NetEye

MONITORAGGIO IN TEMPO REALE GRAZIE ALL'INTELLIGENZA ARTIFICIALE

Con la rapida digitalizzazione delle aziende, la disponibilità dei servizi IT sta diventando prioritaria per garantire la continuità del business. Downtime non programmati non sono più contemplati, ma l'operatività va garantita 24x7. Gli amministratori IT devono essere in grado di individuare possibili disservizi ancor prima che possano avere un impatto per i processi aziendali. Ecco come AIOps supporta questi obiettivi.

PATRICK ZAMBELLI, NetEye Product Manager in Würth Phoenix

Monitoraggio in tempo reale grazie all' intelligenza artificiale

La trasformazione digitale sta cambiando il modo in cui le aziende operano. Nuovi prodotti e servizi necessitano che l'infrastrutture informatiche siano affidabili e sempre funzionanti. Ecco perchè business analytics e data lakes rivestono oggi un ruolo indispensabile per l'economia. Durante la rivoluzione industriale del XIX secolo il motto era „Le ruote devono continuare a girare". Oggi, analogalmente, l'IT deve sempre garantire la disponibilità ad alte prestazioni. Non è più accettabile avere tempi di inattività. Va garantita l'operatività dei servizi non solo all' interno del proprio data center ma anche attraverso cloud o provenienti da terze parti. In sintesi, una notifica inviata agli amministratori solo quando gli utenti stanno già tempestando l'help desk non ha ormai più alcuna efficacia. Ogni tipo di potenziale malfunzionamento deve essere identificato tempestivamente e risolto prima che possa avere impatti negativi sulla produttività degli utenti. L'adozione dell'intelligenza artificiale (AI) nel monitoraggio diventa quindi un passaggio obbligato. Il motto della nostra epoca è „**Intelligenza artificiale per l'IT Operations**" o semplicemente **AIOps**. Questo termine è stato coniato dal famoso centro di analisi e ricerca, Gartner: „Le piattaforme AIOps utilizzano grandi quantità di dati sulle quali compioni analisi attraverso machine learning e altre tecnologie avanzate per ottimizzare tutte le operazioni IT dirette ed indirette (monitoraggio, automazione e service desk) con approfondimenti proattivi, personali e dinamici."

Machine learning alla base di tutto

Gartner divide gli AIOps in cinque livelli consecutivi, diversamente complessi: eliminare i falsi allarmi, migliorare lo stato attuale, ridurre gli effetti, ridurre al minimo i tempi di inattività e in generale migliorare la gestione del servizio.

Patrick Zambelli
NetEye Product Manager in Würth Phoenix

NetEye
WÜRTHPHOENIX

Würth Phoenix S.r.l.
Via Kravogl, 4
39100 Bolzano
Italia

+39 0471 56 41 11

info@wuerth-phoenix.com
www.wuerth-phoenix.com/neteye

L'intelligenza artificiale ha un ruolo in tutti e cinque i livelli. Da un lato, AIOps si basa sul **machine learning** (ML) per riconoscere modelli nei dati di monitoraggio che **possono indicare incident o condizioni insolite**. D'altra parte, AIOps include l'intelligenza artificiale che prende decisioni in base alle informazioni ottenute. Esistono due approcci principali nell'apprendimento automatico: univariato e multivariato. L'analisi univariata valuta solo una serie di dati, ad esempio lo stato di carico di un processore. Richiede una potenza di calcolo significativamente inferiore rispetto a un'analisi multivariata, ma può già fornire risultati significativi. I carichi di picco e il loro verificarsi nel tempo ne sono un esempio. Tuttavia, i possibili risultati sono ancora troppo vaghi per poterne ricavare delle decisioni significative. Ci vuole molta esperienza per interpretare e leggere tali informazioni. Il problema è simile al monitoraggio classico: se si assume un valore medio che si presume rappresenti la normale operatività, eventuali anomalie non vengono rilevate, ad esempio a causa degli intervalli di tempo impostati. I picchi potrebbero essere annulati dai valori minimi attraverso il calcolo della media e rimanere inosservati. Questa problematica può invece essere risolta con le analisi multivariate che includono diverse metriche, come i carichi di picco di server diversi in relazione agli eventi di registro. Ad esempio, i carichi possono essere suddivisi in singoli carichi di lavoro. Un processo batch genera carichi di picco ciclici? Oppure ci troviamo in presenza di un attacco cibernetico? Collegando metriche diverse, il comportamento analizzato attraverso il monitoraggio può essere meglio interpretato e utilizzato come base per il processo decisionale. Tuttavia, si dovrebbe notare che le analisi multivariate non sono del tutto migliori o possno sostituire quelle univariate. L'analisi di metriche diverse richiede molte risorse e molto tempo. In pratica, le analisi multivariate completano le analisi univariate quando si debbano analizzare situazioni specifiche che richiedono analisi più precise.

NetEye
WÜRTHPHOENIX

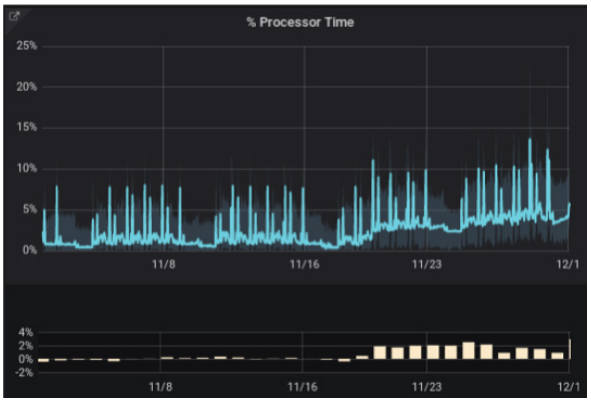
Würth Phoenix S.r.l.
Via Kravogl, 4
39100 Bolzano
Italia

+39 0471 56 41 11

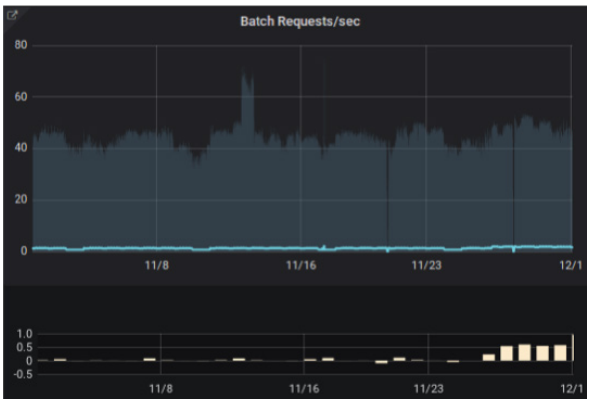
info@wuerth-phoenix.com
www.wuerth-phoenix.com/neteye

Maggior comprensione: l'utilizzo di più metriche

In pratica viene visualizzato nel seguente modo:



Il carico del processore aumenta in modo lineare e viene raffigurato atttravero la curva blu del grafico. L' andamento successivo invece mostra l'aumento del carico della CPU rispetto alla settimana precedente.



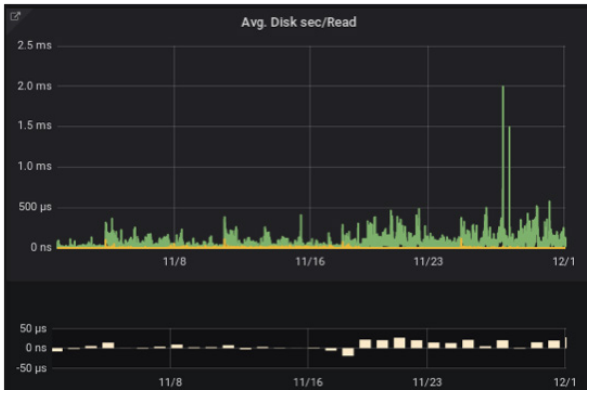
Tuttavia, le richieste in processi batch non mostrano un amento significativo, poichè attraverso il calcolo die valori medi questa variazione non viene percepita.

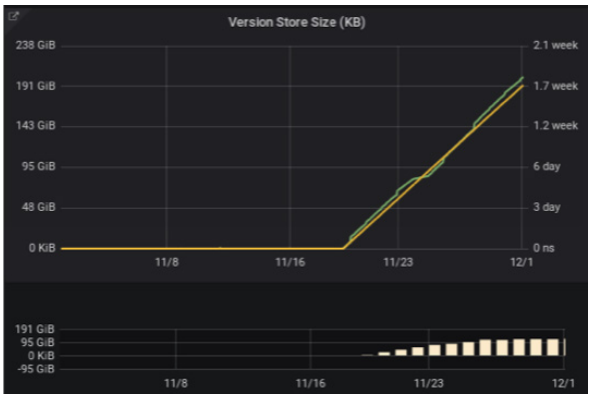
NetEye
WÜRTHPHOENIX

Würth Phoenix S.r.l.
Via Kravogl, 4
39100 Bolzano
Italia

+39 0471 56 41 11

info@wuerth-phoenix.com
www.wuerth-phoenix.com/neteye





Un'analisi congiunta con la latenza del disco rigido, del version store size e della longest running transaction mostra un quadro più preciso e spiega in modo più dettagliato l'utilizzo del processore – in questo caso andrebbe fatto un controllo del database e della configurazione corrispondente . L'intelligenza artificiale è in grado di filtrare tali costellazioni dai dati di monitoraggio e presentarli graficamente per una miglior comprensione da parte degli amministratori, permettendo di identificare in modo più veloce e semplice la fonte dell'errore. Inoltre, **l'intelligenza artificiale può cercare modelli replicabili per suggerire attivamente una soluzione** collaudata anche in situazioni simili o addirittura agire in autonomia per singoli casi.

NetEye
WÜRTHPHOENIX

Würth Phoenix S.r.l.
Via Kravogl, 4
39100 Bolzano
Italia

+39 0471 56 41 11

info@wuerth-phoenix.com
www.wuerth-phoenix.com/neteye

Anche il SIEM può beneficiarne

Queste casistiche non si applicano solo alle operazioni IT. L'approccio dell'analisi dei dati di monitoraggio tramite l'intelligenza artificiale può essere utilile anche per l'IT security. Anche nel **security information and event management (SIEM)** si devono analizzare e aggregare grandi quantità di dati provenienti da diverse fonti. Tutti i dati di monitoraggio disponibili devono essere considerati per identificare possibili anomalie relative alla sicurezza e alla protezione dei dati. Ed anche in questo caso la sfida consiste nel riuscire a filtrare grandi moli di dati e renderli comprensibili per gli amministratori. Non è sempre così immediato e semplice identificare correttamente eventi complessi come un incident di sicurezza. Nel caso di eventi complessi, la combinazione di singoli eventi non critici potrebbe in realtà celare possibili problemi. I rispettivi eventi non devono necessariamente essere in una relazione immediatamente riconoscibile tra loro. Senza l'utilizzo delle tecniche di machine learning e dell'intelligenza artificiale, un intervento rapido e mirato nel SIEM è possibile solo nel caso si possegga una vasta esperienza e si abbia a disposizione un considerevole periodo di tempo.
Il valore aggiunto in una soluzione SIEM deve per forza di cose essere la flessibilità e la completa personalizzazione di ogni parametro. Entrambi aspetti che all'interno della soluzione di Würth Phoenix sono presenti. E che configurati con il corretto tuning possono permettere di avvisare chi di dovere prima che il guaio diventi così profondo!

Conclusione

Il machine learning e l'intelligenza artificiale hanno un impatto significativo su tutte le aree delle nostre vite e del nostro lavoro. L'IT non fa eccezione. Le moderne soluzioni di monitoraggio come **NetEye di Würth Phoenix utilizzano queste tecnologie per semplificare le attività di controllo** e prevenzione che i reparti IT devono compiere. Senza un

NetEye
WÜRTHPHOENIX

Würth Phoenix S.r.l.
Via Kravogl, 4
39100 Bolzano
Italia

+39 0471 56 41 11

info@wuerth-phoenix.com
www.wuerth-phoenix.com/neteye

supporto tecnologico, è semplicemente impossibile soddisfare i requisiti attuali e futuri che le aziende impongono al settore informatico. Ad oggi, questi sistemi sono in grado di supportare l'analisi delle cause di possibili disservizi filtrando e valutando le informazioni disponibili. Si può presupporre che le soluzioni di monitoraggio semi-autonome non tarderanno ad arrivare. Ciò che è certo, tuttavia, è che **AI e AIOps non possono sostituire il tradizionale APM** (Application Performance Monitoring). Piuttosto, AIOps diventa un potente strumento che aiuta i dipendenti IT durante le loro attività quotidiane per identificare e affrontare i problemi in modo più rapido e preciso. **L'esperienca e l'intervento umano rimarrà comunque indispensabile** ancora a lungo.

Intelligenza artificiale e machine learning

I termini intelligenza artificiale (AI), machine learning (ML) e deep learning (DL) sono spesso usati in modo intercambiabile. In realtà, compongono diversi lati della stessa medaglia: il machine learning è il metodo matematico utilizzato per estrarre informazioni dai dati esistenti. Ad esempio, un server presenta picchi di carico insoliti. L'utente decide quali dati vengono elaborati e con quale algoritmo. L'intelligenza artificiale analizza le informazioni generate per poter prendere delle decisioni. Nel caso di carichi di picco, , ad esempio, genera l'allarme automatico per gli amministratori. Al contrario del machine learning, il deep learning utilizza una cosiddetta rete neurale, che decide quali informazioni vengono trasmesse e in che modo esse vengano ponderate. Il deep learning agisce come un cervello umano e richiede molta capacità di elaborazione: il programma AlphaGo, che ha ottenuto successi sensazionali nel gioco Go nel 2017, utilizzava una rete di computer con oltre 1000 CPU.

NetEye
WÜRTHPHOENIX

Würth Phoenix S.r.l.
Via Kravogl, 4
39100 Bolzano
Italia

+39 0471 56 41 11

info@wuerth-phoenix.com
www.wuerth-phoenix.com/neteye