



iQ.Clustering

**High-Availability, Fail-Safety,
Load Balancing, Distributed Computing**

▶ Contents

1 Introduction	1
2 Overview	1
2.1 Domino Cluster.....	1
2.2 Operating System Cluster	2
2.3 iQ.Clustering.....	2
3 Mailbox Checking	6
4 Grabber Checking	7
5 Installation Requirements	7
6 Benefits of iQ.Clustering	7
7 About GROUP Technologies AG	9

1 Introduction

In recent years, e-mail has become a major concern within companies, comparable to other business-critical applications such as ERP, MIS, Accounting or Controlling systems.

Business-critical applications are expected to provide permanent availability, good performance and high scalability. Further requirements include load-balancing capacity, usability in heterogeneous environments as well as easy system management.

The solution offered by IBM Lotus is the Domino Cluster, a technology that meets these demands at database level.

Regarding e-mail security, highest priority is given to permanent, efficient and reliable monitoring of the entire e-mail traffic, e.g. to ensure virus and spam protection. To achieve this, a Domino Cluster is not enough.

Focussing on the security and efficiency of the e-mail traffic, iQ.Clustering offers the ideal complementary solution for e-mail security within a Domino Cluster.

2 Overview

2.1 Domino Cluster

A Domino Cluster is a group of two or more Domino servers. It ensures permanent and efficient access to the users's data, even in growing environments.

A Domino Cluster offers the following features:

■ High-Availability of Critical Databases

As the databases are replicated between the servers belonging to the cluster, the user has permanent access to all databases, even when a server is not available. This process is called Failover. It also allows to upgrade hardware or software components without interfering with the user's normal workflow.

In the Domino Cluster, the databases are permanently synchronized, so that the information is identical on all servers.

■ Load Balancing

If a particular server is heavily loaded with requests, then additional requests are automatically redirected to a less-loaded server within the cluster. This functionality allows to more or less evenly distribute the overall load across all servers in the cluster and thus to ensure a high performance of the system.

■ Scalability

It is possible to add further servers to the cluster in case the performance becomes insufficient. Typically, a growing number of databases or users will make such an expansion of the cluster necessary. With further servers integrated in the cluster, all databases on these servers become available while the load-balancing function ensures that requests are redirected to the new server(s).

■ Data Synchronization

To ensure permanent access to all data even when a server is momentarily unavailable, the data is continuously synchronized through replication mechanisms.

■ Hardware/Software, System Management

To support heterogeneous environments, the various servers within a Domino Cluster can be run on different platforms or operating systems. In other words, it is not necessary to run all of the servers within the cluster under the same operating system or on the same hardware platform.

It is thus possible to upgrade an operating system or a hardware component without restricting the availability of the data.

A cluster is also the key to a successful backup and disaster recovery strategy, as users can still access all of the data when a server is unavailable (due to a failure or a maintenance procedure) since requests can automatically be redirected to another server. Of course, it is also possible to use individual servers within the cluster as pure backup servers.

2.2 Operating System Cluster

Another option is to set up an operating system cluster, such as Sun Cluster, Microsoft Cluster Services and IBM AIX HACMP. These clusters guard against a failure of the operating system and other server tasks, including the Domino servers.

As a Domino Cluster, all of these have their specific benefits, but they are restricted to a specific operating system. For further details, please refer to the documentation provided by each manufacturer.

Combining an operating system cluster with a Domino Cluster is the best way to take advantage of all benefits.

2.3 iQ.Clustering

As part of iQ.Suite, iQ.Clustering is an application-clustering product. After installation on a Domino server, iQ.Clustering is enabled once licensing is complete. iQ.Clustering does not replace but complements the function of a Domino Cluster. A Domino Cluster is **not** required to run iQ.Clustering. A cluster managed by iQ.Clustering comprises several Domino servers (reasonably not more than 4 to 6) with iQ.Suite installed.

To ensure correct functioning, iQ.Clustering requires an identical or replicated configuration on all servers included. The network connection between clustered servers must provide sufficiently high data transfer rates, e.g. such as provided by LAN connections.

iQ.Clustering enhances the following functionalities in a Domino environment:

■ High-Availability

iQ.Clustering can be used to optimize the iQ.Suite system availability according to the requirements of major installations. Within iQ.Clustering, the e-mail traffic is monitored by the Mail.box while the e-mails are processed by iQ.Suite.

Whenever iQ.Suite is not available on an iQ.Clustering server, e.g. during a virus scanner update, the other iQ.Clustering servers take over the tasks of the unavailable server.

□ Example

If running a backup computer center for your Domino servers, iQ.Clustering can be used to ensure that the cluster computer in the backup computer center immediately takes over whenever the main server becomes unavailable. This would be a typical scenario for using a Domino Cluster in combination with iQ.Clustering.

■ Fail-Safety

In case of an iQ.Suite failure on an iQ.Clustering server, the other servers in the cluster automatically take over and redirect the corresponding information accordingly. With iQ.Clustering, the probability of an iQ.Suite failure and its associated risks can thus be considerably reduced.

□ Example

If running multiple Domino servers, iQ.Clustering can be used to ensure that whenever there is an iQ.Suite failure on one server, the other servers in the cluster fully take over that server's tasks.

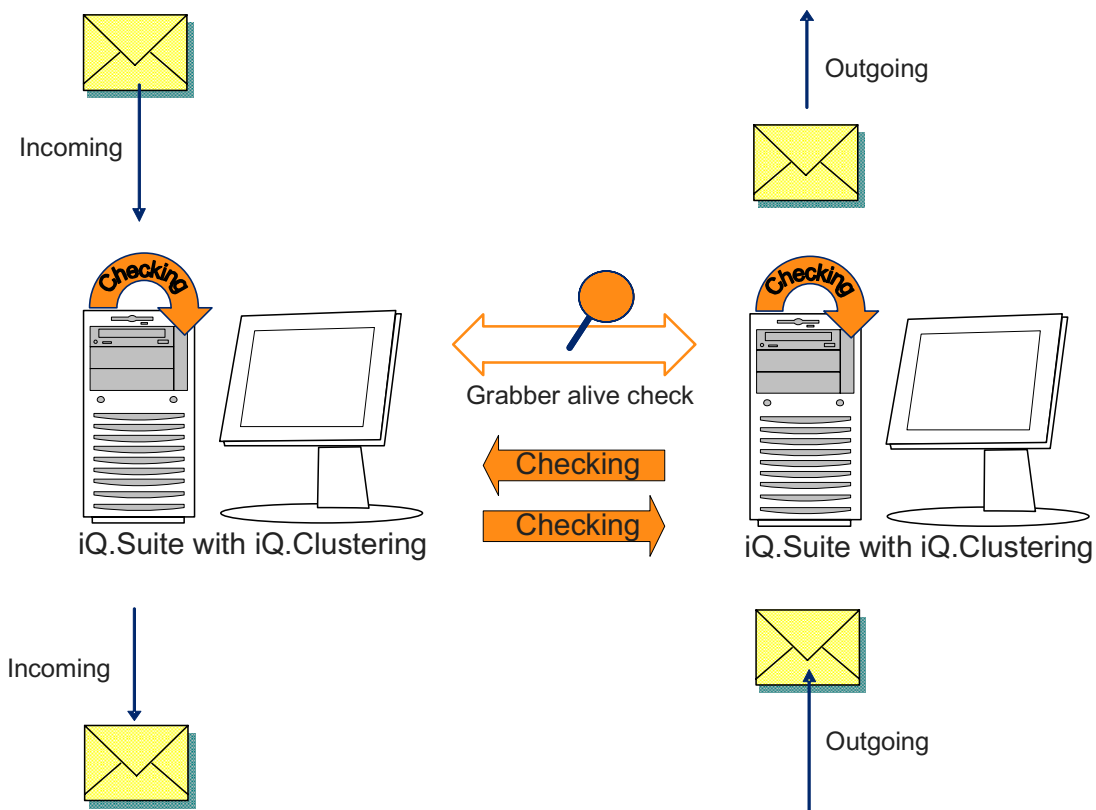
■ Load Balancing

With iQ.Suite installed, iQ.Clustering allows to evenly distribute server loads within the cluster, i.e. an idle or less loaded server takes charge of the e-mails arriving on a heavily loaded iQ.Clustering server and returns them after having executed the required processing tasks. This allows to reduce the risk of e-mail bottlenecks to a minimum.

□ Example

At your main site, multiple Domino servers are operated as Internet gateways. If, for instance, the gateway for incoming e-mails is more heavily loaded than the outgoing mail gateway, the iQ.Clustering load balancing function will shift some of the processing tasks from the more loaded server to the less loaded one.

The graph below illustrates how two computers mutually monitor each other's mailboxes as well as the MailGrabbers:



■ Distributed Computing

Not all iQ.Suite modules are available for some of the operating systems supported by Domino. This particularly applies to Mainframe systems, e.g. iSeries, zSeries.

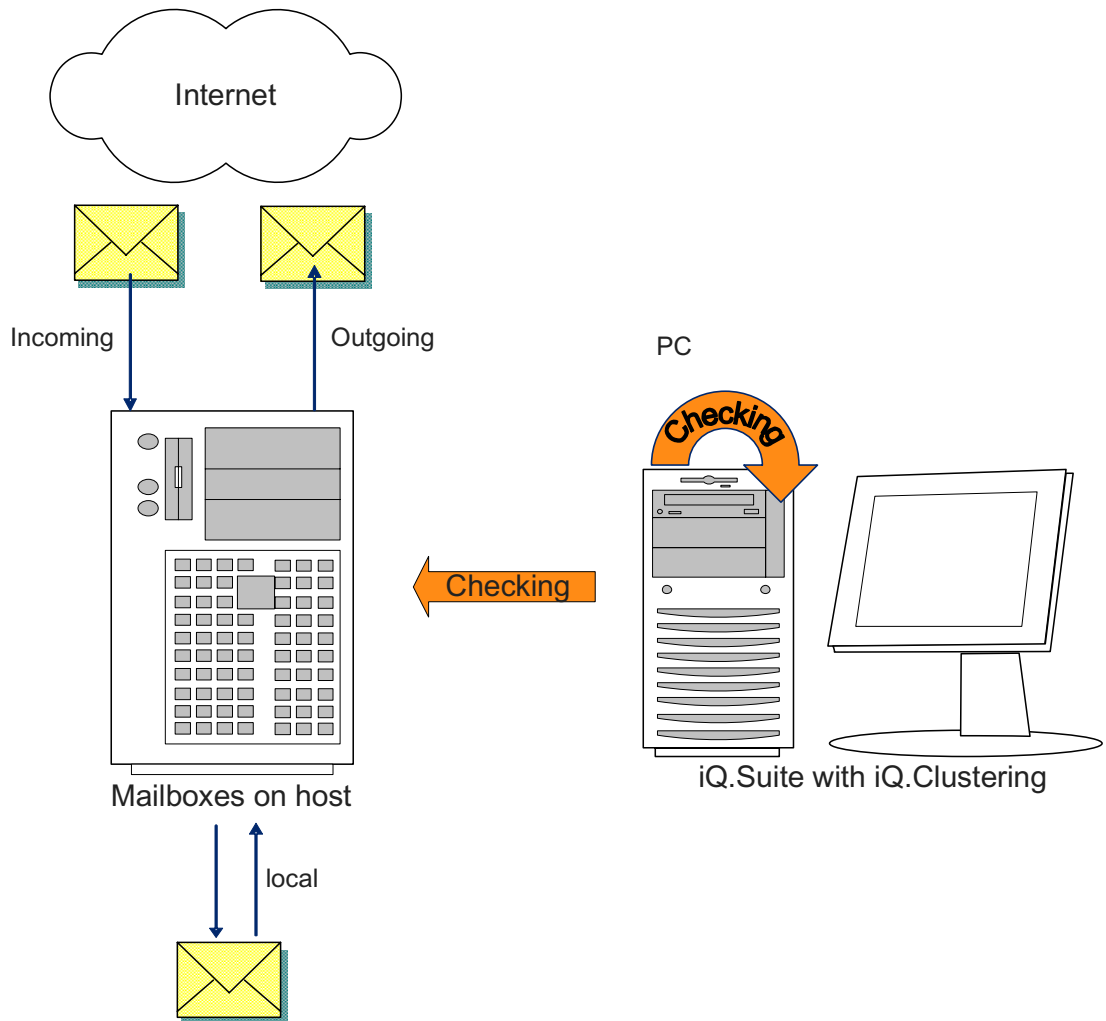
In environments under such operating systems, iQ.Clustering allows to process e-mails on a separate computer. The host system and the separate computer are interconnected via a LAN and independent of each other. It is thus possible to use **all** of the iQ.Suite modules. At the same time, the load is distributed across one or more - typically less expensive - computers. All that is required is a separate computer with a Domino server installed and running iQ.Suite.

□ Example

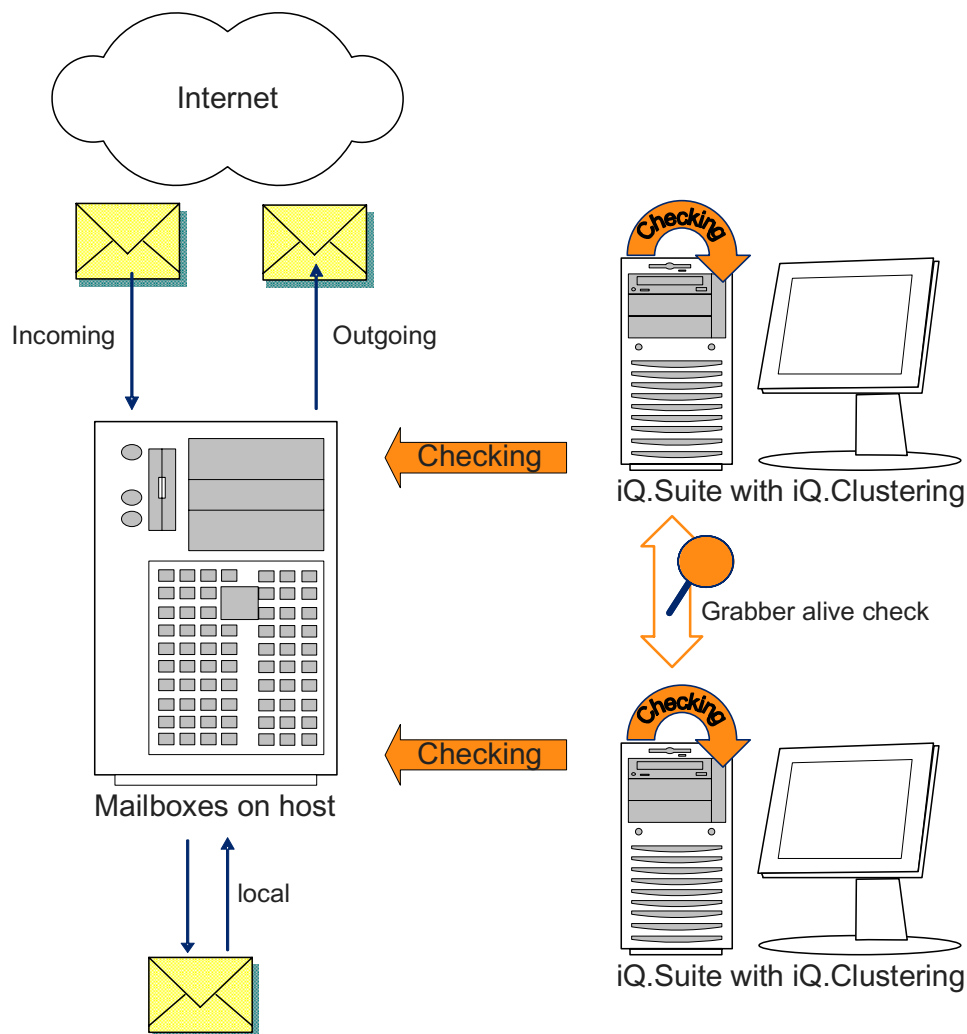
iQ.Suite is to be installed on an existing mail host (with Domino server) in a non-Windows environment in order to check e-mail attachments for viruses. The virus scanner to be used is not available on the operating system platform. To solve this problem, the virus scanning function can be shifted to a Windows computer. To do so, iQ.Suite and the corresponding function modules (in this case Watchdog) are installed along with the virus scanner on this Windows computer. On the mail host, only the EXTMGR_ADDIN te_hook utility is installed. The e-mail is simply marked for processing by the hook and the MailGrabber installed on the computer running iQ.Suite then processes the e-mail as required.

In addition to virus scanning, iQ.Clustering also allows to run any other module in any environment, as it is always possible to run e-mail checking functions on a platform where the module is available.

The graph below illustrates how the mailboxes on a host computer are monitored by a PC:



The graph below illustrates how the mailboxes on a host computer are monitored by two PCs with simultaneous mutual monitoring of the MailGrabbers:



3 Mailbox Checking

Using iQ.Clustering, e-mails are processed in the following order:

1. The MailGrabber checks the Mail.box(es) to be monitored for new documents.
2. The MailGrabber attempts to reserve any documents found;
→ new status in the **dispatched for <server name>** view.
3. The working threads only process documents that have been successfully reserved by the server.
This is determined through the `$TKCheckServer` field.
4. If a reserved document is not processed within 15 minutes, it is returned to the "general pool".
5. If there are any reserved documents when the MailGrabber is shut down or started, the reservation is removed.

4 Grabber Checking

1. On the servers to be monitored, the MailGrabber checks the Mail.box / Mail1.box for a profile document.
2. This profile document contains the last action (with date/time) performed by the Grabber on the monitored server.
3. This profile document is written by the Grabber to be monitored (at least once per minute) and it is read and deleted by the monitoring servers (approx. every 5 minutes).
4. If no profile document is found, the last status read is considered to be the current status.

5 Installation Requirements

The following requirements have to be met on the PCs used in addition to the general iQ.Suite installation requirements:

- One of the following operating systems: Microsoft Windows, Linux, Sun, AIX
- Fast network connection
- Virus scanner (for securiQ.Watchdog)
- PGP (for securiQ.Crypt)

6 Benefits of iQ.Clustering

Using iQ.Clustering provides the following major benefits:

■ High-availability of e-mail traffic analysis

iQ.Clustering ensures that all e-mails are checked according to corporate policies concerning security issues (such as virus protection or non-disclosure of sensitive information) and thus enables a considerable reduction of security-relevant risks. Updates and upgrades are possible without restricting the user in any way .

■ Fail-safety of iQ.Suite

Ensuring uninterrupted processing of all e-mails according to corporate policies, iQ.Clustering considerably reduces security-relevant risks.

■ Load balancing

iQ.Clustering ensures an even distribution of iQ.Suite processing tasks. As less loaded servers take over tasks from more heavily loaded servers, there is no bottleneck in the Mail.box of a Domino server when checking an e-mail according to corporate policies takes quite a long time. iQ.Clustering thus ensures fast delivery of time-critical e-mails.

■ Distributed Computing

iQ.Clustering also supports Domino-supported operating systems under which not all iQ.Suite modules are available (e.g. Mainframe systems such as iSeries and zSeries). This significantly increases the flexibility of iQ.Suite in enterprise environments.

7 About GROUP Technologies AG

GROUP Technologies is one of the world's leading manufacturers of e-mail security, organization and management software. The company's solutions have made GROUP one of the leaders in technologies in these areas. The optimally coordinated products are available for the Lotus Domino, Microsoft Exchange and SMTP platforms.

GROUP's performance ranges from e-mail cryptography and virus protection to anti-spam and secure archiving, all available out of one hand and in best quality. Using GROUP's iQ.Suite enables companies to optimize the cost and efficiency of their e-mail environment and raise work productivity.

The iQ.Suite is modular, scalable company-wide and offers customers the required degree of investment security. All iQ.Suite products are server-based and can be administered centrally and economically.

GROUP Technologies customer base includes a wide variety of renowned companies, such as Deutsche Bank, Ernst & Young and Honda. The products are available through direct sale and from OEM and business partners. Over five million users utilize GROUP Technologies iQ.Suite to protect their systems.

GROUP Technologies headquarters is in Karlsruhe, Germany. The company maintains offices internationally both in Europe and in Boston, Massachusetts, USA.

www.group-technologies.com

© 2005 GROUP Technologies AG

The product descriptions are general and descriptive in nature. They can be interpreted neither as a promise of specific properties nor as a declaration of guarantee or warranty. The specifications and design of our products can be changed at any times without prior notice, especially to keep pace with technical developments.

The information contained in this documentation deals with issues as assessed by GROUP Technologies AG at the time of publication. As GROUP Technologies AG is bound to react to changing market requirements, this document by no means represents an obligation by GROUP Technologies AG and GROUP cannot guarantee the correctness of the information presented in this document after its publication.

This documentation is intended for information purposes only. GROUP Technologies AG hereby excludes any warranty, express or implied, for this document. GROUP Technologies AG is unable to guarantee, either explicitly or tacitly, the quality, execution, standardization or suitability for a specific purpose.

All product or company names in this document may be protected brand names of their respective owners.

Headquarters

GROUP Technologies AG
Ottostrasse 4
76227 Karlsruhe / Germany



Fon +49(0)721-4901-0
Fax +49(0)721-4901-199
info.de@group-technologies.com
www.group-technologies.com

North American Headquarters

GROUP Technologies Inc.
120 Quarry Drive, Suite B214
Milford, MA 01754/USA

Phone +1 508-473-3332
Phone 877-476-8755 (US and Canada)
Fax +1 508-473-9940
info.us@group-technologies.com
www.group-technologies.com