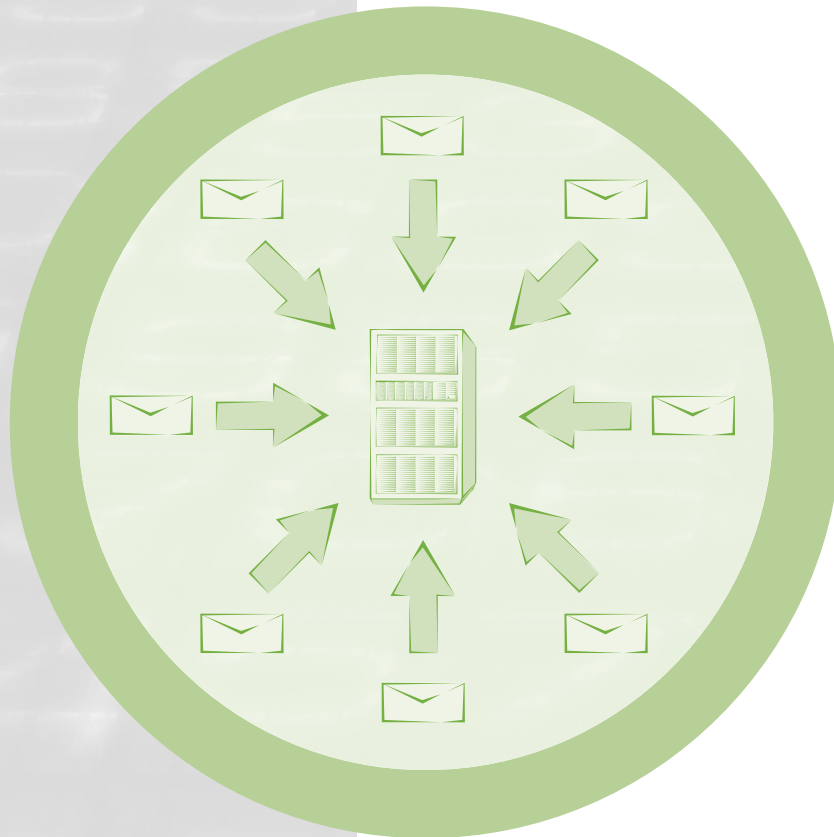


# SUSE

## eMAIL SOLUTIONS BASED ON SuSE LINUX ENTERPRISE SERVER 8



# SUSE

## eMAIL SOLUTIONS BASED ON SuSE LINUX ENTERPRISE SERVER 8

<b>1 OVERVIEW</b>	.....	3
<b>2 VALUE PROPOSITIONS</b>	.....	3
<b>3 SYSTEM STRUCTURE</b>	3.1 System Structure Diagram.....	3
	3.2 Standards.....	4
<b>4 IMPLEMENTATION</b>	4.1 Administration/Directory Service .....	4
	4.1.1 Account Data .....	4
	4.1.2 Integration in Existing Structures .....	4
	4.1.3 Scalability/High Availability .....	5
	4.1.4 OpenLDAP2 .....	5
	4.2 Mail Routing/MTA .....	5
	4.2.1 E-Mail Transmission/Reception/Routing ..	5
	4.2.1.1 Sendmail.....	5
	4.2.1.2 Postfix .....	6
	4.2.2 Viruses/Spam .....	6
	4.2.3 Scalability/High Availability .....	6
	4.3 Mail Storage .....	6
	4.3.1 Reception.....	6
	4.3.2 Data Management.....	7
	4.3.3 Backup .....	7
	4.3.4 Scalability/High Availability.....	7
<b>5 LOCATIONS</b>	.....	7
<b>6 SECURITY</b>	6.1 Base System.....	7
	6.2 Transport Encryption .....	7
	6.3 Virus Protection .....	7
	6.4 Audit/Supervision .....	8
<b>7 CLIENTS</b>	7.1 E-Mail .....	8

## 1 OVERVIEW

This document describes the concept for the setup of scalable e-mail systems on the basis of the operating system SuSE Linux Enterprise Server. The concept represents a complete e-mail solution for medium-scale enterprises, public administrations, and all who depend on professional e-mail communication. By means of additional high availability and cluster concepts, the solutions presented here can be expanded for advanced requirements.

The utilization of proven Open Source components allows the realization of large and very large projects. SuSE Linux Enterprise Server is an ideal platform for establishing mail infrastructures that can be scaled from a few hundred to hundreds of thousands of users and customized according to their individual needs. The availability of SuSE Linux Enterprise Server with the same code basis for all common hardware platforms from PCs to mainframes enables the gradual expansion of the implemented solution and direct recycling of its customizations and configurations. This helps to reduce investment costs and increases the investment security.

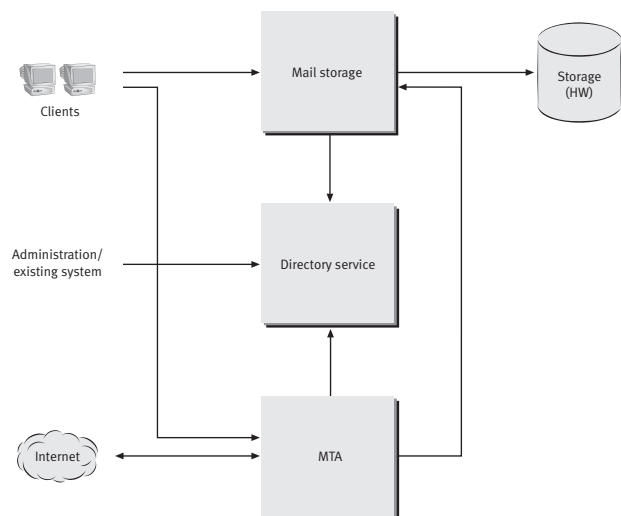
## 2 VALUE PROPOSITIONS

Open standards guarantee the perfect integration in existing structures and the interoperability with other systems. Furthermore, the underlying Open Source development model ensures optimum maturity of the software with a view to security and stability. The utilized technologies deliver performance, high availability, and an unusually high degree of scalability: SuSE's e-mail solution simply grows along with the requirements. The e-mail solutions based on SuSE Linux Enterprise Server are characterized by the following customer advantages:

- Modular and flexible structure
- Standardized interfaces
- High scalability and availability
- Possibility to configure an unlimited number of domains
- Use of an unlimited number of e-mail aliases
- Integration of an unlimited number of separate locations
- Support of all IMAP/POP3 clients

## 3 SYSTEM STRUCTURE

SuSE Linux Enterprise Server includes all components required for the establishment of a highly scalable e-mail system. The setup presented in this whitepaper is implemented using various tested modular components. All individual systems can be configured as scalable and highly available elements, resulting in an extremely flexible and expandable overall system. As only standardized Internet protocols are used, the modular approach enables the integration of some existing structures from the customer infrastructure.



### 3.1 SYSTEM STRUCTURE DIAGRAM

Basically, a modular e-mail system consists of the following logical components:

- **Directory service (see 4.1):**  
The directory service centrally provides all required administration data.
- **MTA (Mail Transfer Agent (see 4.2):**  
The entire incoming and outgoing e-mail traffic as well as their internal distribution and the content check takes place by way of the MTA.
- **Mail storage (see 4.3):**  
The local e-mail messages are stored and made available to the respective users in the mail storage.

## 3.2 STANDARDS

Only SuSE Linux Enterprise Server packages with standardized Internet protocols and formats are deployed within the scope of the solution presented here. The use of internationally recognized standards provides several substantial advantages.

For example, the integration of such an e-mail solution in existing structures – such as directory services – can take place in an entirely transparent manner. Furthermore, the individual solution components can be selected in a flexible way in accordance with the on-site customer requirements.

Instead of using proprietary blackbox developments, only tested services that are available around the globe are utilized, ensuring maximum functionality and security.

The standardized protocols and services used for the scalable e-mail solution include the following:

Internet e-mail	RFC 822
SMTP/ESMTP	RFC 821 1651 1854 1869 1870 2554 2821
SMTP/TLS	RFC 2487 2246
LMP	RFC 2033
IMAP	RFC 1730 2060
POP3	RFC 1225 1939
TLS for POP2/IMAP	RFC 2595
LDAP	RFC 1777 2247 2251-2256 2307 2596 2829-2831 2849 3062 3088
TLS for LDAP	RFC 2830
Sieve	RFC 3028
MIME	RFC 2045 2046 2047 2048 2049

## 4 IMPLEMENTATION

### 4.1 ADMINISTRATION/DIRECTORY SERVICE

The directory service is a basic component of the e-mail system, which centrally provides all information required for the operation.

#### 4.1.1 Account Data

The directory service contains all relevant data regarding the individual users and their accounts. An “object” is created for each account. The following information is stored in this object:

- All user-specific authentication data (user name, password, etc.) for the login to the system. This information is utilized by the IMAP/POP3 server.
- The alias information for an unlimited number of aliases for each account. These data are utilized by the MTA (Mail Transfer Agent).
- All mail routing information for the subsidiaries and an unlimited number of subdomains. These data are also utilized by the MTA.
- Information regarding the mapping of the users to their mail storage systems. This information is required by the IMAP proxy server and the MTA.
- Additional user-specific information such as phone and fax numbers, department details, etc. This information is utilized by the client.
- The private address book of the user. This information is also utilized by the client.
- All authentication data for administrators for remote maintenance purposes. This information is utilized by all systems.

#### 4.1.2 Integration in Existing Structures

The use of the open standard LDAP (Lightweight Directory Access Protocol) as directory service facilitates the integration of existing structures such as LDAP servers, X500 services with LDAP interface, or any databases with LDAP interface. LDAP is a TCP/IP-based directory access protocol that is widely accepted as the standard solution for the intranet/Internet. The integration of the existing structures is possible either by enabling direct access to existing structures or by synchronizing the information in regular intervals.

In this way, it is possible to adopt or integrate existing central administration systems instead of completely replacing them – which would cause additional work and costs. The package `nss_ldap` which is required for direct access to LDAPv3-compliant servers is included in SuSE Linux Enterprise Server.

### 4.1.3 Scalability/High Availability

The system component “directory service” is highly scalable, as all data can be replicated on an unlimited number of hosts. In order to relieve the LDAP server and especially the network traffic, an LDAP server can be deployed in LDAP caches by way of replication.

This means that all changes on an LDAP server are directly replicated to its caches without any delay. These caches are especially suitable for use on local target systems (MTA, proxy, IMAP server) for the purpose of minimizing number of LDAP queries over the network.

### 4.1.4 OpenLDAP2

The OpenLDAP2 service, which is available with SuSE Linux Enterprise Server, has proved to be suitable even for large installations, and offers support for specifications and features such as the following:

- LDAPv3 (RFC 2251-2256, 2829-2831)
  - Strong authentication (SASL) (RFC 2829)
  - Start TLS (RFC 2830)
  - Language tags (RFC 2596)
  - DNS-based service location (RFC 2247 + 3088)
  - Password modify (RFC 3062)
- LDAPv3 extensions
  - Enhanced language tag/range option supports
  - Object class-based attribute lists
  - LDAP who am I? extended operation
  - LDAP no-op control
  - Matched values control
- LDIFv1 (RFC 2849)
  - Enhanced standalone server
    - Transaction-oriented database backend
    - Named references/ManageDsaIT
    - Enhanced access control subsystem
    - Thread pooling
    - Preemptive threading support
    - Multiple listener support
    - SASL authentication/authorization mapping
    - SASL in-directory storage of authentication secrets
    - Improved Unicode/DN handling
    - Meta backend
    - Monitor backend

## 4.2 MAIL ROUTING/MTA

The task of the MTAs is to distribute incoming and outgoing e-mail messages to the locations and the mail storage systems in accordance with the information in the directory service. Furthermore, they make sure that every single e-mail message is checked by the content filters.

### 4.2.1 E-Mail Transmission/Reception/Routing

The MTAs receive e-mail messages from external sources as well as from internal senders via SMTP (Simple Mail Transfer Protocol – a simple TCP/IP protocol). All required information for resolving the aliases and for the mail routing is retrieved from the directory service, thus allowing the entire mail routing to be centrally administered. Instead of the LDAP server, these data can also be retrieved from text files, indexed tables, or database queries.

Following the content check, outgoing e-mail is forwarded to the outgoing mail relays (systems that enable the transmission of e-mail and that prevent the unauthorized transmission of messages).

For incoming e-mail, initially all virtual users/domains are resolved in order to determine the final destination (local, external mail server, connected locations). If the recipient of the e-mail message is in the local system, the e-mail is forwarded to the mail storage system via LMTP (Local Mail Transfer Protocol). If the recipient account is maintained at a different location, the e-mail is forwarded to the respective MTA via SMTP.

#### 4.2.1.1 Sendmail

The development of this mailer started shortly after the release of the SMTP protocol in 1986. The many years of development have produced a very complex product which meets almost all requirements with its many standards and which has become a standard itself due to its widespread use. Due to the complexity and the monolithic structure usually, newcomers are usually confronted with numerous difficulties, which however can be tackled with the help of a variety of excellent books related to this subject. SuSE Linux Enterprise Server is shipped with Sendmail version 8.12.6.

#### 4.2.1.2 Postfix

Postfix (formerly IBM Secure Mailer) was written for IBM by Wietse Venema as an alternative to Sendmail. Administrators appreciate Postfix for its easy configurability. The mailer was especially designed for speed, efficiency, and security. For this reason, it is very popular for use on mail relays. In contrast to the monolithic Sendmail, the partial functionalities were strictly separated in the form of precisely parameterizable subsystems that communicate with each other via UNIX domain sockets. Almost all Postfix processes can run in a chroot environment with strictly defined minimum permissions without requiring the root ID as user. Therefore, there is no direct way from the network to the security-critical local delivery programs, and potential intruders would have to break through a long chain of programs. To prevent such an event from happening, all kinds of preventive measures have been implemented, as can be seen from the fact that even the individual Postfix components do not trust each other – neither the queue files nor its own IPC news.

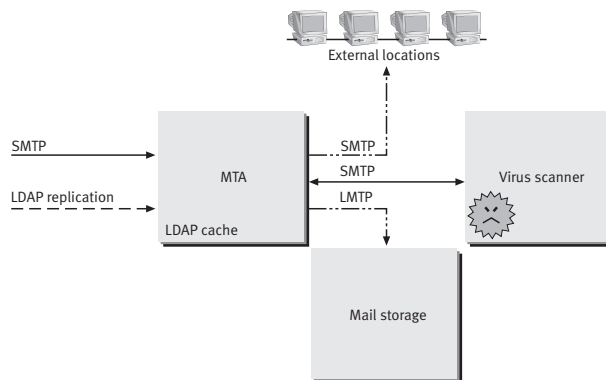
Due to the high level of compatibility of the interfaces and tables, an existing Sendmail installation can usually be adopted directly.

#### 4.2.2 Viruses/Spam

In order to distribute the load as efficiently as possible, the virus scanning function can be installed on an additional/standalone host. Depending on the existing virus scanners, two solutions can be deployed:

- **SMTP virus scanner:**  
The virus scanner receives all e-mail messages via SMTP, checks them, and returns them to the MTA.
- **Non-SMTP virus scanner:**  
A minimum MTA instance receives the e-mail messages via SMTP and transmits them to an external program that dissects the individual elements of the e-mail message and forwards them to a virus scanner. Following the successful screening for viruses, the e-mail message is returned via SMTP. In this way, any virus scanner available for Linux can be used.

Additionally, a content filter can be integrated in the MTA system, enabling spam messages (undesired or dangerous e-mail messages or advertising) to be sifted at an early stage.



#### 4.2.3 Scalability/High Availability

The MTA system is scalable to a virtually unlimited extent, as several MTAs can easily be operated concurrently. For detailed concepts, please refer to the respective whitepapers in this series.

### 4.3 MAIL STORAGE

The local e-mail storage takes place in the mail storage system. SuSE Linux Enterprise Server offers Cyrus IMAP of the Carnegie Mellon University, a very mature and widely used server that has been successfully used in the SuSE Linux Business Products for many years.

The access to the stored messages is possible via IMAP (Internet Message Access Protocol) and POP3 (Post Office Protocol Version 3).

#### 4.3.1 Reception

The MTA can use two different methods for the delivery of the e-mail messages to the mail storage system. Apart from the classic approach of passing on the data to a mail delivery agent (usually procmail) via UNIX pipes, some systems (including the Cyrus IMAP) offer the LMTMP protocol which was specifically designed for this purpose. Thus, if TCP/IP is used, the MTA and the mail storage system can easily be operated on separate hosts. The forwarding of the recipient information to the mail storage, which takes place in the scope of this concept, provides a number of additional advantages such as the single storage of messages.

### Filter/Automatic Response

User-defined filters and vacation notifications are processed on the mail storage system when e-mail messages are received.

Depending on which of the above-mentioned variants is used, the rules for these filters are either integrated directly in the procmail configuration or should be processed directly by the server if LMTP is used. Cyrus IMAP uses the scripting language Sieve for this task. This simple programming language and the RFC standard were especially developed for the automatic processing of e-mail over the network.

### 4.3.2 Data Management

In Cyrus IMAP, all e-mail messages are stored in a file system. For each e-mail message, a file is created in the user directory. An index enables the quick allocation of header information, i.e. administrative information such as the sender, recipient, sender system, time, subject etc. can be seen immediately. Thus, all critical information is stored in a reconstructable form (plain text), so that a loss of data can only come about in the event of a failure of the underlying file system. Cyrus IMAP offers possibilities for the transparent partitioning of the mail boxes, allowing the setup of mail storage systems of a virtually unlimited size by connecting modern NAS filers or SAN systems. The integration of hierarchical storage management solutions in the file system is easy and generally does not cause any problems.

### 4.3.3 Backup

As the e-mail storage is based on the file system, every folder of an account and every message can be restored individually.

### 4.3.4 Scalability/High Availability

The mail storage system can be arranged in a cluster comprising an almost unlimited number of hosts. High availability can be achieved with various concepts. Please refer to the respective whitepapers in this series.

## 5 LOCATIONS

With the help of the components described above, an e-mail system can be expanded to include any number of locations by means of separate implementations. Depending on the existing infrastructure, the e-mail exchange between the locations can be realized in two different ways:

- **Distribution via DNS (Domain Name Service):**  
The resolution of all aliases and virtual users takes place on the central MTA. Subsequently, the e-mail message is forwarded to the respective location via MX resolution in the DNS.
- **Distribution via LDAP:**  
The resolution of all aliases and virtual users takes place on the central MTA. Subsequently, the e-mail message is forwarded to the respective location by way of the transport configured in LDAP.

Of course, these two mechanisms can also be combined. For small locations, the system can be installed on a minimum of two redundant hosts.

## 6 SECURITY

### 6.1 BASE SYSTEM

SuSE Linux Enterprise Server offers various programs for a restrictive configuration and for external protection. In this connection, please refer to the respective whitepapers in this series.

### 6.2 TRANSPORT ENCRYPTION

Allmost all kinds of communication between the hosts in the system can take place with SSL/TLS\* encryption:

- LDAP replication
- IMAP access
- POP3 access
- SMTP

### 6.3 VIRUS PROTECTION

Virus protection can be integrated in the system at two points:

- Every e-mail message is scanned for known viruses when it enters and leaves the system.
- As e-mail messages are stored in files, all saved messages can be scanned continuously for any existing viruses.

\*Secure Socket Layer/Transport Layer Security: protocol for the encryption and authentication in the client/server communication

## 6.4 AUDIT/SUPERVISION

All log information is consolidated centrally and can therefore be supervised and analyzed centrally.

## 7 CLIENTS

Thanks to the use of standard protocols, the selection of possible clients is very flexible.

### 7.1 E-MAIL

Any IMAP/POP3 client can be used to access the stored e-mail messages. Both encrypted as well as unencrypted access is supported.

Any SMTP client can be used for sending messages. Both encrypted as well as unencrypted access is supported.

Furthermore, many free web frontends can be used as clients on the basis of the SuSE Linux Enterprise Server package apache with the modules for the scripting languages PHP and Perl.

© SuSE Linux AG 2003

Linux is a registered trademark of Linus Torvalds.

UNIX is a registered trademark of The Open Group.

All other company, product, and service names or designations may be trademarks or service marks or registered trademarks or service marks of other companies around the world and shall be treated as such.