

Testing the Axigen, Kerio, and Merak commercial mail servers

MAIL CALL

Deutsche Post World Net

They run on Red Hat Enterprise Linux, cost money, and juggle email messages: these three commercial mail servers aim to convince admins they are worth the price. **BY JÖRG FRITSCH, PATRICK NEST**

The task appears so simple: a mail server receives and sends email. Suitable software has been around since the birth of the Internet. The major players include Sendmail, Postfix, Q-Mail, Microsoft Exchange, and Lotus Notes. But right now, many new Linux-based products are starting to leave the developer labs. These new products aim to be quicker and better than the industry favorites.

We tested three candidates from this new breed of mail servers. Our test entries include commercial mail servers by Axigen [1], Kerio [4], and Merak [7]. All of these products are new developments that are not based on existing Open Source servers. We used Red Hat Enterprise Linux 4 as our test platform. The core test criteria were administration, look and feel, webmail functionality,

suitability for groupware, and performance on powerful hardware.

Axigen Mail Server

The Axigen mail server is the only product in the test that does not claim to be an alternative to Microsoft Exchange or Lotus Notes. Instead, it competes with the commercial version of Sendmail [9]. Axigen provides a neatly structured

browser-based admin GUI. After a short learning curve, admins will have everything under control in a single window (Figure 1).

Axigen supports legacy webmail functionality, including a simple folder structure. A practical feature for the admin: users can easily handle many daily tasks, modify views and user data, or even change passwords. Our stress test demonstrated that the webmail GUI can easily handle several thousand emails.

Limited Webmail

The program lacks a search feature for keywords in the subject line or body of

Buying the Axigen Mail Server

Axigen Mailserv version 1.2.4 comes in variants called Gateway, Business, and Serviceprovider [1]. Axigen Gateway (EUR 95 / US\$ 120) entitles you to use the product as a front-end relay server without local domains and mailboxes. Business and Serviceprovider differ with respect to the licensing. The price for Axigen Business depends on the number of local mailboxes (25 mailboxes for EUR 190 / US\$ 240; 1,000 mailboxes for EUR 1,450 / US\$ 1,810). The price of the Serviceprovider license variant depends on the number of hosted domains (50 domains for EUR 535 / US\$ 669; 300 domains for EUR 1,700 / US\$ 2,124). The unlimited edition costs EUR 2,900 / US\$ 3,624.

<http://www.axigen.com/mail-server>



the email, as well as a multidrop function (catchall). The multidrop feature stores emails not addressed to a specific user in a generic folder. Improved anti-virus and anti-spam features would be nice, too. According to Axigen's support, most of these features will be incorporated in the next version 2.0.

Generally speaking, filtering is difficult with Axigen. If you intend to automatically flag mail as spam or virus-infected, or according to your own criteria, you will have to get to know the sieve standard (RFC 3028 and 3685, [3]). The Axigen server will handle user-defined Sieve scripts [2] that filter and sort messages

Listing 1: Sieve Script

```
01 require ["fileinto",
02 "comparator-i;ascii-numeric"];
03 if header :value "gt" :
04   comparator "i;ascii-numeric"
05   "X-SPAM-SCORE" "7" {
06   fileinto "inbox.junk";
07 }
```

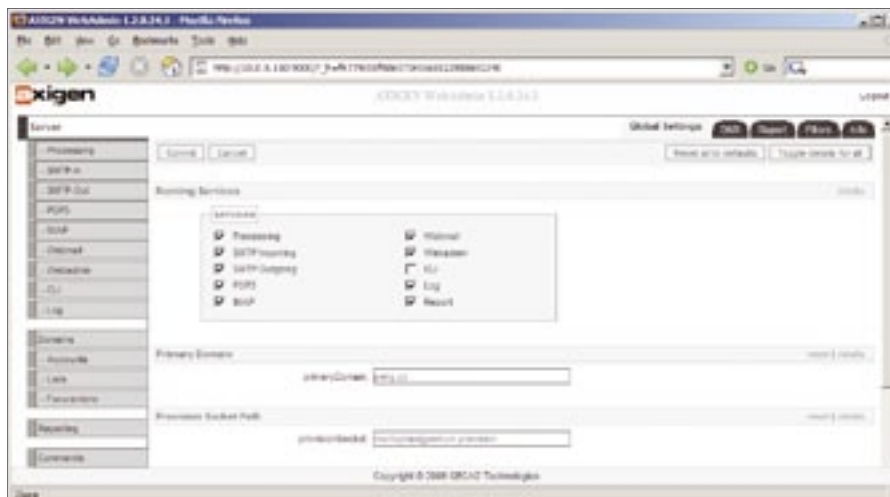


Figure 1: The clear-cut Axigen web administration interface, showing the service selection and other basic settings.

based on their headers. The Sieve example in Listing 1 passes messages tagged by SpamAssassin with a score of 7 or more to a junkmail folder in the user's inbox. You can also use Sieve to create header rules for messages.

Proprietary Scripting

Axigen use a proprietary scripting language, AFSL (Axigen Filters Scripting Language) to communicate with virus and spam filters. AFSL scripts specify the application to handle incoming mail first, possibly to support spam and virus tagging. The sieve scripts then evaluate the tags. Axigen provides scripts for the free Clam-AV virus scanner. If you intend to use a different scanner, you will need to write the script yourself, or get in touch with the support team, who proved to be very responsive in our case.

Axigen also implements the Sender Policy Framework (see the "SPF and Caller-ID" box). You can enable the mechanism via the Web GUI.

Kerio Mail Server

The Kerio mail server [4] shone right from the installation phase. Kerio was

the only candidate to detect the sendmail daemon running on Red Hat Enterprise Linux 4 and occupying port 25. The server continued to provide convincing service, including good integration of virus and spam protection features (Figure 2). With its Outlook connector, and a web GUI for groupware, Kerio deserves to be taken seriously as an alternative to the Microsoft Exchange Server 2003.

Kerio provides client software for administration and monitoring. The client, which will run on various operating systems, just like the mail server itself, organizes management tasks in a style reminiscent of Microsoft. You can't help thinking that Kerio has tried to emulate the Exchange Server management interface in a Linux product. And this makes a lot of sense, if you take the target market into consideration: Kerio aims to attract customers away from the Microsoft product, and give them a familiar environment at the same time.

Multiple user task and address book management is also organized along Microsoft lines. We had no trouble organizing appointment and coordinating task-

Buying the Kerio Mail Server

The basic license for Kerio 6 for 20 users without an AV scanner costs EUR 500 / US\$ 625. Another 20 user licenses are available for EUR 200 / US\$ 250; 100 additional users cost EUR 870 / US\$ 1,087; a 250 user package costs EUR 1,950 / US\$ 2,435. 1,000 users cost just less than EUR 8,000 / US\$ 9,996; Kerio does not offer an unlimited license. See http://www.kerio.com/kms_home.html.

Kerio mail is available with a pre-licensed antivirus scanner. McAfee increases the price by about one half. The basic version includes one year's software maintenance. Kerio also provides other maintenance options.

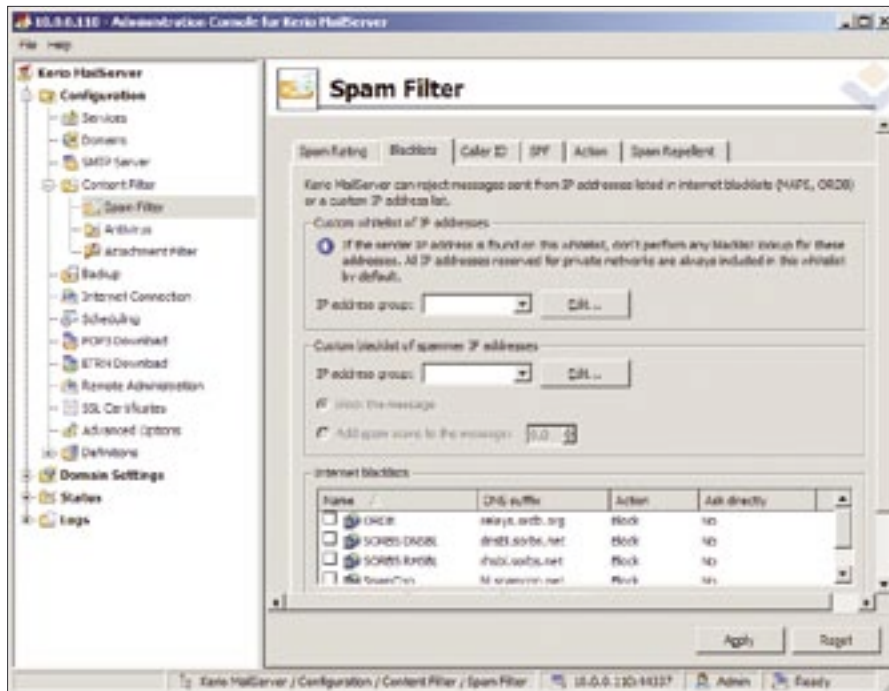


Figure 2: Kerio integrates virus and spam protection nicely with the mail server and administration software. The GUI gives useful explanations of individual settings.

within group projects via the webmail interface with Outlook, Entourage, and other clients [5].

Kerio provides its own Active Directory Extensions (for Microsoft AD), and Open Directory Extensions (for the Apple equivalent) to help integrate the product into existing directory service infrastructures. In a Microsoft environment, the administrator can install the extensions on an AD catalog server, and then add the *Kerio Mailserver Account in Users and Computers* on the Active Directory Management Console. This gives administrators the ability to manage

mailbox credentials centrally via Active Directory.

Virus and Spam Protection

The Kerio mail server includes a licensed version of the McAfee Antivirus Engine. In our lab, the program automatically detected other virus scanners (such as Sophos AV) and listed them as options in a selection menu. You can even scan with two antivirus products. This is a good idea to help you catch new viruses, as the time span between a new virus becoming known and the manufacturer publishing a pattern update can vary.

In contrast to security-only products for email ([11]), Kerio does not give administrators the ability to notify internal recipients of incoming viruses. On a more positive note, Kerio will block email attachments based on the Mime

type or file extension. This helps administrators adhere to enterprise policies that ban executables and MP3 files, for example.

The Kerio mail server has a wide range of anti-spam features, from the proprietary Spam Eliminator to Blacklists such as ORDB and Spamcop, to Caller-ID [6] and Sender Policy Framework (see the “SPF and Caller-ID” box) or the delayed SMTP Greeting dialog.

Merak Mail Server

The Merak mail server [7] surprises administrators with its feature-richness at first, but on closer inspection, many useful features are concealed by the unintuitive user interface. For example, Merak has functions for testing an antivirus scanner with the Eicar test virus, and it combines Spamassassin with Bayesian filters.

After completing the installation, the command line wizard helps you set up the admin user, and a default domain. The program then gives you a choice of three tools: one for the command line, the second a browser-based GUI, and a third a remote administration console. The three tools differ greatly with respect to feature scope and application: only the console (Figure 3) gives administrators central access to the full set of features. We also had a problem with the fact that the Merak mail server will act as a relay for all private IP addresses (RFC 1918) by default.

Although the server achieved just one sixth of the throughput claimed by the Merak website in our lab (according to Merak it should be able to handle 20,000 emails per second on a dual Pentium system), it still had the highest throughput of all the mail servers tested. The webmail interface includes a collection of skins and layouts. In contrast to its

Buying the Merak Mail Server

Merak 8.5 comes in variants with six to seven plugins/modules. The standard version with an unlimited number of users and domains (including the web mailer) is EUR 735 / US\$ 918. Add-on modules for anti-spam, anti-virus, or groupware are licensed by the user. Groupware for 500 users costs EUR 860 / US\$ 1,074. The Merak Mailserver Lite Bundle for 12 users, including anti-spam, anti-virus, and groupware, costs EUR 315 / US\$ 393. <http://www.merak-mailserver.com>

All prices include one year's software maintenance. A migration tool is available. Merak charges EUR 50 / US\$ 62 for the smallest version (50 users).

SPF and Caller-ID

The Sender Policy Framework (SPF) is an SMTP extension introduced in 2003 that allows users to identify messages with spoofed email sender addresses. To allow this to happen, the DNS zone file of the sending domain has additional information that specifies which SPF clients are allowed to send mail via the mail server in the domain. For each incoming message, the receiving mail server checks if the remote server is al-

lowed to send mails for this from address, based on the policy published via DNS. <http://www.openspf.org>.

SPF is the successor to the RMX (Reverse MX) project and merged with RMX in 2004. RMX only supported evaluation of the standard MX record in a zone file. In contrast to this, SPF supports complex policies that allow you to authorize servers in third-party domains or clients on the LAN as relays for your own domain.

two competitors, Merak was incapable of handling several thousand email messages in a user inbox. In some cases, we were unable to open jam-packed user mailboxes in the webmailer.

Unlike Kerio, Merak can't offer full integration with a directory services environment. Although the server supports LDAP for allowing mail clients to access its internal directory structure (address books, public folders, calendars), it can't sync with Active Directory or use AD's user administrator features. This leaves the administrator no alternative but to maintain user data separately, both on the Merak mail server and in Active Directory. After setting up a user account on both systems, users can at least authenticate against Active Directory on the mail server or web client.

Again in contrast to Kerio, Merak sells separate licenses for the groupware function. The Merak licensing model is complex and difficult to understand. To help administrators understand, the console provides a license window, which also gives you a useful overview of add-in features.

The Merak mail server was originally developed by a Czech software company, Icewarp [8], and the same people developed the virus scanner used by the Merak mail server. The GUI supports the AVG, F-Secure, and McAfee engines. You

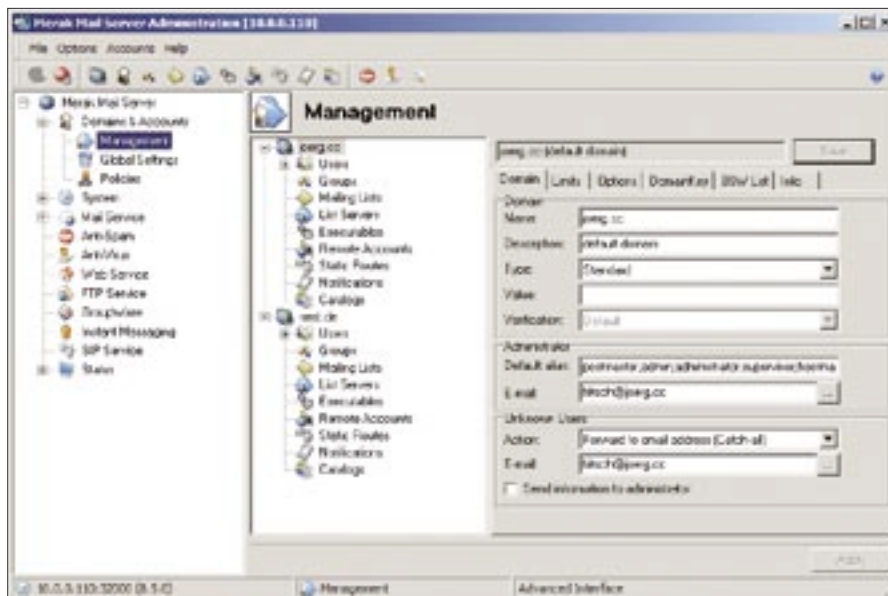


Figure 3: Only the console gives administrators central access to all of the Merak mail server's settings. The product has such an enormous range of functions that the cluttered interface can't hope to cover them all.

can add other products manually, simply by specifying the path to the executable or shared library. Merak was the only product in our test that notified internal users of virus-infected emails. To provide spam protection, Merak implements greylisting and SpamAssassin [12].

Benchmarks

All three candidates had to prove their value under lab conditions. For our

benchmarks, we ran the software on a lab machine (see the "Test Environment" box.) The most important test criterion was the number of test messages, all of 10 Kbytes each, that the mail server would accept for local users in boxes within one minute [13].

A mail server can be set up at different locations on a LAN. It can reside behind a mail relay, behind a virus scanner, or as a mail gateway between the Internet

Table 1: Benchmark

Product	Single connection, 10-KByte mail	Single connection, Header only	200 connections, 10-Kbyte mail	Error with 200 Connections	POP3 ³	Webmail ³	IMAP ³
Axigen	1,295 [Msg/min]	105,694 [Msg/min]	4,174 [Msg/min]	41 [Err/min]	–	✓	–
Kerio	1,353 [Msg/min]	156,410 [Msg/min]	8,477 [Msg/min]	0 [Err/min]	5,414 [Msg/min]	✓	–
Merak	1,363 [Msg/min]	24,878 [Msg/min]	16,981 [Msg/min]	7 [Err/min]	1,333 [Msg/min]	–	–
Sendmail ¹	984 [Msg/min]	925 [Msg/min]	1,520 [Msg/min]	1,988 [Err/min]	n.a.	n.a.	n.a.
Sendmail ²	not tested	not tested	5,221 [Msg/min]	0 [Err/min]	n.a.	n.a.	n.a.

1) Default configuration 2) Optimizations: *MaxDaemonChildren* and *RefuseLA* set to 248 3) Tested with 1000 mails in the Inbox

ADVERTISEMENT

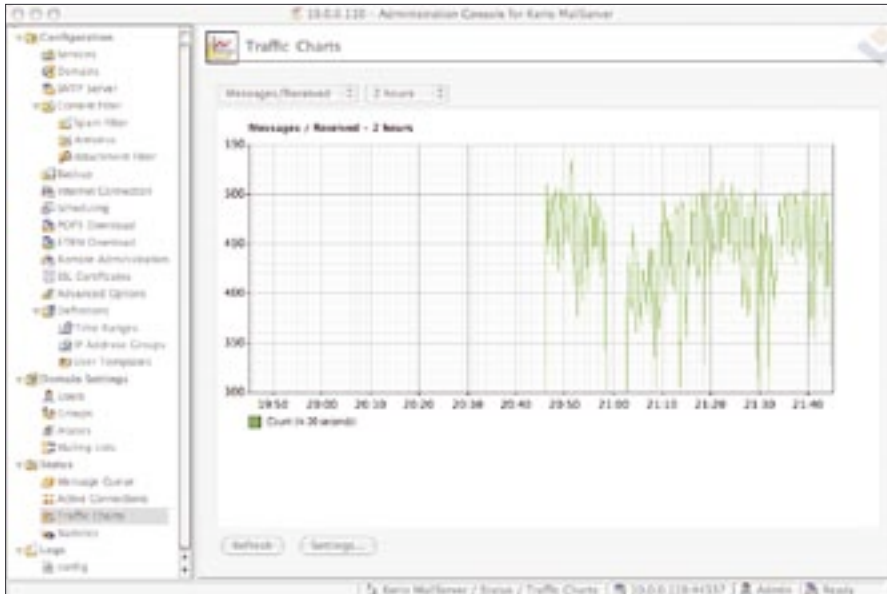


Figure 4: The reporting tool on the Kerio admin console confirms our test results. The test software delivers 10 Kbyte messages via a single connection. Kerio can handle about 500 messages within 20 seconds, at a rate of 1,500 messages per minute.

and the internal network. The requirement profile differs greatly in all cases. A mail server on a LAN behind a relay or AV scanner has to accept as many emails as possible over as few simultaneous TCP connections as possible (one to four). Our test for this scenario used a single connection.

A server that is used as an Internet mail gateway has to handle a large volume of messages from a large number of systems. To cover this application, we ran a throughput test with 200 simulta-

neous TCP/SMTP connections. In both scenarios, the test software sent 10 KByte messages. A third test ruled out overhead from filesystem activity; we simply required the server to process email headers; the messages did not have a body.

The final test concerned POP3 server performance, if the product came with a POP3 server. In this case, the client attempted to empty a jam-packed user inbox – in other words, the server only had to maintain one connection.

The tests were performed for 60 to 90 minutes, however, the results stabilized after approximately 10 to 15 minutes and did not vary until the end of the test. We included the results for a Sendmail daemon [10] as reference values. We ran Sendmail in its default configuration with a typical tweak: 248 child processes (*MaxDaemonChildren*) and a *RefuseLA* value of 248.

Table 1 gives the results of the test (see also Figure 4). In our lab, the three test candidates achieved surprisingly good throughput rates, and this qualifies them as candidates for medium-sized to large enterprises.

The Axigen mail server appears to be better suited to Internet providers, due to its configuration options, however, the throughput is not as good as the other two servers.

Merak shone with fast throughput, although the unintuitive configuration,

and the confusing feature scope detract slightly from Merak's performance. The Kerio mail server was the most trustworthy mail server in the test. Kerio was the only server not to make a single error under lab conditions.

Favorite

If you ask us which of the test candidates was our favorite, we would have to go for the Axigen mail server. The server is not suitable for companies looking for a mail server with groupware functionality, or wishing to migrate from Microsoft Exchange to Linux. But if you are looking for a good mail server with excellent webmail support, you will be very happy with the Axigen server.

The Kerio mail server is a well designed product that impresses with its groupware functionality and Active Directory integration. And the Kerio server proved its reliability under strict lab conditions. The Merak server left us with an ambivalent impression. The product attracts users with its enormous feature scope, but Merak takes much more time to understand than either of its competitors in the test. ■

INFO

- [1] Axigen Mail Server: <http://www.axigen.com/mail-server/>
- [2] Email filter samples with Sieve: <http://wiki.fastmail.fm/index.php/SieveExamples>
- [3] Sieve RFCs: 3028, 3685, 3598, 3431, and 3894: <http://www.ietf.org/>
- [4] Kerio mail server: http://www.kerio.com/kms_home.html
- [5] Kerio groupware functions: http://www.kerio.com/kms_collaboration.html
- [6] Kerio info on Caller-ID: <http://www.kerio.com/callerid>
- [7] Merak mail server: http://www.merakmailserver.com/Products/Merak_Linux_Mail_Server_Software/
- [8] Icewarp: <http://www.icewarp.com>
- [9] Sendmail.com: <http://www.sendmail.com>
- [10] Sendmail.org: <http://www.sendmail.org>
- [11] Clearswift Mimesweeper: <http://www.mimesweeper.com>
- [12] Spamassassin: <http://spamassassin.apache.org>
- [13] Postal benchmark utility for mail servers: <http://www.coker.com.au/postal/>

Patent Pitfalls

The Caller-ID draft was proposed by Microsoft in 2004. The technology and implementation are similar to SPF. However, Microsoft's Caller-ID syntax is XML-based, and parts of it are patented. In 2004, there were several attempts to merge SPF and Caller-ID as the Sender-ID, however, the attempts failed due to problems with patents. <http://www.microsoft.com/spam>

Besides these technologies, Yahoo's DK (Domain Key) <http://antispam.yahoo.com/domainkeys>, and its successor DKIM (Domain Keys Identified Mail), which was developed and standardized by the IETF <http://mipassoc.org/dkim/> are worthy of mention. DKIM aims to ensure the integrity and authenticity of messages on the path between mail servers. The method is based on additional DNS information, and on cryptographic methods.