White Paper

How Evolven IT Operations Analytics Works

This document provides a technical description of how the Evolven Analytics approach works including information on the Evolven knowledgebase, various information dimensions, and how Evolven analyzes configuration over time and across environments.

EVOLVEN

TABLE OF CONTENTS

Managing Complexity and Dynamics in Today's Environments

Evolven collects extremely detailed configuration and bill-of-material information across all the layers of IT environments (application, middleware, databases, infrastructure etc.) and across different types of environments (pre-production, production and disaster recovery). Evolven analyzes this information over time identifying changes and across environments identifying differences. Due to the very granular nature of the collected information changes and differences detection yields significant amounts of results. The purpose of analytics is to narrow down these results to the specific changes and differences relevant for the particular use case where analytics are applied.

Change and Difference Detection

Evolven analyzes collected information in two dimensions – over time and across environments. Over time analysis investigates multiple dimensions of changes to environment configuration and bill-of-materials including but not limited to a time dimension, distribution of changes across different types of environments, criticality and impact of changes etc. Analysis across environments investigates differences between configuration and content of comparable software and infrastructure components running on the same server or device, different servers and devices that are part of the same IT environment, different environments such as pre-production, production and disaster recovery. Evolven can combine two types of analysis investigating differences within or between environments over time. An example of such analysis could be a comparison of current configuration of a production server having some issue with a historical "golden baseline" configuration of a server of the same type.

Evolven Analytics Architecture

Investigation of changes and differences by Evolven Analytics rely on three main pillars:

Knowledgebase

Evolven provides an out-of-the-box knowledgebase for a number of commonly used technologies such as operating systems (e.g. Windows, Red Hat Linux, AIX, etc.), databases (e.g. Oracle, MS SQL, Sybase, etc.), messaging infrastructure (e.g. Tibco, Websphere MQ, etc.), application servers (e.g. Websphere, Weblogic, JBoss, etc.), web servers (e.g. IIS and Apache) etc. This knowledgebase contains information on potential impact and severity of change to most configuration parameters in the supported technologies.

The impact is divided into a number of pre-defined categories including performance, availability, functionality, security etc. As an example, a change in a locking policy of an Oracle database is a major change that can impact functionality, performance and availability of a business system using this database. This information on potential criticality and impact of a change is kept in the knowledgebase. The knowledgebase can be customized by Evolven users allowing them to update out-of-the-box criticality and impact assessment as well as add information for parameters not listed specifically in the knowledgebase. The content of the knowledgebase is created, maintained and enhanced by industry experts collaborating with Evolven. This way Evolven ensures scalability, quality and relevance of the collected knowledge.

Statistic algorithms

Evolven IT Operations Analytics employs several statistic algorithms. One of the algorithm types gets the combination of granular changes and differences into groups related by certain context. The purpose of such grouping is to simplify the review of large sets of changes and differences. For example, let's say over a 24 hour period Evolven detects 1,000 changes in the production environment, the analytics then identifies that 800 of this 1,000 is related to Windows hotfixes and updates. By grouping all of them together, the analytics makes it easy to review the remaining changes.

Frequency analysis of the Analytics algorithms

Other analytics methods can be applied to the changes group, like consolidating Windows updates to ensure that these updates were implemented consistently across all the relevant servers in the production environment. This type looks for certain patterns that can help to identify anomalies or to categorize information as noise.

Heuristic analysis methods

Heuristic analysis is based on Evolven's understanding of change processes and experience with typical configuration problems. An example of this method is consistency analysis. In many cases the same change is deployed across a number of servers, devices or environments. For example, a change can be deployed in a cluster, Also a change can be first deployed in pre-production for testing and only then in production etc. Consistency analysis relies on an assumption that risk from a change that was deployed inconsistently only on part of the servers or deployed differently is much higher than the risk of a consistent change

Filtering Analysis Results

The analysis process can include filtering steps that are applied for intermediate analysis. Filtering narrows the analysis results down to a particular area of interest that can be used as a final result or as a basis for further steps in the analysis process. Filters can be applied for each dimension of change and difference information like time period, name and type of environments where the changes were detected, their severity and impact, configuration sources and many more. Evolven also filters for hidden results associated with noise such as insignificant changes, changes with frequently toggling values etc.

Multi-dimensional Breakdown of Analysis Results

Analytics allows for the breakdown of filtered or unfiltered change and difference information by each of the analytics' dimensions. These dimensions include inherent properties of change and difference information (e.g. source environment, configuration item that changes, changed configuration parameter, type of change etc.) or certain properties calculated through statistic or heuristic methods (consistency of the changes, its' frequency, authorization of the changes etc.) The results of the break down can be further broken down allowing Evolven users to focus on narrow sets of changes or differences relevant for their use case.

For example the first tier of production support can break down change information covering the several hours leading up to an incident to identify what types of environment components were changed in the environment where incident was reported. Knowing these components the IT team can hand off the investigation to the second support tier, who can break down the results set, first looking for unauthorized changes and then for high priority changes, estimating priority by leveraging Evolven's knowledgebase. The resulting changes can be clustered, then automatically grouped into related context groups to identify subsets that can be associated to the investigated incident.

Fine-tuning of Evolven IT Operations Analytics

Evolven IT Operations Analytics can effectively process environment information right out-of-the-box using a built-in knowledgebase and other types of algorithms. Based on the understanding of monitored IT environments, gradual fine-tuning of the knowledgebase and analysis rules can quickly improve efficiency of the analysis. A number of simple actions can be done via the user interface when carrying out the analysis process, adding virtually no overhead while reducing noise and increasing the accuracy of the analysis results:

- Re-classification of detected changes or classification of changes not matching out-of-the-box knowledge
- Marking expected changes
- Setup of matching rules between comparable environments.

Correlation with Other Types of Data

Evolven collects specifically detailed environment configuration and bill-of-material. Valuable insights can be derived strictly from this information. At the same time correlation with other types of IT information can create additional analytics dimensions, leading to more effective insights.

For example, such additional data types could be log information, performance and availability monitoring metrics, transaction monitoring data etc. Correlation of changes with server login events from the system log will help to pinpoint the likely culprits are who made the changes. Correlation of the change information with performance and availability data allows IT teams to be more accurately determine which changes caught by the system or application performance monitoring tools could be at the root cause of an incident.

About Evolven

CORPORATE HEADQUARTERS
2500 Plaza 5, 25th floor,
Harborside Financial Center
Jersey City, NJ 07311
Email: info@evolven.com.
Tel: 1-888-841-5578
UK: +44 (0) 20-3002-3885

R&D CENTER
16 Ha'Malacha St.
Rosh Ha'Ayin, 48091 Israel
Email: info@evolven.com
Tel: +972-77-777-5999
Fax: +972-77-777-5900

Evolven's IT Operations Analytics provides intelligent answers to key IT operations challenges: how to accelerate incident resolution, how to avoid harmful and risky changes, and how to assess and optimize IT operations performance.

Evolven's new analytics approach to the chronic change & configuration challenges dramatically minimizes the risk of downtime and slashes incident investigation time.

Leading industry analysts have recognized Evolven for "transforming change and configuration management" and as the "Industry's most adaptive change management analytics."

Evolven was recently named a "2013 Cool Vendor in IT Operations Management" by Gartner, Inc.

Evolven is a privately held company headquartered in the U.S. and has a development center in Israel. Evolven's executive team and advisory board include world-renowned experts from the world of enterprise software. Evolven is backed by leading venture capital firms: Pitango (www.pitango.com) and Index Ventures (www.indexventures.com).

See more about Evolven at www.evolven.com and follow updates at @evolven.