Technical Brief

Evolven Architecture

This document provides an overview of the Evolven architecture, focusing on lack of agent overhead, minimal impact on the network, the absence of security risks, and how Evolven handles complex networks where segments are physically separated.

EVOLVEN

TABLE OF CONTENTS

Agent based Evolven Architecture

Evolven Agents collect configuration information, querying various environment components through the interfaces provided by these technologies. So for example, part of a Windows configuration is collected querying WMI, part – analyzing Windows configuration files, and part – registry. Information collection for each such component is driven by its configuration model (application definition in Evolven's language).

The models include a set of dynamic rules describing the architecture of the component configuration. An example of such a rule could be that an application stores its configuration in XML files under a folder where it was installed. Following this rule, the Evolven Agent will scan the installation folder of the application recursively searching for XML files and parsing them, except for the cases when these files do not look like a configuration. So for example, if an XML file has a size of tens of megabytes it probably does not hold configuration information. All the parsed information is consolidated, normalized and then transferred to a central Evolven repository.

Evolven provides out-of-the-box models for numerous commonly used technologies such as operating systems, databases, application servers, web servers etc. Starting with common technologies supported by Evolven out-of-the-box allows Evolven to understand an organization quickly and generate operational value from the first day of setup.

INTELLIGENT COLLECTION ON SERVERS

Evolven agents have an intelligent collection mechanism, architected to capture dynamic configuration information. Agents don't just grab a configuration file or issue API queries to pull the configuration, rather it is more discerning about the collection. From a performance perspective, Evolven Agents are highly sensitive towards resource consumption. Every agent has a limited amount of CPU and memory it consumes, while collecting environment information. By default, an agent consumes up to 5% of the total server CPU and 128Mb of memory, CPU is only utilized when the agent is actively collecting. These thresholds are configurable and can be controlled from Evolven's administration console for specific agents, a group of agents or all of them.

When the overall CPU usage on a scanned host exceeds a designated percentage, meaning that the system could be overloaded, the agent automatically shuts down, ensuring that all the resources are diverted to the business system.

In addition to collection, timing can be controlled to avoid clashing with critical business activities. Agents can be run on demand, run 24x7, or by a custom schedule. Users can create time windows in which the agent is permitted to run so that for any other time period the agent will be in 'sleep' mode, not consuming any of a scanned machine's resources.

All these capabilities make the agent an intelligent mechanism, highly aware that it is functioning in a landscape where the business systems have the highest priority.

INTELLIGENT OPERATIONS ON THE NETWORK

With Evolven collecting tens and hundreds of thousands of parameters on every system, sending every single parameter each time over the network would significantly slow network operations. Instead Evolven agents act intelligently to limit impact to the network by applying a piecemeal approach.

After an original snapshot is taken, collection is only done incrementally. Evolven agents only collect new information when a higher level environment object is different. Only deltas are collected and sent to an Evolven Server over the network. For example, if a configuration file hasn't changed there's no reason for the Agent to parse it again. The benefit of such an incremental approach is speed of collection with minimum overhead.

The Evolven agent collects environment information in two stages:

- **Initial collection:** the agent initially collects and parses all of the configuration data on each monitored server. Though the data amounts vary in accordance to the applications installed on the machine, in general Evolven collects between 10Mb to 50Mb of configuration information from each machine. This information is transmitted to the Evolven server in chunks over the course of the initial scan, taking anywhere from just minutes to several hours depending on the size of configuration and CPU threshold.

- **Sequential change detection:** following the initial scan the agent only sends to the server the parameters that changed. This means that only a few kilobytes of information are sent in each scan, making for a very low impact on the network.

SECURITY CONSIDERATIONS

From a security perspective, the Evolven agent collects information in 'read-only' mode. It doesn't change, write to or remediate any files. Evolven is focused on providing information, and it does not update any of the components in the monitored IT environments.

The agents communicate with the Evolven server using secure HTTPS protocol. A customer can provide their own SSL certificates to control the agent to server authentication. In addition, credential based agent authentication can be configured. If that communication approach is not sufficient, there is an option following collection for additional encryption of sensitive configuration information.

For handling situations in complex networks where segments are physically separated, Evolven can collect information locally. The agent generates an XML file with the collected results, thus later this file can be transferred and uploaded to an Evolven server.

Configuring Support for Custom/In-House Applications

Evolven discovers and collects detailed configuration out-of-the-box for numerous common technologies (operating systems, databases, application servers, web servers etc.). Evolven also captures applications deployed on top of application servers without any customization efforts. However Evolven does not have any prior knowledge of an application or technology developed internally by an organization, in-house. In this case a new application configuration model should be defined. For most organizations, there is a 90-10 ratio for 'out of the box' Evolven capabilities versus additional customization requirements.

In order to define a custom application configuration, Evolven provides a GUI based modeling wizard, allowing users to define basic collection processes without any technical expertise required. Examples of such basic collections can be:

- Picking configuration files under certain directories
- Collecting from registry, from database tables etc.

Evolven recognizes and automatically handles common types of configuration such as XML, INI, properties and other types of configuration files. Evolven can model more sophisticated situations, for example when some parameters in configuration files refer to another set of configuration files or some databases or API queries should be issued to extract configuration information.

Taking, a gradual implementation approach and leveraging 'out-of-the-box' capabilities first, more elements can incrementally be added to Evolven's capabilities as users gain experience with Evolven. For example, for leveraging an external script, or carrying out a special parsing of a configuration file, users will need to apply scripting skills. However, organizations that need to implement these collections typically have those skills in-house.

Most importantly, Evolven's guiding principle is to collect as much as possible environment configuration then narrow down analysis results to minimal and effective actionable data sets. This means that users do not need to spend time handpicking configuration information for collection. Many of applications are modeled successfully just by telling Evolven to build a complete bill-of-material of the application environment while looking for all the possible configuration files

About Evolven

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.