



#GlobalAzure
#GlobalAzureMilano



Trova e riduci i problemi in produzione adottando AIOps in Azure Monitor

Giulio Sciarappa – Head of Azure&AI @Lobra Futura

Sponsor

#GlobalAzure
#GlobalAzureMilano



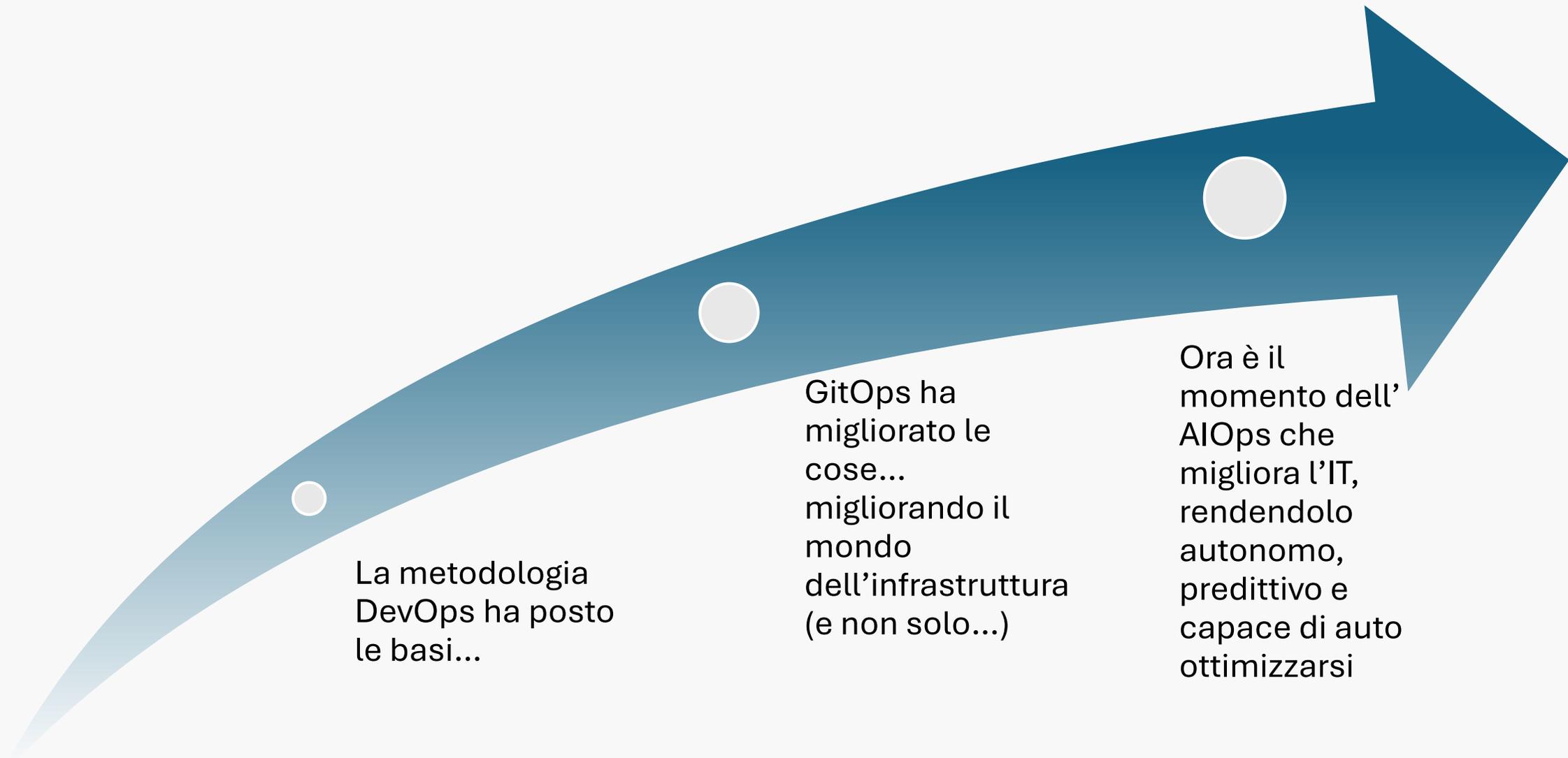
Monitoring (la sottile arte di avere tutto sotto controllo)

- Troppi log
- Difficoltà ad automatizzare processi
- Difficoltà nel trovare il problema



#GlobalAzure
#GlobalAzureMilano

DevOps -> GitOps... e ora AIOps



La metodologia
DevOps ha posto
le basi...

GitOps ha
migliorato le
cose...
migliorando il
mondo
dell'infrastruttura
(e non solo...)

Ora è il
momento dell'
AIOps che
migliora l'IT,
rendendolo
autonomo,
predittivo e
capace di auto
ottimizzarsi

Azure Monitor: la risposta a (quasi) tutte le domande!

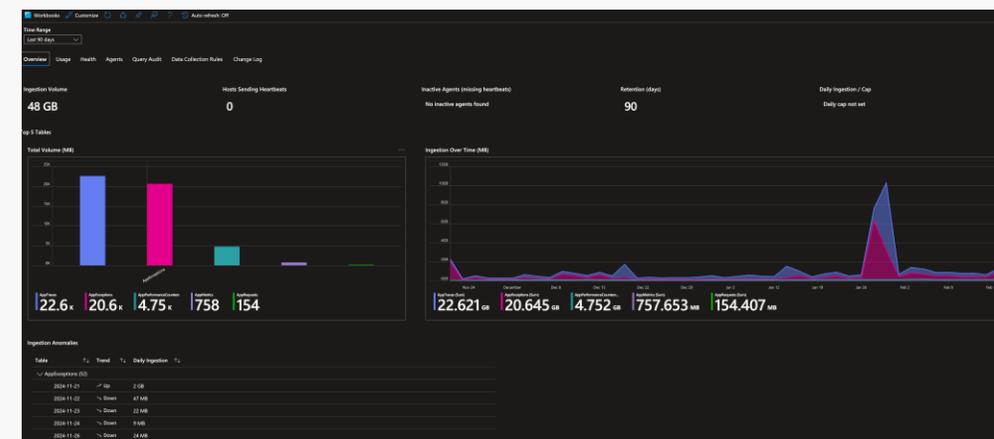
- Log Monitoring
- Application performance Monitoring
 - Metric Alerts
- Virtual Machine Scale Set

Azure Monitor: la risposta a (quasi) tutte le domande!

Azure Monitor mette a disposizione un intero set di funzionalità per analizzare i cosa sta succedendo all'interno del log workspace

Se ne può infatti:

- monitorare l'ingestione
- Scoprire anomalie
- Trovare le query più pesanti
- Controllare il funzionamento degli agent sulle macchine
- Etc...



Log Monitoring (Kusto Query Language time series analysis and machine learning functions)

#GlobalAzure
#GlobalAzureMilano

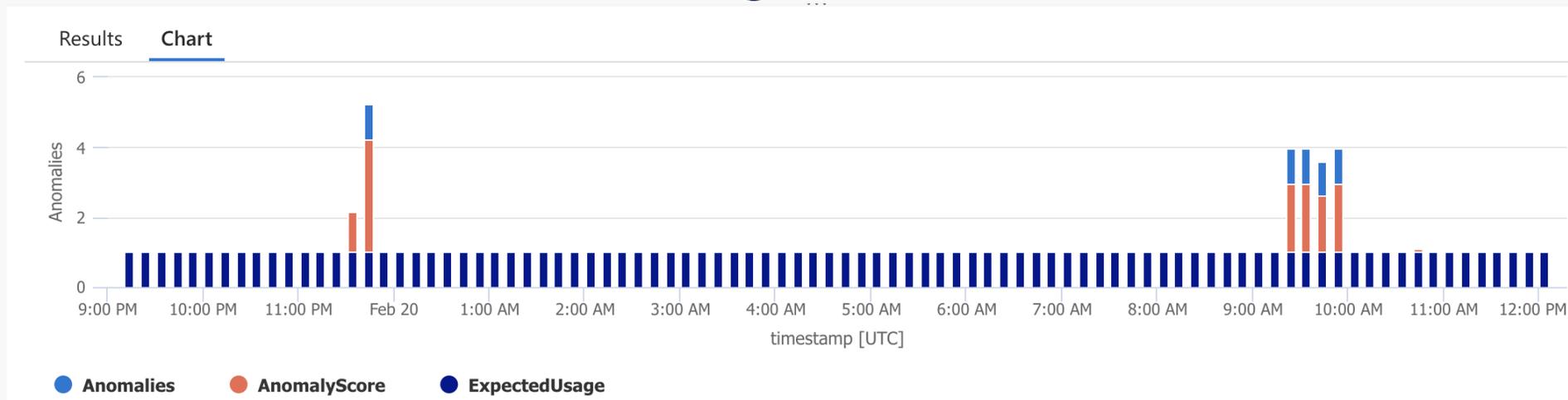
- Le time series permettono di analizzare attraverso un grafico temporale eventuali pattern nei log.
- Tramite il comando make-series si ottengono facilmente

```
| make-series Aggregazione = Funzione(valore)  
  [by Categoria]  
  on TimestampColumn  
  from Inizio to Fine  
  step Intervallo
```

Log Monitoring (Kusto Query Language time series analysis and machine learning functions)

#GlobalAzure
#GlobalAzureMilano

- Una volta ottenuta una time series possiamo applicare la funzione
- `series_decompose_anomalies(Serie, Threshold [, Method])`
- La funzione analizza la serie e ne estrapola le anomalie, dandogli uno score basato su trend, e stagionalità



Log Monitoring (Kusto Query Language time series analysis and machine learning functions)

#GlobalAzure
#GlobalAzureMilano

Altre funzioni che implementano ML

- **series_outliers():** Identificazione di anomalie nei dati.
- **series_fit_line():** Regressione lineare sulle serie temporali.
- **series_periods_detect():** Identifica i pattern ciclici.
- **series_fill_linear():** Interpolazione lineare per dati mancanti.

Log Monitoring (Copilot in Azure)

Copilot for Azure ci aiuta a gestire le nostre indagini nei log usando un linguaggio naturale

Use Case:

- Supporto nelle query Kusto al suo interno
- Cercare informazioni nelle subscription
- Avere informazioni su quanto si sta spendendo

What is the distribution of resource types across my subscriptions?

Copilot AI-generated content may be incorrect

Querying your [selected subscriptions](#) using Azure Resource Graph...

```
resources  
| summarize count() by type
```

Run

Copilot AI-generated content may be incorrect

Here is a snapshot of the distribution of resource types across your selected subscriptions:

Resource Type	Count
microsoft.network/connections	1
microsoft.insights/webtests	1
microsoft.insights/datacollectionrules	1
microsoft.network/localnetworkgateways	1
microsoft.operationalinsights/querypacks	1

This table shows only the first 5 of 52 total results. You can explore all the query results in the [Azure Resource Graph Explorer](#). The query was executed against your [selected subscriptions](#).

How can I view more details about a specific resource type?

Can you show me the distribution of resources in a specific subscription?

What are the most common resource types in my subscriptions?

I want to ...

0 / 500

Log Monitoring (Copilot in Azure)

#GlobalAzure
#GlobalAzureMilano

Ci sono dei limiti però...

Qualsiasi azione eseguita su più di **10** risorse deve essere eseguita all'esterno di Microsoft Copilot in Azure.

Puoi effettuare solo **15** richieste durante una determinata chat e hai solo **10** chat in un periodo di **24** ore.

Alcune risposte che visualizzano elenchi saranno limitate ai primi **cinque** elementi.

Per alcune attività e query, l'uso del nome di una risorsa non funzionerà e sarà necessario specificare l'ID risorsa di Azure.

Microsoft Copilot in Azure attualmente è disponibile solo in **inglese**.

Demo time!

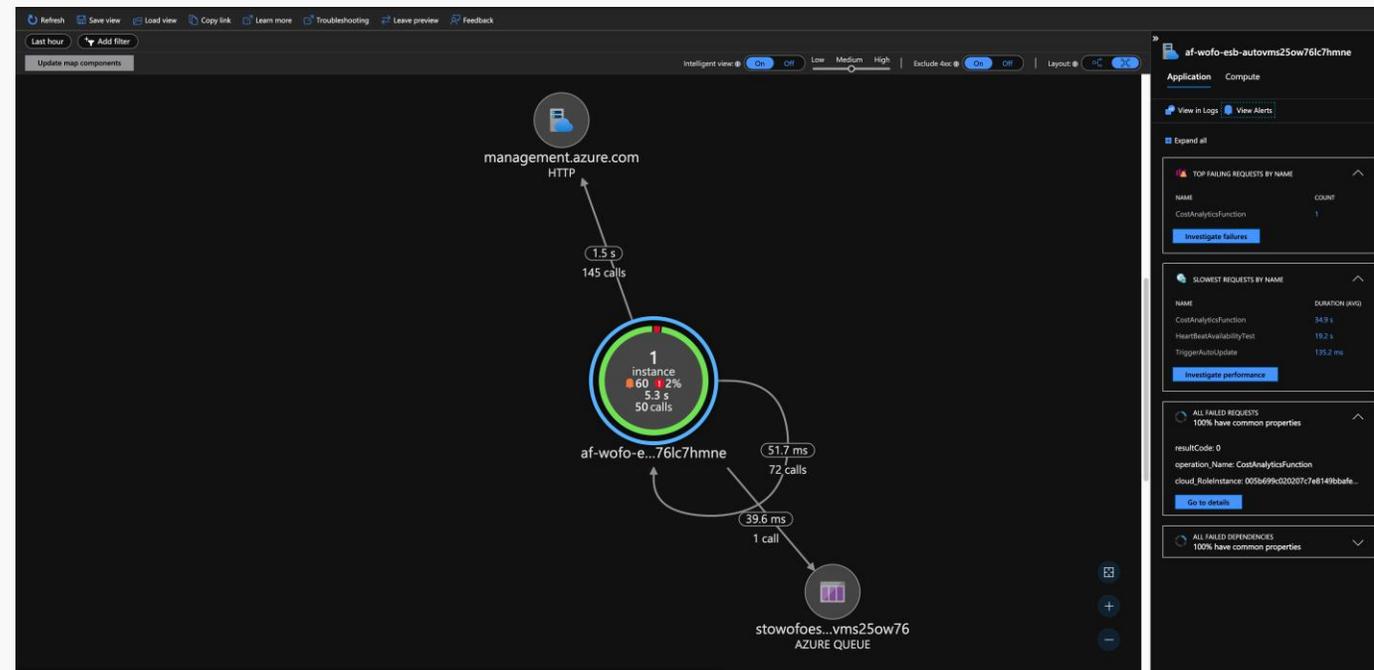


Application map intelligent mapping

Permette di analizzare le applicazioni distribuite attraverso la creazione (tramite ML) di mappe che evidenziano le connessioni tra i vari componenti

I componenti sono le parti dell'applicazione distribuita i cui log sono visibili a chi usufruisce del servizio.

Permette di andare in dettaglio sulle performance e gli errori riscontrati di ciascun componente, andando fino a livello di stack di chiamate

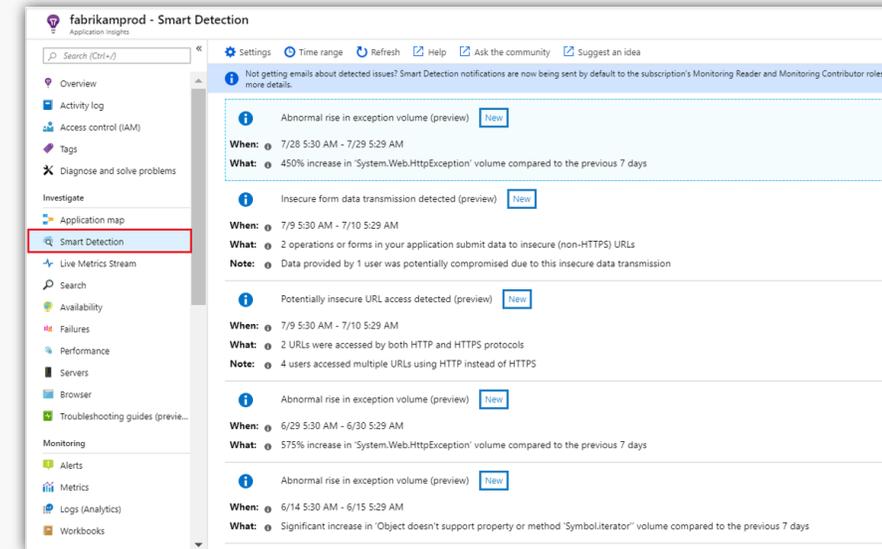


Smart Detection

Alerting + AI = Smart detection!

Se l'applicazione manda sufficienti informazioni l'AI andrà alla ricerca di:

- Pattern di errori e di sicurezza
- Mutazioni anomale nei log (molti di più del solito, ad esempio...)
- Problemi di performance
- Memory leak e molto altro...



Dynamic thresholds alerting

Se si è incerti su quali valori inserire negli alert,

Se non si conosce bene il pattern di comportamento della risorsa,

Se non si vuole creare tanti alert per tante risorse per controllare la medesima cosa (+ alert +€€),

Si possono usare le soglie dinamiche.

Utilizzano i dati degli ultimi **10** giorni per «apprendere» e applicare le soglie più adatte

The screenshot shows the 'Create an alert rule' interface in Azure Monitor, specifically the 'Condition' tab. The interface is dark-themed and includes the following elements:

- Scope:** Condition (selected), Actions, Details, Tags, Review + create.
- Configure when the alert rule should trigger by selecting a signal and defining its logic.**
- Signal name:** Server response time (selected from a dropdown menu). A link 'See all signals' is visible below the dropdown.
- Alert logic:** A blue information icon and text: 'We have set the condition configuration automatically based on popular settings for this metric. Please review and make changes as needed.'
- Threshold type:** Dynamic (selected with a radio button). Static is also an option.
- Aggregation type:** Average (selected from a dropdown menu).
- Value is:** Greater or Less than (selected from a dropdown menu).
- Threshold Sensitivity:** High (selected from a dropdown menu).
- Split by dimensions:** A section with a blue information icon and text: 'Use dimensions to monitor specific time series and provide context to the fired alert. About monitoring multiple time series'. Below this is a table with columns: Dimension name, Operator, Dimension values, and Include all future values. The table currently shows '0 selected' in the Dimension values column and an 'Add custom value' link below it.
- When to evaluate:** Check every: 1 minute (selected from a dropdown menu). Lookback period: 5 minutes (selected from a dropdown menu).
- Advanced options:** A section with a downward arrow and the text 'Advanced options'. Below it is a '+ Add condition' button.

Predictive Autoscale

Nelle VM scale set che hanno un carico periodico permette di gestire autonomamente eventuali anomalie di carico, prima che queste accadano

Utilizza i dati storici di circa 15 giorni (rolling window) per «addestrarsi» e richiede almeno 7 giorni di «addestramento»

L'autoscale «standard» è il riferimento in termini di quando e quanto scalare (oltre che essere un backup)

The screenshot displays the Azure portal interface for configuring a Virtual Machine Scale Set (VMSS). The left-hand navigation pane shows various settings categories, with 'Scaling' selected. The main content area is titled 'TestVMSS | Scaling' and includes a search bar and action buttons (Save, Discard, Refresh, Logs, Feedback). A notification banner at the top right states: 'New! Autoscale has added another powerful feature. Predictive autoscale (public preview). Learn more'. Below this, the 'Configure' tab is active, showing options for 'Scale-In Policy', 'Predictive charts', 'Run history', 'JSON', and 'Notify'. The 'Choose how to scale your resource' section offers two options: 'Manual scale' (Maintain a fixed instance count) and 'Custom autoscale' (Scale on any schedule, based on any metrics), with the latter selected. The 'Custom autoscale' configuration section includes fields for 'Autoscale setting name *' (TestVMSS-Autoscale-530) and 'Resource group' (TestVMSS_group). A dropdown menu for 'Predictive autoscale (public preview)' Mode is open, showing options: Disabled (selected), Enabled, Forecast only, and Enabled. A 'Default *' section shows 'Auto created scale condition' with an edit icon. A 'Delete warning' section at the bottom right contains an information icon and the text: 'The very last or default recurrence rule can turn off autoscale.'

Demo time!



Bonus: ML e AIOps

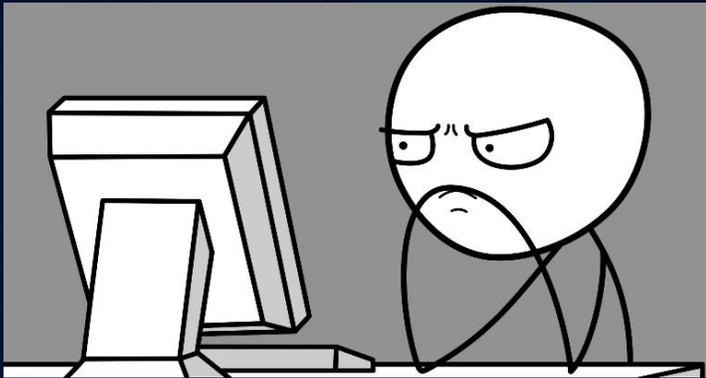
Ovviamente, con moli di dati importanti, KQL e Azure Monitor non bastano più.

Si può lavorare con i notebook oppure chiamare le API di Azure Monitor e poi lavorare i dati in formato PySpark/Pandas DataFrame

Oppure esportare direttamente in un blob storage i dati e da lì far partire la pipeline

	Funzionalità di Machine Learning KQL predefinite	Creare una pipeline di Machine Learning personalizzata
Scenario	<ul style="list-style-type: none"> ✓ Rilevamento anomalie, causa radice e analisi delle serie temporali 	<ul style="list-style-type: none"> ✓ Rilevamento anomalie, causa radice e analisi delle serie temporali ✓ Scenari avanzati di analisi e AIOps
Vantaggi	<ul style="list-style-type: none"> ◆ Introduzione rapida. ◆ Non sono necessarie competenze di data science né capacità di programmazione. ◆ Prestazioni ottimali e risparmi sui costi. 	<ul style="list-style-type: none"> ◆ Supporta scalabilità più grandi. ◆ Abilita scenari avanzati e più complessi. ◆ Flessibilità nella scelta di librerie, modelli, parametri.
Limiti del servizio e volumi di dati	Il portale di Azure o i limiti di query di log dell'API di query in base al fatto che si usi il portale o l'API, ad esempio, da un notebook.	<ul style="list-style-type: none"> ◆ Limiti di query di log dell'API di query se si eseguono query sui dati nei log di Monitoraggio di Azure come parte della pipeline di Machine Learning. In caso contrario, nessun limite del servizio di Azure. ◆ Può supportare volumi di dati di dimensioni maggiori.
Integrazione	Non necessari. Eseguire l'esecuzione con Log Analytics nel portale di Azure o da un Jupyter Notebook integrato.	Richiede l'integrazione con uno strumento, ad esempio Jupyter Notebook. In genere, è anche possibile integrarsi con altri servizi di Azure, ad esempio Azure Synapse Analytics.
Prestazioni	Prestazioni ottimali usando la piattaforma Esplora dati di Azure, in esecuzione su larga scala in modo distribuito.	Introduce una quantità di latenza di dimensioni ridotte durante l'esecuzione di query o durante l'esportazione di dati a seconda del modo in cui si implementa la pipeline di Machine Learning.
Tipo di modello	Modello di regressione lineare e altri modelli supportati dalle funzioni serie temporali KQL con un set di parametri configurabili.	Modello di Machine Learning completamente personalizzabile o metodo di rilevamento anomalie.
Costii	Nessun costo aggiuntivo.	A seconda del modo in cui si implementa la pipeline di Machine Learning, è possibile che vengano addebitati dei costi per l'esportazione dei dati, l'inserimento di dati con punteggio nei log di Monitoraggio di Azure e l'uso di altri servizi di Azure.
Esercitazione	Rilevare e analizzare le anomalie usando le funzionalità di Machine Learning KQL in Monitoraggio di Azure	Analisi dei dati nei log di Monitoraggio di Azure usando un notebook

Domande?





#GlobalAzure
#GlobalAzureMilano

GRAZIE!!!

Le slide saranno disponibili sulla pagina
Global Azure 2025 del sito di Azure Meetup Milano