failed logons, update/patch status, application errors, etc.

¿Por qué zMonitor?

Ventajas de zMonitor:

- Recopilación de información totalmente personalizada.
 - Eventos
 - Performance
 - Espacio en discos
 -
- Unificar monitorización de todos los servicios de Azure.
- Agnóstica al Tenant, a tu suscripción.
- Está basada en OMS.
- Se despliega con apenas 3 clicks.
- Es Open Source.
- Una opción buena, bonita y Barata



Basic tenant monitoring:

Component	Assumptions	Cost (monthly)
Log Analytics	3-4 VMs (Free)	\$ 0.00
Azure Automation	500 minutes (Free)	\$ 0.00
		\$ 0.00

Service Provider / Central

Component	Assumptions	Cost (monthly)
Azure Storage Account (BLOB)	10 GB stored	\$ 0.20
Stream Analytics	1 Unit	\$ 89.28
Azure Cosmos DB	2 GB stored, 400 RUs	\$ 24.31
Azure Automation	500 minutes (Free)	\$ 0.00
		\$ 113.78

Otras opciones

Ventajas frente a otras opciones:

- Event Hub
- Sentinel
- Otras soluciones de €€€€

Recopilación de registros de actividad de Azure en un área de trabajo de Log Analytics entre suscripciones en distintos inquilinos de Azure Active Directory

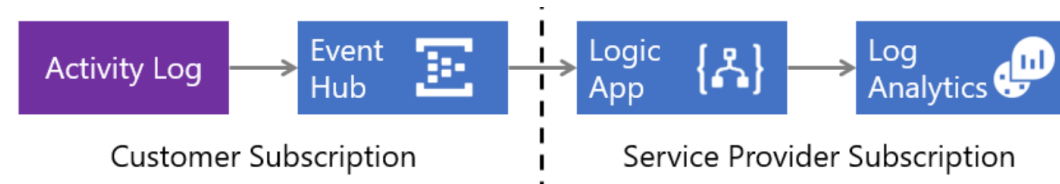
06/02/2019 • Tiempo de lectura: 10 minutos • Colaboradores 🧑

Este artículo se describe un método para recopilar registros de actividad de Azure en un área de trabajo de Log Analytics en Azure Monitor mediante el conector de recopilador de datos de Azure Log Analytics para Logic Apps. Siga el proceso de este artículo si necesita enviar registros a un área de trabajo en un inquilino distinto de Azure Active Directory. Por ejemplo, si es un proveedor de servicios administrados, puede que desee recopilar registros de actividad de la suscripción de un cliente y almacenarlos en un área de trabajo de Log Analytics en su propia suscripción.

Si el área de trabajo de Log Analytics está en la misma suscripción de Azure, o bien en una suscripción diferente, pero en la misma instancia de Azure Active Directory, siga los pasos de la [solución de registro de actividad de Azure](#) para recopilar registros de actividad de Azure.

Información general

La estrategia utilizada en este escenario consiste en que el registro de actividad de Azure envíe eventos a un [centro de eventos](#) en el que una [aplicación lógica](#) los remita a su área de trabajo de Log Analytics.



<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/collect-activity-logs-subscriptions>

Otras opciones

Ventajas frente a otras opciones:

- Event Hub
- Sentinel
- €€€€

Azure Sentinel

VERSIÓN PRELIMINAR

Un vigilante a su lado. Análisis de seguridad inteligente para toda su empresa.

Inicio gratuito >

[Información general del producto](#) [Características](#) [Introducción](#) [Documentación](#) [Clientes](#) [Preguntas más frecuentes](#) [Precios >](#)

Cree operaciones de seguridad de nueva generación con la nube e inteligencia artificial

Vea y detenga las amenazas antes de que causen daños, con tecnología SIEM reinventada para un mundo moderno. Azure Sentinel le ofrece una vista completa de su empresa. Aproveche el conocimiento de la nube y a gran escala que ha adquirido Microsoft durante décadas de trabajo en materia de seguridad. Utilice inteligencia artificial (IA) para detectar y responder a amenazas de un modo más inteligente y con más rapidez. Elimine la configuración y el mantenimiento de la infraestructura y escale los recursos de forma elástica para satisfacer sus necesidades de seguridad, al tiempo que reduce los costos de TI.



Recopile datos a escala de nube de todos los usuarios, dispositivos, aplicaciones y de toda la infraestructura, tanto en el entorno local como en diversas nubes.



Detecte amenazas que antes no se descubrían y minimice los falsos positivos usando análisis e información de amenazas sin parangón de Microsoft.



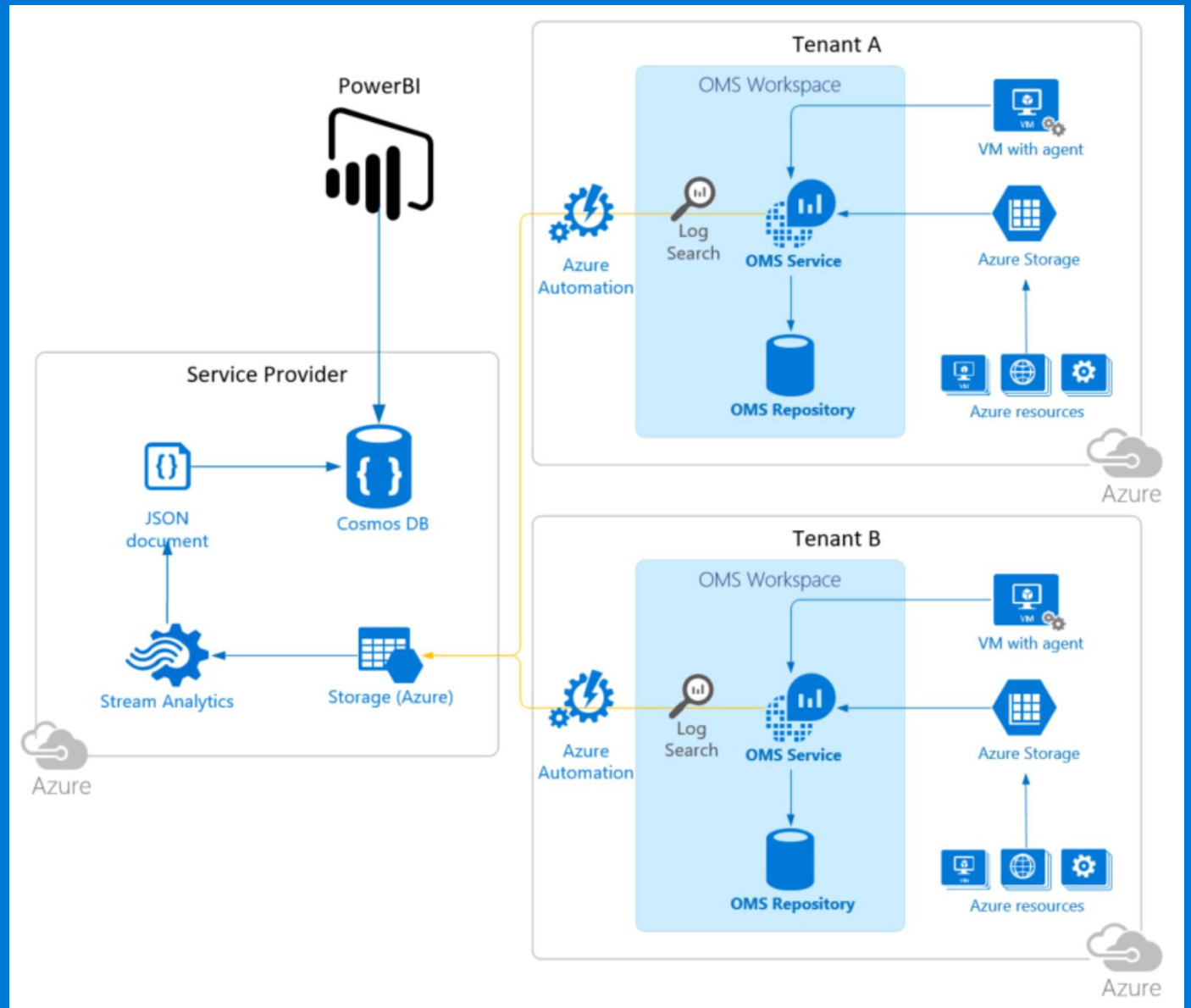
Investigue las amenazas con inteligencia artificial y busque actividad sospechosa a escala, aprovechando el trabajo en ciberseguridad que ha llevado a cabo Microsoft durante décadas.



Responda a los incidentes con rapidez usando la orquestación y la automatización de tareas comunes integradas.

<https://azure.microsoft.com/es-es/services/azure-sentinel/>

Arquitectura de zMonitor



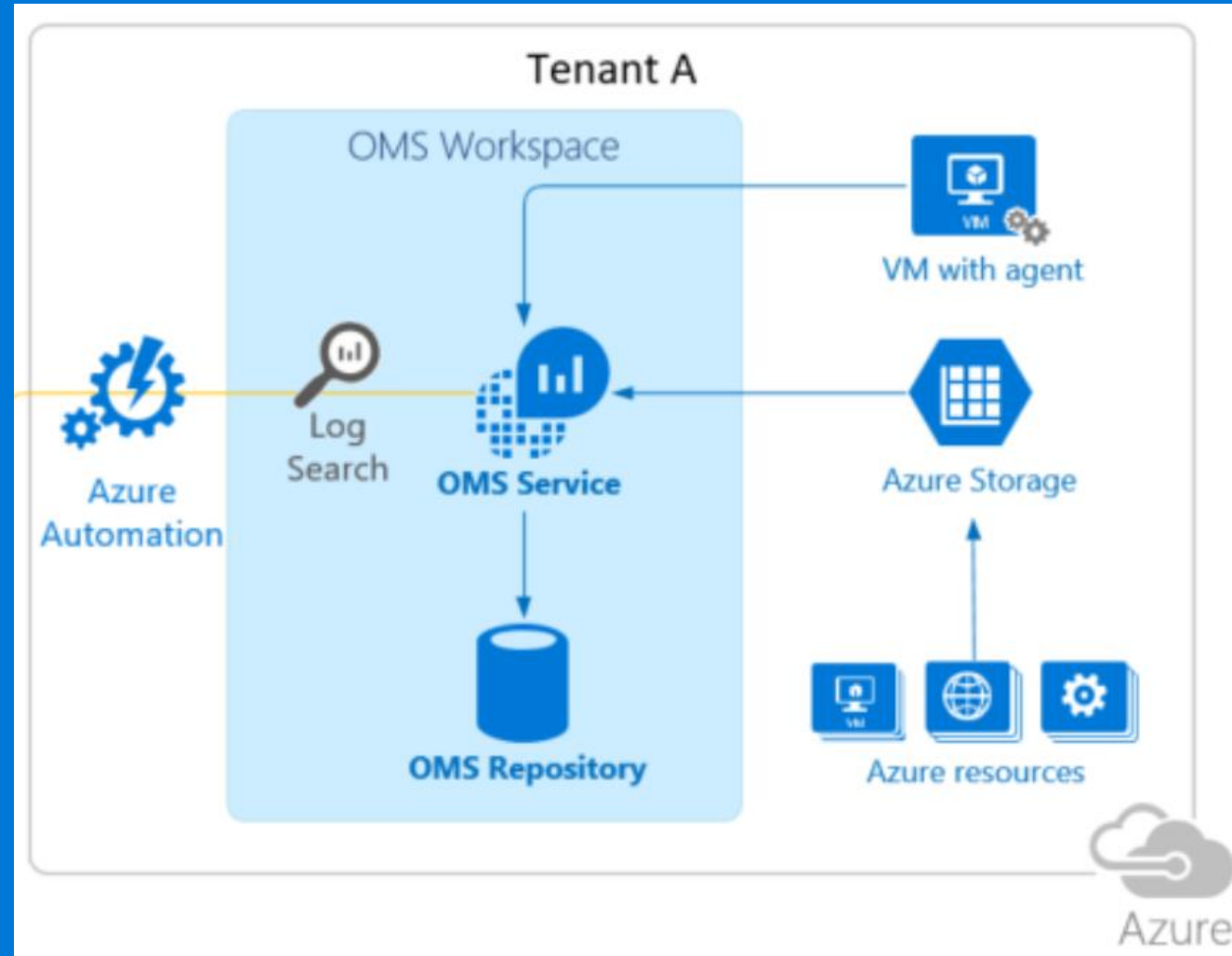
Arquitectura - Tenants

Tenant 1
Tenant 2















.....

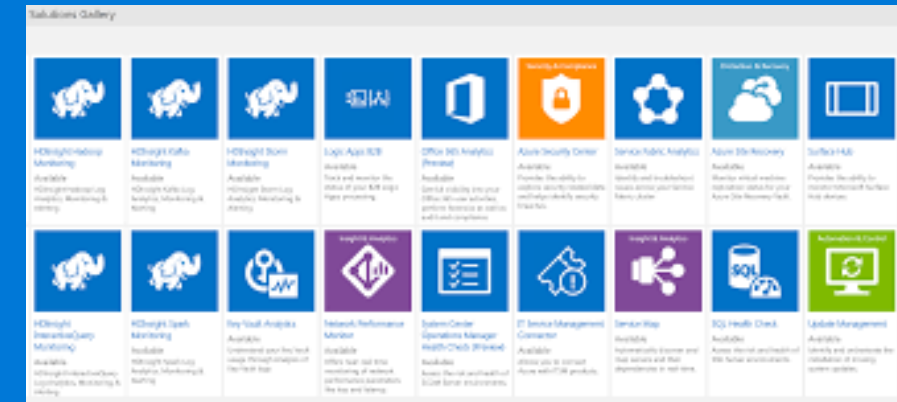
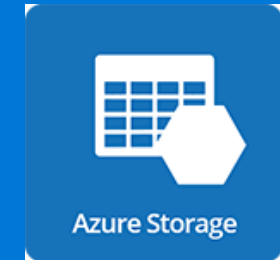
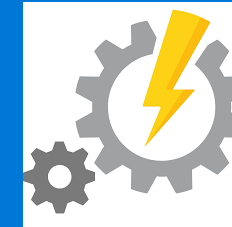
.....

Tenant n+1

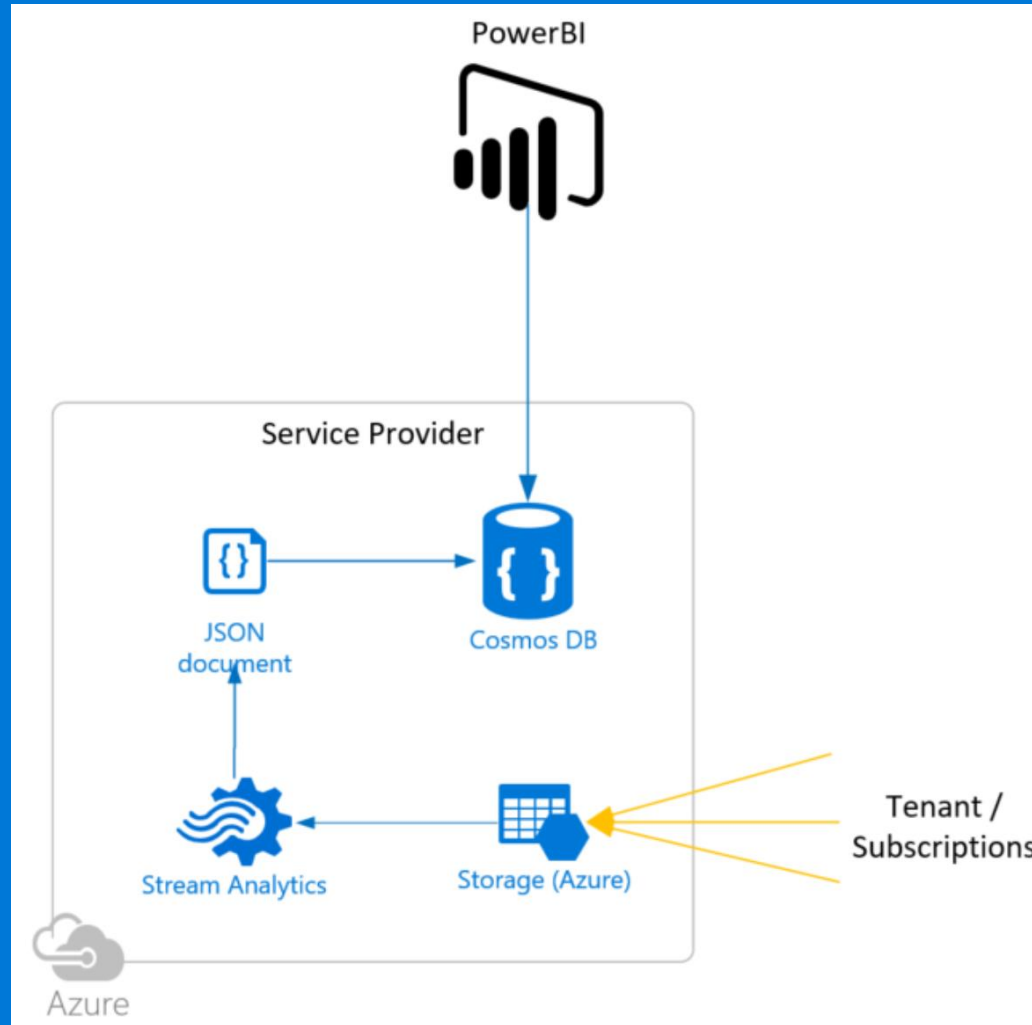


Arquitectura – Tenants - Componentes

NAME ↑↓	TYPE ↑↓
 ADAssessment(robertotejerohotmail)	Solution
 AgentHealthAssessment(robertotejerohotmail)	Solution
 asrj36esfeuft2ty	Storage account
 AzureActivity(robertotejerohotmail)	Solution
 AzureAutomation(robertotejerohotmail)	Solution
 ChangeTracking(robertotejerohotmail)	Solution
 robertotejerohotmail	Automation Account
 robertotejerohotmail	Log Analytics workspace
 RB-Ops-Daily (robertotejerohotmail/RB-Ops-Daily)	Runbook
 RB-Ops-Hourly (robertotejerohotmail/RB-Ops-Hourly)	Runbook
 RB-ProcessLogs (robertotejerohotmail/RB-ProcessLogs)	Runbook
 Security(robertotejerohotmail)	Solution
 Tenant	Recovery Services vault
 Updates(robertotejerohotmail)	Solution







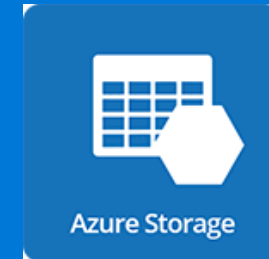
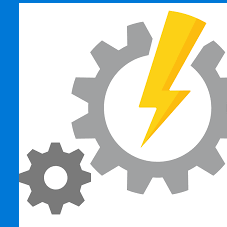
Arquitectura – Servicio Central



Arquitectura – Servicio Central - Componentes

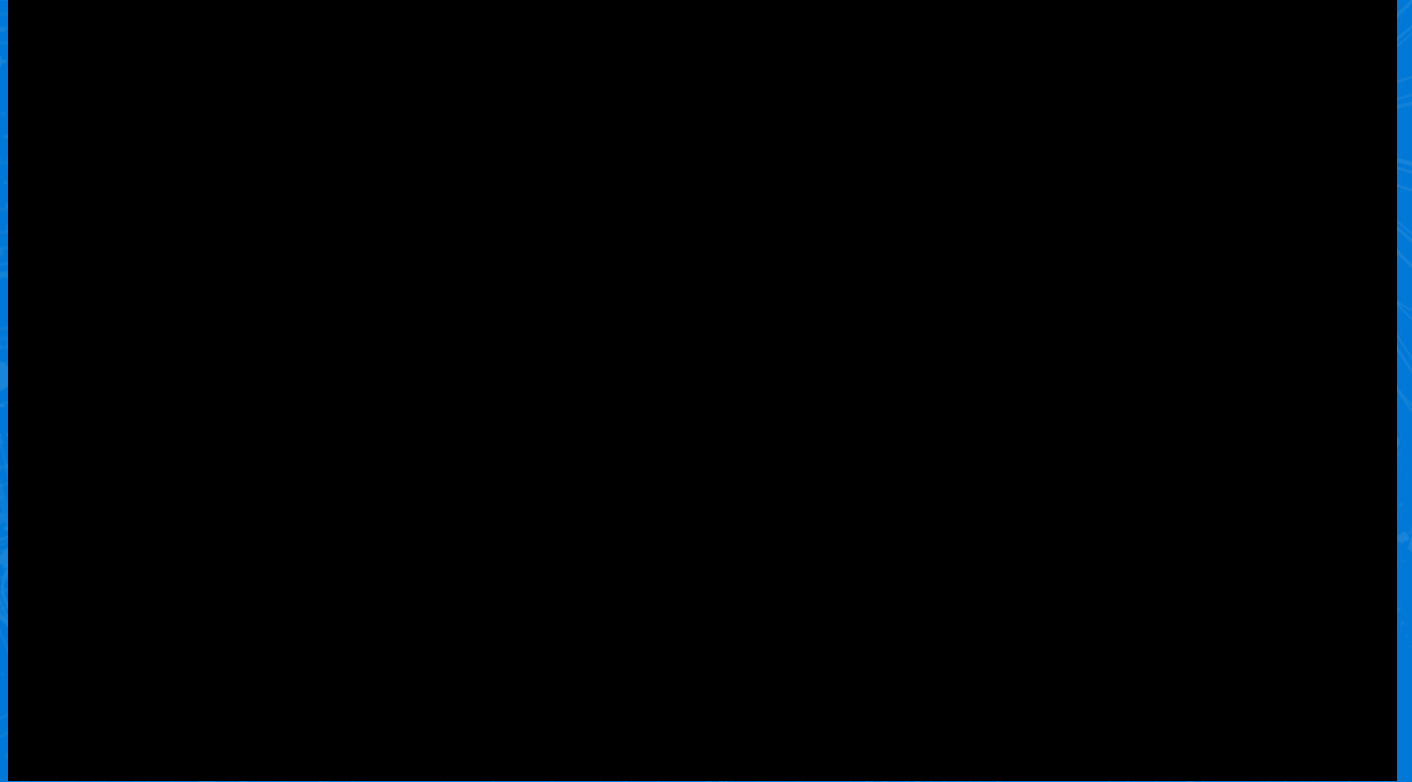
4 items ☐ Show hidden types ⓘ

<input type="checkbox"/>	NAME ↑↓	TYPE ↑↓
<input type="checkbox"/>	 servicecentralautomation	Automation Account
<input type="checkbox"/>	 zmonitorcentral	Storage account
<input type="checkbox"/>	 zmonitorcentraldb	Azure Cosmos DB account
<input type="checkbox"/>	 zmonitorlogprocessor	Stream Analytics job



Demo Time!!!!

zMonitor Kusto



¡Gracias!

Patrocinadores Locales



Colabora





2019

Global **Azure**
BOOTCAMP

