



# **eG Suite**

---

***A virtual Private Monitoring and  
Optimization Solution for Multi-Domain IT Infrastructures***

W h i t e P a p e r



### **Restricted Rights Legend**

The information contained in this document is confidential and subject to change without notice. No part of this document may be reproduced or disclosed to others without the prior permission of eG Innovations Inc. eG Innovations, Inc. makes no warranty of any kind with regard to the software and documentation, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

### **Copyright**

© Copyright 2003 eG Innovations. All rights reserved. eGurkha and eG ASPLite are trademarks of eG Innovations. All other trademarks, marked and not marked, are the property of their respective manufacturers. Specifications subject to change without notice



## Monitoring of Multi-Domain Internet Environments – An Overview

The last few years have witnessed a radical shift in the way Internet servers are operated and managed. Many corporations and enterprises have begun to outsource the hosting, monitoring, and maintenance of their servers with specialized Internet Data Centers (IDCs) and Managed Service Providers (MSPs). Even within a large enterprise, the IT department that operates and maintains the IT infrastructure often functions as a service provider to the other departments. Often, while the service provider is responsible for the hardware, the network, and software infrastructure, the actual service operating on the hosted servers is the responsibility of the customer.

The presence of multiple, independent domains of control and responsibility poses interesting challenges in operating and maintaining outsourced Internet services.

- The performance of a service depends on the network, system, and application components that it uses. Since the network and system components are the responsibility of the service provider, and the maintenance of the application components is the responsibility of the customer, there is very often a lot of finger pointing when a problem occurs. Faced with severe competition, service providers have had to expend a lot of resources in troubleshooting problems, in order to ensure customer satisfaction.
- A second complication in multi-domain environments is that different customer servers and applications can be hosted in the same network. Sometimes, different customer applications may even be supported on the same hardware (such a configuration is often referred to as shared hosting). Usage, performance, and availability measurements pertaining to a customer's IT infrastructure is perceived as being sensitive information that cannot be revealed or shared with other customers.
- In other cases, the different customer systems may be in different domains, probably using different IP address ranges. To protect the integrity of the customer environments, these systems may even have private, internal IP addresses that are not accessible from the global Internet. Consequently, a monitoring system for multi-domain environments must be capable of monitoring environments with multiple demilitarized zones, each with a set of IP private addresses.

Traditionally, monitoring systems have been viewed as a cost-center, being mostly used to improve the efficiency and internal operations of enterprises and corporate IT departments. Since most monitoring systems are internally focused, service providers have used these systems primarily for their internal operations. Typically, customers of the service providers do not have a real-time view of the status and performance of their services and servers. Instead, they have to be content with weekly and monthly reports mainly focused on server and network usage.

Many existing monitoring solutions do not handle the challenges posed by the multi-domain nature of today's Internet/Intranet environments. Furthermore, these solutions lack the ability to clearly demarcate whether a problem is caused in the customer domain or in the hosting provider's domain. Faced with severe competition, many service providers are also looking to offer new, value-added monitoring and optimization services to their customers.

### **An ideal monitoring solution for multi-domain environments must be capable of:**

- Offering real-time views of the status of a customer's environment. The view displayed to a customer must be customizable for the specific customer – i.e., the customer must only be capable of viewing the status of the infrastructure that they have paid for. More importantly, real-time access to performance information can enable a customer to understand changes that are happening in their infrastructure in real-time and to react to these changes instantly so as to be able to offer optimal performance to their customers.

- Handling security issues across customers – i.e., one customer should not be able to view the status of another customer’s environment.
- Clearly demarcating where a problem may originate – i.e., whether in the customer domain or in the service provider domain. Such a capability can significantly decrease support costs for the service provider.
- Operating across customer environments in different IP address ranges, with multiple levels of firewalls between these environments.

Many service providers are retrofitting existing monitoring solutions to meet these needs. While using existing monitoring solutions, service providers have to use separate management consoles for each customer (Figure 1).

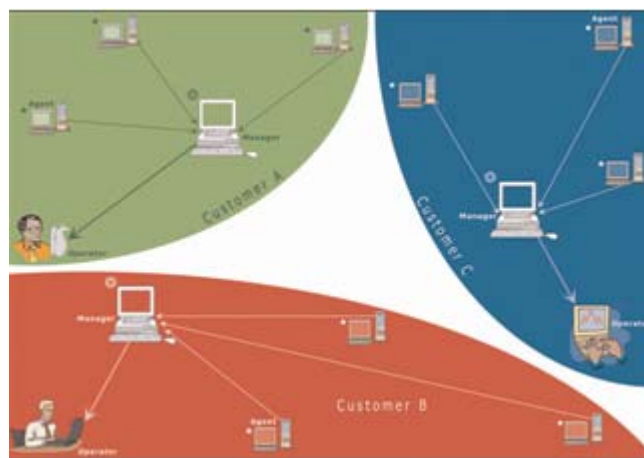


Figure 1 : Retrofitting existing monitoring solutions for multi-domain environments

**The limitations of the above approach are:**

- The need to own and operate multiple managers, one for each customer. First, separate hardware is required to host each manager. Second, the software costs – for the manager, the manager’s database, etc., have to be borne individually by each customer. This need for multiple independent managers makes the overall solution very expensive.
- Even if the same hardware is used to host different customers (i.e., shared hosting), the agents required per customer may have to be distinct, so as to preserve the security of each customer’s data.

**The eG Suite**

The eG suite is a virtual, private monitoring solution for multi-domain Internet/Intranet environments (see Figure 2). The eG suite is virtual, because it does not involve a dedicated manager per customer. Instead, the cost of the manager component is amortized among all the customers. Moreover, the eG suite is private because although the manager component is shared, this component is designed so as to preserve the privacy that is provided to customers in a dedicated solution. The eG suite enables automatic upgrade of hundreds of agents whenever a new release is available, without the need for any manual intervention. The eG suite is a 100% scalable, web based architecture model enabling remote and secure monitoring across geographies using HTTP/HTTPS protocols. eG’s web-based user interface supported by the manager enables different customers to login to the central manager and obtain personalized and customized views of the monitored environment.

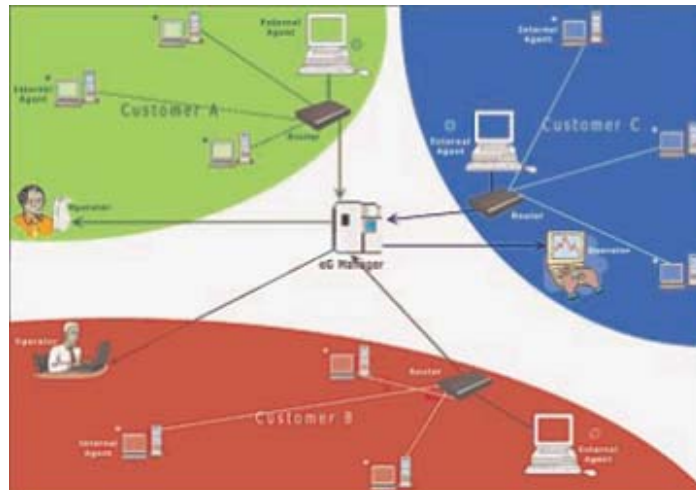


Figure 2 : How the eG suite works in multi-domain environments

The main advantages of the eG suite are:

- Remote monitoring and control across geographies using HTTP/HTTPS protocols over the web.
- Auto-upgradable agents facilitating auto upgrade of hundreds of agents whenever a new release is available.
- Capability to offer personalized displays of the status of the target environment based on each customer's preferences and privileges. This capability enables customers to view the status of just the servers and applications that they own/lease. While the eG suite is ideally suited for service providers, large enterprises too can benefit from its capabilities. For example, personalized views can be provided to the different domain experts (e.g., mail administrators, database experts, etc.) to enable them to effectively monitor the applications, databases, servers, or network elements under their control.
- Amortization of hardware and software costs among different customers. This includes the usage of a single manager software component, the use of common hardware, a shared database server for storage of measurement results, etc.
- Ability to support new, revenue-generating monitoring service to a service provider's customers. Rather than using monitoring solutions just as a cost center that improves the efficiencies of their operations, service providers can use the eG suite to offer new, revenue generating monitoring services. Rather than receiving just weekly and monthly reports, the eG suite enables customers to view the instantaneous status and usage of their servers and applications in real-time, through a web browser interface, and also receive real-time alerts in the event of problems.

The eG architecture comprises of the following components:

## Agent

Agents are software components deployed at various points in the target infrastructure. By running pseudo-periodic tests, the agents collect information about various aspects of the system. The test results are referred to as measurements. The agent components are responsible for collecting and reporting a variety of measurements to the manager. For example, a Process test reports the following measurements:

- a. Number of processes of a specific type executing on a system.
- b. The CPU utilization for these processes.
- c. The memory utilization for these processes.

The tests can be executed from locations external to the servers and network components that are responsible for the operation of the IT infrastructure. Agents that make such tests are called external agents. For example, the eG suite can be specially installed on a server for the purpose of monitoring the environment and an external agent on the server can invoke a test that emulates a user accessing a web site. Such a test can provide measurements of the availability of the web site and the performance (in terms of response time) seen by users of the web site

Often external agents alone may not be sufficient to completely gauge the health of an IT infrastructure and to diagnose problems when they occur. For example, it may not be possible to measure the CPU utilization levels of a web server from an external location. To accommodate such situations, the eG suite uses internal agents that are to be installed on the servers and network elements of the IT infrastructure.

To address the needs of multi-domain environments in which each customer site may have its own internal Intranet with different private addresses, the eG suite supports multiple external agents. One external agent can be installed in each customer Intranet being monitored. The eG suite architecture also allows for the same service to be monitored by multiple external agents, so that monitoring can be performed from multiple perspectives (e.g., an IT business site can be monitored from Boston as well as San Francisco).

## Manager

The eG manager is responsible for receiving and storing measurement results from the agents. Users can access the measurement results from the data repository that the manager maintains via a web-based graphical user interface. The eG suite manager comprises of two major components:

- **Virtual manager:**

The eG manager is designed as a number of virtual managers, one for each customer. A virtual manager corresponds to a specific customer, and is responsible for providing customized displays of the hosted environments for the customer. The virtual manager also handles license tracking for a customer and generation of alerts in real-time for the customer. The virtual manager uses a core set of functions supported by a second manager component called the main manager.

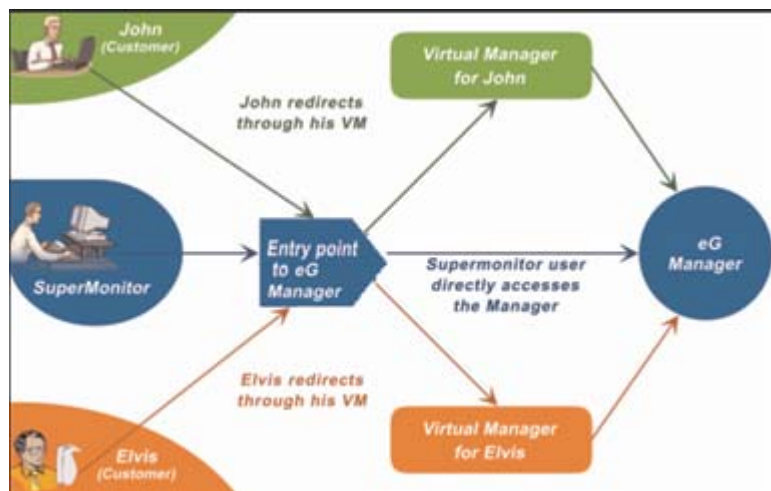


Figure 3 : The virtual, private manager architecture of the eG suite

## ▪ Main Manager:

This component implements the core set of functions of the manager such as the receipt and storage of the measurement results, threshold computation for the collected results, analysis of the stored data for trending and service-level audits, alarm correlation for root-cause diagnosis, user login, configuration of the user's virtual monitored environment, etc.

Figure 3 depicts the virtual private manager architecture. Multi-domain environments typically include multiple demilitarized zones. From a security perspective, most IT infrastructure operators view SNMP and other proprietary protocols suspiciously. On the other hand, HTTP is not perceived of as a serious security threat. Consequently, the eG suite uses HTTP/ HTTPS for all communications between the manager and the agents. Moreover, to ensure that only the eG agents can report measurements to the manager, the eG suite uses a proprietary authentication mechanism through which the manager authenticates each incoming connection before accepting the measurements reported over the connection. All communications from the agent to the manager can also be encrypted, if so desired.

## User Management

One of the key functions of the eG manager is its user management capability. There are three types of users that the eG suite supports:

### Administrative users:

An administrative user is the super-user of the system. Multiple administrative users can be configured in the system, but all the administrators have similar rights. Each administrative manager can choose what hardware and application servers are to be monitored by the system, where the agents should be executed to monitor the hosted environment, what tests these agents should run, and how often these tests should be executed. The administrative user also has the rights to add and delete other users.

### Monitor users:

Monitor users have restricted access to the eG suite. Each monitor user is associated with a mail address where alarms will be forwarded. The user's profile also includes information regarding the customer's alarm preferences – whether alarms have to be forwarded in text or HTML mode, whether a complete list of alarms has to be generated each time a new alarm is added, or whether the new alarm alone should be sent via email, etc. Each monitor user is associated with a subscription period. The eG suite allows the customers to access the system until this period only. Figure 4 depicts the addition of a user to the monitoring system.

The screenshot shows a web-based user administration interface. At the top, there are navigation tabs: CONFIGURE, COMPONENTS, SERVICES, AGENTS, and USER ADMINISTRATION. The main content area is titled 'ADD USER' and contains a form with the following fields and options:

- USER TYPE: Member (dropdown)
- USER ID: john (text input)
- PASSWORD: [masked] (password input)
- RETYPE PASSWORD: [masked] (password input)
- SERVICES: eg-agent, eg-agent, eg-agent (list box)
- SEGMENTS: eg-1, eg-2, eg-3 (list box)
- VALIDITY: 02/04/2003 (text input) with a 'No Entry' checkbox
- MAIL ID/MODULE NO: john@eg.com (text input)
- TYPE OF ALARMS: Critical, Minor (checkboxes)
- TYPE OF NOTIFICATION: New, Complete List (checkboxes)
- MESSAGE MODE: HTML, Text (checkboxes)
- REMOTE CONTROL: Enable, Disable (checkboxes)

At the bottom of the form are 'NEXT' and 'CLEAR' buttons. The footer of the page includes copyright information: © 2003 eG Innovations, Inc. All rights reserved. and the eG logo.

Figure 4 : Adding new users through the eG user interface



### Supermonitor users:

A supermonitor user takes an overall perspective of the target environment. This user has an unrestricted view and he/she can receive alarms pertaining to the whole infrastructure that has been configured by the administrative user. Figure 3 depicts the addition of new users to the eG system. The subscription information provided (i.e., the validity time in Figure 3) is used by the eG manager to automatically track subscriptions to the monitoring service it offers. The manager itself takes care of alerting users when their subscription is about to expire. Interfaces exported by the eG manager to the service provider's billing systems can be used to automatically turn on and off user subscriptions.

### Features of the eG suite

The eG suite includes all of the key monitoring and diagnostic features that make it a preferred monitoring solution for IDCs, MSPs, and large enterprises.

#### a. Integrated monitoring of an entire infrastructure - ranging from networks to systems to applications.

Figure 6 summarizes the monitoring capabilities of the eG suite.

<b>Web servers</b>	Apache 1.x, iPlanet 4.x/SunONE, Microsoft IIS, IBM HTTP Server, Oracle HTTP Server
<b>Web application servers</b>	WebLogic, ColdFusion, ATG, iPlanet 3.6 or higher, SunONE, Microsoft transaction server, WebSphere, SilverStream, Jrun 3.0 and 4.0, Orion, Tomcat, Oracle 9i OC4J, Oracle Forms Servers, Borland Enterprise Servers (BES)
<b>Database servers</b>	Oracle, Microsoft SQL server, DB2 UDB, Sybase, MySQL, SQL clusters, Backup SQL
<b>Network devices</b>	Cisco routers, Cisco Catalyst switches, Baystack hub, Network nodes, Local director
<b>Microsoft Applications</b>	Active Directory, BizTalk server, Windows Internet Name Service (WINS), Terminal server, DHCP server, MS Print server, MS Proxy Server
<b>Firewalls</b>	Check Point Firewall-1, Cisco Pix
<b>Terminal Servers</b>	Citrix MetaFrame Presentation 1.8, XP servers, Terminal servers
<b>Email servers</b>	Microsoft Exchange, Lotus Domino P5, iPlanet/ SUN ONE Messaging
<b>Backup servers</b>	Veritas Backup Exec server
<b>Messaging servers</b>	MSMQ, IBM MQ, FioranoMQ, Novell Groupwise
<b>Others, LDAP, DNS</b>	FTP, MTS, Event Logs, Tuxedo domain servers, Printers, Windows Domain Controller, NetApp filers and NetCache.

Figure 5: IT infrastructure components monitored by the eG suite



**b. Automatic infrastructure triage and correlation capability:**

To ensure that IT infrastructures operate with minimum downtime, it is critical to perform problem detection and diagnosis instantly and accurately. Correlation of various problems reported at the network, system, and application layers is critical for speedy and accurate problem diagnosis. Most application monitoring solutions do not include any specialized correlation capability – manual analysis of the collected data is essential to determine the root-cause of problems. In contrast, the eG suite uses a novel, patented correlation and automatic infrastructure triage technology. To implement this capability, the eG manager incorporates a series of heuristics that take into account the configured site topologies and pre-built models of different network and application components. By automatically correlating across the network, system, and application layers, the eG suite is able to accurately identify and report the root-cause of problems. The out-of-the-box correlation capability that it includes makes the eG suite unique as compared to most other monitoring solutions.

**c. Virtual manager architecture:**

This allows service providers to offer revenue-producing monitoring services to customers. The main feature enabled by the virtual manager architecture is personalization. Every customer of a service provider has exclusive access to specific infrastructure and application components being supported by the service provider. To provide personalized views of the hosted environment for every customer, the eG manager is designed as a number of virtual managers, one for each customer. A virtual manager corresponds to a specific customer, and provides customized, real-time views of the infrastructure for each and every customer enabling him/her to remotely track their on-line presence. To enable service providers to offer monitoring as a service, the eG manager allows subscription-based access for customers. At the same time, to make it simpler and less time consuming for service providers to support the monitoring service, the eG manager provides automated subscription tracking and alerting.

To demonstrate the virtual manager capabilities of the eG suite, consider a scenario in which two monitor users, namely John and Elvis have been added to the eG suite system via its administrative interface. John and Elvis are respectively associated with web sites buy.abc.com and www.abc.com. Figures 6a and 6b depict the views that the eG suite provides to users John and Elvis. As is evident from the figures, both the users, John and Elvis are permitted to monitor their corresponding sites only.



*Figure 6a : The web sites being monitored by the user john*



*Figure 6b : The web sites being monitored by the user elvis*

The virtual manager architecture also enables personalization of the alarms displayed to the monitor users. Figure 7a shows the alarm window corresponding to john. Only the alarms pertaining to the web site buy.abc.com, which is being monitored by john, appear in this view. Figure 7b shows the alarms being displayed to elvis at the same instant.



Figure 7a : The eG suite's alarm window for the user john



Figure 7b : The eG suite's alarm window for the monitor user elvis

Through the ubiquitous web browser interface, the eG suite also provides users with integrated views that provide real-time alerts and in-depth analysis of the status and performance of their servers and services. Customized displays of the status of the hosted environment based on each user's preferences and privileges enables customers to view the status of just the servers and applications that they own/lease.

**d. Proactive real-time monitoring of real web transactions:**

The experience that IT businesses offer to its customers is governed predominantly by how well its application components perform. Many existing monitoring products use emulated transactions to monitor an e-infrastructure. The main drawbacks of this approach are:

First, all application transactions cannot be monitored by simple emulation of the transactions. For example, it may not be possible to emulate a user making a payment, or a user registering to the site.

Second, emulation-based techniques mainly sample the target environment. Hence, if a specific transaction is failing, say 10% of the time, the chance that emulated monitoring is able to detect the problem is only 10%. Hence, emulated monitoring is able to consistently detect problems only when the extent of the problem is significant enough that a majority of the incoming transactions are failing.



Figure 8 : Real-time monitoring of real web transactions

The eG suite overcomes the above drawbacks using its unique web adapter capability, which performs internal monitoring of real web transactions (not emulated ones). The web adapter is a layer that fits between the TCP/IP stack and a web server. It can be thought of as a passive probe that watches the requests received by the server and the responses produced by the server. By applying a fast, pattern-matching algorithm on the packets that flow by, the web adapter collects and reports a variety of statistics regarding web sites and the transactions executed by users at these sites.

The ability to offer real-time monitoring of real (not emulated) transactions, without the need for explicit, expensive logging is an important feature of the eG suite. Since it monitors all transactions to a web site, this unique capability allows the eG suite to accurately quantify any performance degradations and to proactively alert operators about potential problems with their infrastructure.

Figure 8 depicts the eG suite's capability to monitor real transactions in real-time. The scenario shown in this figure demonstrates monitoring of an on-line retail site using the eG suite. The left hand panel of Figure 8 indicates that at the current instant, three of the transactions are not performing effectively. For any chosen transaction, the right hand panel displays the measurements last made by eG's web adapter. As is evident from the figure, the eG suite is able to pinpoint the reason(s) for why a transaction is not performing to expectation. In the scenario of Figure 8, the failure of the transactions is associated with a 100% of requests being aborted by users.

**e. Novel layered presentation model:**

eG's web presentation model is specifically tailored for multi-domain Internet/Intranet environments wherein the service provider is responsible for the hardware and network infrastructure, and the customer is responsible for the software applications. By depicting each infrastructure component as a collection of layers, and monitoring each of the layers independently, the eG suite is able to pinpoint which of the layers is the root-cause of problems (see Figure 9). The isolation of problems that this layered presentation model enables is especially useful for clearly demarcating between problems in the service provider domain and the customer domain, and can significantly reduce support costs for the service provider.



Figure 9 : The user interface depicting the layered representation model of a Sun ONE web server

**f. Centralized administration and update via a centralized web console:**

A centralized user management module simplifies the creation and administration of custom views. The distributed operation of the agents can be controlled from a web-based administrative interface. Auto-discovery of servers, configuration of the server topology, turning on and off individual tests, changing the frequency of a test and the test's parameters, updating the thresholds for every individual measurement, changing alarm policies, can all be made from an administrative interface.



**g. Scalable, 100% WEB-BASED architecture:**

The eG architecture itself is built along the lines of multi-tier web architectures and hence supports small and large IT business infrastructures equally well. All communications between the manager and agents use HTTP or HTTPS. All user accesses to the monitored information is also via the web. The key advantage of this approach is that it permits the manager and agents to be in different physical locations, possibly separated by multiple demilitarized zones. In fact, the agents can even reside within private Intranets and still be managed by an eG manager in a central location. This architecture is ideally suited for large enterprises and managed service provider environments.

**Benefits of the eG suite**

- 100% scalable web based console enabling remote and secure monitoring and control using HTTP/HTTPS protocols across geographies.
- eG's auto-upgradable agents ensure that hundreds of agents can be upgraded automatically without any manual intervention as and when a release is available.
- eG offers personalized and customized user views to all customers as per their requirements thereby clearly demarcating the problems and successfully eliminating finger pointing.

**Conclusion**

The eG suite is an ideal solution for service providers to offer value-added, revenue-producing monitoring services to their customers. In large enterprise environments too, using eG's personalized view generation capabilities, domain experts can continue to back the status of servers and applications in their purview. At the same time, service operators/ administrators can proactively monitor the quality of IT infrastructure services end-to-end and use eG's automatic infrastructure triage capability to identify when, where, and how remedial action must be initiated to ensure peak performance.