(ops) logix

EZalert

Optimized Alert Intelligence

White Paper

Copyright

Table of Content

"Optimized Alert Intelligence"

OpsLogix introduces EZalert, a software solution based on sophisticated machine learning algorithms that can be trained to classify alerts and filter out potential alert storms caused by false positives. This keeps the Active Alerts view of the Operations Manager console free of irrelevant alerts.

Introduction

The ability to maintain service health is crucial for any business or industry reliant on its IT infrastructure. Every enterprise relies on its underlying services and applications for everyday business and user productivity.

System Center Operations Manager (OpsMgr) is a powerful monitoring and reporting tool that is capable of monitoring thousands of servers, applications and clients and delivering a comprehensive view of the health of an IT environment. This includes the fabric monitoring of cloud deployments. OpsMgr checks the performance and availability of each object within an IT infrastructure and alerts administrators to potential problems.

The alerts or operational health states, are color-coded much like standard traffic lights, with green being healthy (optimal), yellow indicating warning and red being a critical issue. In addition to the alerts mentioned, OpsMgr can also generate informational alerts. Health state thresholds can be configured per object and alerts offer possible root causes or corrective action using knowledge base articles that greatly increase troubleshooting resolution speed.

Complex IT infrastructures mean that initial OpsMgr deployments can result in a very "chatty" Alerts view, where administrators may be bombarded by daily alert storms caused by false positives that are not of true service or application critical relevance.

OpsLogix EZalert is able to learn and mimic systems administrator behavior setting resolution states, including of course closing alerts in SCOM. Using sophisticated machine learning algorithms, EZalert can be taught to recognize alerts by evaluating the specific alert properties and corroborate this with the behavior of the systems administrators. After being trained and activated, EZalert will proceed to automatically close or process alerts caused by false positives presenting administrators with an Alerts view of relevant business-critical services and applications.

OpsLogix – EZalert Community

This white paper is written for policy makers, IT managers and IT administrators who work for any enterprising company with an IT infrastructure. A prerequisite is that the company uses Microsoft System Center Operations Manager.

- System Center Operations Manager 2012 SP1, R2 and 2016

EZalert and Legal Compliance and Security

All OpsLogix products are developed with the same standard security policies that are dictated to Microsoft and are compliant to the (USA) Federal Cyber Security policy. Additionally, OpsLogix products make use of FIPS (Federal Information Processing Standard) compliant encryption in all its Management Packs and software.

OpsLogix EZalert

It is a well-known fact that the biggest practical hurdle with new OpsMgr deployments is the large number of false positive alerts that may be generated in the Active Alerts view.

The Operations Manager framework enables the monitoring of a vast scope of applications, components, devices, hardware and software systems, all of which end up, in their relevant health state in the OpsMgr console. Initially, administrators may painstakingly go through, what may literally be 100s, if not 1000s of alerts in order to check their validity and close them according to critical service and application relevance.

However, when the alerts return on a daily basis and users confirm that critical business applications and services are still operational, all too often, this results in OpsMgr email rules being set up and monitoring alert messages being sent directly into a folder and ignored. In the worst cases, system administrators start ignoring the OpsMgr Alert view itself because:

"*The environment is running fine but my Active Alert view is always full of yellow and red alerts*".

When the systems administrator is called by someone in Billing and Finance who says they are unable to use a particular application or an onsite engineer calls in to say they can't control a pipeline valve, the use of Operations Manager has, to all intents and purposes, failed.
The situation has been allowed to escalate a degree where it demands a reaction as opposed to acting on relevant alerts in a proactive manner thereby preventing downtime.

It unjustifiably demotes OpsMgr to being an expensive post-analysis tool rather than maximizing its full potential as a powerful all-encompassing proactive monitoring tool.

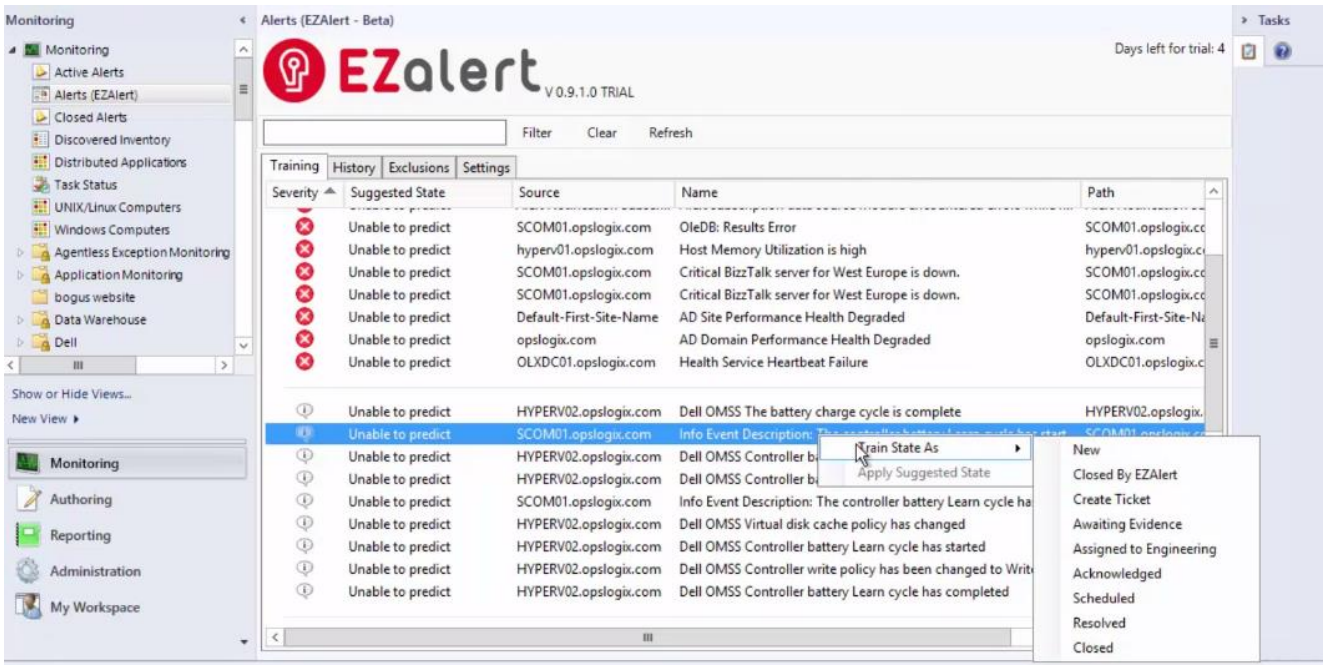
OpsLogix believes in providing simple logical solutions to optimize practical functionality in IT environments. EZalert is a trainable software tool powered by machine learning algorithms designed to enhance the use of Operations Manager.

Its objectives are, to increase early Operations Manager adoption rates by being able to capture tuning knowledge and logic and apply this directly to the operation of OpsMgr itself. EZalert will embolden proactive action by filtering out monitoring alert "spam" and always presenting administrators with relevant business-critical application and service alerts.

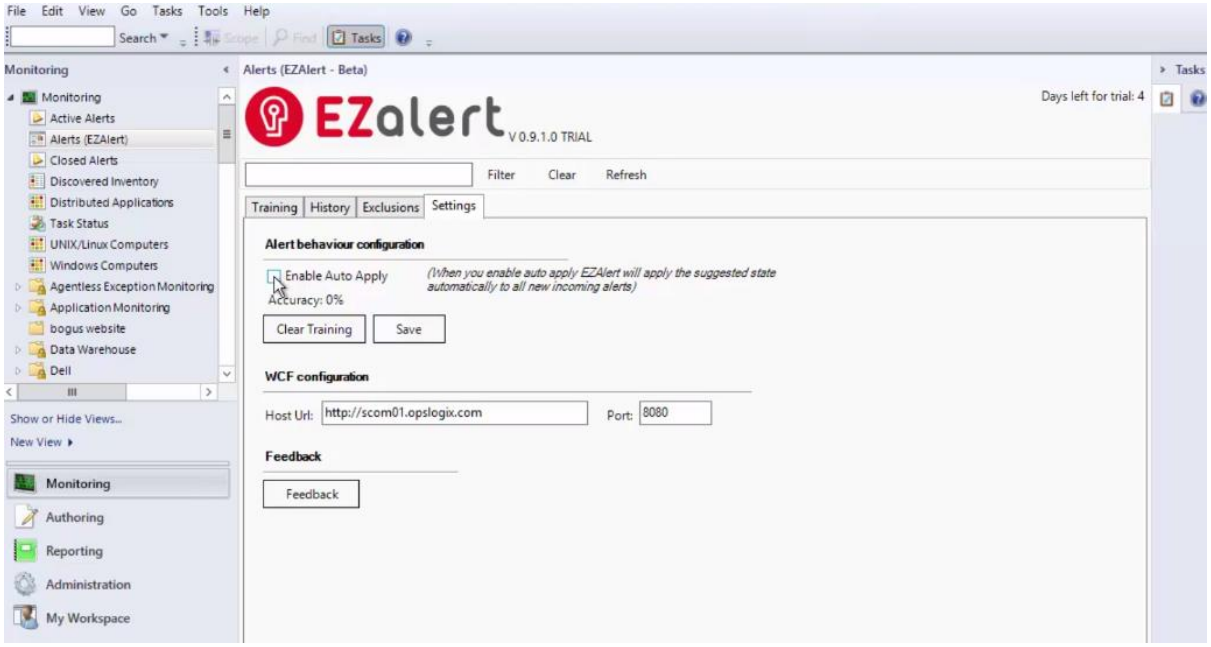
Functional Solution

System Center Operations Manager is a superbly powerful monitoring tool. Its seamless compatibility with the Operations Management Suite means that it is the perfect all-in-one solution for any business enterprise that is looking to the future.

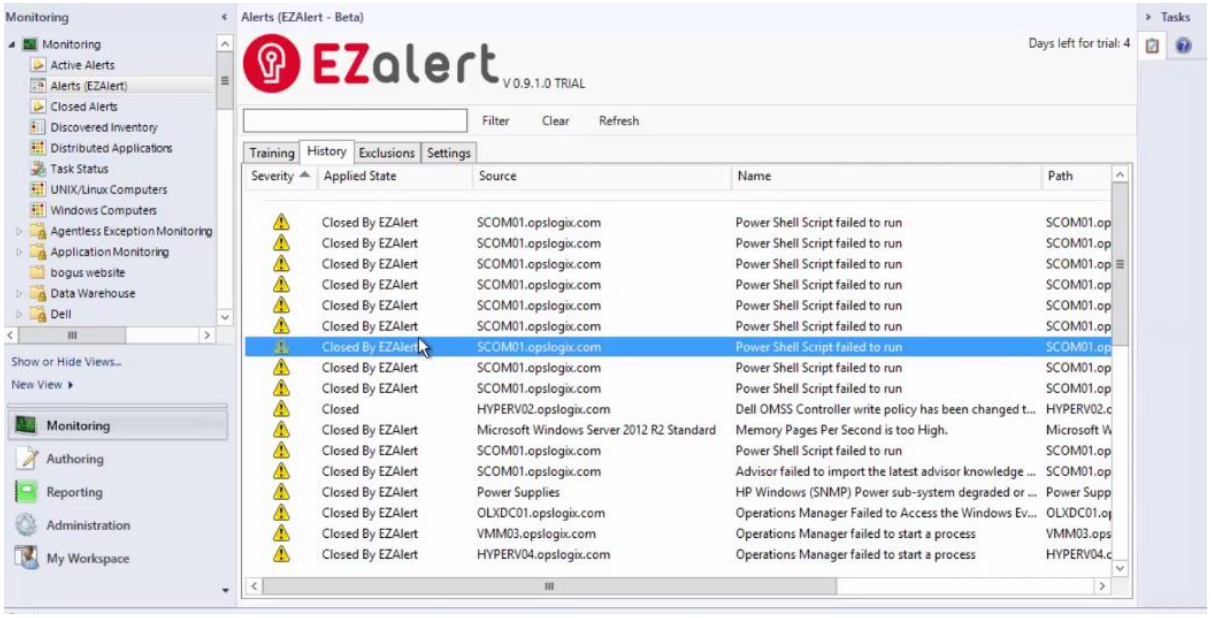
EZalert is aimed at fully optimizing the use of OpsMgr as the powerful deep-dive monitoring tool that it is. By filtering out alert storms caused by false positives and "chatty" MPs it heightens alert awareness and encourages proactive administrative action.



The more time and care invested in the training of EZalert, the more effective it will be in assisting system administrators in their daily activities.



The Alert accuracy percentage and choosing to apply and enforce a particular behavioral pattern can be found in the Settings tab.

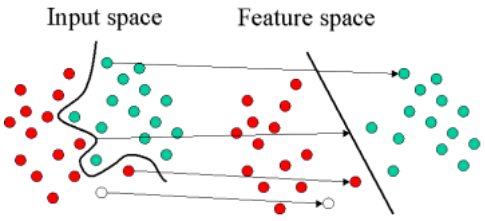


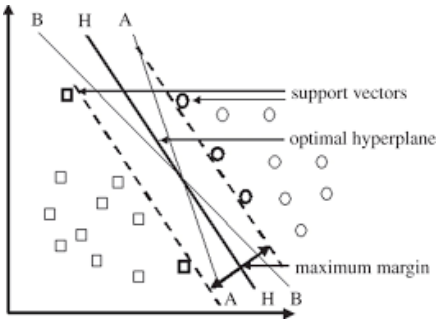
The History tab grants an overview of the behavioral tuning decisions and an Exclusions tab displays chosen alerts that will be excluded from the EZalert scope and always comply to specifically configured or default OpsMgr behavior.

Technical Solution

EZalert is based on machine learning algorithms. Machine learning is a subfield in computer science that has evolved from the study of pattern recognition and computer learning model theories. It's the foundation of artificial intelligence, or AI, and gives computers the ability to learn without being explicitly programmed. It explores and constructs self-learning algorithms that can learn how data is handled and from there make predictions on the data.

The machine learning logic of EZalert is based on are Support Vector Machines, or SVMs. This learning model analyzes data used for classification and regression and assigns the data into one of the categories. An SVM model is not based on probability, it is a binary linear classifier.





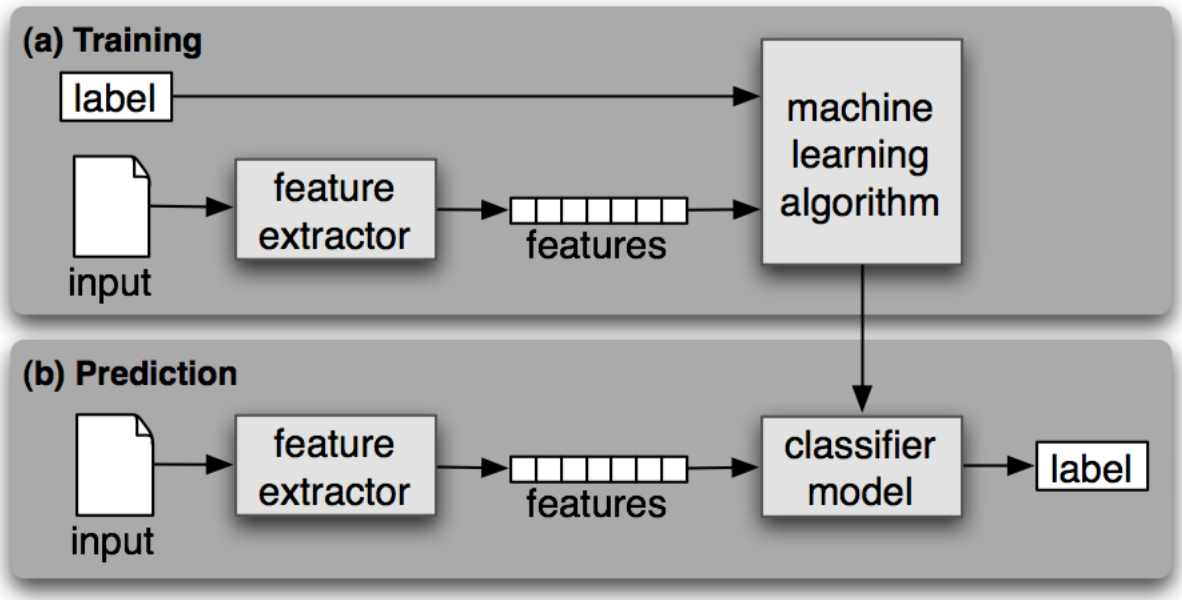
The SVM model is based around points in space that occupy an area where there is a clear gap between 2 categories. New points or variables are then mapped into the space and predicated to belong to a category depending on its defining parameters.

Classification is based on choosing the correct class label for a given input. In basic classification tasks each input is isolated from all other inputs, the classifying parameters being already defined. Variants include:

- multi-class classification, where inputs are assigned multiple labels
- open-class classification, where inputs have no clear stand-alone definition and classification is based on timing or volume
- sequence classification, where inputs are jointly classified

Classifiers fall under 2 types of learning, supervised and unsupervised learning. Both classifiers follow a set protocol or manual defining how inputs should be labeled. This may result in something as straightforward as color coding by corresponding color, i.e. red goes with red, blue goes with blue etc. To more complex steps such as determining whether the word 'bank' refers to a 'river bank', tilting to the side, or a financial institute. A supervised

classifier needs to be trained in order to establish its logic base. The EZalert logic is a supervised multi-class classifier.



(a) During training, a feature extractor is used to convert each input value to a feature set. The feature sets capture the basic information about each input that are used to classify it. Pairs of feature sets and labels are fed into the machine learning algorithm to generate a model.
(b) During prediction, the same feature extractor is used to convert unseen inputs to feature sets. These feature sets are then fed into the model, which generates predicted labels.

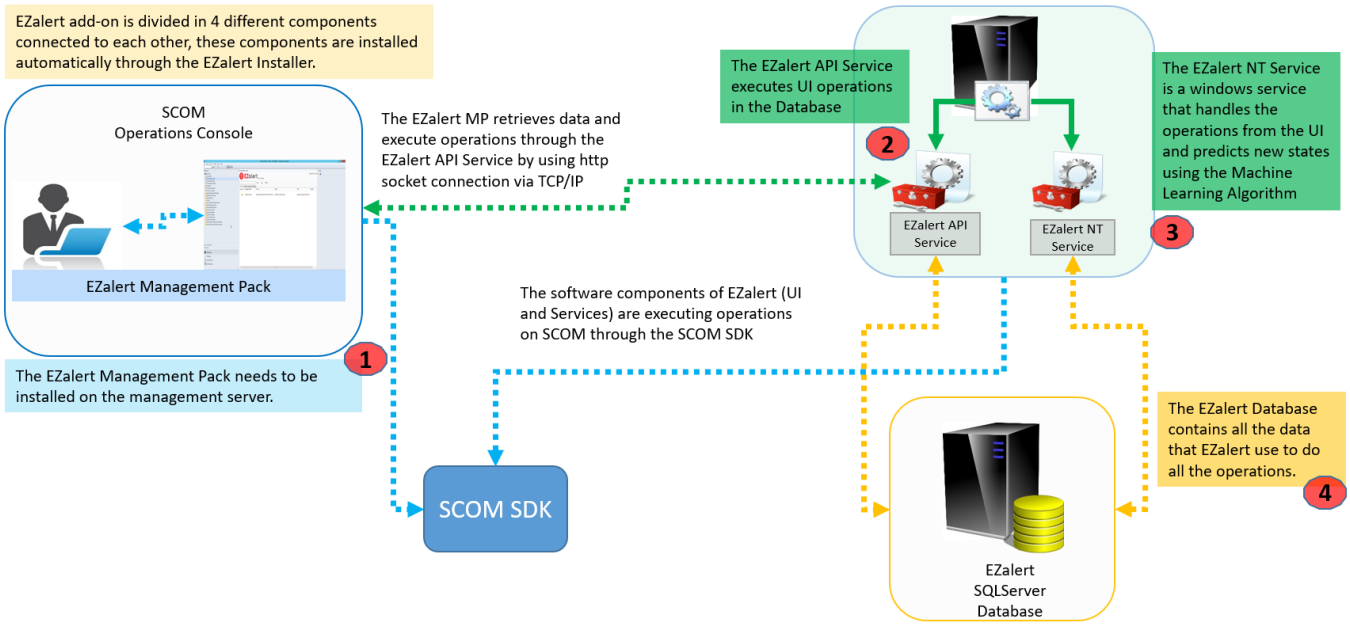
The more precisely a model is trained, the more accurate its predictions. Similarly, the longer a classifier model is used, the larger its knowledge (data)base becomes.

Microsoft®
System Center
Operations Manager

Operations Manager enables end users to improve their availability and performance metrics through enhanced service level monitoring, while their IT operations staff are able to have the improved access key functionality that they need to maintain and enhance the service they deliver to their end users. The product delivers capabilities that extend the value of existing Operations Manager customers already see in their Windows Server deployed applications to UNIX and Linux. End users are also able to meet their service level agreements doe applications in the data center in3 core areas:

- End-to-end Datacenter Service Management
- Best of breed monitoring for Windows and beyond
- Increased efficiency and control

EZalert architecture is based on 4 components:



These add-on components are:

- **EZalert Management Pack** contains the UI for OpsMgr. This is where users can train the EZalert tool, follow alert history as well as exclude alerts that should not be processed by EZalert. The Settings tab displays the configuration of alert behavior, its accuracy (measured by percentage), the WCF configuration and a Feedback button.
- **EZalert API service** is a WCF Windows service that facilitates the data flow between the EZalert tool and the EZalert SQL database. The API sends and receives data through the protocol TCP/IP web socket (not the web API).
- **EZalert NT Service** is a Windows Services and core of the EZalert add-on. The EZalert NT Service runs the data cycles and AI flow of EZalert.
- **EZalert Database** has 6 tables and stores the data used by EZalert add-on.

EZalert is designed to maximize ROI with System Center Operations Manager. By training the tool to recognize false positive alerts and best-practice behavior, EZalert is capable of preventing alert storms and streamlining daily OpsMgr administrative tasks thereby increasing monitoring efficiency.

Benefits

Optimize IT

EZalert optimizes IT by successfully delivering a solution that will help administrators filter through the false positive alerts and alert storms that OpsMgr can produce. It presents OpsMgr administrators with an Active Alerts View that contains immediately relevant alerts enabling immediate proactive resolution.

Decrease operational risk

There is an increasing amount of legalization and standardization that IT organizations will have to meet both now and in the future. OpsLogix Management Packs and software are in compliance with (USA) Federal Cyber Security policy. FIPS encryption in OpsLogix products reduce data security risk factors.

Reduce costs

EZalert reduces costs by optimizing OpsMgr alert management. By knowing which alerts impact key business processes and services and identifying how these can resolved in the most cost-effective way, EZalert directly contributes to decreasing TCO (total cost of ownership).

Conclusion

The OpsLogix EZalert tool is a software solution that assists successful IT monitoring and thereby proactive management through OpsMgr. EZalert provides administrators with an intelligent trainable alert filter for OpsMgr. Its key feature is in enhancing an existing System Center Operations Manager infrastructure and delivering a simple optimized means of alerts management.