Migration Guide

A guide to migrating the basic software
components on server and workstation
computers

Version 1.0 – July 2003

If you are interested in publications by KBSt currently available or further information concerning the documents, please contact

>> **Bundesministerium des Innern**
>> **Referat IT 2 (KBSt)**
>> **11014 Berlin, Germany**

>> **Tel.: +49 (0) 1888 681 - 2312**
>> **Fax.: +49 (0) 1888 681 - 52312[1]**

>> **KBSt homepage:** http://www.kbst.bund.de

---

[1]Frau Monika Pfeiffer (mailto: monika.pfeiffer@bmi.bund.de)

Migration Guide

A guide to migrating the basic software components on server and workstation computers

Version 1.0

July 2003

Published by the
Federal Ministry of the Interior

Contents

CONTENTS

1   Introduction

"A product replaces another one if it offers customers an incentive for a change which outweighs the change costs or which overcomes the resistance to change. A replacement product offers an incentive for change if, compared to its price, it offers customers a higher value than the product that was previously used."

M.E. Porter

1.1   About the project

There is hardly any statement that describes the core of the intensive public debate on the use of open-source software better than this relatively simple statement by this Harvard Business School professor on the fundamentals of competitiveness. Linux as the open-source flagship has a long history as an established (from the point of view of competition theory) "replacement product", whilst other products, such as MySQL or Open Office, are still on the way to this. (Should you miss the OSS classic, Apache, in this enumeration, please note that the authors of this guide consider this product the original rather than a replacement).

The Linux operating system, in particular, is one of the few software products today that records continuous growth rates and which is already successfully used in more than 40% of German companies and organizations[2], and this trend is still growing. In view of this development, it should be fairly easy to answer the question concerning the incentives which led to the development of the open source software.

However, this assumption is not true - on the contrary: There is hardly any other subject that is as controversial in the information and communication industry as the pros and cons of open source software. Considering the fact that annual sales of Windows operating systems alone exceed USD 10 billion, it is, however, easy to see that the debate on alternatives is influenced by substantial economic interests.

The technological properties of the products and the economic parameters of the alternatives compared will be discussed in addition to the fact that the license model is unique and in addition to the frequently voiced questions concerning the influence of this model on the innovative capacity of the IT industry. This leads to a multi-dimensional and hence inevitably complex study which is open to interpretation. Furthermore, the competitors - i.e. open source vs. Microsoft - are no longer isolated software products but an almost complete platform with a wide range of software.

An objective and comprehensive analysis plays a key role in this situation which is determined by the most varied interests and a high degree of complexity. Such

---

[2] Berlecon Research, 2002

a study should address not just the technical properties of the software in question, but also the concrete starting situation for its future use, in particular, the specific financial, structural/organizational and political frame of reference of public administration in Germany.

1.2   About this guide

The title of this document already suggests that - initially irrespective of the general decision to introduce open source software - the "natural" life cycle of the Microsoft software requires several migration decisions. A good example is the phasing out of support for Windows NT which is still widely used, with its successor operating system requiring a fundamentally different approach towards the design of domains.

In order to differentiate between the replacement of this software by OSS products and a change to subsequent generations of Microsoft products, the terms *"replacing"* and *"continuing"* migration are generally used in this guide. The migration guide focuses on recommending the optimum and economically reasonable solution rather than strictly aiming to replace products already in use.

The migration guide is designed for decision-makers in charge of planning and implementing IT strategies and projects in public administration.

The first part (chapter 2) deals with the starting situation of the IT software which led to the development of migration plans and gives an overview of the basic architecture of the Microsoft software and the alternative platform based on open standards / open source. The so-called system landscape map shows which functions are covered by concrete products or solutions and visualizes the correlations between individual product and software layers.

The second part (chapters 3 and 4) addresses the issue of potential migration or new introduction of systems and infrastructures. The individual application areas of the software are analyzed both from a technical and from a commercial point of view. Whilst the technical analysis focuses on the identification and evaluation of alternative solutions to Microsoft products, the commercial analysis addresses the question as to how the change in software can be handled in the most economical way possible.

The third part (chapter 5) contains the migration recommendations for the different public agencies as a summary of the technical and commercial analysis. These recommendations include concrete proposals for small, medium, large and specialized public agencies. The pros and cons of different migration paths are additionally weighed. The third part finally shows the factors critical for the success of migration projects. Although replacing a software is generally nothing new, experience from the migration projects carried out in public administration confirms that the introduction of software products must be carefully planned and that the success of these projects is strongly dependent on the preparation of the staff involved in the migration task.

Introduction

During the several months of work on this migration guide, it once again became apparent that this subject is a very dynamic and rapidly changing field. The number of software packages available under Linux, both under GPL and of a commercial nature, increased visibly during the term of this project. This also applies to the number of manufacturers who not only voiced their strategic commitment to the Linux strategy, but who also launched concrete products or at least a release plan. Besides large software suppliers, such as SAP, Oracle, Sun or IBM, small and medium-sized software companies are increasingly offering a growing number of specialist applications and systems. This is a positive development for open-source supporters which contributes towards the increasing maturity of the OSS offers on the one hand, but also makes it increasingly difficult to maintain a clear overview of what has already been achieved.

At the end of the day, it is left to the readers themselves to identify the "change incentives" which apply to their specific situation. The authors hope that the migration guide will be a good and reliable aid for technical and commercial considerations.

1.3 How to use this guide

The following section contains a short introduction of how to use the internal structure of this document. It is designed to provide readers with navigation support, so that they can easily find the contents relevant for them in this rather weighty volume. The guide addresses two different target groups. One target group is made up of decision-makers in charge of planning and implementing IT strategies and projects. The second group comprises IT managers in public agencies who will certainly be very interested in detailed technical descriptions. We recommend that both target groups read the following information.

This chapter ends with a section specifically for decision-makers. The section titled "Information for decision-makers" contains a summary of the most important contents and results of the migration guide in concise form.

No reader of this migration guide should skip the first four sections of chapter 2. These sections contain important terminological definitions which are important for the rest of the guide. Furthermore, the components of the IT landscape underlying a migration project are described. The components after replacing and after continuing migration are described.

Furthermore, the individual explanations in chapter 3 begin with a summary of the aims and results of the technical explanations concerned, so that decision-makers can obtain an overview of the results of the technical explanations of the different migration components.

Chapter 4.7 contains a summary of the results of the commercial analyses. Moreover, chapter 5 also contains recommendations related to the economic effects of the different migration methods.

The commercial analysis (chapter 4) deals with the financial aspects of migration projects and is hence particularly relevant for readers who have to make fundamental strategic and economic decisions. Different scenarios are used in order to study the monetary aspects of possible migration projects.

The chapter on "Migration recommendations" provides details of the decisions relevant for a public agency. This chapter contains recommendations for combinations of suitable system components for different migration scenarios[3] for different public agency structures[4]. These recommendations are based on the preceding technical and commercial analyses. The explanations in the section titled "Gentle migration" address the interesting question as to which conditions and factors have to be considered for a successful implementation of the project. This constitutes the important and relevant information which decision-makers need. However, every decision-maker is free to read the other contents of the guide as well.

The complete guide is probably interesting for IT managers. The structure of the guide is such that chapter 2 titled "Focal points of the migration guide" which follows the introduction contains general information which is important as a basis for understanding the complete guide. The sections following the first four sections already mentioned contain information related to different Linux distributions, open source license models and, above all, information related to the data basis for this guide.

The technical details discussed in chapter 3 are likely to be the most important source of information for IT managers who are familiar with the specific technical requirements of their agencies when it comes to issues such as those below:

What is technically feasible and/or where are problems?

How can known problems be resolved or by-passed?

What is important from a technical point of view when it comes to migrating a component?

Which functionalities can continue to be used after migration, and/or where are restrictions?

And much more.

Within the individual sections, the system components are discussed from a technical point of view. The different aspects first describe the technical starting situation and subsequently address aspects of replacing and continuing migration. An overview of the different technologies is presented to technically competent and interested readers. Readers will find detailed information concerning the suitability of the different solutions and products. The sections dealing with replacing migration contain a host of information especially for

---

[3] Fully replacing migration, fully continuing migration and partial migration.

[4] Small, medium, large and specialized public agency.

readers who are not yet familiar with Linux-based technologies or who have only had limited contact.

Chapter 5 compiles the technical and economic analyses of the preceding chapters to form concrete recommendations. This chapter presents different scenarios which are explained in a differentiated manner, depending on the size and specialization of the public agency concerned. Readers can retrieve targeted information depending on their needs and concrete starting situation.

1.4 Information for decision-makers

1.4.1 General recommendations

As already mentioned in the preceding section, the migration guide generally analyzes both routes, i.e. replacing and continuing migration. The general result can already be mentioned here: The number of scenarios where replacing migration using open source products is the more favorable approach for public agencies has increased. This is, on the one hand, due to the results of the evaluation of economic efficiency where OSS products are generally quite successful. On the other hand, today's advanced maturity, penetration and compatibility of OSS products are particularly paving the way for migration projects and thus contributing towards lower change costs than in the past. The evaluation of economic efficiency, in particular, confirms that substantial savings can be achieved not just when license fees are no longer charged, but also - and above all - due to the competition that is growing between operating systems and Office products.

The results of the guide primarily refer to the starting situation which still prevails in many public agencies. These environments are characterized by Windows NT 4 as the operating system and the related Microsoft software products, such as MS Exchange 5.5, Internet Information Server 4 and MS SQL Server 7.

1.4.2 Continuing and replacing migration

This configuration is the starting situation for continuing migration within the Microsoft product family. Special emphasis is placed here on the migration of the above-mentioned products to 2000 and the 2000 product series - also with a view to Windows XP and Windows 2003. The focus on Windows 2000 does not mean that readers who have already completed the change to Windows 2000 should put this guide aside now. This guide provides useful information even for those public agencies, both in its technical analyses and in its recommendations. The discussion of these and the downstream measures for reducing internal dependency ensures that all options can be kept open with a view to future migration. These recommendations are primarily written for public agencies that have just completed the migration to Windows 2000 on the one hand, and for public agencies that are determined or (for whatever reason) forced to continue using the Microsoft product line for the time being.

A look at replacing migration shows that the results and recommendations should be differentiated in view of the number and diversity of solutions. The important

criteria for selecting the right solution are, in particular, size, intensity of IT use and the degree of "specialization" of public agencies which provide IT services for other public agencies. Matching products and configurations as well as the correct migration scenarios must be identified. This guide here differentiates between selective, far-reaching and complete migration - depending on the "reach" within the IT. Selective by replacing individual components of the IT landscape, such as the MS Office Suite or MS Exchange. Partially by replacing the complete server infrastructure whilst retaining or continuing the Windows clients. Completely by replacing all Windows systems with a Linux-based system landscape.

The recommendations of the migration guide here show which solutions should be given preference for which requirements and for which public agency structure from today's point of view.

1.4.3   Migration paths

The selection of the migration path, the choice between one-step and gentle migration, plays an important role. One crucial aspect is that it is technically possible to set up and operate heterogeneous (hybrid) system environments largely without difficulty. This gives public agencies the opportunity to replace individual components of their IT landscapes with open source software or commercial software for Linux within the scope of a migration project. The optimum migration route is determined by several factors. One-step migration (as the name suggests) means complete, replacing migration in one pass. Taking aspects of economic efficiency into consideration, this is the method of choice if IT infrastructures and systems already feature a high share of Unix penetration or if a public agency has a major demand for modernization (and a so-called investment backlog). Gentle migration is normally the better route. Gentle migration is carried out in one to three steps as partial and/or selective migrations. Gentle migration enables a gradual development of know-how concerning the new technology within the public agency and a gradual familiarization of administrators and users with new technologies and environments.

Irrespective of the selected migration route, the critical success factors must be taken into consideration in order to ensure successful migration. These success factors are pointed out in the recommendations. These factors include, for example, the necessary preparation, measures for information dissemination and creating user acceptance, the necessary training, management tasks or project organization in general.

Although adequate solutions are available for almost every demand and every requirement, a change from the familiar to the new often involves difficulties and subjective "pain" in many a case. One general aspect which both migration routes have in common is that system planners and administrators will be faced with a lot of new things. This is also true for users, even though changes are normally less striking on a user level.

1.4.4   Comparability of alternatives

It is an established fact that it is not possible to mirror all functions of Windows and other Microsoft products under Linux with open source software and/or commercial software for Linux. However, user experience with both platforms and migration projects already completed confirms the finding that both software alternatives are generally comparable.

Since special functions and concrete properties may well be important in the individual case, every public agency should evaluate the criticality of diverging functionalities for itself. Differences of this kind are found primarily in the field of Office applications, in particular, in the integration of special and Office applications, as well as in the field of document exchange compatibility between Microsoft Office and OpenOffice.org and/or StarOffice. Due to compatibility problems, common editing of documents with OpenOffice.org and/or StarOffice and MS Office is possible to a very limited extent only. Common editing is, in principle, possible at a contents level only.

The technical analyses show that generally adequate open source solutions and/or commercial solutions for Linux-based systems are available for the existing Windows system components and infrastructure services.

With regard to infrastructure services, Samba and OpenLDAP play an important role for the implementation of heterogenous system environments. CUPS is an innovative and at the same time tried-and-tested print service which meets with any requirements for an up-to-date, economically efficient and complex print environment. The number of increasingly complex software solutions for system management services is growing. However, Linux-based systems are also sometimes offered for the commercial management systems running under Windows.

Alternative solutions for MS Exchange include, for example, free software products, especially for use as pure mail servers. Samsung Contact is a full-scale replacement that enables the continued use of the Outlook client for medium and large environments and Exchange4 Linux for smaller environments.

Several free database management products are available. Examples include SAP DB, MySQL and PostgreSQL. Furthermore, commercial database systems such as Oracle and DB2 are tried-and-tested solutions under Unix/Linux and hence do not require further technical analysis.

The list can be continued for almost all applications and infrastructure areas. The migration guide contains separate sections on these issues, such as high-availability solutions or thin clients. Relevant differences between or restrictions to the alternatives discussed are explained.

1.4.5   Future key issues

In order to give the technical analysis the necessary future-orientation, the role of the components which pay a central role in Microsoft's new software architecture

will be discussed in addition to a description of the starting situation. These are, above all, the .NET Framework with its major components, i.e. web services and XML as well as the SharePoint portal server.

The following results can be summarized:

Both the .NET-Framework and the Java/J2EE alternative generally offer two possibilities for implementing the reusability of components and the interoperability between platforms and applications.

The reusability which can be achieved via the use of the same component model (COM+ in the case of Microsoft and JavaBeans in Java) will be referred to in this document as *deep integration* because of its dependency on the runtime environment and/or programming languages. The applications generated using a component model can be used within the same platform only.

XML will serve as the document and data exchange format and hence form the basis for the use of web services which, thanks to their independence from a concrete runtime environment and thanks to the use of protocol interfaces, can be used for *shallow integration* of services. The services based on web services can be used beyond platform boundaries.

In view of security problems which are currently still unresolved in conjunction with the use of applications offered via web services, it is at present not possible to give a general recommendation for the cross-platform *shallow* integration model. This will be a key task of ongoing development work.

A general recommendation for the component model with the *deep integration model* has already been laid down in the SAGA standardization recommendation and specifies JSE/J2EE as the mandatory component model because of the general platform independence. The use of any technology other than this preferred technology must be justified (for example, by significant commercial advantages) (in favor of the .NET-Framework, for example).

The use of XML as the data format which SAGA already specifies as the "universal and primary standard for the exchange of data between all the information systems relevant for administrative purposes", as well as the SAGA specification of PDF as the document exchange format will probably lead to a substantial improvement (however, certainly not to a complete elimination of all problems) in conjunction with the interoperability of the Office products with MS Office 2003 and higher.**Economic efficiency**The evaluation of the economic efficiency in the migration guide focuses on two key aspects:

To determine general statements concerning the economic efficiency of open source products

Introduction

> To describe methods and aids for the determination of agency-specific evaluations of economic efficiency and project-related calculations of migration costs.

With the migration cost matrix and an evaluation of economic efficiency tailored to the conditions of migration projects (WiBe 21)[5] two methodological approaches towards calculating the profitability of migration projects are described. This guide contains annotated model calculations for different scenarios in order to explain these methods in more detail. In order to consider the special features of the migration process, these model calculations include proposals for the analysis criteria to be selected as well as new analysis criteria and recommendations concerning the evaluation of the benefit analysis under the aspect of the preparation of an evaluation of economic efficiency according to WiBe 21. This means that this guide not only enables the assessment of a project in economic terms, but also helps determine ratios for the profitability or urgency and/or strategic importance of these projects. The migration cost matrix is also a quick and pragmatic form of support for the evaluation of economic efficiency.

We can conclude that the evaluations of economic efficiency particularly showed that the degree of integration into the Windows and MS Office environment will be one key decision factor in favor of or against replacing migration. The number of existing Office applications, the extent and complexity of the macros, scriptings and templates used, as well as the number and availability of the source code of the special applications used which can only run under Windows determine the economic efficiency and feasibility of replacing migration. This is why, especially with regard to this issue, some recommendations are aimed to reduce dependencies and increase interoperability.

---

[5] IT-WiBe 21 – Empfehlungen zur Durchführung von Wirtschaftlichkeitsbetrachtungen in der Bundesverwaltung, insbesondere beim Einsatz der IT, Version 3.0 – 2001, KBSt publication series, Volume 52, May 2001.

2 Key issues of the migration guide

2.1 Important definitions

Some terms used in everyday life are understood differently by different people. This concerns, for example, open source software, free software, proprietary software, commercial software, etc. Furthermore, this guide also introduces new terms.

In order to avoid misunderstanding when reading this guide, the most important terms are briefly defined in the following.

2.1.1 Open source, free software

The terms "open source software" and "free software" are used synonymously in this migration guide. The abbreviation used for this is OSS.

OSS enables every user to read and modify the freely available source code. This openness enables users to learn from the source code and/or adapt it to their personal requirements. The software is freely available, users do not have to pay any license fees. The modified software may be copied and distributed . The freedom of the software is defined and protected by the related licenses. Chapter 2.4 contains a description of the most important license models.

OSS should not be mistaken for software which, although freely available, may not be modified or amended by the user and/or which is subject to a license which prohibits the use of the software for commercial purposes.

2.1.2 Proprietary software

Proprietary[6] software is not OSS. It is owned by an individual or organization, usually the manufacturer of the software (copyright). The use of the software is subject to the terms of the license which the owner of the software has laid down. These terms usually prohibit duplicating, disseminating and modifying of the software.

Software of this kind is sometimes also offered for free on condition that the applicable terms of the license are adhered to.

2.1.3 Commercial Linux software

Commercial Linux software (COLS) includes the group of proprietary software products which can run under the Linux operating system. This software features the use of standards and the resultant interoperability as well as precisely defined interfaces.

---

[6] Latin: owner

2.1.4   Replacing migration

This guide differentiates between replacing and continuing migration. What is the difference between these two forms of migration?

Replacing migration means a change from Windows applications and services as well as complete Windows-based system environments to OSS or COLS platforms. Examples are:

> from Windows NT to Linux
>
> from MS Office to OpenOffice.org
>
> from MS SQL Server to Oracle

2.1.5   Continuing migration

Continuing migration means the continued use of the Microsoft product lines, for example, migration from NT 4 to Windows 2000, Windows XP or Windows 2003. Examples are:

> from Windows NT 4 to Windows 2000
>
> from MS Office 97 to MS Office 2003

2.2   Migration paths

Many public agencies and organizations are currently faced with the question as to how their future IT system landscapes are to develop in the years to come. The reasons for this are very diverse:

> Manufacturers phasing out support for key products
>
> Increased technical requirements
>
> Consolidation of existing system landscapes
>
> Strategic aims, such as increased manufacturer dependence and increased interoperability.

They are hence at present faced with the question as to which systems and components are to form the future basis of their IT structures. The migration guide analyzes and examines the following general migration paths:

> Replacing migration using Linux and open source software (OSS)
>
> Replacing migration using Linux / open source software and commercially available Linux products (COLS)
>
> Continuing migration with MS Windows 2000 and successor generations as well as the related Microsoft applications and systems.

Furthermore, options for hybrid migration paths must be considered because one cannot expect that alternative OSS/COLS solutions can be recommended for all the components of a legacy system, be it for technical and/or for commercial reasons.

Completely exhaustive analyses are not possible within the scope of this guide. This would be impossible both due of the complexity of the IT landscapes to be discussed and because of the very specific requirements of certain public agencies. Instead, the migration guide is meant more as a source of answers and help for decision making on the key questions which public authorities have to ask most of all.

2.2.1 Microsoft Windows as the starting situation

The illustration in Fig. 1:   System landscape – the starting situation

 shows the Microsoft system landscape which can be found in this or in a comparable form in many public agencies and organizations. The picture gives an overview of the services and software modules which form part of the assumed starting situation for the relevant migration analyses. Chapter 3 begins for each of these components with a technical description of the actual situation in terms of the functionalities and special characteristics available with a view to migration. This description is followed by a technical analysis of one or, if applicable, several adequate solutions for replacing migration. The third step is the technical analysis of continuing migration. The fourth and last step of the technical analysis is an evaluation and recommendation of one or the other migration path.

System landscape - the starting situation

Desktop Officesuite 97/2000	**Groupware** Exchange 5.5	**Database** MS SQL Server 7.0	**Web server** Internet Information Server 4.0

COM, DCOM

Infrastructure services NT 4.0 server

Authenti-cation services	File services	Print services	Network services	System manage-ment services
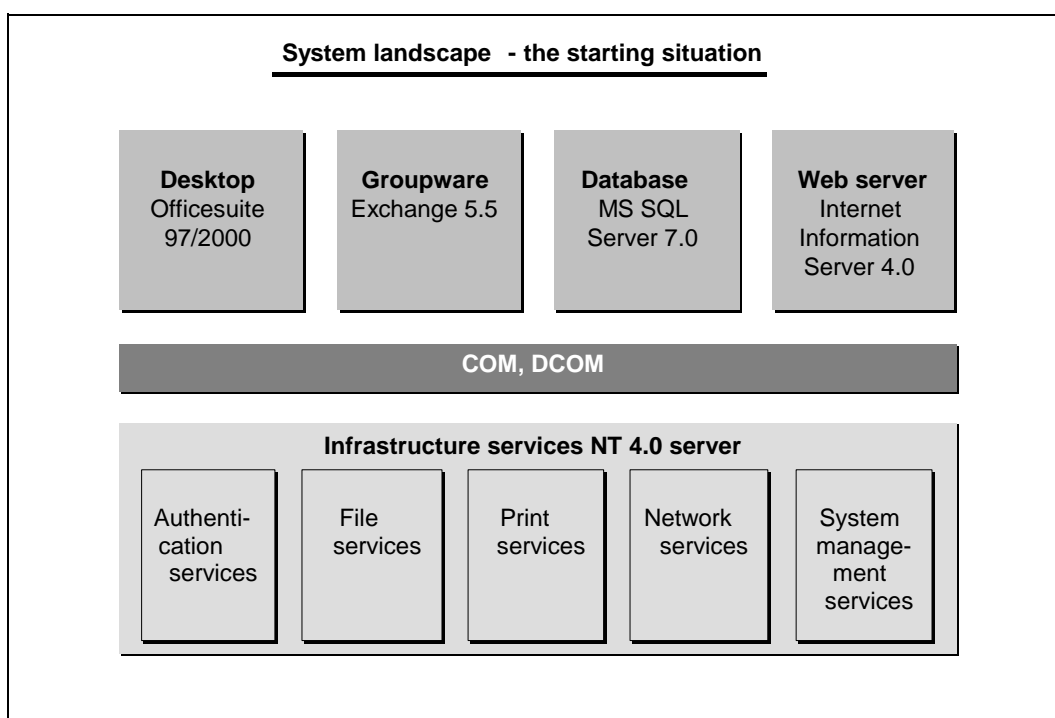
Fig. 1:   System landscape – the starting situation

Assumptions concerning the concrete features of an IT infrastructure were sometimes necessary when this guide was written. Unless any assumptions to

the contrary were made within the scope of the technical and commercial analyses, the following assumptions were made.

2.2.1.1   Server platform

It is assumed that the given starting situation at the public agencies is based on one of the two customary NT domain models.

Environment with an NT domain in which user and computer accounts are kept.

Environment with an NT account domain which includes the user accounts and several resource domains which keep the computer accounts and trust the account domain.

Within this environment, different infrastructure services, applications and integration components are made available on the basis of Windows NT 4 server.

The following key infrastructure services were considered in this guide:

Registration service - authentication

File services

Print services

Network services

System management services.

With regard to the server applications, this guide focuses on the following areas because of their wide-spread use in public administrations:

Internet Information Server (IIS) version 4 as the web server for intranet and Internet presence

Exchange 5.5 as groupware and messaging solution

SQL-Server 7 as the database management system for most database applications.

The different services and applications were normally linked and integrated on the basis of the

Component Object Model (COM) and

the pertinent Distributed COM (DCOM) service.

Windows NT 4 services can be provided using two different operating system variants:

Windows NT 4 Server

Windows NT4 Server Enterprise Edition.

The second variant (Enterprise Edition) enables the implementation of the services by two nodes (servers) in a cluster.

2.2.1.2   Client platform and applications

At the user end, one may expect that the Windows NT 4 Workstation will be the dominant operating system. Other operating system variants, such as Windows 95 or 98, are neglected in the analysis. The Microsoft Office suite is used as the most important application software in the basis of the operating system. Both version 97 and version 2000 must be considered in this context as the variants that are currently most frequently used. Users use them in their daily work. The programs which they use in this context are word processing, spreadsheet, presentation support programs as well as the messaging and groupware functions.

Besides these standard products, a host of special applications are used for agency-specific tasks which are often strongly integrated into the Windows desktop. These must be analyzed in detail with a view to migration. Since these applications are essentially affected by the migration of the underlying IT infrastructure, strategies for interim solutions must be developed, depending on their number and complexity. Some proposed and recommended procedures are described in this guide.

Finally, various further standard applications and tools (such as file manager, packer) are available to support users during their routine tasks. These applications and tools will be needed by the users even in the new system landscape.

2.2.2   System landscape with replacing migration

The illustration in Fig. 2:   System landscape – replacing migration

 gives an overview of an alternative Linux-based system landscape. The illustration shows the most important systems and applications for which replacing migration is possible.

Over the past decade, many software manufacturers developed their products and services for Linux or ported them to Linux. Besides large suppliers, such as IBM, SUN or Oracle, numerous smaller companies offering special solutions should also be mentioned here. Given the information and distribution basis which exists in the field of commercial software, it is not necessary to examine these products in more detail with a view to feasibility. The migration guide focuses on partly less well-known open source software solutions and on the solutions which made replacing migration possible in critical areas only recently.

The illustration in Fig. 2:   System landscape – replacing migration

 shows that more than one alternative solution is available for certain applications. This is why traditional open source software solutions initially move to the foreground of the technical analysis. In cases where adequate open source applications are not available, software solutions will be examined which represent a proprietary alternative under Linux and which are at the same time based on open standards.

System landscape - replacing migration

Desktop	Groupware	Datenbank	Webserver
OpenOffice , StarOffice	Php , Groupware , Kroupware , Exchange 4linux, Samsung, Contact ,....	My SQL, PostGreSQL , SAP DB, Oracle, DB 2, ...	Apache

OpenLDAP , J2EE

Infrastructure   Linux

Authentica-tion services (Unix, Samba m. OpenLDAP)	File services (Unix, Samba)	Print services (CUPS,Samba)	Network services	System manage - ment services
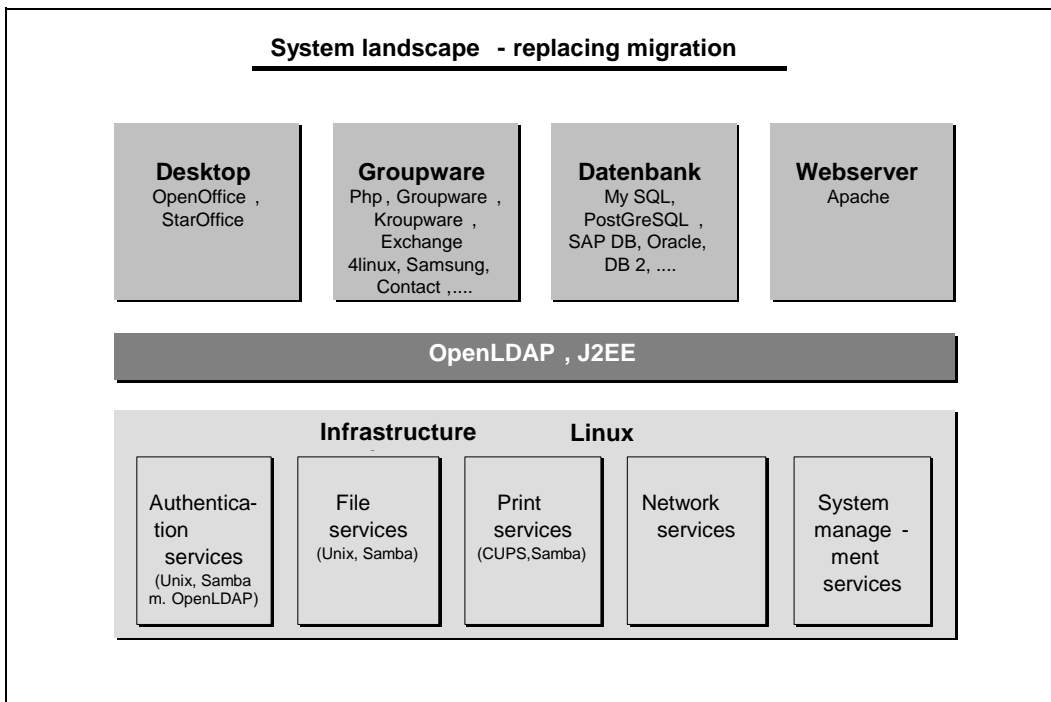
Fig. 2:   System landscape – replacing migration

2.2.3   System landscape with continuing migration

Continuing migration focuses on the replacement of the existing Windows NT 4 environment by newer versions. The illustration in Fig. 3: System landscape – continuing migration

shows that the products of the 2000 versions will stand in the foreground of the analysis. On the basis of the Windows 2000 server with its infrastructure services, chapter 3 discusses the special technical features and the technical and conceptual measures for the individual services and server products necessary for migration. Furthermore, the repercussions of the technical changes and innovations will be analyzed and evaluated.
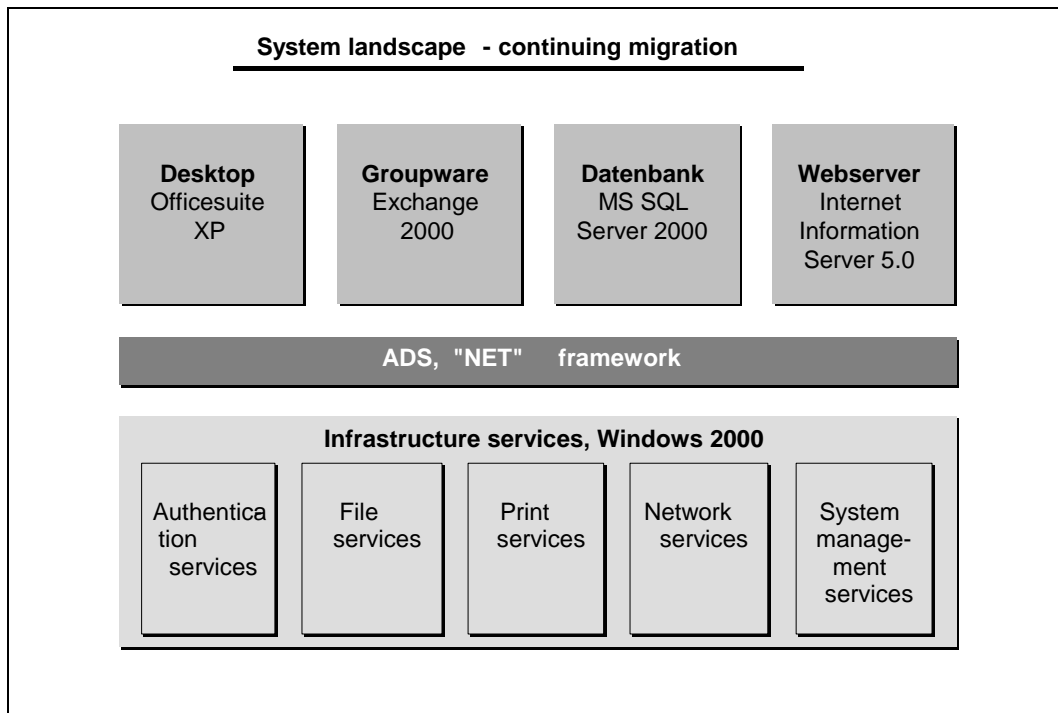
Fig. 3:   System landscape – continuing migration

Besides the server end, the desktop is analyzed analogous to the procedure for replacing migration. In this case, however, the analysis focuses on Office XP.

The analysis is ultimately extended – whenever the information available permits this - to include the introduction of the server and office products of the 2003 version.

2.2.4   Internal dependencies within the Microsoft system landscape

System architectures which are mainly based on Microsoft products are subject to internal dependencies of varying degrees. The following section explains some of the internal dependencies within an infrastructure determined by Microsoft.

One relatively obvious dependency is the fact that Microsoft application software can be installed and used on Microsoft operating systems only. This applies to the server applications of the back-office product range (i.e. MS SQL Server, MS Exchange, etc.) and, with a few exceptions, (Office 98 for MacOS, Internet Explorer 4 for Unix) also to the desktop applications (e.g. Office) and system-near client software (e.g. MS SQL client components).

Server applications in general typically require a user administration in order to authenticate the users and authorize access to resources. Microsoft offers different variants with regard to the user database to be used. The variants are enumerated below using the example of MS SQL Server.

Variant A:
An SQL-specific user management system is used.

Variant B:
The local user database of the server operating system is used.

Variant C:
The user database of a Windows domain structure is used on condition that the server is a member of this structure. Since the launch of Windows NT, this variant has been offered for almost all Microsoft server applications and enables a single sign-on for the user in a pure Microsoft environment.

Variant D:
A variant in which authentication and authorization instances of other manufacturers can be used is not offered.

With Windows 2000 and its successor systems, Microsoft shifts user administration and authentication to directory services (see below) and open standards, such as Kerberos and LDAP, however, without permitted non-Microsoft instances.

With regard to the Windows NT 4.0 world, even further dependencies concerning user administration must be mentioned. It is, for example, not possible to implement Microsoft Exchange environments (versions 4 to 5.5) without the Windows NT domain structure. Another example of the mandatory NT domain is the functionality of the cluster services. The same applies to the distributed DCOM (Distributed Component Object Model) component architecture created by Microsoft with a security infrastructure which requires that the client and the server belong to a common domain structure. A large number of client/server applications (from Microsoft and other manufacturers) use DCOM.

With Windows 2000, Microsoft developed the NT domain model further to the active directory service. Within the active directory, the NT domain model and its properties are still felt and necessary for downward compatibility purposes. The introduction of Kerberos as an authentication mechanism, for example, does not mean the elimination of the NTLM (NT LAN Manager) mechanism, all the more so, since pure Windows 2000 environments continue to use NTLM at certain points (such as clusters). At the same time, the active directory was amended by adding functionalities which were inclined to be handled separately or which did not exist at all in the former Microsoft world. With regard to the functionality of the group guidelines, parts were already known as system guidelines, Internet Explorer Administration Kit (IEAK) or Security Configuration Editor (SCM) under Windows NT. New features are certain functionalities in the group guidelines, such as software distribution, dependency on organization units, domains and sites or logon and logoff scripts.

One completely new feature of the Windows 2000 active directory is the integration of encryption technologies, such as IPsec or EFS (Encrypted File System). If these encryption technologies are to be used, a PKI (Public Key Infrastructure) must be set up that integrates itself into the active directory. In this context, Microsoft also developed the Kerberos protocol in order to enable authentication via SmartCards. Another mandatory requirement of the Windows 2000 active directory is a DNS (Domain Name System) infrastructure for name

resolution. The DNS must at least correspond to BIND version 8.2.2. Windows 2000 includes a DNS of its own.

Exchange 2000 is the first Microsoft product to require a Windows 2000 active directory as a mandatory feature. In contrast to Exchange 5.5, Exchange 2000 no longer has a directory service of its own. Any information of e-mail users and of the Exchange 2000 distribution lists is located in the active directory which must be prepared for the integration of Exchange by a scheme amendment. The Global Catalog service of the active directory plays a central role for Exchange 2000. Exchange 2000 uses this global catalog service in order to request information across domain borders. Outlook 2000, for example, also uses the Global Catalog. Furthermore, Exchange 2000 uses the active directory not just in read, but also in write mode: The Recipient Update Service of Exchange 2000, for example, writes its results into the active directory. The tools for e-mail user administration are completely integrated into the "active directory – Users and Computers" management console.

These correlations and dependencies among Microsoft's operating and application systems characterize an increasing integration depth within this platform and trigger several strategic issues with regard to the potential use of product alternatives.

How can the interruption of a certain product line and of the related update cycles be implemented?

How can the dependency of a product line and the related technical equipment be minimized?

Which measures lead to a reduction of manufacturer dependency and to a diversification of the software landscape?

Is there sufficient replacement for certain software components in the form of more cost-effective alternatives?

In view of the degree of dependency which has been reached by now on a product-internal level, these questions can normally only be answered by a strategic approach which must be considered within the scope of the IT concept of the administrations.

2.3   Linux distributions

2.3.1   Introduction

A host of different Linux distributions are available for implementing server and client systems. Besides the pure operating system, these distributions contain many other software packages. These packages are not just the desktop applications which are usually supplied in the most varied forms, but also software for web servers, database management systems, mailserver, firewall, proxyserver, directory service and many more.

Key issues of the migration guide

Some selected distributions will be briefly outlined in the following, also mentioning their particular features.

Distributions are on offer from many different manufacturers. Normally, they are originally developed and packed with a view to simplifying the installation of the operating system kernel and the related programs. For installation purposes, the distribution companies have developed a number of different administration tools for the free operating system kernel and the surrounding software unit some of which, for their part, were also licensed as free software. The customer of a distribution does not buy Linux itself. What is paid instead is the combination of operating system, utility programs, installation programs and documentation created by the distributor. The purpose of distributions is to reduce administrative and organizational efforts on the part of the user because the operating system kernel does not include any concepts of its own for these demands. This means that the operating system is open for different management and organization concepts.

The buyer of a distribution usually receives the data volumes (today, lots of CDs) and extensive documentation. Although the volume and quality of the documentation vary from distribution to distribution, the documentation normally includes an installation manual and more detailed information for use. The data volumes contain the corresponding versions of the operating system software and a host of further software units. Pursuant to the GNU General Public License (GPL), which applies to many programs and the operating system kernel used under Linux, the distributors also supply the source code of the corresponding programs. This enables users to re-compile the software when problems arise and to modify the software in line with their specific requirements.

The different distributions are available as complete packages (CD, documentation) from dealers against payment or as free copies from the Internet. Packages bought from dealers usually include certain support services by the supplier which are not available for versions downloaded from the Internet. In the case of the three distributions discussed in the following, a further differentiation is possible between versions offered by commercial distribution suppliers and a distribution which was developed by a project group in a joint effort.

Compatibility of the Linux versions and standardization of the different distributions will be important issues in the future. In order to avoid unacceptable differences between the individual distributions, the Filesystem Hierarchy-Standard[7] was defined for the Linux directory structure. Suppliers of distributions usually implement this standard in their distributions. As an important element of the attempt to ensure interoperability, the Filesystem Hierarchy Standard is also integrated into the Linux Standard Base[8] (LSB). The aim of the Linux Standard Base is to define standards designed to achieve maximum compatibility of all distributions and to prevent divergence between the Linux systems. The purpose

---

[7] http://www.pathname.com/fhs/

[8] http://www.linuxbase.org

of standardization is to facilitate work for both software developers and distributors. Given a further proliferation of LSB-conforming distributions, software distribution will in future be possible independently of the respective distribution.

Besides LSB, the Free Standard Group[9] must also be mentioned in the context of standardization activities. This group is a merger of LSB, OpenI18N[10] (formerly Linux Internationalization Initiative Li18nux) and LANANA (The Linux. Assigned Names and Numbers Authority). LANANA deals with the administration of the Linux namespace in order to avoid name collision between applications and drivers. FSG members are Caldera, Compaq, Conectiva, Debian, Dell, Hewlett Packard, Hitachi, IBM, Miracle Linux, The Open Group, Oracle, Red Hat, SCO, Sun, SuSE, Turbolinux, VA Software and the members of the Open Source Entwicklergemeinschaft [Open Source Developer Group]. All the manufacturers of the distributions discussed in this guide are FSG members. The list of LSB-certified distributions is available on the Internet[11].

Criteria for the selection of a distribution are requirements related to the support and administration concept as well as hardware support on the one hand and the financial/organizational frame of reference on the other. Examples of such criteria are the availability of skeleton agreements or offers of applications specifically tailored to the needs of public agencies.

The distributions presented in the following were selected because of their wide-spread proliferation (refer also to chapter 2.5.1).

2.3.2   Debian GNU Linux

The Debian project is run by a host of developers who are developing a free operating system in a team effort. The characteristic feature of this group is the world-wide distribution of its almost 1000 honorary members. The most important feature of the distribution is the fact that the software is freely available in the sense of the GPL and that it can be copied and commercially used without any restrictions.

The distribution can be downloaded from the Internet or purchased from dealers. The Debian distribution is considered to be a non-commercial product. This means that the price of the CDs primarily covers the cost of producing and distributing the data volumes. The Debian project itself does not offer any packs with CDs, a feature which distinguishes this distribution from others.

A characteristic feature of Debian is the way errors and bugs are handled in the developer group. In a bug tracking procedure, a list is published which contains all the open error messages and reports which are then handled by the developers. This quality assurance mechanism makes Debian the most stable and bug-free distribution. Debian is characterized by long version cycles which

---

[9] http://www.freestandards.org

[10] http://www.openi18n.org

[11] http://www.opengroup.org/lsb/cert/cert_prodlist.tpl?CALLER=cert_prodlist.tpl

contribute towards the high quality of the distribution because this means that versions are not launched prematurely.

Another key feature of Debian is the unique packet format and the pertinent system tools. An important advantage is the possibility to easily update the systems and/or individual problems without the need to completely reinstall the software. Packet management is also used for regular system updates in the form of security and stability updates.

Various mailing lists[12] are available in order to support operation and development. If this source of information is not exhaustive, support services are offered by numerous commercial providers.

2.3.3   SuSE Linux distribution

SuSE Linux AG is one of the largest international suppliers of Linux distributions. Traditionally, SuSE Linux AG has a very strong presence in the German market. SuSE started by adapting the international Slackware distribution[13] to the demands of the German market. Some time later, the company developed a distribution of its own. During the course of time, SuSE developed products for various applications. The chart below describes the most important properties of different distributions.

Table 1: SuSE Linux

Products	Key applications
Personal - professional	Recommended by the manufacturer primarily for desktop applications. The distributions come with comprehensive software packages which can be installed on the computers by the installation routines included. The professional version comes with numerous server components on the CDs suitable for use in enterprises.
Enterprise	SuSE Linux servers are server operating systems designed for use in IT environments of any size and orientation. Available for all relevant hardware platforms: For AMD and Intel 32-bit and 64-bit processors, as well as the complete eServer range from IBM, including Mainframe.

The SuSE distribution is based on the RPM packet system developed by Red Hat. The packet system enables what is usually easy installation and deinstallation of software, including software from third parties. However, experience suggests that certain distribution-specific software packages should be installed using the preferred method of the respective manufacturer. The SuSE distributions include the integrated installation and administration system

---

[12] http://www.debian.org/support

[13] http://www.slackware.org

YaST. Users can choose both a text-based and a graphic front-end for system administration.

The main differences between the above-mentioned distribution variants are their recommended applications and the resultant differences in the scope of support offered, in the available license agreements and, last but not least, in the purchase price.

The enterprise solutions are offered for applications in business-critical areas as optimized solutions with a view to availability and scalability. Integrated features include, for example, cluster capability, multiprocessor capability and asynchronous I/O.

Furthermore, different support programs are offered for the different distributions. Depending on customer demands, 24x7 support, customized service level agreements and certifications are offered, for example.

2.3.4   Red Hat distribution

The Red Hat distribution is another commercial product. Red Hat also offers its customers different distribution variants for different applications (refer to Table 2). Red Hat uses an internally developed program administration functionality. The program packages (.rpm) are managed by the Red Hat Package Management which enables uniform and user-friendly software management.

Table 2: Red Hat

Product	Remarks
Red Hat Linux and Red Hat Linux Professional	Both distributions are designed primarily for the workstation area and/or as server solutions for smaller environments. The main differences between the two products are the scope of delivery of the product and the length of installation support. The professional version comes with further tools for use by the system administrator.
Enterprise Linux	The enterprise solutions are offered chiefly for businesses. The systems are certified for various platforms from different hardware manufacturers and include, for example, high-availability clustering technologies.

The main differences between the different products are their recommended applications and the resultant differences in the scope of support offered, in the available license agreements and in the purchase price.

2.3.5   Certifications

Certification is possible for hardware, software and employees.

2.3.5.1 Hardware

Hardware certification includes a test procedure followed by certification of the products for defined Linux platforms and versions. The performance and suitability of the hardware is checked in conjunction with the operation of defined Linux distributions. Hardware manufacturers can have their products certified together with the producers of the relevant distributions. Beside quality assurance, certification is a powerful selling point for hardware manufacturers.

Certification offers customers a higher degree of safety in terms of compatibility of the hardware and operating system used, especially in the case of business-critical applications and solutions, such as EPR systems with RAID or SAN hardware. Certification can be a key buying argument for prospective customers and users.

2.3.5.2 Software

Software certifications are carried out by the software manufacturers (Independent Service Vendor). The individual manufacturers validate and certify the distributions as operating system platforms for their application software. The companies SAP and Oracle, for example, certified the SuSE Linux Enterprise Server[14] as a platform for certain applications. Certifications are also available for systems from the distribution manufacturer Red Hat[15]. The certification process is normally applied only to the enterprise version of a distribution manufacturer. Many customers require software certification as a prerequisite for the use of an operating system platform because the support by the application manufacturer necessary for installation and operation of the application software is often only ensured if the product is certified.

2.3.5.3 Employee certification

Besides hardware and software certification, certification is also required for the employees' technical knowledge and abilities.

Market leaders in the field of certification programs are at present:

the Red Hat Certified Engineer (RHCE)[16]

and the Linux Professionell Institute (LPI)[17]

The aims of both certification programs include the development of standards for employee qualification. Qualification offers employers the following advantages:

Support when hiring staff

Standardized qualification of employees

Certification also offers employees and prospective employees a number of advantages:

---

[14] http://www.suse.com/de/business/certifications/certified_software/index.html

[15] http://www.redhat.com/solutions/migration/applist.html

[16] http://www.redhat.com/training/rhce/courses/index.html

[17] http://www.de.lpi.org/

Qualification for the job

Proof of qualification

Better opportunities on the job market

Both certification programs can be generally regarded as being equivalent, with RHCE focusing more on the company's own distribution. Red Hat started developing the Red Hat Certified Engineer (RHCE) program at a time when no other Linux certification programs existed. It was only after this that LPI developed from within the Linux community. LPI is supplier-neutral, distribution-neutral and at the same time a non-profit organization.

2.3.6   Conclusions

Users can choose between numerous distributions and distribution versions. The identification and definition of requirements are central for the decision. Any decision in favor of a particular distribution must be based on the expectations on the distribution and its manufacturer and the general frame of reference. If, for example, extensive support by the manufacturer is required due to a lack of internal resources, the distributions of commercial suppliers are usually the preferred products. If hardware or software certification is necessary for a specific application scenario, this can normally be offered for the enterprise versions of commercial suppliers only. Which hardware and software products are actually certified for which distribution and version must be checked from case to case.

The Debian distribution is a stable, thoroughly debugged and tried-and-tested distribution for users who do not depend on a commercial variant. If comprehensive support services are required, numerous service providers offer this kind of service.

2.4   License models

Of the various license models which exist in the Linux world, the most important models are briefly outlined and characterized in the following.

2.4.1   GPL

The General Public License (GPL)[18] developed by the Free Software Foundation is the probably the best-known license model. The Linux kernel and most Linux applications are subject to the "GPL" as a license which guarantees, amongst other things, the free availability and the distribution of the source code of these programs. In order to make sure that the software will remain free, even in the future, the GPL sets forth the exact rights and terms of use.

The rights and terms include in detail:

---

[18] The English original can be found at: http://www.gnu.org/copyleft/gpl.html. A German translation is available at: http://www.suse.de/de/private/support/licenses/gpl.html, even though the original version prevails.

Section   0:
The freedom to execute the program for any purpose whatsoever.

Section 1:
Permits the copying and distribution of verbatim source code copies of the program on condition that the copyright notice and the license are also copied and distributed together with such copies. It is explicitly permitted to charge a fee for the physical act of making a copy and for other services, such as warranty services.

Section 2:
Permits modifications of the program and the copying and distribution of the modified version on condition that the modified version contains statements concerning such modifications and further on condition that this is published at no charge and subject to the same license terms and conditions. This does not apply to parts of the program which constitute independent sections and which are distributed separately.

Section 3:
Permits the copying of the program or of a version based on it in object code or in executable form on condition that the pertinent machine-readable source code or a written offer (valid for at least 3 years) to distribute the related source code on request are attached.

The other sections contain provisions concerning the termination of license rights, the disclaimer of liability and warranty, situations of conflict with other claims and a number of other subjects which can be read when necessary.

The terms and conditions of the GPL prevent the privatization of collectively produced software and thereby explicitly promotes the development of the stock of free software.

2.4.2   Lesser GPL

The GNU Lesser General Public License (LGPL)[19] is an alternative form of license. The license was originally drafted under the name Library GPL.

The LGPL is largely identical to the purpose and contents of the GPL. This means that the free copying, distribution and modification of software and libraries must be ensured. Furthermore, the source text – including the source text of modified versions – must be available.

The difference compared to the GPL is primarily the fact that programs which are not subject to GPL or equivalent licenses may use free libraries under LGPL and form an executable entity. If the libraries were subject to GPL, no programs other than programs subject to GPL would be allowed to link these libraries. LGPL, in contrast, permits developers to draft programs which are not subject to the restrictive production of the GPL and, notwithstanding this, use free libraries. Programs using libraries subject to LGPL may be distributed subject to license

---

[19] http://www.gnu.org/copyleft/lesser.html

terms and conditions which can be freely selected. However, the source code for the libraries subject to LGPL must be available to customers, so that they can modify and re-link the code.

2.4.3 BSD license

The BSD license[20] is one of the oldest free license models. UC Berkeley developed the license model for the distribution of modified Unix versions[21].

The BSD license permits the free copying of software with or without user-made modification as a source code and/or as binaries on the following conditions:

When the software is distributed, the copyright notice and the BSD license itself must be included in the files in question.

If the software is distributed in binary form, the copyright notice and the terms and conditions of the BSD license must be contained in the program documentation or elsewhere.

Without written permission, neither the name of the university nor the names of the authors may be used for advertising purposes.

The original version of the license included yet another provision pursuant to which any advertising material for a licensed feature had to include the statement: "This product includes software developed by the University of California in Berkeley and its contributors". This clause was deleted from the old license and the latest Berkeley release was licensed under the new variant. This explains why the terms "old" and "new" BSD license are used.

The BSD license does not include any restrictions for the use and distribution of source code and programs. The only requirement is a copyright provision pursuant to which the BSD license terms and conditions and a waiver of warranty must be attached to the product. The license does not explicitly stipulate that modified software must be distributed as source code. This means that any software company can integrate source code subject to the BSD license into one of its products and subsequently keep the source code undisclosed.

Compared to the licenses described in the foregoing, the BSD license is subject to certain restrictions which can, however, be regarded as being of minor relevance.

2.5 Data sources

The results presented in this guide are mainly based on the following sources:

Experience gained with previous migration projects

Experience from the development of OSS and COLS products

---

[20] http://www.opensource.org/licenses/bsd-license.html

[21] The license exclusively applied to the source code produced by UC Berkeley.

Key issues of the migration guide

Integration of expert know-how

Feasibility studies for proposed migration projects

Detailed migration concepts

Migration documentation

Technical and product literature

Technical information relevant for this guide was compiled through:

intensive literature research

interviews and their evaluation

workshops on specific issues as well as

direct involvement of numerous experts and software manufacturers.

Contents and findings gathered from the above-mentioned information and knowledge sources were compiled, arranged according to subjects, analyzed and evaluated for the purposes of the various issues which are addressed in this guide.

2.5.1 Experience with migration projects

The subject of "Introducing and using OSS" is on the agenda both in public administrations and in industry. This has triggered a number of migration projects in which up-to-date experience and findings can be used. Besides purely technological information and experience, these projects enable important conclusions concerning critical success factors (refer to chapter 5.5.3) and the necessary input to be expected for individual migration steps.

The study was prepared on the basis of various kinds of documents, such as detailed technical concepts, performance specifications and project documentation summaries. This analysis also serves as the basis for the development of interview guides for the individual project studies.

Information was normally gathered in interviews at public agencies and companies performing migration projects and/or with the administrators, users and implementers concerned. The questions concerned the following aspects:

Starting situation

Key aspects of the project

Motivation and targets

Critical success factors

Costs and benefits

Lessons learned

Successor projects – IT strategy development

These questions were supplemented by technical detail questions concerning the individual partial migration projects corresponding to the specific technical challenges of the individual projects.

The migration projects can draw on experience from pilot projects which were initiated by the German Federal Office for Information Security (BSI) on behalf of the Federal Ministry of the Interior (BMI). At the time of the survey, these projects were already completed to a large extent and with considerable success.

Furthermore, projects in public administrations and in industry were surveyed that were conducted on the basis of their own evaluations of economic efficiency. The information and experience from these projects were also considered in this migration guide.

The starting situations of all these projects were and still are very different. Most cases involved Windows NT 4-based systems at the server end which had to be replaced and consolidated. However, hybrid system landscapes with Windows NT, Unix and Linux also existed at the server end. The entire diversity of the Windows world – from Windows 95 to Windows XP – was represented at the client end. Reflecting the current state of equipment at most public agencies, Windows NT 4 workstations accounted for the largest part.

The scope and type of migration were also found to be very diverse. Besides complete migration projects (servers and clients), pure server migrations were also carried out with Windows NT 4 being left in place at the client end. It was possible to a large extent to re-use the existing file and rights structures without having to change the NT clients and without users being affected by the change. Furthermore, one migration project studied was a pure client migration where the Linux clients were integrated into an existing NT4 network. Another migration project should also be mentioned with a server migration on the one hand and the migration of the original fat clients to thin clients on the other. In order to enable the continued use of the required Windows applications (special applications) for which neither a corresponding Linux version nor an alternative under Linux is available, terminal services and emulation software were introduced in this case.

From a technical perspective, experience was available with the migration of important applications and system services. Cases included:

Database migrations, including migration of a database from MS SQL Server to SAP DB, whilst retaining the Visual Basic application at the client end

Migration of infrastructure services

- File services (even in heterogenous systems with Samba)
- Print services
- Authentication services (even with OpenLDAP directory service)
- Network services

Office migration

Key issues of the migration guide

Web server migration

and many more

The pilot projects initiated by BSI were carried out at the following public agencies:

German Federal Cartel Office

Commission of Monopolies

Mariensee Institute for Animal Science and Animal Husbandry

Further projects from which data was also gathered are either still in the process of planning or implementation or have already been concluded at the following public agencies:

The Federal Data Protection Commissioner (BfD)

Bundesverwaltungsamt (BVA)

BSI

Furthermore, several companies contributed valuable information from projects in the infrastructure and application areas, especially on the use of ERP and DBMS systems as well as on the use of terminal server technologies and system management platforms.

2.5.2   Integration of experts

Besides the evaluation of experience and results from the migration projects, various experts from the OSS community and OSS services providers as well as from the software industry were involved in preparing the contents of this migration guide. These experts were primarily involved in workshops, in gathering information and in developing answers to technical problems, as well as active authors of this guide and in quality assurance.

Workshops on selected topics with participation of experts, administrators and users were found to be a particularly effective way to clarify open issues. Workshops were held on the following subjects:

Migration in a heterogenous system environment with Linux and Windows systems using Samba

DBMS migration from MS SQL Server 7 to a free database management system or to a database management system running under Linux

Groupware migration from Exchange 5.5 with a view to use in heterogenous environments with continued use of MS Outlook

Desktop migration with a focus on Office migration (Office 97/2000 to OpenOffice/ StarOffice) and the related re-use of existing documents, templates, macros and scriptings.

Use of directory services, including the use of the OpenLDAP open source directory service, even in conjunction with an active directory in heterogenous system landscapes

Using WiBe21 to evaluate the economic efficiency of migration projects.

3 Technical description of the migration paths

3.1 Introduction

The technical descriptions take a closer technical look at the various products, solutions and services described in chapter 2 in the IT landscapes in question. The following aspects are addressed:

Infrastructure services

- File services
- Print services
- Authentication services
- Network services

Middleware and integration components

- Directory service
- Object component models
- Platforms for distributed systems and web services
- XML

Server services

- Groupware and messaging
- Database servers
- Web servers
- Special services

Desktop applications, including the Office package

The descriptions focus on the technical feasibility of migrating individual Microsoft products to adequate OSS or COLS solutions. The following aspects will be analyzed in detail for the individual components of this landscape on the basis of the Windows-determined IT landscape described in chapter 2.1:

What is the starting situation?

- Which important functions are available?
- Which interfaces are and/or must be served?
- What are the special features during active operation?

Which alternatives are available as OSS or, if applicable, as COLS solutions?

- What are the functional differences?
- Are the critical requirements fulfilled?
- Which interfaces are and/or must be served?

- What must be taken into consideration during migration, where are the problems, how can they be resolved?

- Do multiple alternatives exist, for whom and/or for what purpose can which alternatives be used?

- How can the alternatives be integrated into heterogenous worlds, if necessary, how does interaction work, especially with Microsoft (compatibility, interoperability)?

- What are the repercussions of the potential integration on future Microsoft product lines?

Which potential exists if use of the Microsoft product line continues?

- Which additional functionalities are available?

- Where are the major changes?

- Do the innovations and possible modifications fulfill open critical requirements?

- What must be considered with a view to the independence of the systems?

The descriptions usually end with a brief evaluation. If multiple alternatives exist, these comparable solutions are also commented on, if applicable.

3.2 File system

3.2.1 Overview

The result of the detailed technical descriptions of the filing services can be summarized as follows:

In the case of direct replacement of a Windows NT server as a file storage system with the Windows clients remaining in place, Samba is the system of choice in the open source area. Samba behaves much the same as an NT server in relation to a Windows client. Samba is continuously upgraded and is supported not just by the community but also by a growing number of IT service providers.

Depending on the extent of a Linux migration at the client end, NFS and AFS may also be interesting alternatives. NFS and AFS are widely used in UNIX networks, but special software has to be installed on all clients in order to integrate Windows clients. An NFS client is, for example, included in Microsoft Windows Services for UNIX (SFU 3.0). An AFS client is free of charge and available as an open source from OpenAFS.org. The use of NFS or AFS in an environment with Windows clients always requires far-reaching conceptual changes compared to filing with Windows NT.

If the Kerberos security concept, which also underlies the active directory of Windows 2000, plays an important role when it comes to modernizing the IT infrastructure within a migration project, OpenAFS as an alternative to Win2000

as file server should be evaluated in more detail if use of the Windows product line is to continue at the client end.

Suitable file systems for the physical storage of data on the disk systems of the real servers are, for example, XFS and EXT3. Both systems support journaling functionalities, quotas and the assignment of access privileges at the file and directory levels. Both XFS and EXT3 support extended file attributes abd POSIX-ACLs for the granting of rights.When mapping the Windows-ACL to the POSIX-ACL, note that the fine granularity with which privileges can be defined under Windows is lost. In the final analysis, the repercussions which the restrictions have in the given case and whether these are acceptable must be analyzed.

3.2.2 Windows NT 4

3.2.2.1 Functional requirements

The general functionality of a network-based filing system consists of the following functions:

Receiving (writing) and supplying (reading) files

Creating and presenting a directory structure

Administration and presentation of meta data for directories and files

Implementation of access privileges and restrictions for directories and files

Disabling file access in the case of conflicting accesses

In most environments, Windows NT File Services are used for the following purposes:

Storage of the user-specific files (home directories)

Storage of the server-based profiles if optimized support is required for users roaming between client computers

Storage of group-specific files (group folders) which are to be used by selected users (for a department, for example) only

Storage of file-based databases which are to be used by several users at the same time (such as MS Access databases with separate frontend)

Storage of program files (exe files, dll files, etc. of an application) in order to avoid the need to store these files on the client computer

Storage of database systems that enable the storage of user data on another server under a UNC path

In practical application, the uses described here often lead to strongly varying detail requirements which will be highlighted in the following sections.

3.2.2.2 The NTFS4 file system

The NTFS4 file system is the basis for file storage and management under Windows NT4.

Properties

The properties of NTFS4 include, for example, the following:

Every folder and every file has a so-called Access Control List (ACL) which is stored at the file or folder. The ACL contains so-called Access Control Entries (ACEs) which contain the SID of the group or user account and the authorization. Access is thus controlled via the ACL and it is possible to implement a generally granular access control system. The ACL must be broken down further into the SACL (System Access Control List) and the DACL (Discretionary Access Control List): The DACL contains the SIDs of the groups and users authorized to access the object or not. The SACL determines the way in which the security subsystem monitors access to the object.

In principle, NTFS4 does not support inheritance: Only when a new file is created, the privileges of the folder are copied into the ACL of the file. When the privileges of the folder change, inheritance to the ACL of the files included in the folder must be ordered explicitly. One special feature must be considered: A file which is stored in the UNC path \\server\freigabe\ordner\subordner can be read by a user although the "ordner" folder prohibits reading, if the "subordner" folder permits reading.

There is no limit to the length of path names. File names with up to 256 characters are supported. Apart from a few exceptions (such as *,\), all characters of the Unicode character set (16-bit) can be theoretically used. A short name which corresponds to the 8.3 convention and which is automatically generated by the operating system is stored for each folder and for each file. Although upper case and lower case characters are discriminated during storage, this is normally not the case during access to the file.

Every folder and every file has attributes in the form of flags (write-protect, archive, system, hidden and compressed) as well as the time of first-time creation, last change and last access. The degree of compression is strongly dependent on the contents.

NTFS supports the technology of multiple streams. The frequency of use is relatively low. Multiple streams must be supported by the application in question, and/or must be programmed there. Multiple streams enable, for example, storage of the Folk resource of Macintosh files.

Since Service Pack 4, quotas are supported within NTFS. Assignment and control of quotas are based on the owner property and cover the complete volume (logic drive of the file server). Due to these technical restrictions, the use of quotas must be regarded as the exception rather than the rule in existing environments.

The maximum file size under NTFS4 is limited to 2 TB (terabytes) and the capacity of the logic drive. The maximum capacity of the logic drive totals 2 TB (theoretically 16 exabytes). The real net data amount depends on the cluster size used during formatting. The number of files is limited to 2^{32}-1.

Technical description of the migration paths

NTFS enables auditing of successful and attempted accesses. In this way, it is possible, for example, to diagnose repeated, undesired file delete operations.

NTFS-formatted data volumes are defragmented during ongoing operations. Automatic correction (self-healing) under Windows NT 4 does not take place. If this is required, products from third-party manufacturers must be used.

The NTFS privileges system

Windows recognizes a total of 13 privileges that can be assigned or cancelled for an object in the file system (file or directory) for every user or group:

Browse folder / execute file

List folders / read file

Read attributes

Read extended attributes

Create files / write data

Create folders / append data

Write attributes

Write extended attributes

Delete subfolder and files

Delete

Read privileges

Change privileges

Transfer ownership privileges.

Changes in access privileges are made via the *Security settings* tab of the *Properties* dialog. In order to conceal the complexity of the system of 13 closely related individual privileges from average users, this tab offers a selection of pre-defined items, so-called *Group privileges* as sensible combinations of the individual privileges. Five such group privileges exist for files and six for directories. These group privileges can be enabled or disabled as a group. The 13 individual privileges are completely shown in the *Privilege entry* dialog which is accessed via the *Extended/Display/Edit* buttons.

In this context, the view of the group privileges offered in the security settings is extremely problematic because the presentation can very quickly suggest the absence of privileges which in fact do exist. In the case of full access, for example, where the privilege to write the extended attributes is the only privilege which is not granted, the simple presentation of the security settings shows the picture of a privilege profile which enables reading and executing only. The following table shows which combinations of privileges lead to which presentation as group privileges. Please remember that the checkbox for a group privilege is no longer ticked off if just a single privilege in these aggregations is not set.

Table 3: Properties of the Windows group privileges

Windows group privileges						
	Full access	**Edit**	**Read & execute**	**List folder con-tents**	**Read**	**Write**
Browse folder / execute file	X	X	X	X		
List folders / read data	X	X	X	X	X	
Read attributes	X	X	X	X	X	
Read extended attributes	X	X	X	X	X	
Create files / write data	X	X				X
Create folders / append data	X	X				X
Write attributes	X	X				X
Write extended attributes	X	X				X
Delete subfolder / files	X					
Delete	X	X				
Read privileges	X	X	X	X	X	X
Change privileges	X					

In view of the inconsistencies described in the foregoing, only the extended view in the *Privilege entry* dialog will be considered in the following.

Attribute system

In addition to the privileges, several so-called *attributes* and *extended attributes* are managed for file and directory objects.

Table 4: Windows attributes

Name	**Bit**	**Meaning**
Archive	A	The file was changed since the attribute was last reset.
Write protect	R	The file is write-protected.
Hidden	H	The file is not displayed.
System	S	The file is reserved for the system.
Compressed	C	The file/folder is stored in the medium in a compressed form.
Encrypted	E	The file/folder is stored in the medium in an encrypted form.

Audit

Windows includes far-reaching audit options at the file and directory level. It is, for example, possible to have all privileges audited individually for every user or group. The resultant information is stored in the security log of the domain controller and/or of the related Windows 2000 computer if the audit guideline is enabled in the system guideline.

3.2.2.3   Access control

Access control via the network to files or folders in Windows NT environments is accomplished by two mechanisms as follows:

> Folder unlock (share)

> and NTFS privileges

In order to be able to access a file via the network, one of the higher-level folders must be released. This release is also given an ACL which is stored in the registry. The privileges for this release operation are restricted to the following levels:

> Read

> Edit

> Full access

These privileges apply absolutely. This means that NTFS privileges located below are effectively curtailed by the release privileges. Example: A read privilege at the release level prevents writing even in cases where the NTFS privileges would permit this.

Special attention in Windows NT environments should be paid to the privileges (guidelines for user rights) because these privileges can be important for the file services, for example, by "taking ownership of files and objects" and "saving files and folders".

3.2.2.4   Users and group concept

Every folder and every file is assigned to an owner which can be both a group and a user account. The creating user usually becomes the owner. If the user is a member of the administrator group, this group becomes the owner.

Systematic access control in the Windows NT environment prefers the assignment of privileges to groups. The assignment of privileges to individual user accounts should be left to the user-specific file systems.

The following different group types exist in a Windows NT environment:

> Global groups

> Local groups on member servers

> Local groups on domain controllers

Local groups on domain controllers differ from those on member servers in that local groups exist on all the domain controllers of the domain with the same SID.

Local groups on member servers may be nested (group nesting) with the following groups:

With the global groups of the own domain or

With the global groups of the domains which the own one trusts.

Global groups only have user accounts as members.

Two different "classic" access control principles exist in a Windows NT domain landscape:

U-G-L-R method:
The user is a member of a global group. This global group, for its part, is a member of a local group of a file server. This local group is the only one for which NTFS privileges are set at a file resource (refer to Fig. 4:   U-G-L-R method

).

U-G-R method:
The user is a member of a global group. This global group is the only one for which NTFS privileges are set at a file resource (refer to Fig. 5:   U-G-R method).
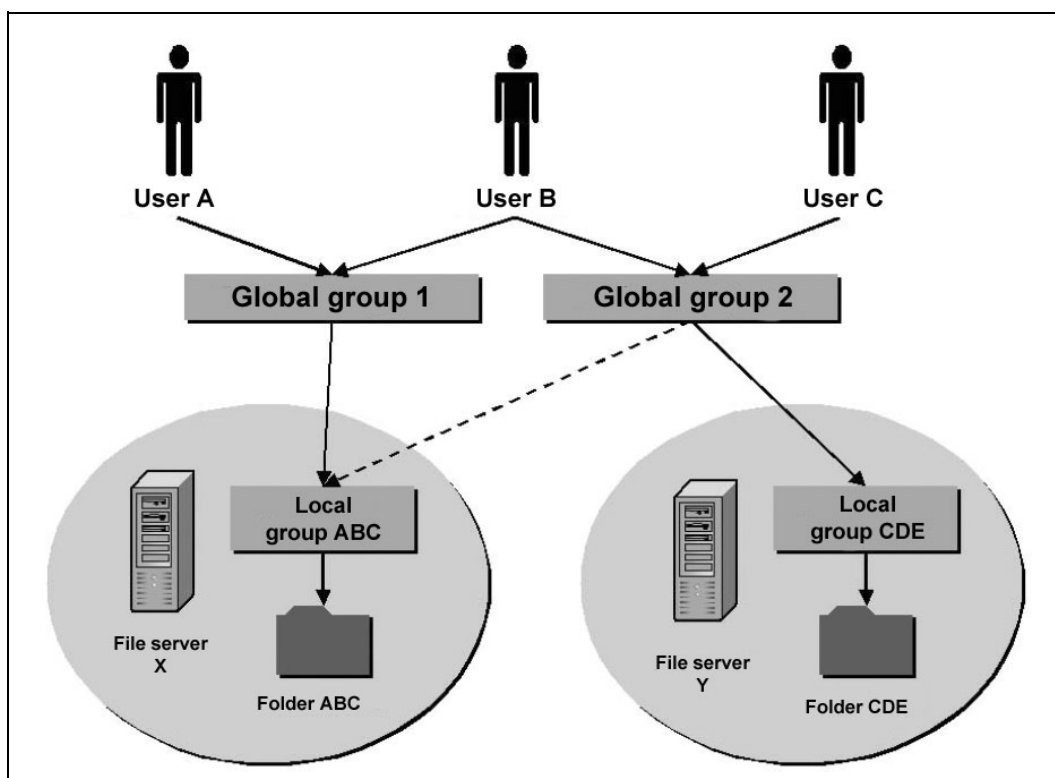
Fig. 4:   U-G-L-R method
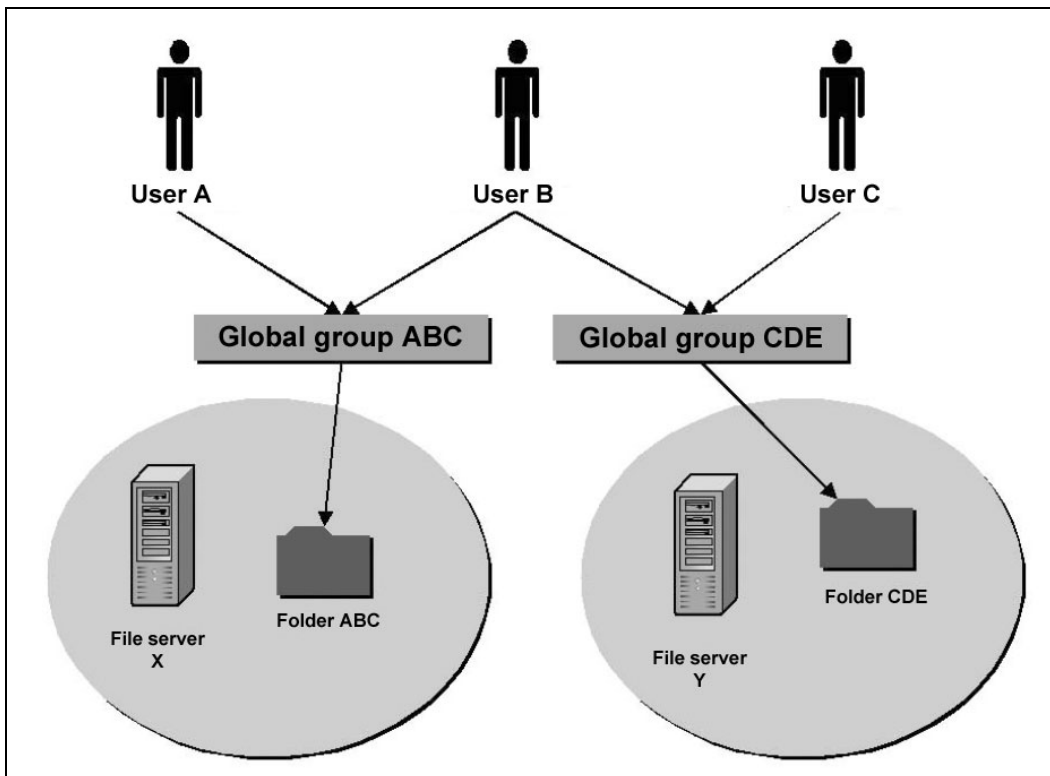
Fig. 5:   U-G-R method

An unambiguous assignment of resource and local group (or global group, respectively) is a precondition for both methods to work without safety risks. This means that the group is used for this resource on an exclusive basis.

If the file services are implemented by a cluster, the U-G-L-R method has the disadvantage that the local groups on the node servers cannot have the identical SIDs. This can be remedied by configuring the nodes as domain controllers or by using the U-G-R method.

3.2.2.5   Tools

Windows NT offers a relatively limited selection of tools for the management of files and folders and their privileges.

With graphic user interface:

NT Explorer (explorer.exe)

File Manager (winfile.exe).

In the command line only:

calcs

Ressource Kit Tools: xcacls, scopy, etc.

The tools supplied with Windows NT usually offer dedicated rather than full functionality. The NT Explorer is the best example of this: It is not possible to set the owner (to accept only) or to copy ACLs. One must hence assume that the administrator of an NT environment uses tools from third-party manufacturers or

self-developed scripts (such as Perl) in order to facilitate administration or to execute very special tasks. This means that the privilege structure displayed by an NT Explorer differs from the access rights actually granted.

3.2.2.6   Network protocols

Communication with Windows NT file servers via the network can be based on different transport protocols:

TCP/ IP

NetBEUI

SPX/ IPX

Appletalk

TCP/ IP, NetBEUI and SPX/ IPX are quite probable in an existing NT environment. It is generally assumed that TCP/IP will be aimed at as the only relevant protocol in the future. This is also the reason why the "Gateway Services for Netware" and "File and Print Services for Macintosh" are not discussed here any further.

With regard to the file services,

SMB (Server Message Block) via NetBT (NetBIOS over TCP/ IP)

can thus be regarded as the standard with the ports 137/UDP/TCP (nbname), 138/UDP (nbdatagram) and 139/TCP (nbsession).

3.2.2.7   Connecting

The releases on the file servers are usually made available to the user in the form of drive letters. This is often accomplished via logon script. Furthermore, users can browse in the Windows network This means users can click the file server and connect to a network drive with the visible releases, or they can open them directly.

3.2.2.8   Special features during productive operation to be considered in the case of migration

Some special features which might turn out to be critical points in a migration project are described in the following.

With regard to the storage of user-specific files (home directory), it is sometimes demanded that data stored there can only be read by the user and by the operating system (for virus protection purposes, for example). Windows NT permits the use of the account system for this purpose.

The storage of the server-based profiles is subject to a complicated process at the client end during writing back. Fault-free communication and a fault-free privilege structure must be ensured especially in terminal server environments which specify server-based profiles as a mandatory feature.

Group-specific files can be used by several users at the same time. It is then helpful to inform the users of this shared use. Example: The user who is

second to open a Word file receives a message stating that user 1 has already opened this file, so that the second user can open the file in write-protect mode only.

Fault-free locking must be ensured in conjunction with the storage of file-based databases which also include, for example, pst files (personal folders in Outlook).

The storage of program files is often not completely possible in write-protect mode. This then requires very granular privilege levels (such as write, but not delete, a particular file).

Only few applications with database systems (such as MS SQL) offer the option to store user data on another server under a UNC path. In such a case, however, fault-free communication and file storage is a particularly critical issue which is subject to release by the manufacturer of the application.

3.2.2.9   Related issues

File services under Windows NT must meet not just with pure file service requirements, but must additionally fulfill other important requirements as a precondition for their satisfactory use by products from third-party manufacturers in legacy environments.

Virus protection:
Virus protection is usually achieved by the local installation of a virus scanner on the file server itself. A locally installed service is a precondition for the scanning of a file during access. This is the way in which many manufacturers of anti-virus software address this problem. The alternative option is to have the drives of the file server scanned by another computer via the network. The disadvantages are obvious: the resultant workload and delay.

Quotation: The quotation integrated into Windows NT is normally not used. The use of third-party manufacturer products is necessary in order to quote user-specific and group-specific file systems.

Data backup: The on-board NTBACKUP tool is used rather seldom. File servers under Windows NT are normally integrated into a data backup concept by installing a suitable component (agent) which ensures central and uniform backup procedures for other target systems (databases, mail). The recovery time in a disaster case is a key criterion in this context. A special feature of the NTBACKUP on-board tool permits the backup of files which otherwise cannot be read by the user.

Archiving: Revision-safe archiving is often carried out within the scope of the data backup concept. Furthermore, some products from third-party manufacturers permit the swapping of seldom-used files to more cost-effective systems/media.

3.2.3 Replacing migration

3.2.3.1 Introduction

With a view to the file storage system, this migration guide assumes that central file storage is possible on at least one NT server and that the files are currently accessed by Windows clients. If alternative migration targets are to be identified outside the Microsoft product line, one must differentiate between migration scenarios where an alternative is sought for the server end only or where a new operating system platform is to be introduced for the clients too.

Two levels must be generally considered for the file storage system in the case of a server migration. On the one hand, every server has a local file system in which it manages all the files. On the other hand, at least a subset of these files is exported to the clients by a server service using a suitable network protocol.

The replacement of Windows NT as a file server involves on the first level in any case exporting existing data and programs from the old system to the new one. This also involves mapping the system of privileges for authorizing access to files and directories as well as adapting operating concepts, for example, for data backup purposes.

The second level involves replicating the existing functionality, be it with the existing clients or with a new client architecture. The second level is the real core of the "file storage system" infrastructure component. The analysis will primarily focus on issues of "access rights at the file and directory level" and "general functionalities of the file storage system".

The following alternatives can be considered primarily if an NT 4.0 server is to be replaced as a file storage device:

UNIX/Linux with Samba – a copy of the file storage system of the NT server

UNIX/Linux with NFS – the traditional, network-based file storage system in UNIX networks

UNIX/Linux with OpenAFS – the network file system with Kerberos authentication released by IBM

Alternative network file systems which are still at the level of university research or which are fully or partially based on proprietary software are not discussed here.

3.2.3.2 General comparison of the functionalities for file servers

In the functional overview of the alternative network file systems, properties of the underlying server file systems indirectly also come to bearing. With regard to Linux-based servers, this comparison is based on the XFS or EXT3 file system.

Table 5: Comparison of file servers

Function	WinNT	Win2k	Samba	NFS	AFS
Windows client without additional software	X	X	X		

Technical description of the migration paths

Function	WinNT	Win2k	Samba	NFS	AFS
Length of tile names (characters)	256	256	256	256	256
Character set for file names	Unicode	Unicode	Unicode	ISO-Latin	ISO-Latin
Presentation of upper case / lower case	X	X	X	X	X
Discrimination between upper case / lower case				X	X
Disk quotas		X	X	X	X
Encryption		EFS	file-wise at client end		
Compression	X	X	[22]	[23]	
Maximum file size[24]	2 TB	2 TB	2 TB	9 EB[25]	2 GB
Maximum path length	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
Change journal		X			
Propagation of releases in the active directory		X			
Distributed file system		DFS	DFS	Standard	Standard
File replication service		FRS	rsync	rsync	rsync
Journaling		X	X (by file system)	X (by file system)	X (by file system)
DACL		NTFS	POSIX	POSIX	AFS
SACL		NTFS	Samba module		
Typical authorization via	NT/ LM PDC	AD / Kerberos	NT/LM LDAP, if AD member then Kerberos	NIS/ LDAP	Kerberos version 4

In the case of direct replacement of a Windows NT server as a file storage system with the Windows clients remaining in place, Samba is the system of choice in the open source area. Samba behaves much the same as an NT server in relation to a Windows client. Samba is continuously upgraded and is supported not just by the community but also by a growing number of IT service providers.

Depending on the extent of a Linux migration at the client end, NFS and AFS may also be interesting alternatives. NFS and AFS are widely used in UNIX networks, but special software has to be installed on all clients in order to integrate Windows clients. An NFS client is, for example, included in Microsoft

---

[22] Available as a patch for Ext2/3 file systems, for example.

[23] Available as a patch for Ext2/3 file systems, for example.

[24] TB Terabyte 1012, PB Petabyte 1015, EB Exabyte 1018

[25] NFSv3 with XFS file system

Windows Services for UNIX (SFU 3.0). An AFS client is free of charge and available as an open source from OpenAFS.org. The use of NFS or AFS in an environment with Windows clients always requires far-reaching conceptual changes compared to filing with Windows NT.

If the Kerberos security concept which also underlies the active directory of Windows 2000 plays an important role when it comes to modernizing the IT infrastructure within a migration project, OpenAFS as an alternative to Win2000 as a file server should be evaluated in more detail if use of the Windows product line is to continue at the client end.

3.2.3.3 Samba

The fundamentally different options, i.e. implementing a central file storage system for Windows clients or for a heterogenous client environment, are initially equivalent options. There is no reason to generally rule out the one or the other approach. With a view to the concepts for application and administration, all options involve more or less far-reaching changes at the administration and application levels. Given a conservative, continuing migration approach, the SMB/CIFS-based Samba and W2K servers offer the best preconditions for the far-reaching reuse of the existing concepts.

Samba is in many respects a replicate of the Windows NT service for file storage, print services, and authentication. To users, Samba presents itself in maximum approximation in much the same way as an NT server. To administrators, on the other hand, Samba is a UNIX server. The handling must be adapted to the philosophy and possibilities of the new operating system.

W2K as the product successor to NT means to users hardly more changes with regard to the NT server than a Samba server. For administrators, however, the introduction of an active directory with the DNS, LDAP and Kerberos components means far-reaching changes.

To what extent the change or the development in one or another direction is considered and regarded as being easier or more favorable will depend not least on the individuals involved. Migration to Samba, Linux and Open Source opens up new degrees of freedom. Such a step towards emancipation from the standards and best practices of a manufacturer means to the individual administrator not just more freedom and more self-reliance, bit also new potential for errors.

The Samba server fulfils the file storage requirements just like an NT server. The users of Windows clients can also obtain their user profiles and logon scripts as well as their home or group directories from a Samba server. The executable programs (.exe) can also be stored on a Samba server (and started from there). This also applies to Access database files or other files with lock mechanisms designed for multi-user access.

In contrast to an NT server, Samba exclusively uses TCP/ IP as the only network protocol. Other Open Source servers (Mars and Netatalk) are available for the services based on the SPX/IPX (Novell) and Appletalk (Apple) protocols which

enable work on a common data base in a heterogenous network environment. An SMB implementation based on the old NetBEUI is not offered by Samba. NetBIOS via IPX is not supported either.

The usual client-end tools for editing/managing the files in the file system continue to be available. Particularly the Explorer and the File Manager as well as cacls, xcacls, etc. can continue to be used. The user manager can also remain in use with Samba 3.0. Although the use of the Server Manager is in principle possible, it is less suitable because this also means that the transparent server configuration (smb.conf) would be abandoned.

The connections to the releases can be established automatically without any changes by logon-scripts or interactively by browsing the network environment.

The privilege system of Samba and Linux makes it possible to give privileged processes (such as a virus scanner on the server) local access to all files in the users' home directories, whilst access via the corresponding network drive is restricted to the user alone.

The Samba server can be used for file storage and authentication even in environments with Windows terminal servers. However, Samba does not support the SAM object extensions specific for terminal servers.

Samba treats file locking (both at file level and in the byte range) in exactly the same way as the NT server. This means that Samba enables both the cooperative use of files and the use of file-based databases in the same manner as an NT server.

Disk quotas (as well as quotas of other system resources) are offered by the Linux operation system and are thus also available for the file storage system offered by the Samba server.

Various open source tools are available under Linux for data backup and versioning / archiving purposes. Furthermore, Linux servers can be easily integrated into the backup concepts of most commercially available products.

High availability which is achieved under NT by clustering with the Enterprise Edition can also be achieved with Samba once again on the basis of shared SCSI or SAN with IP Failover.

Compared to the results of some feasibility studies[26] from recent years, there are now much fewer functional restrictions concerning the use of Samba. Samba version 3.0[27] will permit the establishment of trust relationships between master and resource domains and the implementation of the Windows NT domain concept. Version 3.0 also makes it possible to use the Windows User Manager for user administration purposes, for example, in order to create new users. Replication between the Windows domain controller and the Samba domain

---

[26] Especially a feasibility study for a Federal Ministry conducted in 2001

[27] Currently available as beta version – even though the German Federal Cartel Office is already using this version for productive operations.

controller is still not yet possible, so that pure Windows or pure Samba domain controllers only can be used within a domain. If integration of Windows server services in a Samba domain is necessary, these can be integrated as member servers. SAM replication in a pure Samba domain controller environment is possible without any problems by combining Samba and OpenLDAP. OpenLDAP is used by Samba to manage groups and users and also offers the necessary replication mechanisms.

Comparison of file systems

Table 6: Comparison of file systems

	NTFS	**XFS**	**EXT3**	**ReiserFS**
Length of the file names	256	256	256	256
Character set for file names	Unicode	ISO-Latin	ISO-Latin	ISO-Latin
Presentation of upper case / lower case	X	X	X	X
Discrimination between upper case / lower case		X	X	X
Disk quotas	X	X	X	X[28]
Encryption	EFS	X[29]	X[30]	X[31]
Compression	X	(X)[32]	(X)[33]	(X)[34]
Maximum file size	2 tera	16/ 64 tera[35]	4 tera[36]	16/ 64 tera[37]
Maximum path length	Unlimited	Unlimited	Unlimited	Unlimited
Change journal	X			
Journaling	X	X	X	X

---

[28] Not reliable with certain versions.

[29] Can be implemented via operating system means (crypto-api/loopback and cfs/rpc) for complete file systems or partial trees

[30] Refer to "encryption in XFS"

[31] Refer to "encryption in XFS"

[32] Compression at file system level is possible by loopback.

[33] An attribute for compression is foreseen in the incode of an ext2/ext3 file system. Up to kernel 2.2, patches were available for an e2compr project which, on this basis, permitted transparent file compression using different algorithms. Since Kernel 2.4, this project has been discontinued because the demand for compression effectively no longer exists. Compression at file system level is possible by loopback.

[34] Refer to "encryption in XFS"

[35] Depending on whether 32-bit or 64-bit; theoretical maximum at 9 exabytes; in Linux kernel 2.4 limited to 2 tera in view of the maximum file system size

[36] Depending on whether 32-bit or 64-bit; in Linux kernel 2.4 limited to 2 tera in view of the maximum file system size

[37] Depending on whether 32-bit or 64-bit; theoretical maximum at 1 exabyte; in Linux kernel 2.4 limited to 2 tera in view of the maximum file system size

Technical description of the migration paths

	NTFS	XFS	EXT3	ReiserFS
ACL	DACLs	POSIX ACLs via extended attributes	POSIX ACLs via extended attributes as of the next kernel version	
Auditing	SACLs	(X)[38]	(X)[39]	(X)[40]

Local file storage with client migration

The file storage analysis is based on the assumption that no user data is stored locally on the clients. In the case of migration, a new system with identical functionality is installed without importing data from the old client.

If a large number of identically equipped clients must be migrated, diskless operation on a pure network file system is an option worth considering. This special case of central file storage within a network offers significant advantages especially at administration level: Changes in the client configuration are carried out only once on the server, and are automatically in effect on all the clients using this server. The selection of the server service underlying a "diskless client" basically requires the same considerations which also apply to the selection of the server system for central file storage in general.

Access control: mapping the privilege profiles from Windows to POSIX ACL

The way a Samba server handles the rights to access directories and files largely corresponds to the familiar principles of Windows NT. Under Samba too, individual directories in the file system of the server are made available as shares in the network. The details of access control are determined on the basis of the privileges defined in the file system at the server end for a user who is individually authenticated at the Samba server. Authorization is thus interaction between the Samba server and the operating system and/or the file system.

Shares (releases) and their server-end characteristics – such as directory path, granting of anonymous access and general write protection – are typically handled and shown under Samba in a configuration file which is unambiguous for every server instance. Editing of this configuration file is also possible (after authentication/authorization with encrypted HTTPS protocol) via a web frontend.

The rights to access directories and files are handled with all operating systems in the functional operating system component of the file system. Whereas no owner concept for files existed in the FAT file system under DOS and older

---

[38] Auditing was developed several times under Linux. An early project audit has no longer been updated since the beginning of 2000. The grsecurity project implements a process-based ACL system in the kernel (http://www.grsecurity.net/). This enables complete auditing of files and other system activities.

[39] Refer to "Auditing in XFS"

[40] Refer to "Auditing in XFS"

Windows versions, owners and user groups for files have been discriminated under UNIX from the very outset and under Windows since the introduction of the NT file system (NTFS). The file system uses so-called access control lists in order to determine which users can handle which directories and files in which manner.

Under UNIX, the access rights for reading, writing and executing are defined as a minimum for the owner, an owner group and all other system users. Additional restrictions or the granting of rights to other users or user groups can be implemented with certain UNIX/ Linux file systems via extended attributes and POSIX Access Control Lists.

Samba as the file server keeps its data in a UNIX file system and accesses the data using the effective rights of the user authenticated for access. Although the Samba server can theoretically impose additional access restrictions, the server can never ignore the restrictions laid down in the file system. Both when transmitting the existing access rights from the server to the client and when manifesting changes initiated at the client end, the Samba server applies the canon of privileges of the file system in which it stores and manages the user data. This is why migration requires the Windows privileges model to be mapped to the UNIX world. This mapping process and the special features and restrictions to be taken into consideration are described in the following. The authors of this guide assume in this context that a file system with support for POSIX-ACL is used under Linux. At present, these are the file systems XFS, JFS and with patch EXT2 and EXT3.

Mapping the NTFS-ACL to the privileges system of Linux

When the Windows ACL is transferred to the POSIX ACL of Linux, the system of privileges is reduced to such an extent that the picture largely corresponds to the simple presentation in the security settings.

The only privileges which POSIX ACLs recognize are rights to *read, write* and *execute*. The POSIX ACLs do not provide different types for discrimination, such as *write data, append data, write attributes* and *write extended attributes*. When the Windows system of privileges is mapped via Samba to UNIX, it is thus only possible to map complete aggregations of the Windows privileges to the UNIX file system. This also means, in the opposite direction, that the Samba server cannot report any other privilege aggregations to the Windows client.

Table 7: POSIX privileges and Windows aggregations

		POSIX privileges		
		Read	**Write**	**Execute**
WIND OWS	Browse folder / execute file			
	List folders / read data	X		

Technical description of the migration paths

		POSIX privileges		
		Read	**Write**	**Execute**
	Read attributes	X		(X)[41]
	Read extended attributes	X		
	Create files / write data		X	
	Create folders / append data		X	
	Write attributes		X	
	Write extended attributes		X	
	Delete subfolder / files			
	Delete			
	Read privileges	X	X	X
	Change privileges			
	Take ownership			

At the user end, the Windows dialogs can be used to generate the corresponding combinations of POSIX privileges by combing the appropriate NTFS privileges. Note that the setting of *one* additional NTFS privilege from the Windows list leads to the setting of *all* privileges of the POSIX aggregate to which the NTFS privilege set in this way belongs. If, for example, the *Write attributes* privilege is set in the *Privilege entry* dialog for a file for which read access only was previously permitted, the Samba server automatically adds the privileges for *Write extended attributes, write data* and *Append data*. After the dialog was exited by clicking *OK*, the new, significantly extended scope of privileges is then immediately displayed when the dialog window is opened again. The advantage is that this behavior on the part of the Samba server does not permit misinterpretation of the simple presentation of privileges.

In the simplified presentation of security settings, the picture is consistent. The *Read* and *Write* privileges can be set jointly and severally as well as in combination with *Read/execute*. The latter group privilege cannot be set alone.

The NTFS privileges *Delete subfolder/files*, *Delete*, *Change privileges* and *Transfer ownership privileges* cannot be implemented under POSIX ACLs and thus do not lead to any result on the Samba server when they are set (shown against a gray background in the table). However, in the case of *Full access*, i.e. complete read, write and execute privileges, they are also marked as set.

Table 8: POSIX and Windows privileges

	POSIX privileges

---

[41] Although this is displayed, setting is not permitted because otherwise the complete "Read" aggregate is activated.

		Read	Write	Read and execute	Read and write	Read, write and execute
WINDOWS	Full access					X
	Edit					X
	Read / execute			X		X
	List folder contents (for folders only)			X (for folders only)		X (for folders only)
	Read	X		X	X	X
	Write		X			

Mapping the inheritance function

The POSIX-ACL implementation uses passive inheritance only. Active inheritance of the NTFS type is not possible.

Mapping the attribute system

The attributes which do not exist under Unix can be implemented in different ways. First of all, the *Write protect* flag is not really needed because it is already included in the normal privilege system. It is hence displayed automatically for files and directories without write privilege. The *Archive, Hidden* and *System* flags can be represented by the *Execute* bit of the UNIX file system which is not used, so that these flags exist. The *Compressed* and *Encrypted* attributes cannot be mapped. They can, however, be made available via special services under UNIX.

Mapping the audit functions

The auditing system forms an integral part of Windows. It can be represented under UNIX by other mechanisms. For the Samba server, the auditing functionality can be implemented via a VFS module. Access to files and directories is then logged by the Samba server. At the file system level, auditing in this form has not yet been integrated into the Linux kernel even though several implementation attempts were made and despite the fact that the preconditions have been fulfilled in the existing structures for extended attributes in Linux file systems. In practice, however, this functionality appears to be of so little importance that all attempts made so far were abandoned due to a lack of interest.

Summary of the most important consequences of using Samba with POSIX ACLs

The following applies to writing as an abstract privilege:

There is no distinction between "write data" and "append data"

In the case of folders, there is no distinction either between creating folders and creating files

> There is no distinction between the writing of folders and/or files and attributes

The following applies to reading as an abstract privilege:

> There is no distinction between the reading of folders and/or files and attributes

Reading of privileges is always permitted in principle. Neither audit nor inheritance are implemented in general.

User groups and access privileges

The assignment of access privileges to groups plays a paramount role, especially in conjunction with releases which are commonly used by work groups. NT discriminates between (server-) local and global groups. Local groups can be regarded as alias definitions that refer to one or more global groups. This means that local groups can contain several global groups. Nesting of groups is not possible under Samba (as under UNIX/Linux in general). Samba only permits all UNIX groups to be presented 1:1 as global groups for Windows clients and member servers.

These global groups can, of course, form part of local groups in Windows member servers. This means that the U-G-L-R and U-G-R models described in section 3.2.2.4 continue to be available on these servers.

The introduction of a concept of local groups also for Linux servers is currently not foreseen, so that only the U-G-R model is typically used here. An equivalent functionality can be implemented in an LDAP-based group management system with a corresponding business logic.

Assessment of the repercussions for users

When the Windows ACLs are mapped to the POSIX ACLs, the fine granularity with which privileges can be modified under Windows is lost. In practice, however, only the significantly simpler group privileges of the simple security settings are used in the vast majority of cases.

The further graded privileges are used in isolated cases only. The distinction between attribute and file privileges, in particular, is used extremely seldom.

The *Append data* privilege, too, will be of use in very few cases only. If an Extended 2/3 file system under Linux is used, this privilege can also be set for selected files as an extended attribute in the command line.

The consistent mapping of the simpler privileges model from the POSIX ACLs increases the reliability of the picture of the simple security settings for the average user.

The mapping of certain functions, such as inheritance and auditing, is not possible.

3.2.4   Continuing migration

3.2.4.1   Windows 2000

This section deals with Windows 2000 as the successor to Windows NT4 under the "file service" aspect.

Expanded functionality

Windows 2000 comes with a number of new features with regard to file services. The following key words should be mentioned here.

NTFS5 file system

HSM-API

Inheritance

Encryption (EFS)

SMB over Native IP

Dynamic data volume management

Defragmentation

Group nesting

Remote storage

Indexing service

Distributed link tracking

DFS

Offline folder

Folder redirection.

These subjects are discussed in more detail in the following.

NTFS5 file system

The NTFS5 generally offers the following improvements:

It is possible for the first time to manage access privileges by inheritance. This means that privileges which are set on higher-level folders come into effect in lower-level folders and files without the need to write through (burn-in). The disadvantages of writing through (workload problem, deleting of special privileges in sub-folders) are hence eliminated.

NTFS5 comes with a change journal in which the changes are logged.

NTFS5-formatted data volumes include a hidden folder called "System Volume Information" which can only be accessed by the operating system and in which the additional functions are managed.

NTFS5 offers the so-called HSM API (Hierarchical Storage Management programming interface) which can be used by third-party manufacturers.

NTFS5 supports data encryption. The Encrypting File System (EFS) enables users to protect data against reading by third parties (including administrators). A PKI (Public Key Infrastructure) is necessary for this purpose in enterprise networks.

Although the integration of quotas in the file system is still possible, it continues to be subject to the restrictions of NT4.

Protocols

Windows 2000 still supports the above-mentioned protocols. With Windows 2000, it is possible for the first time to deactivate communication via NetBIOS. For the file services, this means that the "Direct Hosting of SMB Over TCP/ IP" takes place via port 445.

Data volume management

Windows 2000 also offers the possibility to integrate physical harddisks into the system without the need to assign drive letters. These dynamic data volumes can be linked and made available as folders in traditional data volumes. Windows 2000 is the first version to include a tool for data volume defragmentation.

Changes concerning access control

Significantly more access control operations can take place under a Windows 2000 active directory because *more* group types can be nested and to a *larger degree*. Group nesting of this kind is only possible if an active directory is used in "native mode". The new "Domain Local" and "Universal" group types are available in "native mode". The following table shows the nesting possibilities.

Table 9: Group types

Group type	Can have the following members	Can be a member of
Global group	Users and global groups of the same domain	Global groups of the same domain
		Universal and domain-local groups of each domain
Domain-local group	Users, universal and global group of each domain	Domain-local groups of the same domain
	Domain-local groups of the same domain	
Universal groups	Users, global and universal groups of each domain	Domain-local or universal groups of each domain

Besides these new group types, security and distribution groups must be discriminated in environments with an active directory and Exchange 2000. Although Exchange environments exist for the distributor groups, they do not permit any control with regard to file services.

Remote Storage

Remote Storage is a new service under Windows 2000 which enables the swapping to tape drives of files which have not been used for a long time in the sense of an HSM (Hierarchical Storage Management) functionality.

Indexing Service

The Indexing Service can be optionally activated for file folders in order to index the files stored there. The index enables a quick search for defined contents. The indexing services enables indexing of the following document types in different languages:

HTML

Text

Microsoft Office 95 or higher

Internet Mail and News

Any other documents for which a document filter is available.

Distributed Link Tracking

Windows 2000 file servers enable the programming of applications that support linking and embedding of objects in such a manner that, following relocation of the linked objects, information concerning the current place of storage can be retrieved from the file system. This means that fault-free use continues to be ensured.

Distributed File System

The Distributed File System (DFS) were already available under Windows NT 4 by additional installations on the server and client. Under Windows 2000, these functions were integrated as standard functions and additionally amended both at the client and at the server end. DFS permits that releases of folders which are distributed to several servers can be presented to the client as sub-folders of a single release. This means savings of drive letters with regard to the network drives to be assigned to the user. In Windows 2000, DFS was amended by integrating the FRS (File Replication Service), so that the linked releases and their contents are replicated to further releases and other file servers. In the case of a failure of a server and hence of its release, the client can refer to the replicates without the need to establish new network connections. In Windows 2000, information can be saved and replicated via the DFS tree in the active directory. This means that the client has access to the required connection information almost all the time.

Connecting

The user can be supported in his or her search for releases by publishing the releases in the active directory.

Offline folder and folder redirection

The "Offline Folder" and "Folder Redirection" are primarily functionalities of the client (such as Windows 2000 / Professional) rather than properties of the file

services of Windows 2000. They are, however, mentioned here because they are in principle relevant with regard to data storage and because they must cooperate with the file server. Offline folders are, so-to-speak, the successors to the "briefcase" of previous Windows versions. Users of a notebook, for example, can work on folders and files which are normally stored on file servers without being connected to the network. As soon as the connection to the file server is restored, this data is then replicated. Due to this replication process, the file properties at both ends (client and server) are very important in order to enable faultless replication.

With the folder redirection function, Windows 2000 addresses the fact that the size of user profiles on workstation computers can increase tremendously during operation. This can, for example, occur when the user saves data under "Own files" which would be better stored on file servers. Windows 2000 enables the "twisting" of the system folders of the user profile ("Own files", "Application data") to a network path. These folders then appear to the user in a transparent manner as local folders. Due to the relocation of the folders to the file server, measures must be taken to ensure that access privileges remain in effect.

Data backup

The NTBACKUP on-board tool was modified in such a manner that data backup is now possible on (local or network) drives. This means that local tape drives are better avoided.

Version successor

In the product succession, the following paths must be noted:

> Windows 2000 Server is the successor to Windows NT 4 Server

> Windows 2000 Advanced Server is the successor to Windows NT 4 Server Enterprise Edition (refer to "Cluster Services").

Windows 2000 DataCenter Server is the first operating system from Microsoft which is available only in conjunction with special hardware and from a few manufacturers only. This platform addresses very special availability and/or load scenarios. It is not discussed any further in this guide.

Network Attached Storage (NAS)

Some hardware manufacturers have developed, in cooperation with Microsoft, so-called NAS systems based on Windows 2000 Server. These systems are dedicated to file services and are I/O-optimized.

Practical experience

The following sections contain some remarks on the technical innovations addressed in the foregoing.

> EFS is typically restricted to mobile computers requiring protection of data against privacy violation. The use of EFS is hampered by the necessary PKI (even if the Windows 2000 active directory offers this) on the one hand and is often regarded as not very helpful due to the lack of support for access

mechanisms on a group basis (for the purpose of group-specific file storage on file servers) on the other.

Deactivation of communication via the NetBIOS interface is not mandatory and is typically postponed because of downward compatibility requirements.

The use of the former file and access management tools must be taken into consideration in view of the new file system. An NT 4 Explorer, for example, is unable to implement the inheritance function.

The use of Windows 2000 must be checked from case to case with a view to the continued use of legacy hardware which was already used under NT 4. In the majority of cases new hardware will have to be purchased.

3.2.4.2   Windows 2003 Server

This section deals with Windows 2003 as the successor to Windows 2000 Server (previously "NET Server") under the "file service" aspect.

The far-reaching innovations of this version will be briefly outlined in the following.

Windows 2003 Server will be the first operating system from Microsoft which will also be available in a 64-bit architecture.

The official support of SANs (Storage Area Networks) is improved in such a manner that booting of harddisks is now also possible in the SAN.

The EFS now also enables access by multiple users to a file resource. Groups are still disregarded.

The Volume Shadow will be a new functionality: It includes, on the one hand, that the file and folder structure can be regarded as being static at a given point in time, so that data backup is possible without the need to consider open files. Other new options are that users can now recover files which were deleted by mistake from a "snapshot" without explicitly having to request recovery. The system recovery is facilitated for administration.

3.3   Print service

3.3.1   Overview

The result of the discussion of technical details below is the following.

Under Linux, CUPS is the de-facto standard of all major distributions (SuSE, Debian, RedHat, etc.). CUPS is the system of choice, both in homogenous Linux system landscapes and in heterogenous system landscapes with Windows-based client systems. With Windows-based client systems, the combination of CUPS and Samba offers a full-scale print system.

The functionality of CUPS is designed as a cross-platform functionality due to the implementation of IPP (Internet Printing Protocol). However, CUPS also supports all other relevant print protocols, such as LPR/LPD, Socket/AppSocket,

SMB/CIFS and MS-RPC (in conjunction with Samba). The CUPS/Samba combination also supports automated driver download to the Windows clients.

Furthermore, CUPS offers different options for ensuring data integrity even during printing. These options include SSL-encrypted transmission in conjunction with the use of IPP and user authentication via LDAP or in conjunction with Samba. This offers significant advantages, even with a view to printer access accounting.

Before a migration project is started, the support situation of the printer models used should always be analyzed. This is particularly important if print processing is to take place completely on the print servers because support may not be ensured in a few, isolated cases.

Even in the case of continuing migration at the client end, Windows 2000 clients can print via CUPS servers because Windows 2000 supports IPP.

3.3.2   Introduction

The "print" issue is a much-neglected subject in the IT world. This is valid for all operating system environments, i.e. for both the Windows and the UNIX/Linux world alike. Print problems often cause the most serious friction losses. A substantial part of the administrators' time is spent on resolving routine print problems. On the other hand, printing is often a mission-critical application where failure can cause financial losses and many headaches.

A certain "chaos in infrastructure" is quite common as far as print services are concerned. "Grown structures" have led to all kinds of inconsistencies at many points: A mess of page description languages (PostScript, PCL, PreScribe, ESC/P, PDF...) is almost always the rule. The often "unfriendly" coexistence of print and network protocols causes all sorts of problems: LPR/ LPD, HP JetDirect, SMB/ MS-RPC, usw.

Although migration of print services to a new platform does not necessarily yield a precise 1:1 picture of the existing situation, it should be seen as an opportunity to eliminate existing weaknesses.

Besides technical shortcomings, the cost issue is equally important. The true costs of organization-wide printing (department, company, group, agency-wide) are often not precisely known. Significant savings are possible in this field which can only be quantified when clear data is available.

The most important cost factors are:

    Number of printers

    Paper consumption

    Toner/ink consumption

    Power consumption

The following questions should be answered before starting migration:

    How many printers are there in the organization/building?

    How much paper is consumed?

How much toner/ink is consumed? How much do these items cost per year?

How high are the service (repair, maintenance) costs?

How much does the organization's internal help-desk cost?

How much is spent on electricity?

How much does it cost to print one page?

How are these costs distributed to different printer types?

Is a more efficient use of available print resources possible?

The determination of the actual financial costs often requires a dedicated study. This effort frequently pays off. An exact analysis of cost factors pays off in any case because the resultant savings potential pays back the costs of such an analysis within one year.

Migration of the print environment means significant change – and should be preceded by a demand analysis, the results of which must be considered when the transition is planned.

3.3.3   The starting situation – printing under Windows NT 4

The starting situation described in the following is assumed to apply to the majority of legacy Windows environments.

It is further assumed that the existing environment is based on one of the common NT domain models. Moreover, we further assume that these environments provide print services based on Windows NT 4 Server. The print servers are assumed to be members of an NT domain.

The Enterprise Edition enables a print service which is implemented by two nodes (servers) in a cluster. Failure of one server (node) is compensated for by the remaining node taking over the failed server's duties. The client "notices" this, stepping in – if at all – for seconds only. However, loss of active print jobs cannot be ruled out. The user of such a cluster requires special hardware (refer to "File services).

The following client computers (print clients) are considered:

Windows NT 4 Workstation

Windows 9x

The following print devices are considered:

Printers with network card

Printer boxes with connected printers

The illustration below shows a typical print environment configuration:

Some workstation computers have a printer which is connected locally to LPT1 (local printer).

Technical description of the migration paths

Other workstation computers do not have printers connected directly, but use printers connected to the network only.

The majority of laser printers can be fitted with a network card. Ink-jet printers, in contrast, typically require an additional printer box as a precondition for network capability.
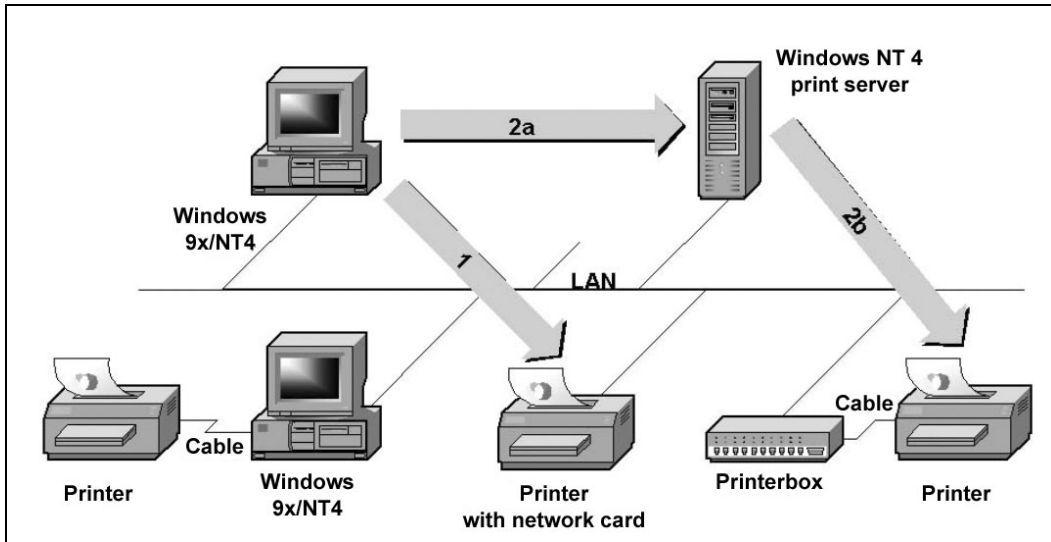
Fig. 6:   Print environment[42]

The illustration shows the two fundamentally different data streams. In the first case, the client prints via the network directly on the printer, whilst in the second case, the client uses an "enabled printer" on a print server. The print server then sends the data to the printer.

These different methods and their variants are discussed in the following.

3.3.3.1   LPR/ LPD under Windows NT 4.0

The LPR LPD (Line Printer Redirector - Line Printer Daemon) method known from the UNIX world entered the Windows world with the launch of Windows NT and is used on NT print servers as the communication standard between server and print device. This method is generally also suitable for communication between client and server or between client and print device. The general disadvantage of LPR LPD is the fact that printer-specific feedback information is not processed.

3.3.3.2   Other network ports

Reputable printer manufacturers have implemented additional ports under Windows NT, such as:

LexMark Mark Vision Print Monitor (Lexmon.dll)

---

[42] Microsoft Windows NT 4 Resource Kit

Hewlett-Packard Network Port Print Monitor (Hpmon.dll).

Unlike the LPR port, these ports can use other transport protocols, too. They support, for example:

DLC

and IPX.

The new network print ports usually enable bidirectional communication with the printers or printer boxes.

3.3.3.3 *Direct printing from the workstation computer*

Direct printing (refer to Fig. 6: Print environment, arrow 1) takes place via LPR/ LPD. This requires the TCP/ IP print server to be installed on the workstation computer under Windows NT 4. Windows 9x systems require a software from third-party manufacturers for this purpose. A so-called LPR port is configured on the workstation computer as the connection for this. The IP address or a corresponding host name (DNS) of the target printer must be entered to this effect. Furthermore, a printer model and thus the appropriate printer driver must be selected. The operating system considers such a printer as being "local". Direct communication between client and print device is quite unusual in Windows NT because local administration on the terminal devices boosts the administrative effort considerably.

3.3.3.4 *Printing via the print server*

Printing from the workstation computer via the print server requires two data streams:

The transmission of data from the workstation computer to the print server (refer to Fig. 6: Print environment, arrow 2a)

The transmission of data from the server to the print device (refer to Fig. 6: Print environment, arrow 2b)

The transmission of data from the server to the print device is usually based on LPR/ LPD (refer to "Direct printing from the workstation computer).

The transmission of data between workstation computer and print server can take place in different ways.

Two general requirements must be fulfilled at the server end in order to enable a client to address a particular printer via the server:

The printer must be set up on the print server (LPR port, printer driver).

The printer must be enabled.

Enabling means in Windows networks, amongst other things, that the printer can be browsed by clicking the related print server.

The communication between workstation computer and print server (printer release) is possible in three different ways:

The NET USE command can be used in order to redirect an existing local LPT port to the printer release (example: net use LPT3 \\servername\printer_release_name). This method requires the user to install a printer (printer driver) on the LPT port, thereby configuring the printer as a local printer. This is often necessary if printing from within DOS applications is necessary. The print data is transmitted in RAW format. This means that the print device can directly use the data received.

A new LPR port can be set up which contains the print server and the name of the printer release as the target address. The print data is also transmitted in RAW format.

The so-called "Point & Print" method can be used in order to set up a network printer on the workstation computer. The advantage of this method is that manual configuration or printer driver installation by the user is not necessary under ideal conditions. The print data is transmitted in EMF format (Enhanced Meta Format). This format cannot be used by the print device and must hence be processed on the print server. The section below describes the "Point & Print" method in more detail.

3.3.3.5 The "Point & Print" method

Microsoft uses the RPC (Remote Procedure Call) protocol for communication between print client and server and implements the so-called Point & Print technology for this purpose. This enables the transfer of the printer drivers from the server to the client on the one hand as well as the transfer of the device-specific settings (paper trays, standard paper formats) to the client on the other. Furthermore, this shifts part of the rendering process to the server, thereby relieving the client during print processing. This relief is a particularly positive effect if terminal servers are used.

Since this is a Microsoft-specific technology, the process is described here in detail. It is assumed that both the workstation computer and the print server use Windows NT 4.

When the user adds a network printer to his print environment, the first step is to reconcile the drivers. A Windows NT client loads the printer driver from the server if the following conditions are fulfilled at the same time:

The print server uses Windows NT.

The print server has the suitable driver (platform: x86, Alpha, etc. and version: 3.1, 3.5, 4).

The NT client has no driver or an older version than that on the server.

After downloading, the driver is installed by the client. This means that entries are made in the client's local registry.

The printing process:

The illustration below (Fig. ßßß: The process with the "Point & Print" method

) shows the sequence of the process which is briefly described in the following.
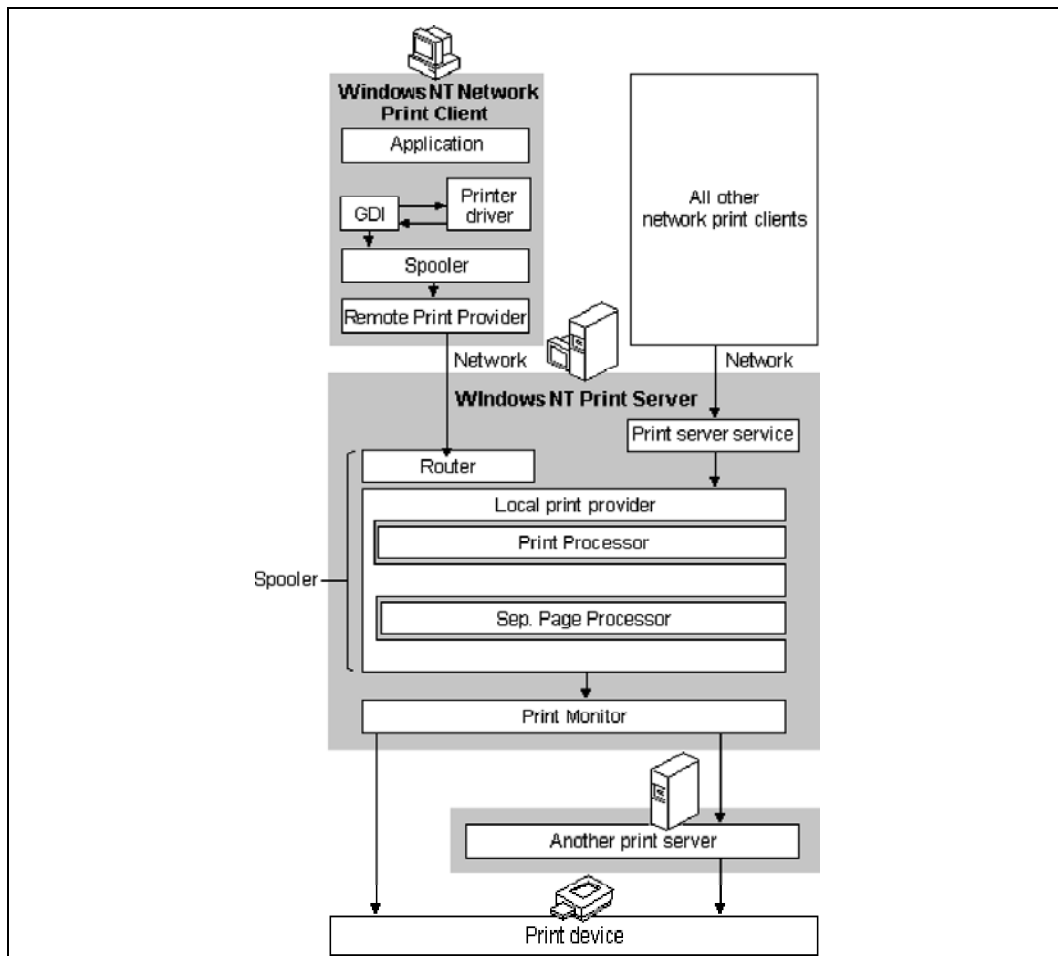
Fig. ßßß: The process with the "Point & Print" method

Step 1:
The user decides to print a document from within a Windows application. The user starts the GDI (Graphics Device Interface). The GDI loads the printer driver of the selected printer. On the basis of the document information from the application and the printer driver information, the print job is rendered for the EMF format in a first process. The application starts the local spooler (Winspool.drv).

Step 2:
Since the client uses Windows NT, the local spooler (Winspool.drv) calls, via RPC (Remote Procedure Call), the spooler of the server (Spoolss.exe) which calls its router (Spoolss.dll) directly via API. The router polls the remote print provider (Win32spl.dll) of the client. The client activates the Spoolss.exe process on the print server via RPC which then receives the print job and its data via the network.

Step 3:
The router of the server receives the print job as an EMF (Enhanced Metafile) and passes it on to the local print provider. Compared to RAW format, print data in EMF format is still relatively independent of the print device and is

usually limited to a smaller volume. Whilst the first part of the "rendering" process took place on the client, the second part is then carried out on the print server by the print processor of the local print provider which writes (spools) the result on the local harddisk.

Step 4:
The spooled job is passed on to the print monitor (despooling) which then calls the port monitor. The port monitor checks whether and, if so, in what way bidirectional communication with the print device is possible, and sends the necessary data.

Step 5:
The print device receives the data, converts every page to a bitmap and prints it on paper.

In the event that the client under step 2 is not a Windows NT client or a Windows NT client which uses a redirected local connection (net use LPT), the print job is completely rendered already on the client and sent in RAW format via the NetBIOS redirector to the print server service.

The job is also sent in RAW format via TCP/IP to the LPD of the print server if the client uses LPR.

3.3.3.6   Network protocols

Communication via LPR/ LPD is exclusively based on TCP/ IP.

In contrast to this, communication between workstation computer and print server can be based on different transport protocols:

TCP/ IP

NetBEUI

SPX/ IPX

The real transmission of print data requires

SMB

or RPC

3.3.3.7   Access control

These Windows NT print servers control access to the network printers (releases) which are controlled by the print servers. The privileges for this release operation are restricted to the following levels:

Printing

Printer administration

Document administration

3.3.3.8 Tools

The administration tools of print servers under Windows NT are restricted to administration of print releases and printer drivers. Management of the print devices is not possible.

Printer manufacturers provide additional tools for printer administration (MarkVision by LexMark, JetAdmin by HP, etc.).

Similar to network drives, automatic connection to printers is desired when the user logs in. This can be achieved via VB-Script or certain tools, such as con2prt.exe.

Script programs (Perl) are conceivable with regard to the granting of privileges for printer releases.

3.3.3.9 Special features during production

The device settings are solely dependent on the individual print device. Even in the case of identical models, these settings can differ due to different type series or features. Parameters, such as RAM, paper trays and paper format must hence be considered in the settings.

Printers with several trays often contain different paper types. In order to facilitate the correct selection, the printer is often published under two different releases. Every release then includes different settings for the standard tray.

In order to ensure optimum support of roaming users, it is conceivable that connection to printers is based on the location of the computer. This can be achieved via additional mechanisms in the logon script on condition that a database can be queried which contains the assignment of workstation computers and print devices.

The manufacturers offer separate printer drivers for a variety of printer models even though these printer drivers are already included in the sources of Windows NT. Although the drivers supplied by Microsoft are tested by Microsoft, they often fail to cover the functionality (several trays, duplex units) offered by the drivers of the manufacturers, so that drivers of the latter must be used. The manufacturers often implement their drivers in the form of additional dll files with the result that the complexity of the print environment is increased. This implies driver selection management.

Existing print concepts often define priorities between postscript and PCL.

User-defined forms and fonts are used in certain environments.

In a Windows NT environment, every user in the standard configuration can access every printer which is released. This is, however, often not desired. The assignment of user-specific privileges in conjunction with printer releases is considerably more difficult compared to the file services.

3.3.4   Replacing migration

This section assumes that a print infrastructure which includes at least one print server exists or is to be created. Such a print server typically works as a central spooling host which is also capable of offering additional services.

Only the "Common UNIX Printing System" will be evaluated as a possible migration path. This system is established on practically all UNIX systems. Apple also recently added this to its Mac OS X operating system. Under Linux, CUPS is the de-facto standard of all major distributions (SuSE, Debian, Mandrake, RedHat, etc.).

If the legacy print environment consists of Windows clients which access an NT print server, options for migration at the server end are analyzed.

3.3.4.1   Functional requirements

As printing is often a "mission-critical" task, the technical infrastructure and internal organization must meet with demanding requirements:

Reliability
A minimum degree of failure safety is indispensable; alternatives must be easy to integrate – the availability of the print services must be ensured even if no IT experts are available.

True rendering
Evaluation criteria are undistorted fonts, clear pictures, color fidelity.

Print quality
Rendering with minimum resolution is expected.

Accounting
Cost control via detailed log and report options should be possible.

Quotas
A requirement aimed at cost control and/or cost limitation.

Redirecting of print jobs
It should be possible without any problems to address an alternative printer without the need for the client to send the print job again. (Important: if the alternative printer is another type, it should nevertheless be able to process the print file in question).

Reprint
Environments with central duplication services often require reprinting of print jobs already completed. A reprint function is necessary in order to implement the "printing on demand" functionality and to increase the number of copies at a later time, or in order to compensate for technical problems (such as paper jam / power failure) and operator errors (such as the use of paper of an incorrect color).

Job history
This function offers an overview of all print processes. Meaningful data concerning total quantities (budget planning), distribution by models and

locations (optimization of resource distribution) as well as peak loads (sensible capital investment) is available at the end of the year.

Integration into proprietary solutions
It is often necessary to adopt or integrate "old" or new proprietary special solutions. This should be possible with reasonable effort.

Cost transparency and control
are vital – both during and after the migration phase.

Security
"Eavesdropping" of confidential data should not be possible (not even by intercepting print files)

Authentication
Certain printers are reserved for certain user groups, or certain "costly" settings (1200 dpi in full-screen mode on photographic paper) are enabled for certain users only (or even completely disabled).

Print "on hold"
Printing at another time or at night (automatically controlled batch jobs).

Without special software to the overview
A web browser ideally gives a quick overview of the queues. Additional command line access is guaranteed, ideally "from everywhere". This is ideally possible for authorized individuals only rather than for everybody.

Integration into heterogenous worlds
A print software must be multi-protocol enabled because a generally used standard does not yet exist in practice. Multi-protocol capability must be ensured both towards the clients (which should be free to chose any protocol for sending their print files) and towards the target printer and/or second-level print server (which are often too "old-fashioned" and this requires certain conventions). Furthermore, full support of the future IPP standard must be in place.

3.3.4.2 Support of established[43] standards for print data transmission

The above-mentioned functional requirements must be fulfilled by the proposed technical solutions. One particularly important aim is to achieve openness by consolidation on existing, generally accepted open standards. Support of conventional or proprietary protocols (and devices based on this) which will remain necessary during a transitional period should be ensured even in future. The functionality of CUPS is designed as a cross-platform functionality due to the implementation of IPP (Internet Printing Protocol – refer also to The traditional protocol for print data transmission [from the client to the print server, from server to server and from the server to the target (network) printer as well as from the client directly to the printer] has many shortcomings: it is not encrypted, it is not authorized, it is not very reliable, it is not bidirectional (no feedback from the

---

[43] Both open and non-open standard.

printer, for example), it is not a "real" standard (hence different implementations which cause problems due to occasional incompatibilities).

). IPP is used as a protocol between CUPS servers, clients and state-of-the-art printers with direct IPP support as a communication and data transmission medium. CUPS modules – so-called "backends" – can be used for communication with conventional printers or print servers. These modules enable communication on the basis of other protocols.Fig. 7:   Printing under CUPS illustrates the use of the protocols at the various interfaces. The functionalities are described in the following.

LPR/ LPD

The traditional protocol for print data transmission [from the client to the print server, from server to server and from the server to the target (network) printer as well as from the client directly to the printer] has many shortcomings: it is not encrypted, it is not authorized, it is not very reliable, it is not bidirectional (no feedback from the printer, for example), it is not a "real" standard (hence different implementations which cause problems due to occasional incompatibilities).

IPP

The Internet Printing Protocol is the Internet standard for printing both in local area networks (LAN) and in wide-area networks (WAN, Internet). The protocol covers all conceivable communication paths, i.e. from the client to the server, from server to server, from the server to the target printer and the direct path from the client to the target printer. The latest and only binding specification is IPP-1.1. The IPP was designed by a working group (the PWG) with members representing printer, operating system and software manufacturers from Europe, the US and Japan, and was standardized by the IETF. The IPP is already installed in all modern network printers. However, as long as the "old" LPR/LPD models are still in use (and they will continue to be operational for years to come), the change will be limited to those cases where it immediately makes sense.

Note**:** Newer versions of Microsoft Windows operating systems include a certain IPP support at the client end (Windows 98SE, Windows ME, Windows 2000, Windows XP) or can be retrofitted at no cost (Windows NT, Windows 95, Windows 98). This then means that these systems can, "quite naturally", print via CUPS servers. At present, however, Microsoft only offers an implementation of IPP version 1.0 which the IETF never "recommended as standard" but which only represented an intermediate stage of the discussion, failing, for example, to define the important aspect of print data encryption and user authentication. A CUPS server must hence omit authentication if it is to be used directly from the Windows client. If CUPS is used in conjunction with Samba and if authentication of the Windows client is necessary, this can then be carried out using the mechanisms implemented in Samba. Commercial CUPS clients for Windows are available on the market if increased security demands must be fulfilled for certain environments.

Socket/ AppSocket

AppSocket (often better known as "HP JetDirect") is a performant transmission protocol for print files. It is more powerful and reliable than LPR/ LPD: it includes a certain measure of bidirectional communication and is faster. Free and commercial administration tools for structuring large networks (such as) HP WebJet Admin) are available for JetDirect. However, it offers neither print data encryption nor user authentication. In practical application, status feedback is only sent from the server to the printer or, in the case of the direct path, from the client to the printer.

SMB/ CIFS

Windows clients use this protocol in order to send print data to print servers (or other Windows computers on condition that these offer "released" printers). The path from the next Windows computer to the target (network) printer must then often be handled via another protocol (unless such target printer is connected locally via a parallel, USB, FireWire or serial interface).

MS-RPC

Windows clients under NT4 and higher can use this protocol in order to send print data to a Windows print server (NT4 and higher). Likewise, automatic driver installation on the clients is possible using RPC methods if the print server provides the necessary files. (The "uploading" of the drivers from a client computer to the print server by an administrator is also based on RPC). Since Samba masters SMB/CIFS, this protocol can also be used by CUPS.

Multi-protocol capabilities with CUPS (overview)
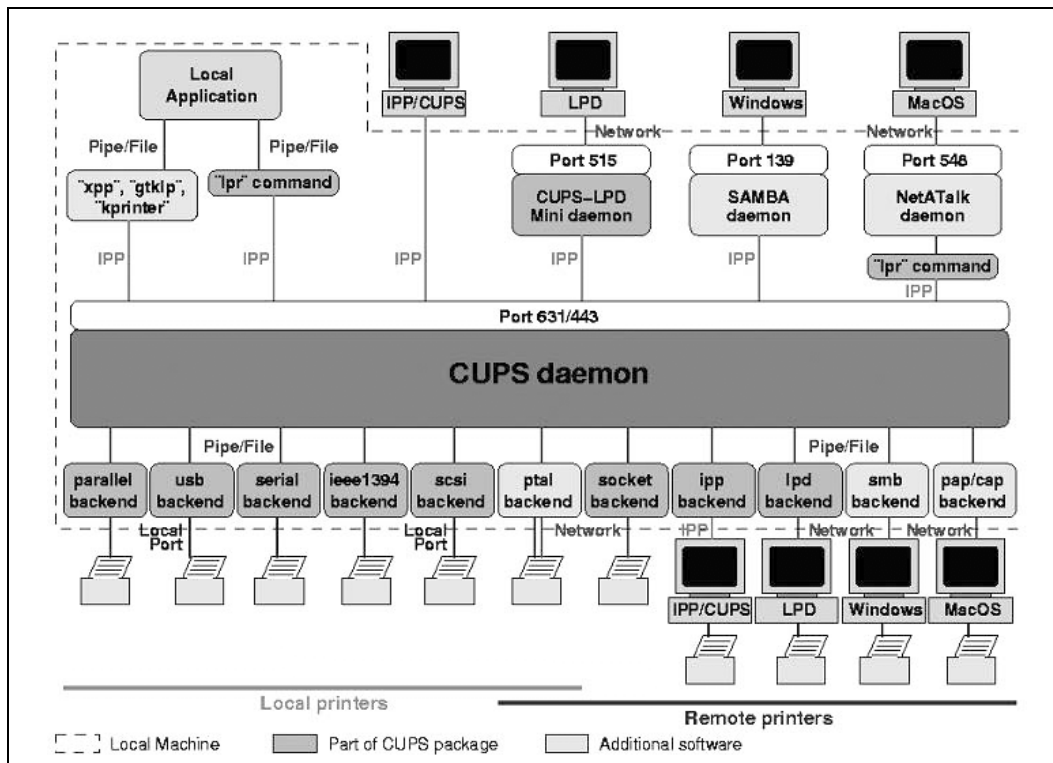
Fig. 7:   Printing under CUPS[44]

3.3.4.3   Integration into Windows client environments

Note on CUPS/Samba integration

CUPS is optimally integrated into Samba – much better than any other UNIX print subsystems which are available. It is the only print system which has integrated its functions into a library (software library). This means that other programs can use its functions by linking to this library. Samba makes use of this capability. By default, Samba is linked to libcups. in this manner. It enables a Samba print server to redirect its incoming print jobs via IPP to CUPS print servers. These CUPS print servers can be installed on another host dedicated to the print service or on the same host as Samba. The IPP is in this case used in a manner that is fully transparent to the administrator or user and does not require any further configuration.

---

[44] Publicly accessible at http://www.linuxprinting.org/kpfeifle/Linux-Kongress2002/Tutorial/

Table 10: client linking to CUPS

Client operating system	Communication
Windows 9x	Win98SE with IPP (version 1.0) supplied – Win98 retrofitting possible
	Via SMB/ CIFS (with the help of Samba)
	Via LPR/ LPD (requires the additional installation of an LPR client)
Windows NT	IPP can be retrofitted
	Via SMB/ CIFS + MS-RPC (with the help of Samba)
	Via LPR/ LPD
Windows 2000/ XP	IPP (version 1.0 installed)
	Via SMB/ CIFS + MS-RPC (with the help of Samba)
	Via LPR/ LPD
Citrix Metaframe and WindowsTerminal Server	IPP can be retrofitted
	Via SMB/ CIFS + MS-RPC (with the help of Samba)
	Via LPR/ LPD
Linux	CUPS and IPP installed
	Via LPR/ LPD
UNIX	CUPS and IPP can be retrofitted
	Via LPR/ LPD
NetWare	IPP installed in NPDS (since Novell 5.0)
	Via SMB/ CIFS (with the help of Samba)
	Via LPR/ LPD
Mac OS 9	Via AppleTalk
	Via LPR/ LPD (requires the additional installation of an LPR client)
Mac OS X	Via CUPS and IPP installed since OS X 10.2
	Via LPR/ LPD (requires the additional installation of an LPR client)

Driver download and installation by clients with "Point and Print"

The CUPS/ Samba combination supports the automated driver download to Windows clients by the "Point and Print" functionality. For this purpose, Samba must be configured in such a manner that it simulates an NT print server. The configuration is described in detail in the Samba HOWTO Collection. However, only a few actions are required. Uploading of drivers from a client machine by an administrator is also supported.

The printer drivers are then located on the Samba server. They are automatically installed in the background on the Windows client system when the user searches or identifies the printer for the first time in the network environment and selects the printer (with a click of the right mouse key) in the "Connect..." context menu.

Automatic driver installation via logon scripts

Technical description of the migration paths

The use of "logon scripts" makes life even easier for users and administrators within a domain. All that is necessary is the following line:

„rundll32 printui.dll,PrintUIEntry /in /n„\\SAMBASERVERNAME\printer_release_name"

in the logon script. It automatically installs the correct printer for the user who logs on (other options in this respect are installation of several printers, setting a standard printer, deleting of obsolete print queues, etc.). This option enables the user-friendly administration of printer drivers and reduces the administrators' workload. Environments with different features can be assigned to different user groups via different logon scripts.

Security and authentication

CUPS also enables encrypted communication between the client and server systems. SSL 3 or TLS can be used for data transmission if the IPP is used.

Another option to meet with increased security demands is user authentication by LDAP. CUPS offers an LDAP interface which can be used to control access to the print system. Furthermore, the directory service can be additionally used for the user-specific configuration of privileges and quotas.

Windows clients typically authenticate themselves at Samba rather than at CUPS. This authentication is used automatically in the case of printing via Samba. Samba then administers the privileges. All that is necessary in this case is to ensure that the Samba server is authorized to use the CUPS print server.

Publication of CUPS printers in LDAP and active directory

Samba can enter its services in an LDAP directory or in an active directory. This, of course, also benefits CUPS printers and CUPS print servers. Further integration stages into an AD environment (or into an LDAP environment which largely simulates an AD environment) are possible. A forthcoming CUPS version which masters linking to LDAP "on its own" is already in an advanced beta test phase.

Platform-independent web interface

CUPS comes with an "installed" web interface. It can be accessed via the following URL: "http://CUPS-DRUCKSERVER:631/". It gives all users informative access to the functions of the print server. Users can by default monitor the status of print jobs, abort print jobs, restart print jobs, reprint historical jobs, etc. (depending on the particular configuration).

Administrators or help-desk staff can create new printers (queues), delete, reconfigure, start, stop, close or open printers (queues) as well as cancel, suspend or restart any print jobs via the web interface. The options for using the web interface can be restricted and/or expanded by configuring the CUPS server accordingly. The web interface is subject to the same access checks as the general CUPS resources. Every object of the print server (access to own jobs or individual printers, access to all printers or all jobs, etc.) can be provided with differentiated access privileges: "User Müller has administration rights" on

condition that he accesses from computer A or B", "All users can delete their own print jobs, but not other users' print jobs", etc.).

3.3.4.4 Adaptability

The print system can be easily amended in many ways by adding filters and backends beyond the direct CUPS functionality.

Filters

CUPS internally uses a modular filter system. It is based on open interfaces. and can be amended at any time. Any script languages (Shell, Perl, Python) or programming languages (C, C++, Java, etc.) can be used in this context. Wrapper scripts enable proprietary binary programs to be linked in a very simple manner.

BackEnds

"Docking" of new backends is simple. Be it for environment-specific adaptation to specific requirements (such as automatic replication of certain print jobs in a remote department, for example, in order to archive business letters), be it because technological innovation (Wireless LAN, Bluetooth, FireWire) makes this an attractive option.

3.3.4.5 Page description languages

CUPS uses the so-called PostScript Printer Descriptions (PPD) for printer control. The PPD specification was originally defined by Adobe and is mastered by practically any print system which controls postscript printers and uses its device-specific options (duplex printing, tray selecting, punching, binding, etc.). Such PPD files are available together with CUPS even for printers without a postscript interpreter of their own. CUPS uses these well-defined printer descriptions in order to enable the corresponding configuration settings via the web frontend or via the configuration masks of the clients.

In the case of printers with no postscript capability, the CUPS server uses so-called "filters" in order to convert the data supplied by the client. Under Linux, the ghostscript program already includes very comprehensive filter packages for converting postscript to various manufacturer-specific and device-specific page description languages. CUPS includes an adapted version of ghostscript.

3.3.4.6 Technical implementation of the driver function

Two different models are available for converting the print file to printer-conforming bitmaps. These models are:

The driver functions are executed completely at the client end.
This means that the client prepares the print file in a manner ready for printing. The print server has pure spooling functions for "raw" print files. Drivers can be offered to the client for downloading and automatic installation.

The print data is processed on the print server.
In this case, the clients send the print data in postscript format to the print server. The clients require a corresponding postscript driver which the server

can offer for automatic installation. The server sends the processed print data to the selected printer. Print processing for a non-postscript printer is carried out by special software (refer also to 0).

The second model offers several advantages compared to the first one:

It automatically supports all postscript devices with all print options (like under Windows NT).

Furthermore, it also supports the vast majority of all customary non-postscript printers (depending on support by ghostscript or other driver packages).

Automatic accounting
Print time, number of copies, target printer, user name, print ID and sender IP are automatically logged for every page. This information is available for subsequent evaluation (cost control, statistics).

Quota option
Print quotas (according to number of pages and/or volume of print data) can be assigned to users for every printer.

Reprint function
Jobs can be saved for a certain period of time and are thus available if reprinting becomes necessary (without the client having to search, open and send the file again).

Redirect function
Print files can at any time be redirected to another target printer (even if the original printer was a postscript model and if the new printer is not PS-enabled). Print options can be adapted to the particular model of the new target device.

Driver consolidation
All clients ultimately use the same core postscript driver (which is only modified by an ASCII file, the "PPD").

This model is, however, also subject to the following restrictions:

Increased resource demand
Central print data processing on the server requires more RAM, CPU and HD capacity (these parameters can be reliably determined in advance if the anticipated print demand is known).

Minor restrictions with regard to the printer models supported
Although the majority of customary printer models are supported, it may sometimes happen that this is not the case. The "Linuxpriniting.org" database contains a list of manufacturers and models supported.

3.3.4.7 Print system architectures

The following list outlines potential architecture options in conjunction with the use of CUPS, with increased failure safety being a crucial requirement for many application scenarios.

Server:

Every CUPS computer that communicates directly with a printer can offer the print functions as a service to other computers and thus works as a CUPS server. This requires the corresponding PPDs and filters for the print-conforming processing of the print files.

Client:

Every computer which sends print files to a server is a CUPS client. A client does not require any local filters or PPDs. However, if the print options used during printing are to be defined on the client, the server automatically sends the PPDs to the client.

Zero administration for native CUPS clients:

CUPS servers send information concerning the printers installed in the network to the clients. The clients thus know which printers can be used in the network. This information is published by UPD broadcasting. An alternative approach is that the client polls the servers in order to obtain this information. Targeted polling is also possible with servers which are separated by routers. Servers which are located in different networks can be configured as BrowseRelay, they can retrieve the data concerning the available printers and send this information to the clients of their own broadcast domain.

Clustering for failure safety and failover:

Two or more CUPS servers can be configured in such a manner that fail-safe print services can be implemented. This can be achieved by configuring the servers with the same printers and printer names. Implicit classes are automatically generated on the CUPS servers. These classes consist of the printers with the same name. The server that is first ready then accepts the client's print job and sends it to the printer. This configuration can also be implemented by forming classes manually. These classes may even consist of printers with different names.

3.3.5   Continuing migration

3.3.5.1   *Windows 2000*

This section deals with Windows 2000 as the successor to Windows NT4 under the "print service" aspect.

Expanded functionality

Windows 2000 introduces certain new features related to the print services. The following key words should be mentioned here.

Standard TCP/ IP Port Monitor

Internet printing

Publication in the active directory.

The following sections address these issues in more detail.

Server-printer communication

With Windows 2000, Microsoft introduced SPM (Standard TCP/ IP Port Monitor). SPM is compatible with SNMP. The LPR port type continues to exist in beside SPM. Compared to LPR, SPM enables the retrieval of detailed status information.

SPM can use two different printer server protocols, i.e. RAW or LPR. RAW is the standard protocol for most print devices.

Publication in the active directory

The active directory enables the printer release to be published (on Windows NT or 2000 servers) in such a manner that the user no longer needs to know on which server the printer release is located. The user can simply have the active directory browsed.

Internet printing

Windows 2000 features the option to publish printers on the web and to enable their installation.

Hybrid environments

It is not possible to store drivers for Windows 2000 or XP clients on Windows NT servers. The drivers must be installed separately in environments of this kind.

Drivers for Windows NT clients can be stored on Windows 2000 servers. It may, however, happen that the transfer of the device-specific settings fails if manufacturer-specific drivers are used (must be used). The reason for this is the shifting of the printer drivers from kernel mode under NT to user mode under Windows 2000.

3.3.5.2   Windows 2003 server

With regard to the Windows 2003 version, no new features compared to Windows 2000 were known at the time this guide was written.

3.4   Authentication services

3.4.1   Overview

The detailed discussions in the following sections come to the conclusion that a secured authentication of user and computer objects is possible with both continuing migration and replacing migration and, in the final analysis, even in heterogenous environments thanks to the tools and means available. This is where Samba and OpenLDAP play a key role.

In a heterogenous system environment, Samba as an alternative to the Windows NT server offers similar functionalities for the Windows clients as an NT-based primary domain controller. Samba as a database for user accounts can use OpenLDAP as directory service. Samba in conjunction with OpenLDAP implements a Windows NT domain for the Windows clients. With regard to the administration of user, group and host information, a directory-based solution is implemented with all the resultant advantages. Such a solution avoids, for

example, the familiar scaling problem with Windows NT which often requires an infrastructure to be split up into different domains.

Samba enables the establishment of trust relationships between different domains, as well as the implementation of a WINS service. Although Samba 3.0 also offers a program for WINS replication, this program is at present not yet considered to be sufficiently tested. Samba supports the concept of PDC and BDCs for compatibility reasons. This support, however, is limited to the fact that Samba servers present themselves to Windows clients as PDC or BDC, depending on the given configuration. Samba itself does not support replication of the SAM database between PDC and BDC. Replication of the SAM can, however, be carried out by OpenLDAP.

In the case of continuing migration, minor restrictions must be observed with regard to authentication in heterogenous system environments. These restrictions concern the interaction between Samba/OpenLDAP and the active directory as well as between Samba/OpenLDAP and the Kerberos authentication.

Note in this context that no Kerberos authentication of Windows 2000/XP clients is possible in relation to Samba/OpenLDAP. The NTLM protocol must be used in cases like this. This will not pose any problems as long as Microsoft continues supporting this, for example, in order to enable the continued integration of Windows NT clients too. On the other hand, a Linux-based Kerberos server with an active directory domain can be used, so that a uniform credential management for Windows and Linux can be implemented based on Linux.

In a purely Linux-based system environment, authentication of the users is possible using Kerberos, with authentication by OpenLDAP also being a viable alternative.

3.4.2   The starting situation – Windows NT 4

This subsection deals with the logon and/or authentication services of the Microsoft products. Aspects discussed include the following:

> User databases
>
> Integration of computers and network services
>
> Authentication

For this purpose, we will begin with a discussion of the technical fundamentals of a Windows NT environment with a view to logon services.

3.4.2.1   *Domain*

The structure unit "domain" is the core technology of the logon services under Windows NT. The domain is an administrative unit which combines the computer and user accounts via a shared database in a common security context. This database is called SAM (Security Accounts Manager). During runtime, it is kept in the registry of special server systems called the domain controllers. Besides user and computer objects, groups are also administered in the SAM. Each of these three object types can be unambiguously identified by a so-called SID (security

identifier) which should not occur more than once, not even in different domains. A SAM account name which can normally consist of a maximum of 15 alphanumeric characters (with certain special characters being permitted) exists for every SID (being a relatively long number string). The SAM account name is the name which users use for identification.

Computers based on

> Windows NT
>
> Windows 2000
>
> Windows XP

can be members of a domain. In contrast to this, it is not possible to create a computer account in a domain for systems like Windows 3.11 or 9x, for example. When a computer becomes a member of a domain, groups of the domain (global groups) become members of the computer's local groups in the SAM of the computer. In this way, the "domain user" group becomes a member of the local "user" group. In this way, it is possible, for example, for users who can log on on an NT computer against a domain to get local access to the resources of the computer used.

A domain requires at least one domain controller, the so-called PDC (Primary Domain Controller). The PDC keeps the SAM of the domain, and the contents of the SAM can only be changed there. So-called BDCs (Backup Domain Controllers) are used for reasons of load balancing and redundancy. The BDCs keep a copy of the SAM which is regularly updated by the changes in the PDC.

The advantage of the "domain" as an administration unit is obvious: All that is needed to enable users to access local resources or resources on systems in the network is to create one user account in the SAM of the domain rather than on every system. Protection of resources, i.e. authorization, is carried out separately on the systems which make the resources available. Windows 9x users can also log on at a domain and thus use resources in the network without the need for any further logon operations.

3.4.2.2   *Multiple domains and trust relationships*

Multiple domains can be connected to each other via trust relationships. In this way, users or groups of other domains can be authorized to access resources (such as file services) of one's own domain. The primary purpose is to thus enable access to resources across domain boundaries.

A trust relationship between NT domains is not necessarily bidirectional: if domain A trusts domain B, this does not mean that B also trusts A. Furthermore, trust relationships are not transitive either: if A trusts B and if B trust domain C, A does not implicitly trust C. This means that every trust relationship must be explicitly created.

The following circumstances have led to the establishment of multiple domains in IT environments:

In many cases, parallel insular solutions developed within an infrastructure which had to be merged at a later stage using trust relationships because of shared work processes. This is also applicable if two infrastructures are merged.

The domain boundaries are the boundaries of security. Administrators of domain A are not necessarily administrators of domain B where one is trusted and which trusts in one. Political considerations play a role in this area.

The unfavorable option of delegating tasks was compensated for by multiple domains.

The number of objects (computers, users, groups) in the SAM is limited because during runtime the SAM is kept in the registry of the domain controllers, the size of which is also limited. The only remedy was to distribute the objects to multiple domains.

The single-master principle of the PDC restricts the scaling of a domain in strongly distributed, decentralized environments because all changes in the SAM can be implemented in the PDC only.

These circumstances have led to different domain models some of which were even proposed by Microsoft itself:

Single domain

Master domain (several domains all trust one master domain, with resource domains typically trusting the account domain)

Multiple master domain (multiple resource domains all trust (several) account domains

Complete trust domain (all the domains trust each other)

3.4.2.3   *NT as a directory service*

In the broadest sense, Windows NT domains are also directory services because user objects are contained in a domain. Microsoft calls this the NTDS (Windows NT Directory Service).

The number of attributes of a user object in an NT domain is relatively small, and is more or less limited to technically relevant attributes and properties. The attributes are thus not comparable to the directory service based on X.500.

The user properties include, for example:

User name (SAM account name)

Complete name and description (technically irrelevant)

Account information (such as account deactivated, password will never expire, expiration of the account, account type)

Group memberships

Environment parameters (logon script, home directory, path of the server-based profile)

Valid logon times, valid client computers

RAS (Remote Access Service)/ dialup parameters: permitted, with/without callback

Furthermore, attributes are stored which are managed by the operating system, such as:

SID

LastLoginTime

etc.

There is no possibility foreseen for amending this list by user-defined attributes. With the introduction of "Windows NT 4 Server Terminal Edition" and Citrix Metaframe, Microsoft itself has implemented additional properties for the user object (additional home and profile paths and further Citrix parameters).

A hierarchical structure of the NTDS is not possible, assignment of privileges at attribute level is not possible. The flexibility to assign privileges to user objects is strongly limited.

3.4.2.4   Delegation

The possibility to delegate administrative tasks within an NT domain is limited:

to the use of built-in groups (domain administrators, account, server, backup, print and reproduction operators); this variant is, however, very inflexible

to the installation of additional domains.

These restrictions and shortcomings were probably the reason why delegation and existing role concepts were implemented as web-based applications.

3.4.2.5   Network basis

A Windows NT domain can be based on the following transport protocols:

TCP/ IP

NetBEUI

SPX/ IPX

The NetBIOS interface is necessary in each of these cases.

In the TCP/ IP networks which are considered as the standard in this migration guide, the resolution of NetBIOS names (computer names and user names as well as further name types, such as work group) is mandatory as a precondition for faultless communication. A user wishing to change his domain code word, for example, must identify the PDC and/or know its IP address.

The resolution of NetBIOS names is possible in different ways in Windows networks:

By broadcast

By querying a WINS server (Windows Internet Name Service)

Or by evaluating the LMHOSTS file

The most elegant solution to this problem is probably the use of WINS servers. WINS servers are the only means that enable name resolution across the borders of IP sub-networks, dynamic contents and minimizing of broadcasts. The WINS service is often implemented on the domain controllers.

The browser service is implemented in Windows networks irrespective of the selected transport protocol. All Windows operating systems can theoretically be home to the browser service. The browser service enables the sending of a list of all the active computers in the network to a requesting client (using the "new view" command, for example). If this list is to be valid even across the borders of IP sub-networks, the browser service must have access to the information of the "domain master browser" in the local network. This is made possible through the use of WINS.

3.4.2.6   File replication

The domain controllers (PDC and BDCs) provide logon scripts and system guidelines under their NETLOGON release which are queried by the user logging on.

The contents of this release should be identical on all the domain controllers of a domain in order to ensure that the user always gets the same adaptations of his environment.

For this purpose, the servers must exchange the contents between each other. The so-called directory replication service (LMRepl) ensures that the contents of the so-called export server are replicated to the import servers. Changes in contents are permitted on the export server only.

3.4.2.7   Administration tools

Windows NT 4 comes with graphic on-board tools, such as the user manager and the server manager, for the administration of user objects, groups and computers.

Furthermore, the "NT Resource Kit" includes tools which can be executed primarily on the command line and which can be used to create scripts for automatic administration.

Furthermore, administration of a domain is also possible via the web interface. This requires the use of Microsoft's Internet Information Server (IIS).

A certain lack of user-friendliness of the on-board tools motivated third-party manufacturers to design further tools. These tools chiefly use the APIs of Windows NT.

Microsoft itself added the Microsoft Management Console (MMC) which was finally integrated into Windows 2000.

As another ex-post feature, Microsoft introduced ADSI (Active Directory Service Interface) as a COM-based interface which also administers Windows NT domains.

3.4.2.8   Saving passwords

The passwords of the users (and of the computers) are saved in a domain in the SAM of the domain controllers. The password is stored in a hash value rather than as plain text. Furthermore, Windows NT enables additional encryption of the SAM itself (SYSKEY.EXE). The hash values of the passwords are generated by different methods which have been further developed:

LM (LAN manager)

NTLM

NTLMv2

On NT systems other than domain controllers, the logon information of the users who logged on last are temporarily stored in order to enable logon even if no domain controller can be reached (typically: notebooks). This information too is stored in a hash value.

3.4.2.9   Authentication mechanism

Authentication within an NT domain landscape is based on the NTLM mechanism.

Consider the following scenario. A resource domain trusts an account domain. A functioning WINS environment is in place. A user starts a Windows NT workstation which is a member of the resource domains, and logs on at the account domain. The picture below (Fig. 8: Logon scenario) illustrates this scenario.
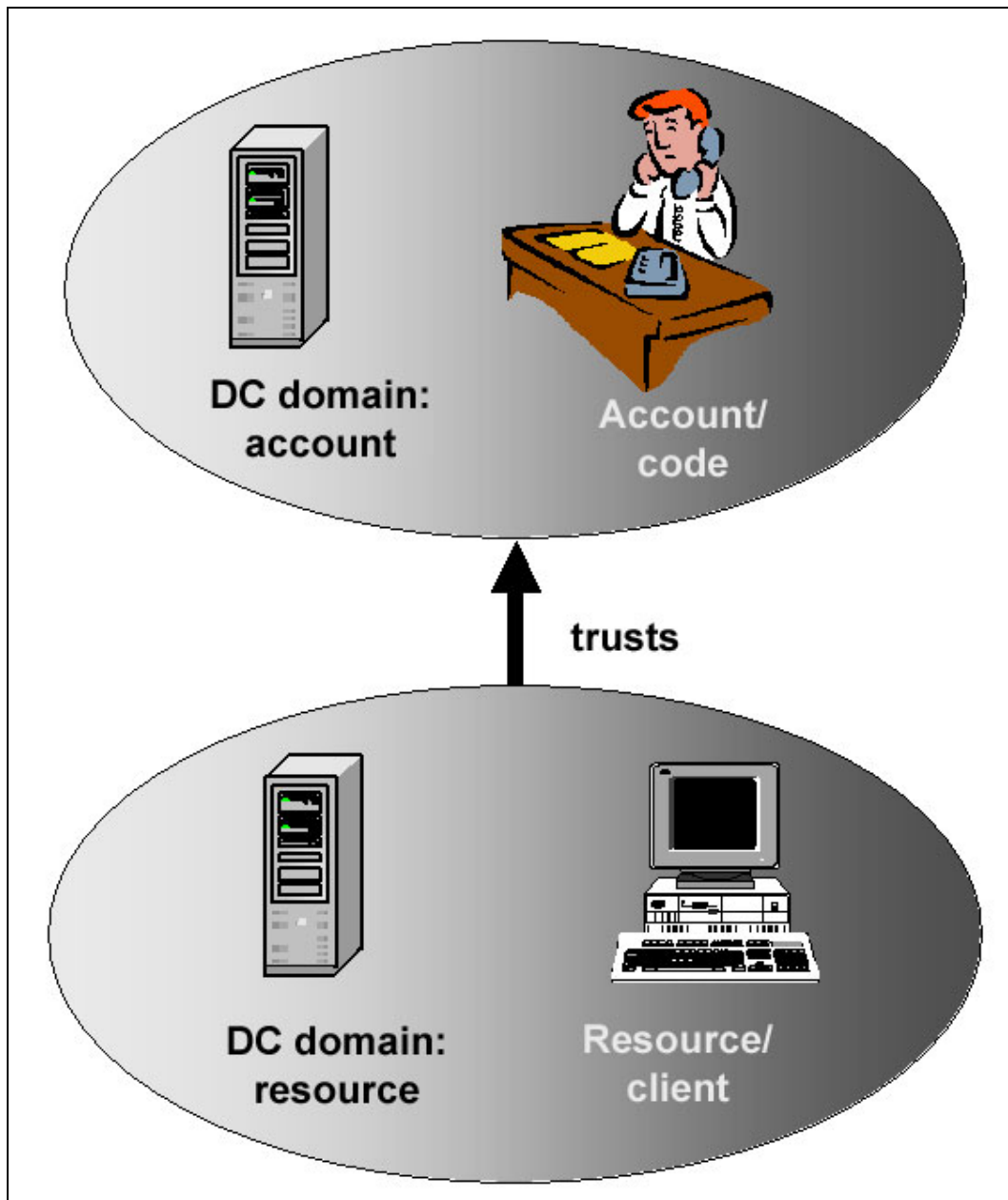
Fig. 8: Logon scenario

When the Windows NT machine is started, it requests via WINS a list of the domain controllers (DCs) of the resource domain. At first, a netlogon request is sent by broadcasting. If this is not answered by a DC of the resource domains, the netlogon request is sent to the DCs of the requested list. The logon information is validated via a so-called "secure channel" with the DC which replies first.

Then, the NT machine requests a list of the trusted domains from the DC of the resource domains.

After the user has selected the account domain from the logon mask and entered his code and password, the logon process of the user account takes place. The

NT client sends the logon information for the so-called "pass-through validation" process to the DC of the resource domain with which the machine has a secure channel. The DC of the resource domain sends this request to a DC of the account domain (at first locally, and after this, in directional mode via the secure channel). The logon information, once validated, is returned via the DC of the resource domain to the NT client. The NT client then opens a direct connection to the DC of the account domain in order to load the logon script, system guidelines or the user profile there.

The following logon process must be considered in addition: when the user connects to resources (such as file storage media released by a file server, e.g. net use), the file server must check the logon information by contacting the domain controllers once again.

3.4.2.10 Single sign on

The domain concept of Windows NT enables a quasi single sign-on procedure within the Microsoft family. The user signs on once at his Windows NT workstation and, on condition that the resources and/or server systems are members of his own or a trusting domain, can then access services, such as:

- File and print services
- Exchange
- SQL
- Intranet (Web, Internet Information Server)

Third-party manufacturers of software can implement their products in such a manner that the single sign-on remains in effect. They must, however, normally provide their applications on Windows NT 4 servers which are members of a domain.

3.4.2.11 Directives

Directives can be issued in Windows NT domains concerning

the handling of passwords (term of validity, minimum length, repeated entry of incorrect passwords)

the privileges (user rights) to be granted to users or groups (changing system time, local logon, etc.).

3.4.2.12 Auditing

An audit function for accesses made and/or attempted can be activated in Windows NT domains. This enables, for example, auditing of

logon and logoff operations

the user of user privileges

the user and group administration

changes in security guidelines.

3.4.2.13 Smart Card (powerful authentication mechanisms)

The so-called "Smart Card Base Components" were launched for Windows NT 4 and Windows 9x, enabling the development by third-party manufacturers of Windows applications with Smart Card functionality.

Solutions for strict authentication are offered by third-party manufacturers.

3.4.3 Replacing migration – Linux, Samba and OpenLDAP

A discourse on replacing migration must, above all, consider the requirements for an authentication service in a heterogenous system environment with Linux and Windows systems. It is obvious that the use of a directory service – also with a view to the active directory with Windows 2000 and higher – stands in the foreground in this context. Furthermore, the combination of Linux, Samba and OpenLDAP discussed in the following was found to be a tried-and-tested authentication solution long before the active directory. This means that it is difficult to clearly differentiate between the use of the directory service as an integration service on the one hand and as part of the authentication service on the other (Refer to chapter 3.7 for details).

3.4.3.1 Authentication with Linux / OpenLDAP and Samba

Samba can offer to Windows clients functions which are comparable with those of a Windows NT-based primary domain controller (i.e. including, but not limited to, file, print and authentication services). Samba as a database for user accounts can use OpenLDAP as a directory service. In this respect, the combination of Samba and OpenLDAP constitutes a kind of hybrid form of Windows NT domains and active directory. From the point of view of the Windows clients, it is a Windows NT domain. With regard to the administration of user, group and host information, it is, however, a fully directory-based solution with all the resultant advantages. A Samba/OpenLDAP-based solution avoids, in particular, the familiar scaling problem with Windows NT which often requires an infrastructure to be split up into different domains.

3.4.3.2 Password synchronization

If Linux / OpenLDAP are used as the directory service for Windows clients in conjunction with Samba, authentication of the Windows clients is carried out using the NTLM protocol. This is why the same encoded passwords must be stored in the directory which are stored in the SAM database under Windows NT/2000/2003. With this qualitative restriction (no Kerberos authentication for Windows 2000/ XP clients), it is thus possible to implement a full-scale authentication functionality for Windows clients on the basis of Linux, OpenLDAP and Samba.

In this context, a problem seems to exist at the first glance in that UNIX and Linux use another password encoding algorithm than Windows NT/ 2000. In the case of an OpenLDAP/Samba-based solution, UNIX and Windows passwords must

hence be saved parallel in the LDAP directory and synchronized with each other. From a technical point of view, this is, however, less of a problem because Samba can be configured in such a manner that it also changes the UNIX password when the password of the Windows client is changed. In the opposite direction, the PAM (Pluggable Authentication Module) mechanism can be used to configure UNIX programs in such a manner that they also change the Windows password when the UNIX password is changed. Given the appropriate configuration, password synchronization is thus not a problem.

Furthermore, authentication of UNIX-based services is possible, as with the active directory, via Kerberos. The two "MIT Kerberos" and "Heimdal" Kerberos implementations are two equivalent Kerberos implementations for Linux for this purpose. When Kerberos is used, the synchronization of passwords can also be ensured by the above-mentioned mechanisms. (A similar form of password synchronization must also be ensured internally by Actove Directory in order to enable both logon via Kerberos and of older clients via NTLM).

3.4.3.3   Trust relationships

Samba 3.0 supports the familiar trust relationships of Windows NT. These can be set up both between Windows and Samba domains and between two domains which are both based on Samba.

3.4.3.4   WINS service

Samba includes a built-in WINS service. With Samba 3.0, a program for WINS replication is also available. However, this program is at present not yet considered to be sufficiently tested.

3.4.3.5   Restrictions related to the use of OpenLDAP and Samba

As already mentioned, Samba corresponds – from the point of view of the Windows clients – to a Windows NT-based server. This means that the features for the administration of Windows clients which were newly introduced with the active directory are not available. Above all, Group Policy Objects (GPOs) and software distribution via the active directory are not supported. In practical applications, however, it is often completely adequate to replace these features with other techniques.

GPOs

Samba supports the so-called system policies which can be used to define registry settings for users, user groups and client computers. System policies also enable a large part of the settings available with GPOs (restrictions of the function of the Windows user interface, selection of executable programs, etc.). The "editreg" tool is integrated into Samba as a tool which enables dynamic editing of system policies.

Furthermore, local policies can be used in a Samba-based environment which can in principle be used to make the same settings as with GPOs. Since local policies can be easily saved in the file system, they can be easily synchronized from a prototype to a large number of clients.

Software distribution

The software distribution functions offered with the active directory are limited to software which is available in the form of MSI packages. A more comprehensive software distribution solution is chosen in most practical cases. Several commercial solutions are available in this context which work even without an active directory and which often even use Linux as operating system.

Samba supports server-based profiles. It is thus possible to set up mandatory profiles with which the configuration of user interface and applications can be prescribed to users.

Logon scripts can be used to determine further host, group and user-specific settings on Windows-based clients.

3.4.3.6   Combination of OpenLDAP and active directory

In cases in which the features of an active directory are indispensable, it is possible to replicate user and group data from OpenLDAP to the active directory. Thereafter, users and groups must be updated in the OpenLDAP directory only, but are also available in the active directory, so that the related properties (such as GPOs) can be used, with the single point of administration being retained. In this context, Windows can be configured in such a manner that a common (Linux-based) Kerberos server can be used for both parts of the environment. This is, however, subject to the restriction that it is then no longer possible for Windows 95/98/NT-based systems to authenticate themselves in relation to active directory / Kerberos. In the case of such a combination, authentication of these clients in relation to Samba / OpenLDAP is hence recommended.

3.4.3.7   Tools for migration of Windows NT to Samba / OpenLDAP

Certain tools which form part of Samba enable the export of the user database of an existing, Windows-based domain controller and the import of this into an OpenLDAP directory. This method enables a migration process that is fully transparent to users and client systems. It is then no longer necessary to re-enter the clients in the migrated domain, and users can continue using their logon names / password pairs used under NT.

During the migration process, all services other than the authentication service should at first be removed from the domain controllers and migrated on member servers. In the next step, the Windows NT-based domain controllers can then be migrated to Samba/ OpenLDAP. During a transitional period, the Windows-based member servers can then still be used in the domain which is now migrated to Samba/ OpenLDAP, and can be gradually migrated to Samba.

3.4.3.8   PDC and BDCs in a Samba domain

In the interest of compatibility with Windows NT domains, Samba also supports the concept of PDC and BDCs. This support is, however, limited to the fact that Samba servers present themselves to Windows clients as PDC or BDC, depending on the given configuration. Samba itself does not support replication of the SAM database between PDC and BDC. However, the replication can be

carried out by OpenLDAP in conjunction with the saving of the SAM in an LDAP directory. The Samba server which is configured as PDC then usually has write access to the OpenLDAP master server, so that it is authorized to implement changes in the user database. The BDCs are configured in such a manner that they have read access only to an OpenLDAP slave server which is typically executed on the same computer as the Samba BDC. When the SAM database is then changed via the PDC, the PDC writes this change into the LDAP directory. The change is then transferred from there via LDAP replication to the BDCs, so that the changed database is then also available to the latter.

Furthermore, the contents of the netlogon shares (containing, for example, policies and logon scripts) are also synchronously kept in a Windows NT domain. Under Linux, this can be achieved with the rsync program, for example.

3.4.3.9   *Samba as a member of an active directory domain*

Furthermore, Samba is able to use Kerberos tickets of an active directory server for authentication. This means that Samba can be used as a full-scale member server in AD domains.

3.4.3.10   *Administration tools*

User and group administration in a Samba/OpenLDAP-based domain can be carried out using the administration tools of Windows NT (usrmgr.exe). However, the special advantages of the directory service-based solution (such as different privilege levels, nested directory structure) cannot be used in this case because these features are not supported by Windows NT. Concerning the administration tools for OpenLDAP, please refer to chapter 3.7.4.7.

3.4.4   Continuing migration

3.4.4.1   *Windows 2000*

With regard to the logon services, it is not correct to say that Windows 2000 is merely an "update" of the operating system. It is not just the updating and installation process which is a comprehensive and complex procedure, the fundamental change in architecture towards the "active directory service" is another far-reaching novelty.

At this point of the guide, we will not describe the logon service of Windows 2000 as a subject isolated from the active directory and hence from the subject of the directory service. The same problems exist here with regard to a clear distinction from the active directory as an infrastructure on the one hand and as part of the authentication service on the other. Please also refer to chapter 3.7.5 which also discusses the Windows Server 2003 successor product.

3.5   Network services

3.5.1   Overview

The result of the discussion on technical details in the following suggests that migration is possible without any problems. No restrictions are to be expected in

migrated heterogenous or homogenous system landscapes (fully replacing migration or continuing migration).

3.5.2 The starting situation – network services under Windows NT

This subsection deals with the following network services:

WINS

DNS

DHCP

Client and server systems are differentiated when necessary.

In a broader sense, the following services

RAS (Remote Access Service) and Routing

Web Proxy

SNA Gateway

can also be regarded as network services. Microsoft offers separate server products or additional products (such as SNA Server 4.0 or Proxy Server 2.0). These products are not discussed in this subsection.

Instead, we will only briefly discuss new features of the above-mentioned network services related to the introduction of Windows 2000.

3.5.2.1 Windows Internet Name Service (WINS)

Microsoft Windows Internet Name Service (WINS) can be installed on the Windows NT 4 Server operating systems.

WINS is an RFC-conforming service which enables the resolution of NetBIOS names to an IP address, and at the same time also constitutes a server service that eliminates the need for the NetBIOS name resolution by

broadcast

locally saved LMHOSTS file.

WINS thus enables the resolution of NetBIOS names beyond IP subnetworks.

WINS can be used both dynamically and statically. Dynamically means that the WINS clients themselves can enter themselves dynamically. Statically means that the administrators enter the names and their IP addresses manually.

WINS saves its data in a database (Jet-Engine, wins.mdb), the contents of which can be reconciled by several WINS servers with each other. For this purpose, the WINS servers are configured as so-called "push" and/or "pull" partners. The contents are written according to the multi-master principle. This means that every WINS server can make entries.

Furthermore, the use of a WINS proxy is also possible. A computer that represents a WINS proxy does not keep a database of its own. Instead, it receives requests from clients and passes these on to a full-scale WINS server.

Technical description of the migration paths

All the Windows operating systems so far launched (Windows 9x to Windows XP and all server operating systems) can represent a WINS client. The WINS client itself can be configured on the basis of its so-called node type in order to determine whether and, if so, how it has to resolve NetBIOS names.

The NetBIOS namespace is a shallow namespace and, rather than being restricted to computer names, also covers user names, services, names of Windows domains or Windows work groups, etc.

The overview in the table below shows the NetBIOS name types which can be identified by the 16th byte of the NetBIOS name.

Unique names and group names are discriminated. Group names can be used and thus entered by several computers at the same time.

The following table shows the unique identifications.

Table 11: Unique identifications of NetBIOS names

16th byte	is the unique identifier for:
<00>	*the NetBIOS name of the computer*
<03>	the message service both for the computer and for the logged-on user
<1B>	the domain master browser which is made available by the PDC of a domain
<06>	an RAS (Remote Access Service) on a computer
<1F>	a NetDDE service on a computer
<20>	the server service of a computer (particularly important in the case of folder releases)
<21>	a computer with an RAS client
<BE>	a network monitor agent
<BF>	a computer with the so-called "network monitor utility"

The table below shows the identifications which can be used by several computers.

Table 12: Multivalue identifications of NetBIOS names

16th byte	is the multivalue identifier for:
<1C>	a name of a domain
<1D>	the name of the master browsers
<1E>	a normal group name
<20>	a special group name (called the Internet group)
MSBROWSE,	instead of a single 16th byte, "_MSBROWSE_," can be appended to a domain name, so that the domain can be made known to another master browser

3.5.2.2 *Domain Name System (DNS)*

Domain Name System (DNS) is a service that can be installed on the Windows NT 4 Server operating systems. It supports the RFCs 1033, 1034, 1035, 1101,

1123, 1183 and 1536 and is compatible with the Berkeley Internet Name Domain (BIND) implementation.

DNS of Windows NT 4 Server supports BIND in version 4.9.4.

DNS is the Internet standard which enables, amongst other things, the resolution of computer names into an IP address and vice versa (reverse lookup) within a hierarchical namespace. The use of a DNS server eliminates the need to use locally saved entries in the HOSTS file.

The hierarchy of the namespace is reflected by the "." separator in the notation of the names. The so-called fully qualified domain name (FQDN) consists of two parts as follows: the first part before the first dot identifies the host name, the second part the DNS domain. Example: computer1.microsoft.com describes the computer with the name computer1 in the microsoft.com domain. It is not a mandatory requirement that the FQDN consist of three parts. Valid characters in the FQDN are the characters a to z, A to Z and the minus sign.

Since DNS is an Internet standard, free selection of the domain name is not possible. The domains must be registered with the relevant national or international administration bodies. If, however, the DNS namespace is visible within the own organization (enterprise) only, it is also possible to use non-registered names. Registered names and/or zones should be used which are not used on the Internet. This approach avoids that zones registered for other organizations and/or individuals are used.

DNS includes mechanisms that enable partitioning of the underlying database, i.e. to adapt it to distributed environments. The name resolution can be delegated for special domains on the one hand, and the replication (zone transfer) and administration can be controlled by creating zones on the other.

The implementation under Windows NT 4 is BIND 4.9.4-conforming in that DNS works as a purely static system (i.e. it does not support any dynamic entries) and in that changes can be made in the primary server of a zone only (single-master principle).

One special feature of the DNS implementation under Windows NT 4 is the possibility to exit the DNS service and additionally to use a WINS server for name resolution.

DNS supports not just the entries for computer names, but also further resource records. The following table shows an overview of the DNS resource record types supported in Windows NT.

Table 13: Overview of the DNS resource record types supported

Record type	Brief description
A	Address entry (the classic entry for a host to be resolved into an IP address)
AFSDB	Special entry for the Andrew File System (AFS)
CNAME	Alias (or canonical name)

Technical description of the migration paths

Record type	Brief description
HINFO	Special entry for hardware information according to RFC 1700
ISDN	Entry for ISDN (Integrated Services Digital Network) in conjunction with the RT (route through) type
MB, MG, MINFO, MR	Special entries for mailboxes, mail groups, mailbox information
MX	Entry for mailrouting via SMTP (Simple Message Transfer Protocol)
NS	Entry for a DNS server (name server) of a DNS domain
PTR	Reversed address entry (pointer resource record) resolving an IP address into a host name
RP	Entry for the responsible person of a special DNS domain
RT	The route through resource record specifies an intermediate host that routes packets to a destination host. The RT record is used in conjunction with the ISDN and X25 resource records. It is syntactically and semantically similar to the MX record type and is used in much the same way.
SOA	Entry for the primary DNS server (start of authority)
TXT	Entry for text information
WINS	Entry for the IP address for WINS server to be additionally used for forward resolution
WINS_R	Entry for reverse lookup via WINS server
WKS	Entry for well-known service
X.25	Entry for an X.121 address

All the Windows operating systems so far launched (Windows 9x to Windows XP and all server operating systems) can represent a DNS client. Systems with Windows 2000 or higher also support dynamic DNS (DDNS) as a client. Concerning DDNS, please refer to chapter 3.5.2.3.

3.5.2.3   Dynamic Host Configuration Protocol (DHCP)

DHCP (Dynamic Host Configuration Protocol) is the industry standard for the dynamic IP configuration of computers or other TCP/ IP network devices (such as network printers). DHCP is based on RFCs 1533, 1534, 1541 and 1542.

The implementation in Windows NT 4 server supports the options according to RFC 1541 which are shown in the table below. Options printed in boldface are used by DHCP clients up to Windows NT 4.

Table 14: DHCP options

No.	Option name	Explanation
0	Pad	
255	End	
1	**Subnet mask**	Subnet mask
2	Time offset	
3	**Router**	IP address of the standard router (gateway)
4	Time server	
5	Name servers	

No.	Option name	Explanation
6	**DNS servers**	IP addresses of the DNS servers
7	Log servers	
8	Cookie servers	
9	LPR servers	
10	Impress servers	
11	Resource Location servers	
12	Host name	
13	Boot file size	
14	Merit dump file	
15	**Domain name**	DNS suffix of the client
16	Swap server	
17	Root path	
18	Extensions path	
19	IP layer forwarding	
20	Nonlocal source routing	
21	Policy filter masks	
22	Max DG reassembly size	
23	Default time-to-live	
24	Path MTU aging timeout	
25	Path MTU plateau table	
26	MTU option	
27	All subnets are local	
28	Broadcast address	
29	Perform mask discovery	
30	Mask supplier	
31	Perform router discovery	
32	Router solicitation address	
33	Static route	
34	Trailer encapsulation	
35	ARP cache timeout	
36	Ethernet encapsulation	
37	Default time-to-live	
38	Keepalive interval	
39	Keepalive garbage	
40	NIS domain name	
41	NIS servers	
42	NTP servers	
43	Vendor-specific information	
44	**WINS/ NBNS servers**	IP addresses of the WINS servers
45	NetBIOS over TCP/ IP NBDD	
46	**WINS/ NBT node type**	Node type of the WINS client
47	NetBIOS scope ID	
48	X Window system font	
49	X Window system display	

Technical description of the migration paths

No.	Option name	Explanation
51	**Lease time**	Validity term of the assignment
58	**Renewal (T1) time value**	Renewal interval 1
59	**Rebinding (T2) time value**	Renewal interval
64	NIS + Domain Name	
65	NIS + Servers	
66	Boot Server Host Name	
67	Bootfile Name	
68	Mobile IP Home Agents	

Another possibility is the use of a DHCP relay agent. A computer that executes a DHCP relay agent service does not keep a database of its own. It receives requests from clients and passes these on to a full-scale DHCP server.

3.5.3   Replacing migration – network services under Linux

The infrastructure-forming services for TCP/ IP-based networks (DNS, DHCP, NTP, routing, VPN, filtering) can be implemented in Open Source software throughout. The comprehensive availability of these network services as OSS is due to the development history of the Internet. The outstanding feature of this world-wide data web is the fact that all the computers connected to it speak the same language. This language consists of a whole family of protocols that are summarized under the term TCP/ IP. One vital requirement is that the "language understanding" is universally the same in order to ensure smooth communication between the most varied systems world-wide. In order to achieve this conformity, most of the Internet protocol standards officially adopted by the Internet Engineering Task Force (IETF) are supported by open source reference implementations. On the basis of these references, all manufacturers can independently develop fully interoperable software. The Internet protocols are manufacturer-independent and constitute open standards both in terms of their definitions and in terms of their open source implementations. This special feature of the Internet protocols was a decisive reason why TCP/ IP prevailed over the proprietary network protocols existing in the market at the same time.

Even if interoperability requirements are fairly limited in local networks because of the limited number of systems involved, maintaining open standards is of essential importance. Especially in the case of manufacturer-specific modifications of and/or amendments to standards, there is always a risk of a "vendor lock-in". The links with this manufacturer are strengthened and may even lead to dependence on the one hand, whilst the power of definition with regard to the further development and interoperability of third-party systems passed to the manufacturer, at least as far as amendments are concerned, on the other.

Against this background, one should always check whether the improvements promised in conjunction with a manufacturer-specific amendment to a standard are also compatible with a long-term perspective. Although the tried-and-tested reference implementations which have existed for many years do not necessarily include each and every feature, they warrant sustained interoperability with all network-enabled systems.

3.5.3.1   *Domain Name System (DNS)*

The reference implementation of the standard for the domain name system which is defined in a entire series of RFC documents is BIND (Berkeley Internet Name Domain) which is upgraded and updated by the Internet Software Consortium in a manufacturer-independent manner. The latest version is currently 9.2.x. However, the 8.3.x version line still accounts for the greatest part of the installed basis of DNS servers and is still kept and maintained by the ISC. Versions 4.9.8 and older versions should not be used any longer.

Bind9 supports, amongst other things, dynamic DNS (DDNS), DNSSEC and Ipv6.

Connecting BIND 9 to external data sources for zone information is possible via a comprehensive BackEnd Database Interface on the one hand, but a simplified interface (SDB) is additionally available which can, for example, be used to implement read-only access to LDAP or SQL databases. However, these links are not included in the BIND software package. LDAP connection is, for example, possible both using SDB implementations as well as pre-defined object classes that permit the implementation of this connection.

ISC bind can be used also in conjunction with Windows NT / W2k. BIND 9, in particular, also supports dynamic updating of service records and can thus perform the corresponding services for W2K servers.

3.5.3.2   *Dynamic Host Configuration Protocol (DHCP)*

The reference implementation of the DHCP is also developed further and updated by the ISC. The protocol and software have the following functions and offer the following options:

Automatic assignment of IP addresses and computer names to clients. DHCP permits both the assignment of static IP addresses (on the basis of the MAC address) as well as the dynamic assignment of a free address from a defined address range.

Automatic transmission of information concerning the network infrastructure. DHCP can, for example, be used for the central administration and distribution to all the clients of the domain name and the name server, the default route and the network mask.

Furthermore, a large number of defined optional fields as well as freely definable information concerning the host configuration can be delivered via the dhcpd. The ISC dhcpd can, for example, also be used to transmit any options which can be used by Windows clients.

Furthermore, the dhcpd can also function as a bootpd and in this capacity send any information necessary for booting to a client via the network.

The ISC dhcpd enables both the administration of individual clients and collective configuration for classes and subnetworks with regard to any information to be

delivered. Furthermore, the conditional assignment of host configuration data by IF statements is possible in the configuration of the ISC dhcpd.

The dhcpd can be used in a failover configuration both for load balancing and for High Availability (HA). The dynamically administered IP areas are then coordinated between the servers which mutually replace each other.

The ISC dhcpd is configured in conventional UNIX style by an ASCII configuration file. A patch is available enabling the configuration of the ISC DHCP server to be dynamically imported from an LDAP repository. The implementation follows the IETF draft LDAP scheme for DHCP.

3.5.3.3   Windows Internet Name Service (WINS)

Following OSS migration, the name resolution for Windows services and computers is carried out by the nmbd of the Samba package. This means that the broadcast-based browser services commonly used with Windows can be rendered both as a client and as a local or domain-wide master browser on the one hand. On the other hand, however, the nmbd can also act as a WINS and in this capacity coordinate the browser across the boundaries of network segments which are normally connected by routers that do not permit any broadcasts to pass through.

3.5.3.4   Network Time Protocol (NTP)

Many network applications require a high degree of synchronization. The Network Time Protocol can be used to synchronize the clocks of the computers in the local networks with milliseconds' precision. Given a permanent Internet connection, the reference time can be synchronized with the official time with milliseconds' precision. Alternative standard time reference sources include, but are not limited to, DCF77 and GPS.

The reference implementation of the standard is further developed and maintained by the Network Time Protocol Project. The software can also be used under Windows NT.

3.5.4   Continuing migration – network services under Windows 2000

The following sections will briefly outline the new features of the above-mentioned network services which result from the introduction of Windows 2000.

3.5.4.1   WINS

With regard to **WINS**, Windows 2000 does not offer any new architectural features. Windows 2000 just comes with an improved management functionality for the WINS database.

3.5.4.2   DNS

The DNS service experienced the most far-reaching changes as a result of the launch of Windows 2000. The main reason for this being that the Windows 2000 active directory uses DNS for the primary name resolution and/or would not work without DNS. An active directory uses DNS for various purposes, including, but

not limited to, finding of the services with regard to logon and browsing (LDAP Service, Global Catalog Service and Kerberos KDC). As a precondition for entering services, the DNS must support so-called SRV Records according to RFC 2052. Since the previous DNS worked statically (entries had to be made manually), a dynamic registration function was implemented in Windows 2000, also with a view to the planned omission of WINS in the future. Computers can enter their A and SRV records dynamically. The implementation follows the RFC 2136 (Dynamic Update) in this context. Computers with Windows 2000 and higher can register themselves dynamically (implementation in the DHCP client). Windows NT and Windows 9x are unable to do this. They need the help of a Windows 2000 DHCP service. Dynamic registration implies a change in architecture of the previous DNS implementation where one DNS server (the primary one) can write the zone contents. Microsoft implements a multi-master principle by integrating DNS into the active directory. The DNS entries are thus objects of the database of the active directory and are replicated in this way. Dynamic registration without AD integration does not exist. Dynamic registration can be subjected to security mechanisms in order to ensure that no computers other than those which can authenticate themselves (such as Windows 2000 of the pertinent domain) can register themselves. Windows 2000 supports the so-called "Secure Update" according to GSS API according to RFC 2078; RFCs 2535 (Domain Name System Security Extensions) or 2137 (Secure Domain Name System Dynamic Update) are not implemented.

3.5.4.3   DHCP

With regard to DHCP, Windows 2000 offers some new features worth mentioning. Under Windows 2000, the current RFCs 2131 (Dynamic Host Configuration Protocol, previously RFC 1541) and 2132 (DHCP Options and BOOTP Vendor Extensions) are supported. Besides improved management, Multicast Scopes, user-specific and manufacturer-specific DHCP options as well as dynamic BOOTP are now supported.

Another new feature is the integration of DHCP and DNS within a Windows 2000 network. Clients with Windows NT 4 or older do not support dynamic registration of their DNS names within the dynamic DNS of Windows 2000. If these clients obtain their IP configuration from a Windows 2000 DHCP server, the DHCP server can carry out the registration in the DNS.

The DHCP client of Windows 2000 can create its IP configuration itself if there is no DHCP server in its subnetwork. The IP addresses of class B network 169.254.0.0 with the 255.255.0.0 subnet mask are used for this purpose.

3.6   System audit and management services

3.6.1   Overview

It should be noted in advance that, due to the fact that only a limited range of system management tools is available under Windows NT and that the functionality of these tools is quite limited, comprehensive tools from third-party

manufacturers are often used, some of which are also available for Linux systems.

Apart from many on-board tools, such as cron/at, Linux includes further COLS products as well as OSS solutions for system administration. Nagios, for example, is a tool for visualization and service auditing. A complex and highly integrated system suitable for all system management tasks is not yet available as an OSS solution.

Microsoft also enhanced its toolkit with the continuation of its product line. Tools worth mentioning in this context are the Microsoft Operations Manager and the Application Center.

3.6.2 The starting situation – Systems Management Server under Windows NT 4

The Systems Management Server (SMS) was launched more or less at the same time Windows NT 4 was launched. SMS version 1.2 can be regarded as the last version of this generation. Version 2.0 came out in 1999. The functionality of this version is described in the following.

SMS integrates several basic functionalities which other manufacturers also cover by an integrated product in a comparable manner. These functionalities are:

Inventory

Remote control

Software distribution

Windows NT Server 4.0, Service Pack 4 or higher, and Microsoft SQL Server 6.5, Service Pack 4 or higher, are required to use the server software.

SMS 2.0 can be used in large environments with more than 100,000 clients. Since it can be embedded into the Windows domain structure, granular security levels are available. SMS also supports Novell Netware NDS and Bindery environments.

SMS 2.0 includes an electronic **software distribution** which installs and deinstalls software in a largely automatic manner, ideally without any work having to be performed locally and without any errors occurring at the user end. Software distribution can be carried out in a rule-based manner. The administrators determine the software configuration by adding and/or removing computers, users or user groups from lists on the basis of defined criteria. SMS logs the status of software installations and operating system updates without the system administrators being informed whether the software was installed correctly. SMS installs software without being supervised and without user intervention. Installation with administrator rights is possible even if a user with less far-reaching privileges is logged in at the computer. NT-based computers do not need to be logged on, so that this feature is suitable for distribution at times other than regular business or working hours. SMS enables time-controlled

software distribution to any combination of users, user groups, TCP/IP network segments and computers. SMS 2.0 determines distribution targets dynamically on the basis of rules for group guidelines and can apply these rules to all sites. When new users join a user group, the correct software can be automatically sent to these new users on the basis of the guideline. The so-called **structured packet distribution** function considers the network topology in order to ensure the efficient distribution of software via slow connections. Site servers then serve as routers that distribute the software in an intelligent and structured manner. This approach ensures that a distribution uses a WAN connection only once. SMS 2.0 can distribute software using **Courier Sender** on CD-ROM or other media. When the medium (the CD-ROM, for example) arrives at the user and is inserted into the user's system, the automated process starts. An installation program is supplied which permits compiling of software packages. It enables system administrators to modify installation packages and to write scripts in order to compile packages for Windows-based applications. **SMS Installer** includes an installation log function in addition to wrapper technologies for software distribution. The installer uses snapshot technology.

SMS 2.0 can prepare **inventories** of hardware and software. In a **CIM-based hardware stock-taking process**, SMS 2.0 collects data in CIM (Common Information Model) format which gives SMS access to many different sources, including Microsoft Win32, SNMP and DMI. SMS collects comprehensive inventory data which can be filtered using options. The **software stock-taking process** collects exact information concerning every single application on every computer. SMS 2.0 searches for version-related resource information in every executable file on a client computer rather than in a predefined database. The inventory data can be used as a database for rule-based software distribution.

The remote control feature enables remote execution of applications, communication with end users via chat windows and the restarting of computers. Furthermore, the screen, keyboard and mouse can be remote-controlled.

SMS 2.0 comes with the following **network management** functionalities: SMS can be used to display and visualize the network topology, clients and operating systems used. SMS prepares an overview map of network servers and devices in order to support system administrators in their network management and trouble-shooting tasks. Monitoring of data communications enables the discovery of network problems, such as protocols that are not needed, IP addresses that were assigned twice, as well as unauthorized attempts to access the Internet. The **network monitor** can interpret results automatically.

SMS 2.0 offers tools for analyzing, monitoring and controlling applications on servers and workstations (**software measurement**). The use of programs can be sorted and monitored in terms of users, groups, workstations, time or license quotas. Furthermore, the use of certain applications can be controlled, contingent quotas can be defined, or unauthorized applications can be determined. This feature also enables monitoring whether the rules are adhered to on any client or server. The software measuring programs also detect different program versions

and can find out whether client agents were deactivated, so that comprehensive protection against manipulation is possible. Software use statistics can be used to plan software license requirements and to measure charges and fees of individual departments as a function of the use of applications (**license management**).

Server monitoring is carried out by HealthMon. HealthMon determines performance data for processes in Windows NT Server and Microsoft BackOffice Server. Critical threshold values or threshold values for alert messages can be determined in the HealthMon console in order to receive exception-based status information in realtime. This information can be grouped according to resources at system level or according to Microsoft server applications and processes.

3.6.3 Replacing migration – Linux

System management for OSS operating systems is based on the basic functionality of the multi-user network operating system. An administrator at his remote terminal can work on any Linux/BSD computer (no matter whether client or server) in exactly the same manner as on a local computer. The graphic user interface is also perfectly suitable for the remote control of computers thanks to the systematic separation of server (with display, keyboard and mouse) and client software which displays its windows and icons/characters and which receives inputs from the server via a network connection, either locally or from afar. Further features include the Secure Shell (ssh) and a well-equipped toolkit with cron/at for time control and powerful command line interpreters, utilities and interpretable programming languages for the far-reaching automation of routine tasks. No further software support is required for the remote control of OSS systems.

The OSS systems also offer additional components for centralized system management in heterogenous networks. At the upper end of the scale, Linux can be integrated into the system management with Tivoli or OpenView. A variety of options exist for automating or supporting specific system management tasks between these solutions which themselves do not form part of the OSS and simple management functions using the operating system tools.

3.6.3.1 *Software management*

Various suppliers offer commercial solutions for stock-taking (inventories), distributing and updating as well as configuration management for software components. Some of these solutions are also suitable for heterogenous systems with a Windows component. An integrated solution ready for production does not exist as Open Source software, especially not for heterogenous environments. However, software package management tools (RPM and APT) enable easy centralization of stock-taking (inventories) and distribution and/or updating of software. Especially the Debian packet management functionality is perfectly suited for central software management because it can work with a hierarchy of central software repositories and because it features a very robust update behavior.

In the security area, Tripwire is the tool of choice for software stock-taking (inventories) and monitoring.

3.6.3.2   Network management

A wide range of programs with different focal points exists for the management of TCP/IP networks.

The "Nagios" monitoring tool is specialized in the visualization of network topology and in the monitoring of services even on servers with other operating systems. Nagios responds to errors or events in a rule-based manner, for example, on the basis of definable threshold values. Escalation of messages and integration of different message channels (such as mail or SMS) are possible in this context.

Nagios uses plug-ins for the active and passive monitoring of the most varied services and system parameters. It is, for example, possible to monitor typical network services, such as Web, mail and LDAP, as well as different RDBMs or Samba. Other plug-ins enable the monitoring of system parameters, such as CPU workload, harddisk space, as well as hardware sensor data (temperature, power supply and fan speed). Bridges exist to other systems, such as MRTG/ RRD, and for the use of SNMP for monitoring. Simple interfaces and templates enable the quick development of user-defined plug-ins.

MRTG/ RRD specializes in the monitoring and analysis of network traffic. MRTG uses the Simple Network Management Protocol in order to collect and store traffic data from the most varied network components. Evaluation and graphic rendering can then be carried out either internally by MRTG or externally by RRD. More than 350 templates are available for MRTG in order to directly connect the most varied SNMP-enabled network components and services.

NeTraMet which also uses SNMP is another tool for traffic analysis and visualization.

Scotty is another tool for visualizing and managing local networks. Scotty also works with SNMP and also enables the editing of SNMP-accessible parameters on remote network components.

Snort specializes in the search for strange patterns in the network traffic in order to detect intrusion attempts or other cases of unauthorized use. As a "Lightweight Intrusion Detection System", Snort is a valuable component for system management in the network.

3.6.3.3   Server management

Linux includes, for example, Ulimits, Quotas and Process Accounting for server management purposes. These functions are used to monitor and restrict the system resources of individual users or processes. The "Nagios" tool introduced in the foregoing in conjunction with network management is used to monitor services and local system parameters.

Technical description of the migration paths

The OSS server services uses a common API for logging messages via the syslogd. This logging service enables hierarchically organized central monitoring of the entire Linux/ BSD/ UNIX infrastructure. Windows servers can also be integrated into a central Syslog system. A host of tools and concepts are available for the automated evaluation of log files, both on an application specific basis and as generic tools. A good overview can be found at http://www.counterpane.com/log-analysis.html

System tools, such as strace, lsof, fuser and netstat, offer good analytical functions for fault-finding and error analysis operations in addition to the regular protocol services. These functions are occasionally necessary for server management

3.6.3.4   Systems of higher complexity

In the field of system management, there is not just the Simple Network Management Protocol, but also the Common Information Model (CIM) with the Web Based Enterprise Management (WBEM) based on this for more far-reaching approaches towards standardized system management in heterogenous networks. CIM/ WBEM, like SNMP, are described in open standards, and are available in reference implementations as Open Source software. However, these components are currently used mainly within the scope of commercial products. The suitability of pure Open Source solutions has yet to be proven in this area.

3.6.3.5   Conclusions

With regard to system management, the OSS operating systems follow the UNIX path, in line with their origin. The OSS systems as multi-user and network systems come with a wide range of functions for central system management and, in some areas, are the model rather than the substituting alternative to a Windows solution. Migration also means conceptual changes for administrators and process organization which enable significant progress, especially with regard to security. The high degree of security and reliability generally associated with Linux systems is not least the result of system management.

A migration project means far-reaching change for those in charge of this system management. Both the analytical features as well as the options for adjusting and correcting the OSS systems give system managers much more freedom than can be found in a closed Windows system. This freedom can be used to emancipate oneself from manufacturers and external service providers whilst at the same time boosting the qualification of one's own staff. The transparency of the open OSS systems contributes towards a fundamental and far-reaching understanding of function and dependencies of the different components in a state-of-the-art IT infrastructure.

3.6.4 Continuing migration – Windows 2000

3.6.4.1 Microsoft Operations Manager

Microsoft Operations Manager (MOM) is based on a development by the company NetIQ and supports the administration of Windows 2000-based server systems with a view to event and performance monitoring and administration.

Microsoft Operations Manager is currently available as version MOM 2000 and includes the following functionalities:

MOM collects a variety of system and application events from Windows-based systems which occur in a distributed IT environment and compiles these events in a central event repository. The result is distributed **event management**. Administrators can use the events collected as a general overview of the availability of servers and services. Rules can be defined within MOM. The rules developed in this way can be used to make the system respond automatically to incoming message data streams. This is carried out in response either to a predefined process which is based on a particular error scenario or to a specific event. These rules enable MOM to respond to certain event patterns and to trigger events and/or alert messages for the administrator. Every MOM rule can be configured in such a manner that it generates specific **warning messages** with distinct security levels assigned to each of these messages. A warning can be generated in response to a single event or to multiple events taking place in several sources. An administrator can trace the development of warnings and the corresponding events at all times. Furthermore, warnings can trigger e-mail messages as well as pages and SNMP (Simple Network Management Protocol) traps. MOM enables the introduction of **performance monitoring** for the systems connected. Performance thresholds can be defined and monitored for this purpose. The development of system and application performance can be monitored by adapting or adding rules for future reference purposes or for capacity planning purposes. Furthermore, local and aggregated threshold values can be determined which lead to changes in reaction in the system or application performance and thereby trigger warning messages and events which require administrator intervention.

The portfolio of services to be managed can be expanded by **Management Packs**. Management Packs contain pre-configured MOM rules. Each pack provides rules for certain applications or services. MOM includes by default a Management Pack which can be used to manage all relevant Windows services, including the active directory service and Internet Information Services (IIS). Further Management Packs are offered by Microsoft and third-party manufacturers. Microsoft offers Management Packs for the following products:

Exchange 2000 and 5.5

SQL 2000 and 7.0

Commerce Server 2000

Internet Acceleration and Security Server 2000

Host Integration Server 2000

Application Center 2000

Site Server 3.0

Proxy 2.0

SNA 4.0.

MOM enables the data gathered to be processed and presented in the form of reports. A graphic reporting tool enables access to pre-configured reports and diagrams. The reports generated enable administrators to check the status of systems and services in the network. Management Packs from Microsoft or third-party suppliers enable further reports to be added to the system. MOM can, in particular, generate HTML-based (Hypertext Markup Language) snapshots of all reports developed. The snapshots can then be exported to a web server and thus accessed by web browsers.

Windows 2000 Server is required for installation. Although MS SQL 2000 is recommended as the database platform, MS Access is also possible.

3.6.4.2   *Application Center*

Microsoft Application Center 2000 is a deployment and management tool for web applications with high availability which were created on the Microsoft Windows 2000 operating system. Application Center 2000 simplifies the administration of server groups.

3.7   Directory service

3.7.1   Overview

Since a directory service is not an integral part of Windows NT with a view to the starting situation, the following discussions do not deal with the replacement or continuation of an existing directory service. However, the directory service plays an important role both in conjunction with replacing and in conjunction with continuing migration. Migration to Windows 2000 and especially migration to Exchange 2000 almost inevitably mean the introduction of the active directory. In the case of replacing migration, the use of a directory service and in this case with OpenLDAP as an OSS solution, offers many advantages, especially with a view to the implementation of user-friendly authentication services.

This means that the following technical discussions are inclined to look towards the future, addressing the special features related to the introduction of the respective directory service and/or its possible applications. A special aspect in this context is the integrative effect of the active directory (AD) and how this can be counteracted.

One can summarize that the AD should only be implemented in a minimum configuration unless it can be omitted completely. Other products and solutions, such as a metadirectory, should be adopted in the case of more demanding requirements.

Furthermore, one should carefully choose the right time for transferring the active directory to native mode in order to maintain possible options.

3.7.2 Fundamentals

A directory service can be used to make information of all kinds available throughout the entire network. A directory service typically consists of a database where this information is stored and a network protocol by means of which the information can be retrieved or edited. The most commonly used directory protocol is at present the Lightweight Directory Access Protocol (LDAP). LDAP was initially developed as a simple way of accessing X.500-based directory services. Today, an LDAP server is typically understood as the combination of database and protocol implementation. LDAP version 3 is defined in the RFC 2251.

A typical feature of a directory service is the hierarchical structure of the information contained there, similar to a file system. Starting at a root point, information is contained in objects, with every object having a number of attributes where the values represent the real information. Every object can have sub-objects (with attributes) which, for their part, can have further sub-objects.

Objects in a directory service are units which can be discriminated from other objects, such as individuals, groups, computers, printers or the conference rooms in a building. The object classes of the object define which attributes an object can have and which attributes an object must have. An object class occurring in many directors has, for example, the name *person* and stipulates that objects of this class must, as a minimum, have the attributes *surname* and *commonName*. It additionally permits optional attributes, such as *telephoneNumber* and *description*. Object classes and attributes are defined in the so-called scheme of the directory.

The possibility to assign multiple object classes to objects (even retroactively) leads to a high degree of flexibility and enables the storing of coherent information in the same place (i.e. in the same object). A person can have several properties which form a coherent context and which must be defined by different object classes (with different and overlapping attributes). A person can, for example, be treated as a user of computer systems, as a telephone directory entry, as an address-book entry or as another person's partner. If these properties were stored in a directory, object classes with attributes would be defined for the "user", "telephone directory entry", "address-book entry" and "partner" property classes. In order to ensure the meaningful use of any of these object classes even without the other object classes, each of these object classes would probably have attributes which also occur in the other object classes required, such as the person's name. However, when the object classes are combined with each other in an object, the *"Name"* attribute is stored just once.

The possibility to implement hierarchical directory structures is normally adopted in order to reflect an organization's structure in the directory. Special objects are normally used for this purpose. These objects are used to structure the directory

and correspond to artificial or real organizational units. The object class often used for this purpose is *organizationalUnit (ou)*. For the sake of clarity, the directory service is often also structured in line with the DNS namespace which exists anyway in organizations. The object class used for this purpose is *domainComponent (dc)*. In practical application, the coarse structure is in most cases oriented towards the DNS namespace, with the detailed structure being based on organizational units and other container objects.

Consider the example of an organization with two sites (Oststadt and Weststadt). The organization uses the DNS domain *bsporg.de* and the subdomains *oststadt.bsporg.de* and *weststadt.bsporg.de* for the two sites. The organization can then use the *"bsporg.de"* object as the root of its directory. In LDAP, this object would be referred to as *dc=bsporg,dc=de* in order to make it clear that the root is an object of the domain component type (*domainComponent, dc*) with the name *bsporg* which is a subobject of the object *de* which is also of the "domain component" type.

This base point would then contain another two objects referred to as *dc=oststadt* and *dc=weststadt* (analogous to the DNS names for these sites). These names are also referred to as the relative names of the objects because they do not unambiguously say where they are located in the directory hierarchy. The use of distinguished names is an alternative which then identifies the exact place of occurrence of the objects in the directory. These names would then be *dc=oststadt,dc=bsporg,dc=de* and *dc=weststadt,dc=bsporg,dc=de*.

Furthermore, suppose the organization has three organizational units at each of the two sites, identified as "Produktion" (production), "Vertrieb" (sales) and "Leitung" (management). This means that the object *ou=produktion* would be created as a subobject of *dc=oststadt* (distinguished name: *ou=produktion,dc=oststadt, dc=bsporg,dc=de*) for the organizational unit "Produktion" at the Oststadt site for the purpose of presentation in the directory. The same procedure would have to be adopted for the other units at this site and at the other site. Objects for persons, groups of persons as well as computers would have to be created within the organizational unit "Produktion". In order to achieve a clear-cut layout, these objects can then be arranged in containers (usually referred to by names or *commonName, cn*) with the names *cn=leute*, *cn=gruppen* and *cn=rechner*. Finally, the entries for the real objects would be generated in these containers. For example, the following object would be created for employee "Karl Schulze" working in the production ("Produktion") unit at the "Oststadt" site in the container *cn=leute,ou=produktion, dc=oststadt,dc=bsporg,dc=de*. The name of this object would then be *cn=schulze,cn=leute,ou=produktion, dc=oststadt,dc=bsporg,dc=de*.

It is obvious that a directory service only makes sense if it is used by as many applications as possible. Ideally, the directory service is the exclusive source of information stored in it in the network. If, for example, the network of an organization includes Windows-based and UNIX-based servers, an intranet application and a web proxy with authentication, user accounts and user privileges concerning the different systems can be configured separately on the

individual systems. The introduction of a directory service now makes it possible to exclusively store the user accounts and the pertinent privileges in the central directory service, with all the systems accessing this directory service. At the same time, address-book applications which are, for example, included in e-mail software, can access the directory and thereby provide the e-mail addresses of the members of the organization without the need to manually enter this data once more.

Directory services can also be used to store passwords (passwords are then typically an attribute of a personal or user account objects). This also serves the purpose of once-off, central data storage and management. Passwords stored in the directory must be created and changed at a single point only and can then be used on all systems and by all applications which can use the directory for authentication. Furthermore, the passwords stored in the directory can also be used for authentication in the case of access to data in the directory itself.

The example of password storage shows that a fine-grained system of privileges must be in place in order to control access to the directory service and to define which objects and attributes can be read or changed by which users. It does, for example, clearly make sense that passwords can be changed by their owners and by administrators. Furthermore, their owners must be able to use them for authentication. In contrast, nobody else who can access the directory may be able to read the passwords at all, even if the passwords are contained in the directory in encrypted form. At the same time, however, other users may be authorized to read the e-mail addresses of user objects. In such a case, different attributes (password and e-mail address) of the same object (person or user) must have different privileges. This is why most directory services implement a system of Access Control Lists (ACLs) which can also be compared to the ACLs at the file system level.

Despite the common practice of using directory services to authenticate services, this must be considered to be a questionable strategy. This concept does not permit a safe method for implementing a single sign-on function because every system and every application requires repeated authentication (albeit with the same password). Furthermore, most directory services were not written with a view to providing a secure authentication mechanism but as a means of central storage for frequently needed information and its quick distribution to clients.We recommend using Kerberos instead.

If Kerberos is used, user names and password are not – in contrast to the standard procedure - sent to every server whose services are used by a user. This is replaced by once-off registration with a Key Distribution Center (KDC, sometimes also referred to as Kerberos domain controller). Following registration, the user receives a ticket which is issued for a defined term and which the user can then use in order to authenticate himself in relation to all other services. Following expiration of the term of validity of the ticket, the user must re-authenticate himself. The use of Kerberos means that the password repository must exist on particularly trustworthy systems (i.e. the Kerberos servers) only. Other systems no longer need to access the password repository. Kerberos tickets can also be used to implement a single sign-on functionality because

tickets can be used to access all the services made available in the network (on condition that the corresponding applications support Kerberos).

As soon as a directory service becomes the central information database of an organization, it becomes a particularly important component of the network which must feature a very high degree of availability. This is why directory services typically support replication methods which can be used to transfer complete directories and changes from one server with a directory service to other servers. This is also why a load balancing option is offered because not all the clients must access the same directory server.

Two different replication methods exist, i.e. master-slave replication and multi-master replication. The master-slave method means that changes can only be made on a central master server of the directory which then replicates the changes to the other (slave) servers. This means that changes in directory contents lead to a certain bottleneck because these changes can be made on the central server only. In the event of a failure of the master server, changes cannot be made until the system is reconfigured in such a manner that another server acts as the master or until the functionality of the original master server is restored. Multi-master replication enables changes in directory contents on multiple servers, so that the above-mentioned problems do not exist. However, consistency problems can occur in the case of multi-master replication if conflicting changes are made at the same time on different servers.

3.7.3   Active directory service (ADS)

This section is designed to give the most comprehensive overview possible of the "Active Directory Service" technology. The following core functionalities are thus addressed:

Directory Service

LDAP

Kerberos

Group guidelines

Delegation

Certificate management

Furthermore, this section also describes

the application

the architecture

and the strategic relevance.

Finally, the differences between the minimum and maximum configurations of an active directory will be discussed.

3.7.3.1   Successor to the Windows NT 4 logon service

With regard to the Windows NT logon services, the active directory (AD) can be called its corresponding successor service.

This is supported by the fact that the call of the installation routine of Windows 2000 on a Windows NT PDC immediately leads to the establishment of an active directory. It would, however, not be correct at this point to say that the establishment of an active directory merely consists of the call of an installation routine on a single server. The establishment of an AD requires a meticulously developed concept and careful migration planning.

The core technology of the logon services in the active directory is still the structural unit of the domain in the same manner as with Windows NT. The domain continues to be the administrative unit which combines the computer and user accounts via a shared database in a common security context. The domain boundary is the boundary of the security context and of the replication of the user database.

The NetBIOS namespace continues to exist. Furthermore, like under Windows NT, computers based on

   Windows NT

   Windows 2000

   Windows XP

can be members of the domain.

If systems like Windows NT and 9x are to be supported, it is additionally necessary to ensure a faultless NetBIOS name resolution (by WINS, for example).

The implementation of an active directory is a characteristic feature of the change in architecture to be carried out. For this purpose, a DNS infrastructure is indispensable requiring not just the selection of a namespace but also the use of suitable DNS servers. This does, of course, imply an existing TCP/ IP network environment.

The migration planning process and a selection of possible scenarios are described in one of the following sections.

3.7.3.2   The Kerberos authentication mechanism

Windows 2000 active directory continues to support the NTLM authentication mechanism. This is necessary for many reasons, for example, simply to validate the registration of systems like Windows NT or 9x.

Authentication via Kerberos is a new feature**.**

Systems like Windows 2000 or XP first use Kerberos by default. However, they switch to NTLM if necessary. Systems like Windows NT or 9x cannot be retrofitted to switch to Kerberos. Windows 2000 DCs communicate via Kerberos.

In Windows 2000, Kerberos version 5 was implemented with add-ons for authentication via public keys. The implementation follows specifications in RFCs 1510 and 1964. The Kerberos Key Distribution Center (KDC) is integrated in every DC of the active directory and uses its user database.

Kerberos requires the system times of the computers involved to be subject to minor deviations only. In order to ensure this, an automatic hierarchical time reconciliation function was implemented in Windows 2000 for the computers which are members of the AD.

Kerberos must be seen with certain reservations if NAT (Network Address Translation) is used in the network because the encrypted load of IP packets contains IP addresses.

Kerberos is more flexible and more efficient than NTLM. In the case of NTLM, an application server must always contact the domain controller in order to authenticate a client. In the case of Kerberos, the application server can check the logon information which the clients presents to it. Under NTLM, servers can check the identity of the clients, whilst with Kerberos, the client can also check the identity of the server (mutual authentication). Windows services must impersonate the client in order to access resources. NTLM and Kerberos can provide the service with the information needed to impersonate the client locally. NTLM is unable to handle distributed applications with the FrontEnd and BackEnd being located on different computers, whilst Kerberos offers a proxy mechanism (delegated authentication). Kerberos can implement, transitive, bidirectional trust relationships between domains.

The Kerberos protocol is made up of three sub-protocols. The sub-protocol via which the Key Distribution Center (KDC) grants to the client a logon session key and a TGT (Ticket-Granting Ticket) is called the Authentication Service Exchange (AS Exchange). The sub-protocol which the KDC uses in order to grant a service session key and a ticket for the service is called the Ticket-Granting Service (TGS Exchange). The sub-protocol via which the client sends the ticket for access to a service is called the Client/Server service (CS Exchange).

3.7.3.3 New features concerning structuring

As already mentioned, the structural unit of the domain continues to exist even in an active directory.

In the active directory, the domain can be regarded as part of an overall structure (forest) and the pertinent tree structures (tree) with a hierarchical structure in a DNS namespace. The individual domains are connected to each other via so-called bidirectional, transitive Kerberos trusts (trust relationships). (The trust relationships via NTLM known from Windows NT can continue to be used).

If an active directory is referred to, this always means the forest rather than individual trees or domains.

The illustration below shows a Windows NT domain structure in which two account domains and five resource domains are connected to each other via trust relationships.

Microsoft presents Windows 2000 domains as triangles, Windows NT domains as ellipses. This convention is adopted for the purposes of this guide. This gives the following picture:
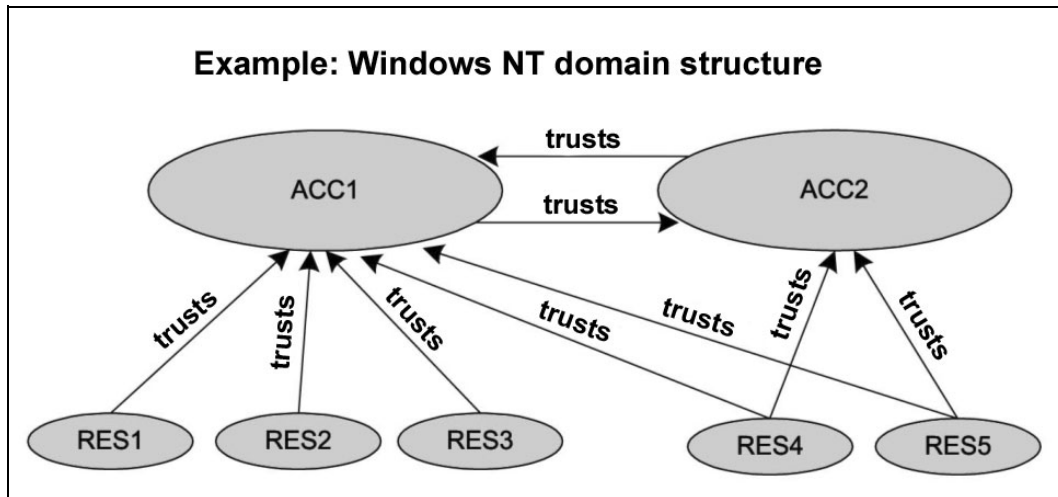
Fig. 9:   Example of an NT domain structure

In an active directory, the forest shown below (Example) would   thus   be conceivable, also consisting of seven domains. The forest consists of two trees in which the domains have a hierarchical structure and in which the domains are connected to each other via Kerberos both in a transitive manner (A trusts B and B trusts C, so that A also trusts C) and in a bidirectional manner (A trusts B, so that B also trusts A).

Technical description of the migration paths

Example: Windows 2000 active directory
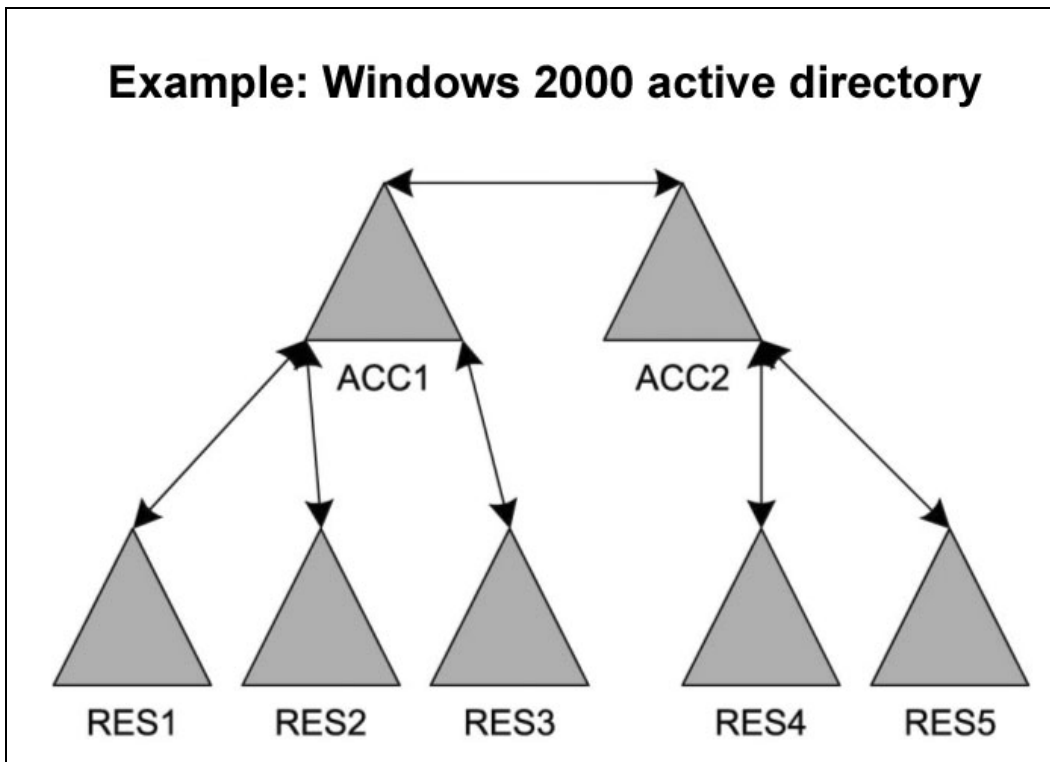
Fig. 10:   Example of Windows 2000

The active directory is made available by domain controllers (DCs). The distinction between PDC and BDC is not continued any further. This reflects the new architectural feature, i.e. the fact that Windows 2000 domain controllers are subject to a multi-master principle: Most changes within the AD can be carried out (written) on any DC. The multi-master principle cannot apply to all changes. Special domain controllers, the so-called FSMO (Flexible Single Master Operation) owners, exist for this purpose.

These FSMOs are:

PDC emulator

Infrastructure master

RID master

Schema master

Domain naming master.

These functions can be placed on specifically selected domain controllers.

The following functions:

Schema master (responsible for the schema of the directory)

Domain naming master (responsible in the case of changes in the namespace)

are unique roles within an overall structure (forest).

The following functions:

PDC emulator

Infrastructure master (responsible for updates of SIDs and distinguished names across domain boundaries)

RID master (responsible for the granting of RID pools to other DCs)

are unique in every domain.

The PDC emulator is responsible for important functions, such as:

Password updating for down-level clients (NT 4.0, 9x) and partners of the Windows NT backup domain controllers

Source of the network time (PDC of the master domain only)

Domain master browser service (NetBIOS)

A forest can be additionally structured by sites. The sizes can (or better should) reflect the physical network structure and correspond to the bandwidths available between the locations (Hamburg, Berlin, Bonn, etc.). The primary purpose of this structural organization is to control the replication process between the domain controllers.

The site topology chosen can be independent of the domain structure. The illustration below shows an example of a topology.
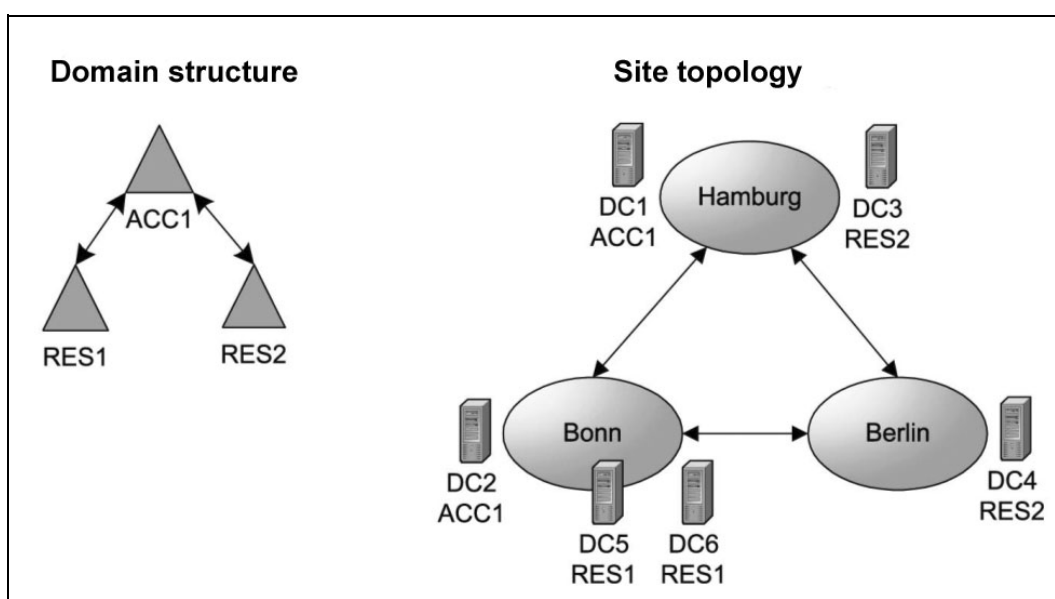
Fig. 11:   Example of a site and domain structure

The so-called OU structure (OU standing for organizational unit) is another new structural feature which is described in the section dealing with the directory service.

3.7.3.4   *DNS namespace and infrastructure*

A DNS infrastructure is indispensable for the Windows 2000 active directory service. The following questions must be answered in this context.

Which DNS namespace is to be assigned to the AD?

In what way must this namespace be fitted into the existing DNS namespace?

Who administers the existing namespace?

On which platform (operating system: Windows 2000, UNIX) is the DNS to be made available?

Which relationship to the NetBIOS namespace must be considered?

Answering these questions is often quite difficult, not just for technical, but also for "political" reasons.

Selecting the platform

The DNS infrastructure for an AD must feature certain properties in order to ensure smooth name resolution and registration of entries.

Windows 2000 with its own DNS implementation generally fulfills all these requirements. The features of Windows 2000 DNS include, for example:

Service records (RFC 2052)

Dynamic DNS (RFC 2136)

Secure dynamic update

Multi-master method thanks to integration into the active directory

Integration of WINS

Support of RFC 2052 is mandatory because this is the only way in which entries for services can be made in the DNS. RFC 2052 is supported by UNIX-based servers from BIND 8.1.2 upwards. BIND 8.2.1 supports further features and is the recommended version.

NetBIOS namespace

The following aspects must be considered with regard to the NetBIOS namespace.

The NetBIOS name of a Windows 2000 domain (such as RES1) can, in principle, deviate from the lowest name of the DNS suffix (such as RES001 from res001.behoerde.de). The use of such a naming system is, however, generally not advisable.

The NetBIOS namespace is without any degree of freedom especially in cases where existing NT domains are to be updated (refer to "Inplace Migration").

DNS namespace

The following discussions are based on the assumption that a DNS environment already exists in the existing infrastructure and that this DNS environment is made available in the basis of Unix Server. This is a relatively general starting situation. Suppose the name of the domain is "BEHOERDE.DE" and the existing BEHOERDE.DE namespace is used internally only. Furthermore, suppose that an internal root domain "dot" or zone exists in the DNS infrastructure. The illustration below outlines the starting situation.
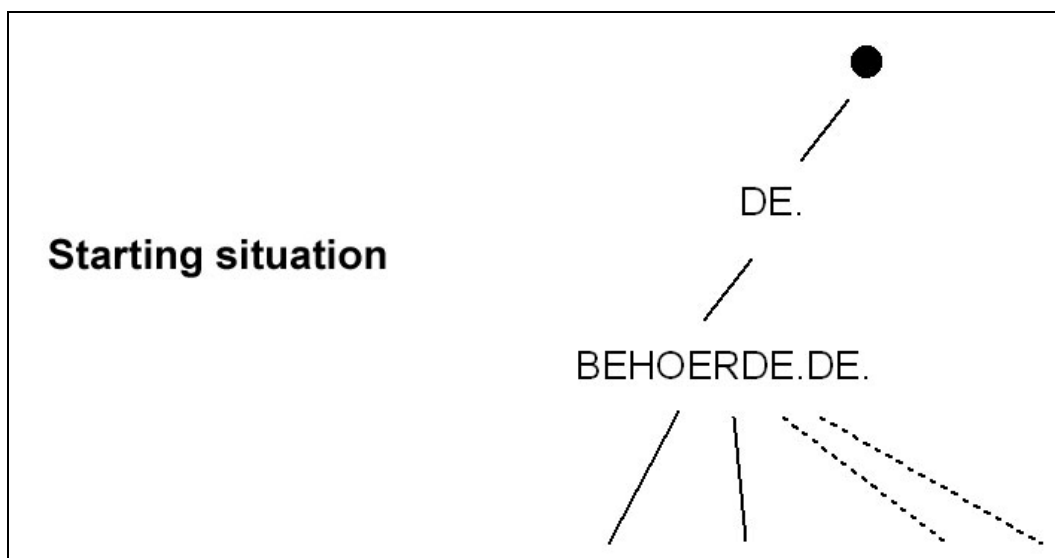
Fig. 12:   Starting situation

The following paragraphs deal with possible solutions for creating a namespace with a view to Windows 2000 active directory. This is to illustrate the complexity of a migration to ADS and the related long-term commitment and dependency from ADS.

Master domain: W2K.BEHOERDE.DE

The existing, internal DNS namespace is used to receive another W2K subdomain (as master domain = first active directory domain).

Technical description of the migration paths
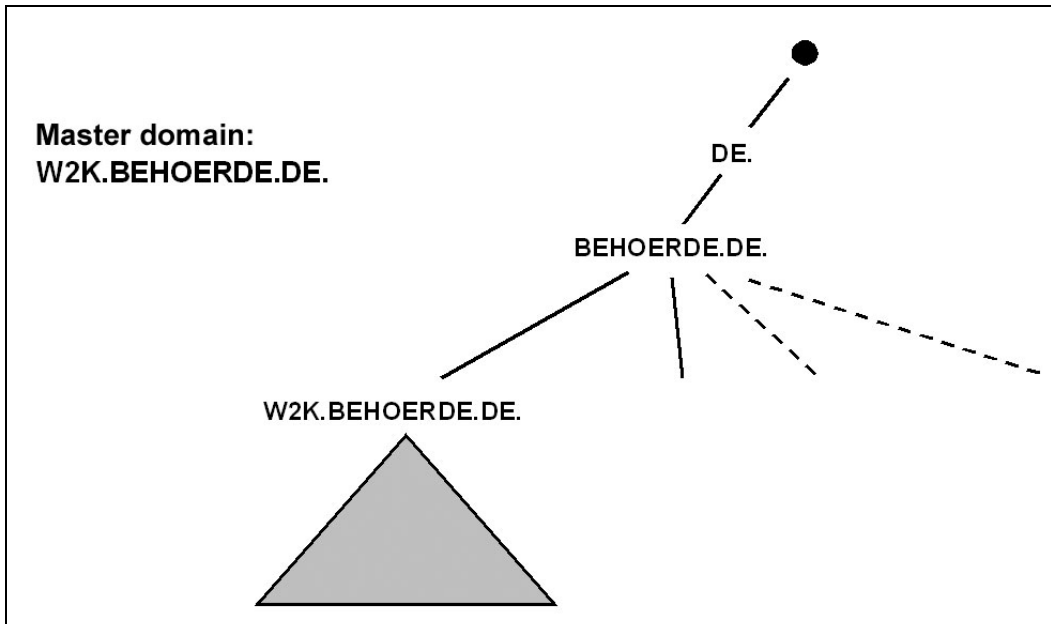
Fig. 13:   Master domain: W2K.BEHOERDE.DE

This master domain offers the following advantages:

No new name tree is created.

Existing root servers remain unchanged.

Any platform can be selected for the DNS services.

The internal and external namespaces remain separated from each other.

The disadvantages of this solution are the following:

The user principal Nname of the user is relatively long (Benutzername @w2k.behoerde.de) or includes a 2nd level domain

If the forest is enlarged (e.g. plus DNS tree ZUSATZ.DE), one of the trees is not a 2nd level domain (technically not a problem)

Part of the name resolution is crucially dependent on the legacy infrastructure.

Master domain: BEHOERDE.DE

The existing DNS namespace is used to determine the name of the master domain.

Fig. 14:   Master domain: BEHOERDE.DE

This master domain offers the following advantages:

No new name tree is created.

Existing root servers remain unchanged.

The user principal name of the user is relatively short (Benutzername@behoerde.de)

If he forest is increased (e.g. plus DNS tree ZUSATZ.DE), both trees are 2nd level domain

The internal and external namespaces remain separated from each other.

The disadvantages of this solution are the following:

The platform for the DNS services cannot be selected

The name resolution is exclusively dependent on the legacy infrastructure.

Master domain: NEU.DE

This approach is independent of the legacy namespace and creates a new, internal DNS name tree. This chosen name, NEU.DE, is unique world-wide and is hence officially registered.
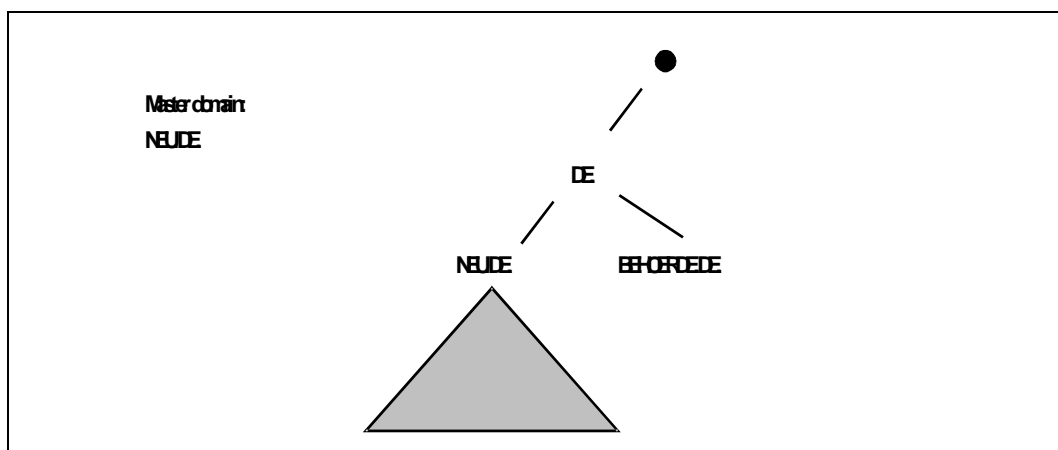
Technical description of the migration paths

Fig. 15: Master domain: NEU.DE

This master domain offers the following advantages:

A new name tree is created, so that no historical burdens are inherited

Existing root servers can remain unchanged.

The platform for the DNS services can be selected

The user principal name of the user is relatively short (Benutzername@neu.de)

If he forest is increased (e.g. plus DNS tree ZUSATZ.DE), both trees are 2nd level domain

The name resolution is hardly dependent on the legacy infrastructure.

The internal and external namespaces can remain separate, depending on future requirements

The disadvantages of this solution are the following:

A new name tree is created, so that new structures and additional guidelines are generated

The complexity with regard to DNS increases and hence also the administrative effort

Master and structure domain: NEU.DE/ INTRA.NEU.DE

This approach is independent of the legacy namespace and creates a new DNS name tree. An additional subdomain is created in addition to the 2nd level domain NEU.DE.

The 2nd level domain NEU.DE exclusively serves as the master domain of the forest, as the so-called structure domain. User accounts are created in the INTRA subdomain only.
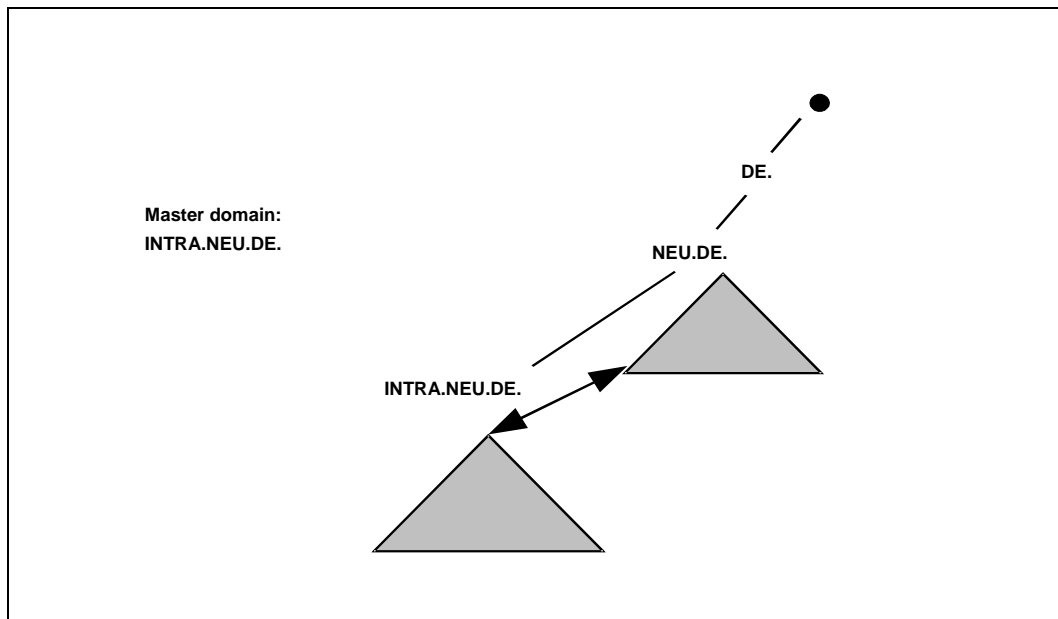
Fig. 16:   Master and structure domain: NEU.DE/ INTRA.NEU.DE

The structure domains offer the following advantages:

A new name tree is created, so that no historical burdens are inherited

Existing root servers can remain unchanged.

The platform for the DNS services can be selected

If he forest is increased (e.g. plus DNS tree ZUSATZ.DE), both trees are 2nd level domain

If the number of domains increases, the new domains can be installed parallel to the INTRA domain

The name resolution is hardly dependent on the legacy infrastructure.

The internal and external namespaces can remain separate, depending on requirements

The disadvantages of this solution are the following:

Two domains are installed in the active directory

A new name tree is created, so that new structures and additional guidelines are generated

The user principal name of the user is relatively long (Benutzername @intra.neu.de)

The number of cross connections increases and hence also the complexity and the administrative effort

Master domain: INTRA.BEHOERDE-ONLINE.DE

Technical description of the migration paths

An existing **external** DNS namespace is used to receive another domain. The existing BEHOERDE-ONLINE.DE namespace was so far used for external purposes only. An INTRA domain must be created for internal use only.
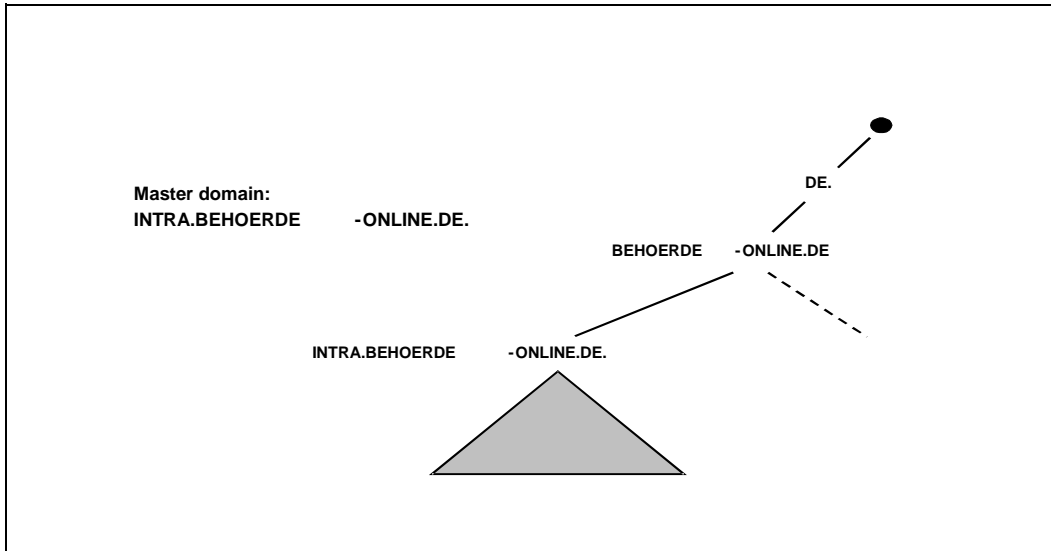
Fig. 17:   Master domain: INTRA.BEHOERDE-ONLINE.DE

This master domain offers the following advantages:

A new internal name branch is created, so that no historical burdens are inherited

Existing root servers remain unchanged.

The platform for the DNS services can be selected

If he forest is increased (e.g. plus DNS tree ZUSATZ.DE), both trees are 2nd level domain

The name resolution is strongly dependent on the legacy infrastructure.

The disadvantages of this solution are the following:

The user principal name of the user is relatively long ([Benutzername@ intra.behoerde-online.de](Benutzername@intra.behoerde-online.de))

A new internal name tree is created, so that new structures and additional guidelines are generated

The number of cross connections increases and hence also the complexity and the administrative effort

The internal and external namespaces are no longer independent of each other

Master domain: AMT.LOCAL

This approach is independent of the legacy namespace and creates a new, internal DNS name tree. The LOCAL top-level domain selected is currently not

supported on the Internet. Official registration of this chosen name is hence not possible. Instead of LOCAL, it would be possible to use a top-level domain name protected under RFC 2606 which is never at risk of being used as a top-level domain by the Internet community.
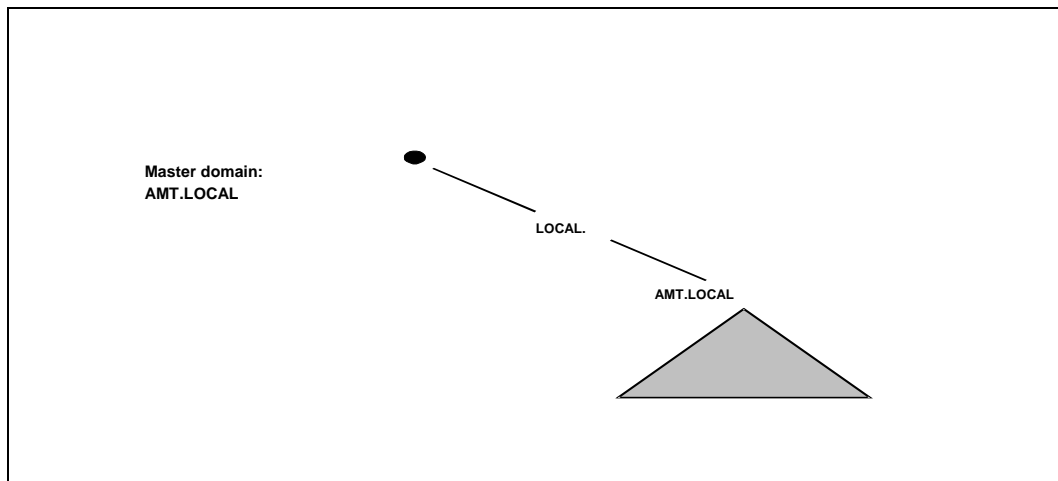
Fig. 18: Master domain: AMT.LOCAL

This master domain offers the following advantages:

A new name tree is created, so that no historical burdens are inherited

Existing root servers can remain unchanged.

The platform for the DNS services can be selected

The user principal name of the user is relatively short (Benutzername@ amt.local)

If he forest is increased (e.g. plus DNS tree ZUSATZ.DE), both trees are 2nd level domain

The name resolution is hardly dependent on the legacy infrastructure.

The disadvantages of this solution are the following:

A new name tree is created, so that new structures and additional guidelines are generated

The internal and external namespaces remain permanently separated from each other.

The number of cross connections increases and hence also the complexity and the administrative effort

Important

> The selection of the DNS namespace becomes much more difficult if the sovereign administration of the DNS namespace is outside one's own sovereign privileges. It is then often necessary to subordinate one's own

> interests to a higher-level interest which can render the decision-making process significantly more time-consuming.

3.7.3.5 *Directory service and schema*

With Windows 2000 active directory, a directory service is introduced which is oriented towards the X.500 standard and which can be administered via LDAP (Lightweight Directory Access Protocol).

The directory service uses a database type which was originally developed for Microsoft Exchange (Extensible Storage Engine). It replaces the architecture of the SAM database. However, SAM continues to be kept ready for possible NT-based BDCs as long as the active directory is not switched to so-called "native mode".

In the schema of the active directory, around 142 (including amendments to Exchange 2000, HIS and ISA: 419) different classes of objects are defined to which up to 863 (including E2K, HIS and ISA: 1928) attributes can be assigned.

It is, in principle, possible to amend the schema, and to amend existing classes by adding new attributes. Schema amendments, once made under Windows 2000, cannot be reversed. They can only be deactivated.

Breaking down the active directory and/or database is accomplished via the structure unit of the domain. This means that breaking down within the domain in the sense of a distributed database is not possible.

The replication of the active directory and/or database is carried out between the domain controllers (DCs). This is carried out on the basis of the so-called unique sequence numbers (USNs) which are administered even at attribute level. Replication is thus possible at attribute level. When the property of an object changes, this means that the change in property rather than the complete object is replicated.

Every DC in the active directory provides an LDAP service. LDAP version 3 is supported. By means of an LDAP client, the active directory can be browsed or administered. The object in question can be read and written via the distinguished name. Take the following LDAP path, for example:

LDAP://dc001.behoerde.de/cn=Hans   Muster,   ou=Unterabteilung,   ou=Abteilung, dc=behoerde, dc=de.

The name dc001.behoerde.de refers to a DC (i.e. to an LDAP server) in the DNS nomenclature. Stating the LDAP server is optional with some LDAP clients on condition that they master the so-called "serverless binding". Any LDAP client implementation, such as OpenLDAP, and/or programming interface can in principle be used such as:

ADSI (Active Directory Services Interface (integrated into Windows 2000)

LDIF (LDAP Data Interchange Format)

and many more

The use of these interfaces involves certain **problems** because

Certain attributes or objects are administered sovereignly by the active directory (such as the SID or GUID attributes)

Certain attributes consist of binary values or hash values the decryption and encryption algorithms of which are not known (for example, the userParameters attribute) and which can be modified via separate interfaces outside LDAP only (for example, Windows Terminal Server API)

The use of the graphic user interface (MMC) triggers additional processes besides the mere writing of the LDAP attributes (when a home directory is determined, this is, for example, created on the file server with the related privileges).

3.7.3.6 ADS as Basis

Windows 2000 active directory is mandatory for Exchange 2000. Exchange 2000 extends the user object and saves its own configuration in the AD.

The following Microsoft products use the AD in order to save their configuration:

HIS Server (Host Integration Server)

ISA Server (Internet Security and Acceleration)

3.7.3.7 Administration tools

The server version of Windows 2000 comes with several graphic tools for administering the information saved by default in the active directory, such as user and group accounts or DNS configuration. The Microsoft Management Console (MMC) is one of the tools used for this purpose. Furthermore, the tools for the command line known familiar with Windows NT are available for creating, deleting and editing users and groups. However, these tools can be used to edit only part of the account information saved in the active directory.

Furthermore, ldifde is a command line-based program which enables the generation of directory entries from an LDIF (LDAP Data Interchange Format) file.

The administration tools supplied with Windows 2000 Server are primarily designed for use by experienced Windows administrators. They are hardly suitable for delegating administrative tasks, such as creating or changing user accounts, to less qualified staff.

ADSI (Active Directory Service Interface) is a COM-based interface which enables automation of a large number of different tasks.

3.7.3.8 Certification services

Windows 2000 enables the establishment of a so-called PKI (Public Key Infrastructure). The Certification Authority (CA) can be integrated into the AD or installed separately. If the AD-integrated variant is selected, this then supports and enables the following security technologies:

EFS (Encrypted File System)

IPsec

SmartCard

Encryption and digital signatures (mail)

and many more

in the internal network.

The distribution and/or activation of the PKI is supported by group guidelines. However, this does not mean that a separate administration concept for keys then becomes superfluous.

3.7.3.9   Smart Card

The establishment of an internal PKI enables user authentication via a SmartCard. Logon via SmartCard to Windows 2000/XP computers can be carried out without the need to use any additional software.

3.7.4   Replacing migration – Samba and OpenLDAP

3.7.4.1   Functional requirements

The key requirement for a directory service is to ensure the quick dissemination of information in the network. Apart from this, the directory service should offer the following functions:

Possibility to change the information made available in the directory

Possibility to give the objects in the directory a hierarchical structure

Use of standard-conforming and commonly used schemas in order to ensure a high degree of compatibility with as many applications as possible. Possibility to add own objects and schemas

Possibility to authenticate users, as well as integration with other authentication services (Kerberos)

Administration of access rights

Use of open standards in order to achieve a high degree of compatibility, if possible, with all services and applications which can use the information stored in the directory

Support of replication processes and techniques

Use of secure transmission protocols for the transmission of information between client and directory service and during replication

3.7.4.2   Products discussed

If a Windows-NT domain is to be replaced by a directory service based on Microsoft Windows or Linux, the following products are the first options of choice:

Active directory with Windows 2000/ 2003 Server

OpenLDAP and Samba (optionally with Kerberos) under Linux

Other directory services, such as Novell Directory Services or SunONE, are not discussed further in this context because they require the introduction of additional products, thereby increasing the complexity of Windows-based and Linux-based IT environments even further.

3.7.4.3 General comparison of the functionalities of NTDS, the active directory and OpenLDAP

Table 15 Comparison of directory services

Function	WinNT	Win2k / ADS	Linux / OpenLDAP
Client without additional software	X	X	X
Possibility to implement a hierarchical structure of the directory		X	X
Expandability by adding own attributes and object classes		X	X
Character set for directory data	Unicode	Unicode	Unicode
Possibility to access the directory via standard protocol (LDAP)		X	X
Secure access per LDAP via SSL/ TLS		X	X
Support of the "starttls" protocol		X	X
Support for SASL			X
Authentication of NT clients	X	X	Via Samba[45]
Authentication of W2K clients	X	X	Via Samba[46]
Authentication of Linux clients	Via winbind	Via winbind or LDAP	X
Possibility to integrate Kerberos		X[47]	X
Possibility to use an independent / higher-level Kerberos service		X[48]	X
Administration of access privileges (ACLs) for attributes and objects		X	X
Delegation of administrative tasks		X	X
Master-slave replication	X	X[49]	X
Multi-master replication		X[50]	X[51]

---

[45] If Samba is used for the authentication of Windows Clients in relation to OpenLDAP, the NT LAN Manager protocol is used between the Windows client and the Samba server.

[46] If Samba is used for the authentication of Windows Clients in relation to OpenLDAP, the NT LAN Manager protocol is used between the Windows client and the Samba server.

[47] Kerberos is firmly integrated into the active directory.

[48] Although the active directory enables authentication in relation to an external Kerberos server, it is then no longer possible to use active directory domains for authentication of Windows 95/98/Me/NT-based computers.

[49] The active directory uses master-slave replication between Windows 2000 DC and Windows NT 4 BDC in "mixed mode".

3.7.4.4 *Authentication with Linux / OpenLDAP and Samba*

The "authentication" and "directory service" issues can be hardly separated. However, since a directory service can always carry out more tasks than the authentication service, and since authentication is an infrastructure service, the authentication process in the interaction of Linux, Samba and OpenLDAP on the one hand and also in the interaction with Windows and ADS is discussed in chapter 3.4 "Authentication services".

3.7.4.5 *Central administration of host information with Linux and OpenLDAP*

Central administration of host information in one directory enables significant simplification of certain administrative tasks. These tasks include:

Preparing inventories of the existing hardware

Creation and administration of DNS name entries

Creation and administration of DHCP configurations

For Windows clients, machine accounts can be stored together with the above-mentioned information.

Furthermore, it is no longer necessary to distribute such information to other computers manually or by other processes because this information can now be distributed to the systems concerned by LDAP replication.

Linux offers several programs which can be used to export host information directly from an LDAP directory.

A patch which enables the DHCP configuration to be exported from an LDAP directory exists for the standard DHCP server (ISC DHCPD).

http://home.ntelos.net/~masneyb/dhcp-3.0.1rc11-ldap-patch

A patch that replaces zone files with LDAP also exists for BIND 9.

http://www.venaas.no/dns/bind/bind-sdb/

Samba can import information concerning machine accounts directly from the LDAP directory.

Furthermore, a whole range of proprietary and free software products is available, permitting transparent generation of the BIND and DHCP configuration from the LDAP directory.

---

[50] The active directory uses multi-master replication in "native mode" (in which Windows 2000/2003-based domain controllers are exclusively used).

[51] The multi-master replication in OpenLDAP is considered as being experimental, and is not activated by default.

3.7.4.6   Integration of other applications

Besides the use of directory services for the central storage of user, group and host information, the benefits of applications increase with the access of as many other applications as possible. A complete list of LDAP-compatible applications cannot be given at this point. It is, however, important to note that more and more applications feature LDAP support, not least Microsoft's Outlook and Outlook Express e-mail programs or the OpenOffice package. These applications can work with both OpenLDAP and active directory as directory service.

3.7.4.7   Administration tools

Linux offers the standard LDAP administration tools (ldapsearch, ldapadd, ldapmodify) for the information stored in a directory. These tools are primarily used to initialize a directory, to import data, to browse directories and for the automated editing of a directory. Some command line-based tools are also available for user and group administration.

Free graphic tools for directory-based user and group administration under Linux are currently in development (for example, the directory-administrator: http://diradmin.open-it.org/files.php).

Web-based tools for the administration of user, group and machine accounts and other objects (mailing lists, DNS entries, etc.) within directory services are equally important and much more flexible. The advantage of this solutions is that they can be used with a web browser independent of the server, with the possibility to use secure data transmission (SSL/TLS)[52].

3.7.4.8   Runtime behavior and resource consumption

Linux and OpenLDAP were found to be stable and sufficiently performant in very large environments with more than 10,000 users. Samba was found to be very reliable, stable and – compared to Windows-based servers – it was found to feature a low resource consumption in several tests and in large installations.

3.7.4.9   User acceptance

Directory services are initially invisible for end users and become only gradually apparent when applications are linked to the directory. The more applications use the directory, the higher the probability that users will be confronted with consistent data which will increase acceptance.

Migration to the Samba / OpenLDAP combination can take place in a manner transparent for users and clients, so that they are not affected by the migration process or by any resultant changes.

A directory service benefits administrators with the introduction of a single point of administration. This single point of administration can be used better the better

---

[52] Examples are the Webmin module (http://www.webmin.com/) idxldapaccounts
  (http://webmin.idealx.org/) and the licensed univention_ admin (http://www. univention.de/) tool.

the administration tools available are adapted to the qualification profile and to the day-to-day duties of the administrators.

3.7.5   Continuing migration – introduction of ADS

The migration of logon services from Windows NT 4 to Windows 2000 active directory usually requires a separate concept and practical tests before the optimum path can be finally determined. A possible migration process will be briefly outlined in the following in order to illustrate the necessary inputs and technical boundary conditions.

3.7.5.1   Sequence of operations

The migration from Windows NT to Windows 2000 is very flexible with regard to the sequence of individual operations. It is, for example, not necessary to migrate the logon services first followed by the clients or vice versa. Nor is it necessary to change a large number of Windows NT clients in a bulk rollout. Only if an existing NT domain is to be upgraded (inplace upgrade), the PDC of this domain must first be upgraded to Windows 2000.

There are two modes in the active directory: mixed and native mode. Switching to native mode is not possible until no more NT BDCs have to be supplied with a replicate of the SAM. <u>Switching to native mode cannot be reversed</u>. However, the native mode is necessary for a migration scenario with reorganization (refer to the section titled "A pure upgrade (inplace upgrade of all domains) would imply that the existing domain structure remains unchanged. Although reorganization at a later time is possible (so-called intra-forest reorganization), this is not without a certain risk (no fallback when accounts are moved).

" in chapter 3.7.5.3).

An optimization potential generally exists with regard to the planning of the sequence of operations. The exploitation of this potential should be oriented towards the legacy environment.

3.7.5.2   Target architecture

The goal should be an active directory structure with one domain or with the smallest number of domains possible. A small number of domains usually means the lowest effort during operation.
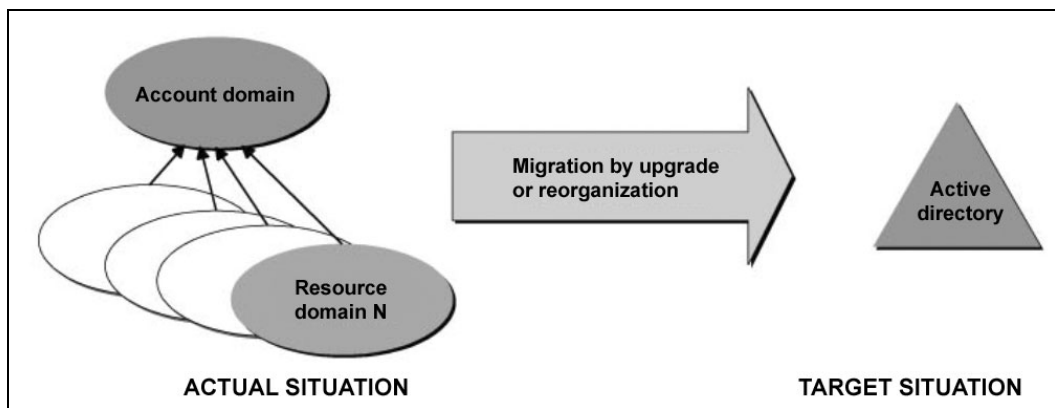
Fig. 19:   Migration by upgrade or reorganization

This corresponds to Microsoft's design recommendations because Microsoft already foresees a high degree of flexibility of migration paths and a high degree of reorganization options with regard to a migration from NT to Windows 2000.

3.7.5.3   Overview of migration variants

The following different migration variants are generally possible.

Pure upgrade (upgrade): The existing domain structure is to be left unchanged. This means that all the domains are upgraded.

Upgrade and reorganization: One or more domains are upgraded. The remaining NT domains are fitted into the structure.

New domain and reorganization: No domain is upgraded. One or more new domains of an ADS serve as the target of a reorganization of the NT domains.

Parallel world plus migration of resources: No domain is upgraded or reorganized. Only the resources (data, printers, etc.) are migrated (copied).

Variant 1: Pure upgrade

A pure upgrade (inplace upgrade of all domains) would imply that the existing domain structure remains unchanged. Although reorganization at a later time is possible (so-called intra-forest reorganization), this is not without a certain risk (no fallback when accounts are moved).

Variant 2: Upgrade plus reorganization

The upgrade or in-place migration includes the upgrade of the account domain to Windows 2000. This is then followed by so-called inter-forest reorganization (implying the dissolution of the resource domains).
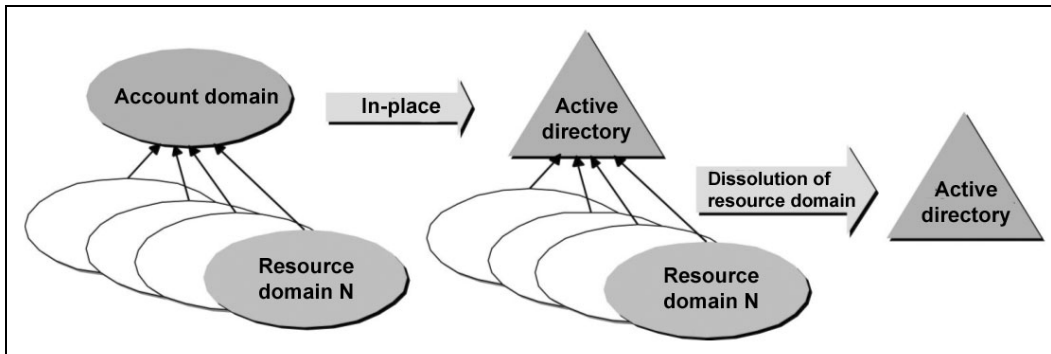
Fig. 20: ADS migration – upgrade plus reorganization

Variant 3: New domain plus reorganization

A new domain and/or a new AD is created first.
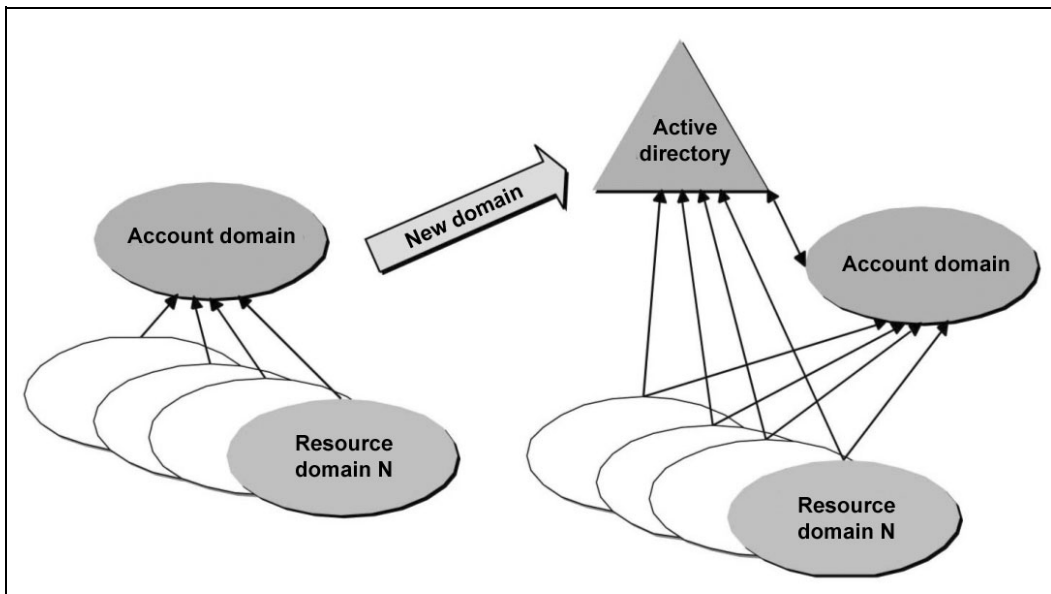
Fig. 21: ADS migration – new domain plus reorganization

The user accounts and the global groups of the account domain are cloned into the new (target) domain (including SID history).
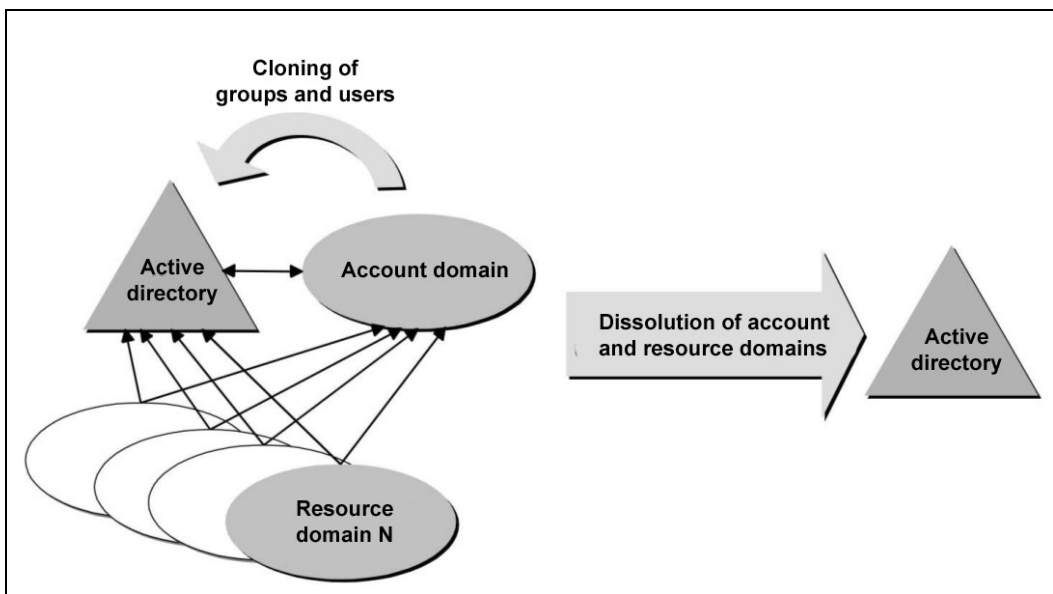
Fig. 22:   ADS migration – cloning users and groups

This approach offers the following advantages:

Uninterruptible migration for the user

Very good fallback

The re-writing of privileges (ReACLing) can be postponed and is not time-critical.

The disadvantage is:

Additional ADS, including hardware, must be available.

Variant 4: Parallel world and migration of resources

A new domain and/or a new ADS is created first.

Technical description of the migration paths
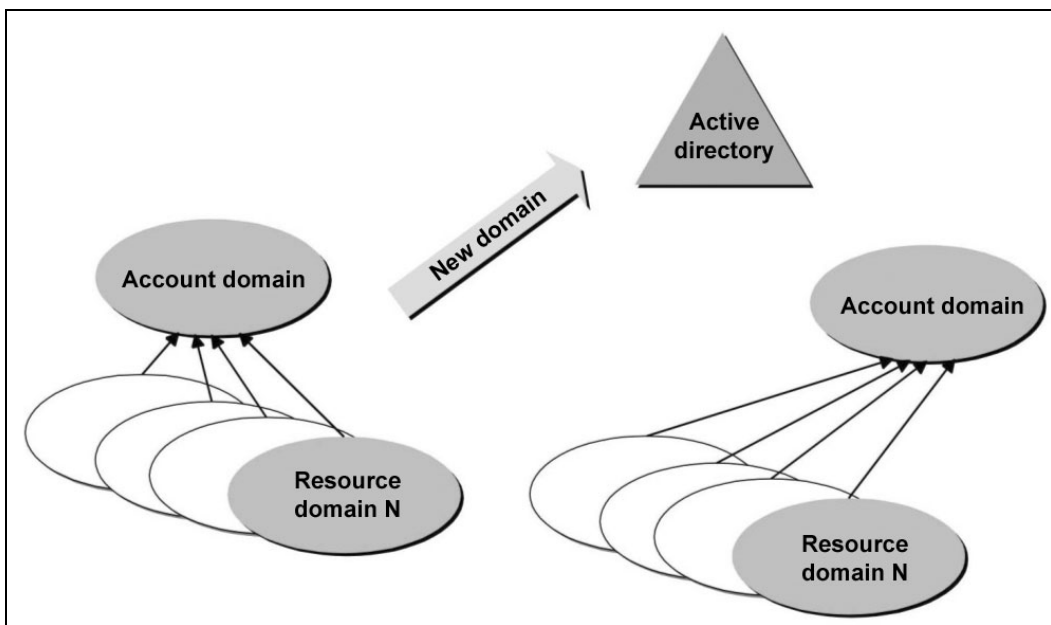
Fig. 23:   ADS migration – parallel world and migration of resources

The parallel world is filled with new user accounts and groups. The existing resources are copied into the new world.
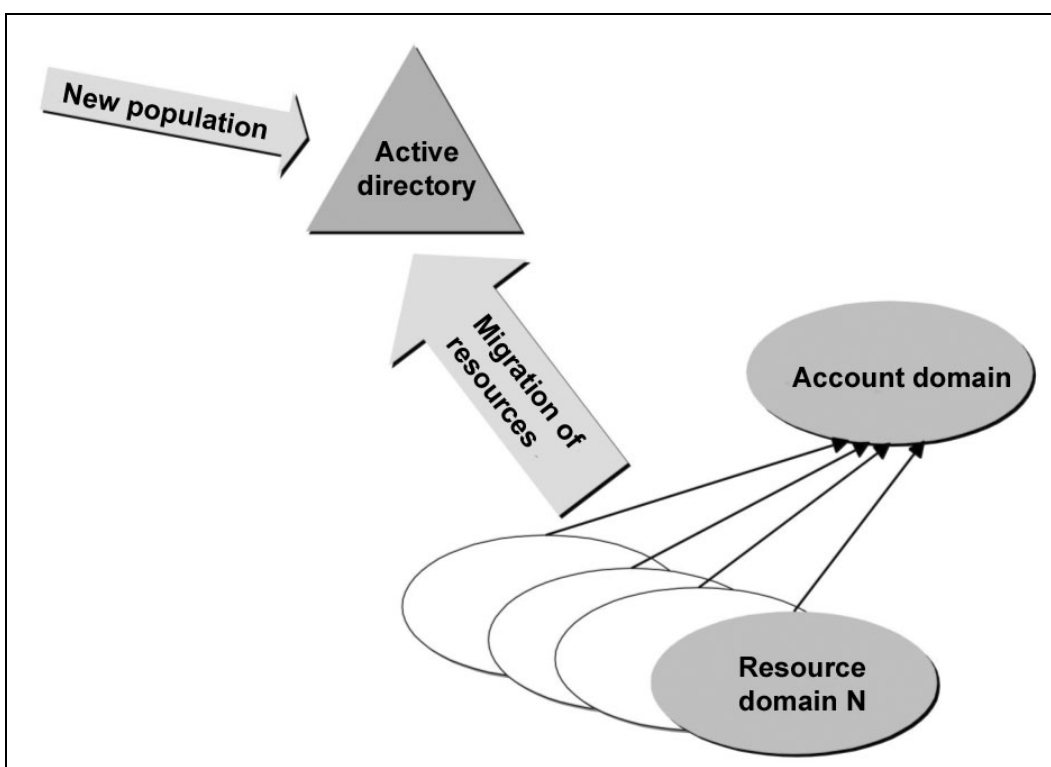
Fig. 24:   ADS migration – filling the parallel world with user accounts and groups

This approach offers the following advantages.

No time-critical migration of servers

No SID history

Access rights must be known and must be "replicated" in the new world

Data migration can mean data reduction

Disadvantages are:

The migration of data requires a significant logistical effort with regard to common access.

Additional hardware devices must be available when data migration is carried out.

3.7.5.4   Migration tasks

Migration to Windows 2000 active directory (replacing NT) or the completely new introduction of Windows 2000 active directory requires meticulous planning and validation in test environments.

The following tasks must be performed within the scope of a migration project.

Written description of the legacy infrastructure

Identification of the requirements for a new environment

Determination of the technical and organizational frame of reference

Evaluation of the existing environment

Concept of the future overall (forest) and domain structure

Determination of the DNS namespace and of the NetBIOS namespace

Determination of locations and placement of the domain controllers

Development of a comprehensive name concept

Connection to other directory services

Development of a concept for the OU structure

Migration concept for logon servers, resources, applications and workstation computers

3.7.5.5   Active directory with a view to Windows 2003

The fundamental architecture of the active directory is retained with the successor product, i.e. Windows 2003.

Some changes should, however, be mentioned here.

An additional partition type is introduced besides the existing types (schema, configuration, domain): the application partition. Replication of this partition type to all the DCs of a domain is no longer mandatory. This means that own partitions can be created for applications from third-party manufacturers in which dynamic data can be increasingly stored. Improved control of this

dynamic data is then possible with a view to replication. The AD-integrated DNS data of the active directory is swapped to such a partition.

Windows 2003 will very probably offer the option of setting up separate LDAP servers without the need to install a DC. Although these LDAP servers (ADAM = Active Directory Application Mode) come with a schema of their own, they subject to the logon services of the AD. In this way, LDAP services can be created for applications without depending on changes in the AD schema.

3.7.5.6 Active directory: minimum configuration

As already discussed, the active directory in its entirety offers a wide range of technologies and functionalities which generally facilitate the rollout of new functions and/or efficient processes in IT landscapes. The dependence on Microsoft products and technologies increases in such a case.

If this is not desired, a Windows 2000 active directory with reduced functionality can be taken as the goal. How such a constellation might look is described in the following.

An active directory with minimum configuration features the following properties and is subject to the following conditions.

The DNS infrastructure is based on an independent implementation rather than Windows 2000, with this independent implementation meeting with the minimum requirements. Manual entering of the SRV records in the DNS may be necessary.

No single forest is created. Trust relationships between domains are implemented in the conventional manner.
The aim being that every former Windows NT domain can administer its own schema in its own forest.

Furthermore, if the domains are not switched to "native mode", the "risk" of reducing the connected, extended groups is reduced.

Furthermore, no OU structure is set up within the domains.
The background: such a structure enables additional functions which might then "nevertheless" be accessed.

The use of group guidelines is restricted to the security settings (such as password (term of validity, minimum length, etc.), privileges (changing the system time, local logon, etc.) audit settings (auditing) in the "default domain policy". These settings are necessary in order to adequately replace the Windows NT settings.
The background: the absence of configuration management of the clients via group guidelines reduces dependence.

An AD-based PKI (Public Key Infrastructure), which would, for example, be necessary for EFS or IPsec, is generally not used.
The background: additional dependence resulting from integrated storage in the AD is avoided.

Use of an AD-based DFS (Distributed File System)
The background: additional dependence resulting from integrated storage in the AD is avoided.

As long as Exchange 2000 is not used, the additional attributes of the user objects remain unused or are limited to the mandatory attributes.
The background: the aim is not to use the AD for storing personal data in order to reduce possible secondary dependence (for example, third-party applications accessing this data via LDAP).

Contact objects in the AD are not used.
The background: the amassing of such information in the AD increases dependence.

There is no publication of printers or releases in the active directory.
The background: users should not get used to finding resources in this manner.

Note**:** The above-mentioned features and actions usually limit the maximum efficiency that can be achieved with an active directory. This is the price of greater independence.

However, the use of sites within the ADS makes sense in order to control the replication process between the individual locations.

However, if Exchange 2000 is used on a domain-spanning basis in a single Exchange organization, the use of a single forest is inevitable because the functions of the Global Catalog were otherwise not available.

3.8   Middleware – COM,.NET, J2EE

The technical discussions show that, although Microsoft's current component technology (COM, DCOM) is continued, a change in technology is taking place at the same time with the .NET Framework. This is opposed by the Java 2 Enterprise Edition (J2EE) as an alternative platform. Fundamental differences between the two platforms which also play key roles in the following discussion of the web services are their platform-independence, the programming languages supported and the number of solution providers. The table below shows the differences in more detail.

Table 16: Comparison of J2EE and .NET

Parameter	J2EE	.NET
General	Industry standard	Product suite
	One language – many suppliers	Many languages – one supplier
Languages	Java	C#, VB, C++, J#, Java and others...
Component model	Enterprise JavaBeans	.NET (Web) Services; COM+
Interpreter	JRE (Java TM Runtime	CLR (Common Language

Technical description of the migration paths

Parameter	J2EE	.NET
	Environment)	Runtime)
Supplier	BEA, IBM, SUN, Oracle...	Microsoft
Operating system	Unix, Windows, Linux, OS/390...	Windows
Browser	Any browser possible, with Java support	Any browser possible
Web server	Any web server possible	MS IIS
Web server components	JSP, servlets	ASP.NET
Database access	JDBC	ADO.NET
Directory service	Any directory service, via JNDI	Active directory

3.8.1 Component Object Model (COM)

Many technologies launched by Microsoft are based on the Component Object Model (COM). Comparable, component-oriented technologies are CORBA (Common Object Request Broker Architecture) from the Object Management Group (OMG) or Java Beans from SUN.

COM is a further development of OLE (Object Linking and Embedding) which was primarily used to create compound documents. COM is a binary standard for components and is hence independent of programming languages. COM can be generated using different programming languages, such as:

C++

C

Java

Visual Basic

Delphi.

At the same time, COM components can be reused with some of these languages. The only requirement for a programming language is that it must be possible to implement pointer structures and to call functions either explicitly or implicitly via pointers. Object-oriented languages offer mechanisms which simplify the implementation of COM components.

The form in which COM components occur most frequently is dll files. Other variants are:

Dynamic Linking Libraries (*.DLL, *.OCX)

Executable Windows files (*.EXE)

Java classes (*.CLASS)

Script files (*.SCT, *.WSC).

With the Distributed COM (DCOM) service, COM offers a transport protocol-neutral middleware for the use of remote components on other computers.

DCOM belongs to the Windows NT standard. The call of components on remote computers is based on Remote Procedure Calls (RPCs). This function hence belongs to ISO/ OSI layer 7 (application layer) and, in theory, can use different transport protocols (such as TCP/ IP, IPX/ SPX) as well as HTTP. The use of HTTP is possible via the COM Internet Services (CIS) of an IIS version 4 in which the DCOM protocol is tunneled by HTTP. The security of DCOM can be administered by the DCOM Configuration Utility (DCOMCNFG.exe) tool. It especially defines which degree of impersonalization is to be used, i.e. the capability of a software routine to change the user context.

The use of COM components is possible under Windows only. Applications accessing the COM components must be adapted for porting to another platform.

The extension of COM and DCOM under Windows 2000 is COM+.

3.8.2   ".NET"

Some central terms frequently used in conjunction with ".NET" should be explained at the beginning. The definitions given by Microsoft at http://www.microsoft.com/germany/ themen/net/glossar.htm will be used here:

.NET:
The Microsoft platform for XML web services which connects information, devices and users in a uniform and personalized manner.

.NET Framework:
An environment for the development, provision and execution of XML web services and other applications. It consists of two main components as follows:

- Common Language Runtime

- Class libraries, such as ASP.NET, ADO .NET and Windows Forms.

.NET My Services:
A user-oriented architecture and a collection of XML services which simplifies the integration of isolated "data islands". The .NET My Services are oriented towards the user rather than a particular device, network or application.

.NET Platform:
Consisting of tools, devices, XML web services, servers and user experience.

The following sections deal with the NET framework primarily as a middleware solution. This somewhat resembles the approach of the Java Virtual Machine (JVM) because the installation of the framework (for example, on Windows 2000) means that the interfaces of the integral parts of the operating system (such as Win32-API) are abstracted and offered in a newly arranged form. This primarily has consequences for the application development. The illustration below gives an overview of the components of the framework.

Technical description of the migration paths
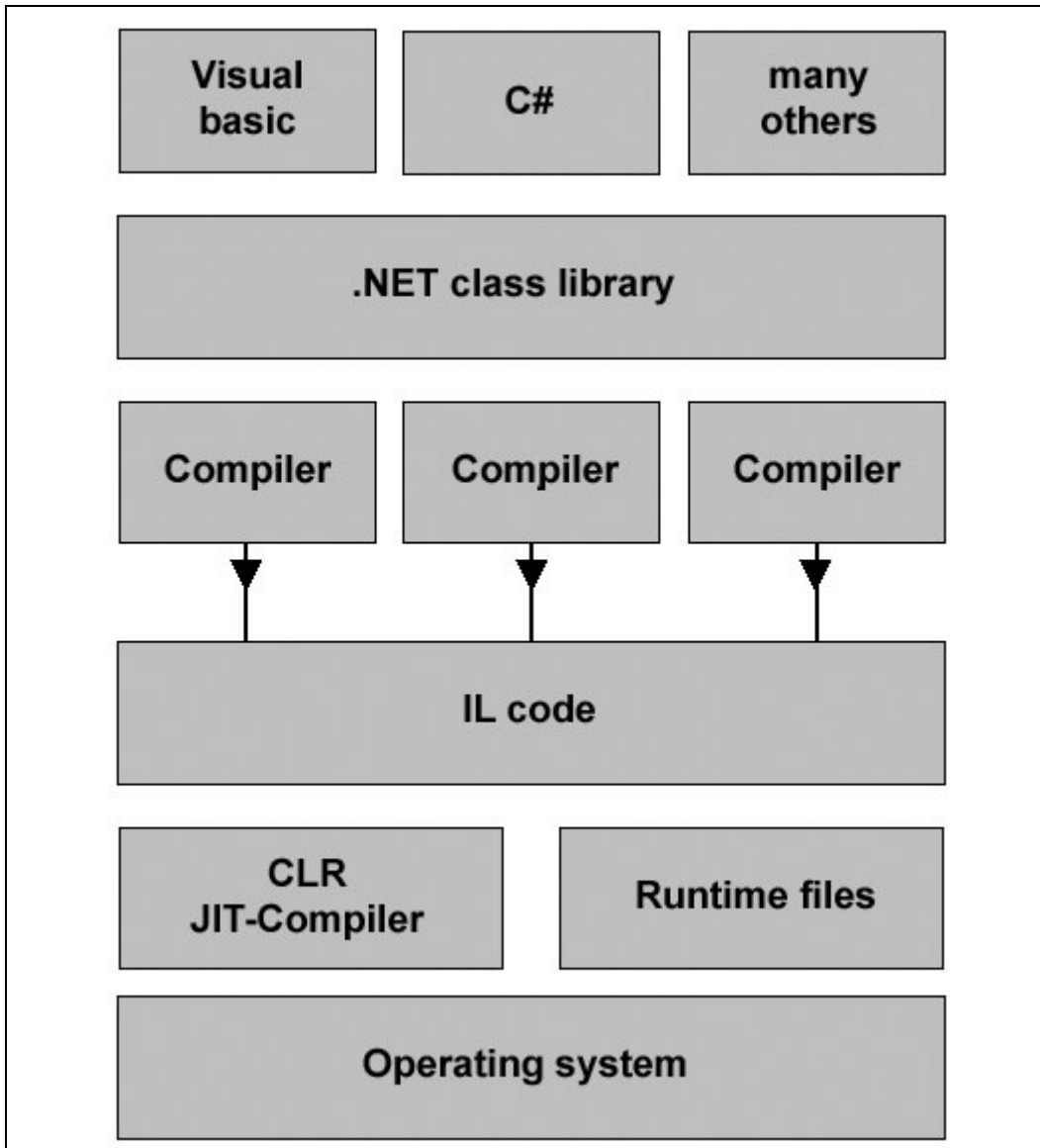
Fig. 25: Components of the .Net framework

The applications are programmed in a language which is supported by ".NET" and have access to the comprehensive ".NET" class libraries. The ".NET" framework supports a large number of programming languages. The compiler translates the source code into a command code (no machine code) which is called intermediate language (IL). The result of this action is, for example, an EXE file. When this EXE file is loaded, the Common Language Runtime (CLR) with its JIT (just-in-time) compiler translates the EXE file into machine code.

Microsoft offers the following tools for creating the source code:

a free Software Developer Kit (SDK) which is already sufficient in order to create ".NET" programs on the one hand, and

Visual Studio.NET, the successor to the former Visual Studio Version 6, on the other.

Unlike Java and the JVM, the .NET Framework can be used for Microsoft operating systems only.

3.8.3 Java 2 Enterprise Edition (J2EE)

The Java 2 Enterprise Edition includes a whole range of middleware services which facilitate the development of applications at the server end. Important components of the J2EE technologies are the following:

Enterprise JavaBeans (EJB)

Enterprise Beans are components at the server end which implement the application logic. The clients can then access the EJBs. Enterprise Beans are installed in an EJB container at the server end. The server provides them with certain services and runtime environments.

Java Naming and Directory Interface (JNDI)

This is a name and directory service which enables, on the one hand, references to remote objects

- to be stored under a defined name and

- to be stored in a defined place (binding).

Furthermore, JNDI enables the finding of bound objects via their names (loopup).

Java IDL / Corba

Java IDL forms an interface with Corba. Java ORBs can be implemented using Java IDL.

Java Remote Method Invocation (RMI) and RMI via IIOP (RMI-IIOP) RMI is used for distributed communication between objects. With RMI-IIOP, J2EE is compatible with CORBA.

Further services are additionally available as follows:

Java Database Connection (JDBC)

Java Message Service (JMS)

Java Servlets / Java Server Pages (JSP)

Java Transaction API (JTA)

Java API for XML (JAXP)

and many more.

Fig. 26: J2EE layer model

 gives a general overview of the layer model of J2EE.
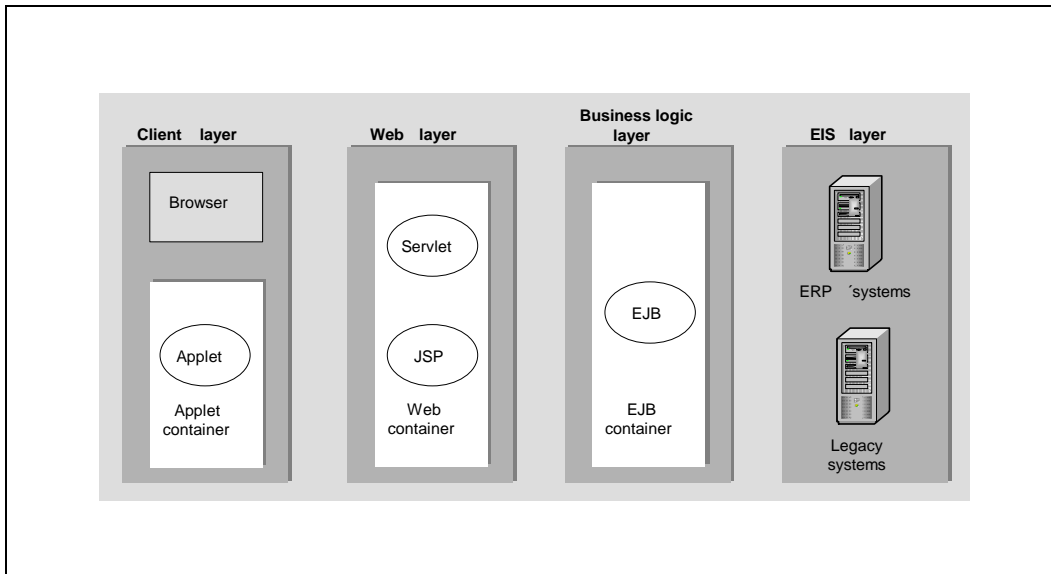
Fig. 26:   J2EE layer model

3.9   Web services

3.9.1   Overview

Web services enable the integration of different platforms and applications in a manufacturer-neutral manner on the basis of standards.

Both the .NET Framework and the J2EE provide an integrated platform for the development and use of web services.

J2EE and .NET are both equally suitable for the development of demanding applications. Other common features are:

    3-tier architecture

    Component orientation, optimized for distributed architectures

    Network orientation

    The Internet as the central infrastructure

    Web browser as the primary user interface, "rich clients" as the secondary user interface

The differences between the two platforms were already outlined in conjunction with the presentation of the .NET Framework.

Due to its higher flexibility and its manufacturer-independence and platform-independence, J2EE is the system of choice. This is also in line with the SAGA[53] recommendations.

---

[53] Standards und Architekturen für E-Government-Anwendungen, Version 1.1, KBSt Publication Series, ISSN 0179-7263, Vol. 56, February 2003, http://www.kbst.bund.de/saga

But what about interoperability between.NET and J2EE? With regard to web services, interoperability should be ensured on condition that all the parties involved adhere to the applicable standards (XML, SOAP, WSDL,UDDI). The only problem in this context is that SOAP in its current version 1.1 still permits too much freedom which can mean that interoperability is lost in practice. However, interoperability must be the aim of web services. This should be better ensured, especially with version 1.2 of SOAP.

3.9.2   Fundamentals

A web service is a service which a client can access via the Internet with a Uniform Resource Locator (URL). The crucial requirement is that the implementation of the service is fully transparent for the client. A web service can be considered as a "black box" with a certain functionality which can be used in a flexible manner without the need to know its implementation details. Web services offer their functionality to the outside world via well-defined interfaces. These interfaces are also called Web Service Contract. Such a contract is described in a language specifically developed for this purpose, i.e. the WebService Description Language (**WSDL**) (being an XML file). Developers can use this as a basis in order to combine the most varied services with each other and to integrate them to form a complete application. These services can be found using **UDDI** (Universal Description Discovery and Integration). UDDI is a standard-based specification for describing and finding web services, i.e. a repository for web services. First implementations have been launched meanwhile by IBM, Microsoft and other manufacturers.

In contrast to the component technologies currently in use, web services do not use an "object-specific" protocol, such as DCOM, IIOP or RMI, because their trouble-free use normally requires a homogenous infrastructure on the client and on the server. Web services are hence based on a different approach. They are based on Internet standards and use the "smallest common denominator", i.e. HTTP and XML (refer to chapter 3.10). A client sends via HTTP a message packed by XML to a server which replies to the query by also sending an XML message. This means that web services are completely independent of particular programming languages and system platforms. As long as both ends agree to a uniform message format and adhere to a jointly defined call sequence, the type of implementation of the service (web service) is only of secondary importance. It can make use of all options of the platform on which it is currently used. **SOAP** is the generalization of this principle. The Simple Object Access Protocol defines how the XML messages must be built up and how the call sequence must look. This means that the most different applications running on different platforms can be combined and integrated into existing solutions via the Internet. The only prerequisite is that the applications use SOAP in order to communicate with each other. SOAP itself can use different protocols (such as HTTP, SMTP). SOAP is a simple, uncomplicated mechanism for exchanging structured and typified information between systems in a decentralized, distributed environment using XML. The disadvantage of SOAP is, however, that it is relatively slow. SOAP

consists of three parts. The SOAP envelope defines a framework for every message. It informs the recipient with regard to what is contained in the message, to whom the message is addressed and whether it is an optional or a mandatory message. This is followed by the encoding rules which define, within the SOAP framework, how data (for example, numbers) are encoded. XML includes encoding rules which feature a high degree of flexibility. SOAP is less flexible because a more limited set of rules is defined, even though this does not play a role.

Web services enable the integration of different platforms and applications in a manufacturer-neutral manner on the basis of standards.

Both the .NET Framework and the J2EE provide an integrated platform for the development and use of web services.

3.9.3 .Net web services

.NET Framework (refer to chapter 3.8.2) supports the development of professional web services. This chiefly concerns a re-edition of Windows DNA (Distributed interNet Applications Architecture).

NET includes its own service layer for web services. The illustration below (Fig. 27: Microsoft .NET Framework

) shows the interaction between the individual modules with regard to the web services.
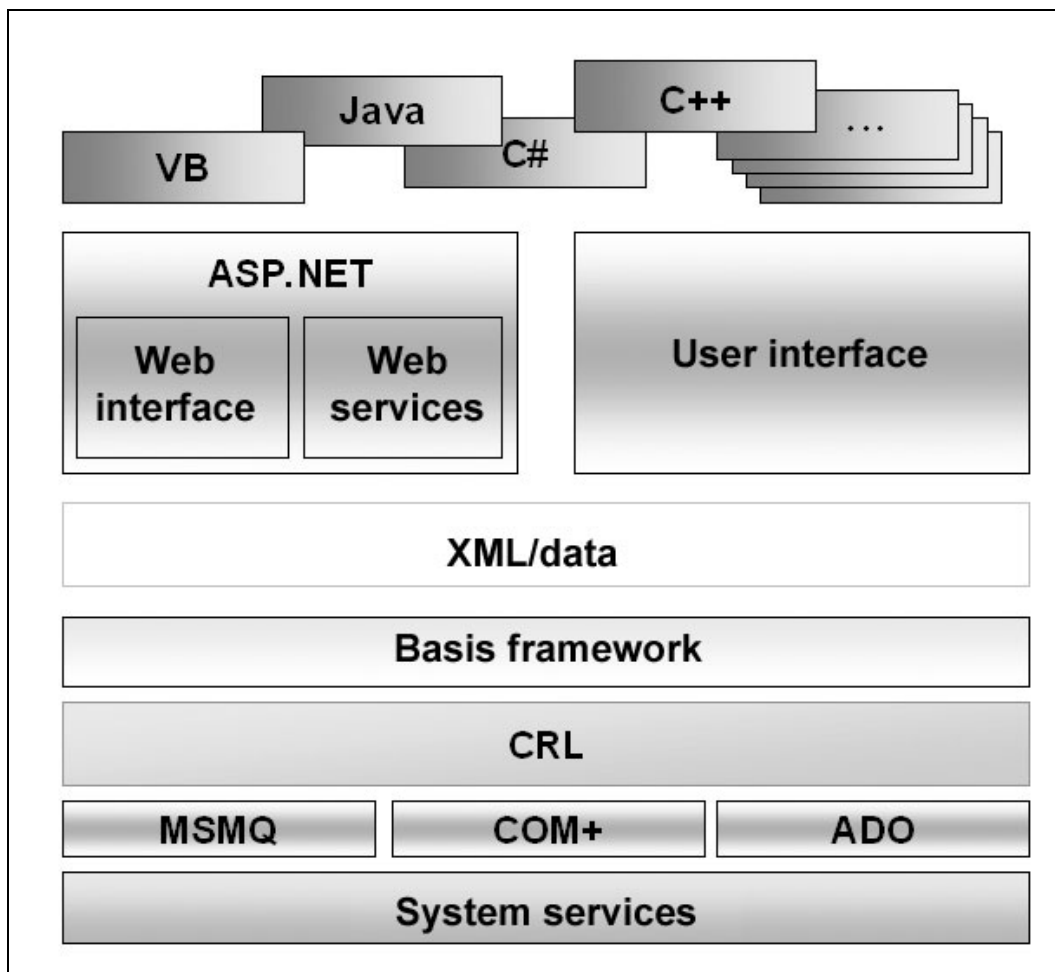
Fig. 27: Microsoft .NET Framework

The introduction of ASP.NET, as the successor to the Active Server Pages, corresponds to the goals of

implementing a development environment which should be as simple and variable as possible

the web services discussed in the foregoing.

On the other hand, Visual Studio.NET offers a relatively simple way of writing (client) applications that use web services on the basis of XML and SOAP.

The Internet Information Server (IIS) (refer to chapter 3.11) is at the heart of the web services under Windows.

3.9.4 J2EE

The J2EE architecture (refer to chapter 3.8.3) is based on the Java programming language. Java offers the advantage that programs written in Java can be used in a platform-independent manner. J2EE was originally developed as an architecture for applications at the server end. The platform was amended by adding support for XML-based web services.

The business logic layer which is implemented with EJB (Enterprise Java Beans) components covers the business processes and the data logic. It ensures connection to databases using JDBC (Java Database Connectivity) and can also access external web services. Access to J2EE applications can, on the one hand, take place using web service technologies, with web service queries being handled by servlets. On the other hand, conventional clients, such as applets or applications, can access EJB components directly and parallel to this in the usual manner. Web browsers and wireless devices are usually connected via Java Server Pages (JSP) to EJB components.

Development environments are offered by different suppliers, including, but not limited to, IBM, SUN and BEA.

3.10 XML (Extensible Markup Language)

XML is considered to be the new universal solution for the presentation of data and data interchange format. XML is not a binary format, but is stored in the form of printable strings. XML offers the following advantages compared to HTML (Hypertext Markup Language):

XML separates the structure of a document from the presentation. XML does not include any formatting commands. Formatting must be defined in XML by a Style Sheet.

XML enables the definition of any kinds of structures through its own elements and attributes.

The validity of the structure can be checked by an XML parser against a structure definition.

XML expects a so-called "wellformedness" which is expressed in rules, such as: "upper case and lower case are distinguished in element names".

XML documents include special elements, the so-called processing instructions (PIs), in which statements and instructions for the XML parser can be stored (such as style sheets).

Structure definitions define the valid structures of XML documents. These are also called "vocabulary". These structure definitions can be implemented by Document Type Definition (DTD) or XML schemas.

A namespace can be defined as XML namespace in order to ensure the unambiguous definition of element names.

XSL (Extensible Style Sheet Language) is an XML-based language for the transformation of XML documents to HTML or other XML documents. The XSL transformation is carried out by an XSL processor.

XML already plays an important role today and, in future, will play an even more important role as a data interchange format and will thus also form an important element of future office applications (including the Office packages already available). Especially due to the separation of data and presentation, XML enables the platform-independent presentation of all conceivable kinds of data and, above all, the editing of data (and document contents) across system

boundaries without users having to worry about the presentation. This will in future mean substantial relief in common work on documents and data and a significant increase in productivity in the creation of documents. Today, users of Office packages still spend a considerable part of their work on bringing the documents into the appropriate shape. This work requires design and layout skills which users typically do not have. The consequence is that more time is spent on design and layout than on the administration officer's real work. Thanks to the separation of contents and presentation, administration officers can once again focus on their real job and use their working time for productive work. The presentation of contents can be left to those who are responsible for laying down uniform and central requirements for all users.

XML is also flexible enough to be adapted to new situations at any time.

According to SAGA, XML is to serve as the universal and primary standard for the interchange of data between all information systems relevant for administration purposes[54]. "New systems to be installed should be capable of interchanging data using XML. Existing systems do not necessarily have to be XML-enabled"[55].

In this respect too, Microsoft and Sun are in agreement: XML is the basis for intelligent web services.

3.11 Web servers

3.11.1 Overview

With a view to web server migration, the Apache web server constitutes an alternative to the upgraded Microsoft products with the Internet Information Server 5.0 and 6.0.

No general technical restrictions have been reported concerning the use of the Apache web server which offers all the functionalities needed for use in a productive environment. Apache has already demonstrated this suitability for use in a large number of practical application scenarios.

However, the effort necessary to migrate a project must be determined in detail from case to case. In the case of migration of simple HTML pages and CGI applications, the migration effort will usually remain within reasonable limits.

In contrast to this, migration of complex applications, especially for generating dynamic contents on the basis of ASP technology, usually requires the re-implementation of applications which means an increased effort. However, there are no problems whatsoever that forbid this from a technical point of view because sufficient alternative technologies, such as PHP and JSP, are available.

---

[54] Standards und Architekturen für E-Government-Anwendungen, Version 1.1, KBSt Publication Series, ISSN 0179-7263, Vol. 56, February 2003, http://www.kbst.bund.de/saga

[55] Standards und Architekturen für E-Government-Anwendungen, Version 1.1, KBSt Publication Series, ISSN 0179-7263, Vol. 56, February 2003, http://www.kbst.bund.de/saga

3.11.2   Introduction

The best-known Internet service is the World Wide Web (WWW). The WWW is a classic client/sever application where the client passively receives information from the server. The World Wide Web is based on the status-less HTTP (Hypertext Transfer Protocol) protocol and the HTML (Hypertext Markup Language) page description language. The server answers requests from the clients and supplies the desired contents. Web servers have the additional task of sending contents generated dynamically, for example, by a database application, to the client systems. Certain interfaces also enable the starting of complete programs on the servers and the execution of actions. The actions are usually initialized by the client systems. This enables the client to trigger certain processes on a server. The propagation of the Internet and of intranet solutions led to an increase in demands on and tasks of web servers, so that different solutions and programs were developed.

3.11.3   Internet Information Server 4.0

The Microsoft Internet Information Server (IIS) is a file and application server for the Internet and for intranet applications. IIS 4.0 is part of the Windows NT Server 4.0 Option Pack. OIIS provides the basic functionalities of a web server on the basis of the Windows NT 4.0 operating system.

The successful interaction between the client and server ends is ensured by support of all relevant Internet protocol services, i.e.:

HTTP 1.1

SMTP

NNTP

FTP.

The HTTP support of ISS 4.0 includes the following features:

Pipelining
This feature enables the sending of many client requests before the web server responds.

Keep Alives
By keeping client/sever connections alive, a client can use a single connection or at least a smaller number of connections for several requests.

HTTP PUT and DELETE
This feature enables the deleting or supply of data by users via a browser. The RFC 1867 support also enables the control of file uploads via other programs.

SMTP support is provided by an implemented SMTP mail service which can send and receive SMTP mail messages. This service can be used for communication between the web server and the customer, for example.

The integrated NNTP (Network News Transport Protocol) service enables the setting up of local discussion groups on a single server. Support of newsfeed or replication is not possible.

3.11.3.1 Web applications

The Internet Information Server offers the following extensions for the server:

CGI programs

ISAPI applications

ASP applications

The Common Gateway Interface (CGI) is one way to generate dynamic contents. The CGI is an interface for calling programs which the server can use. CGI was originally developed for UNIX environments and requires a significant share of system resources under Windows NT. The advantage of CGI programs is that they can be executed by almost every web server and that they are usually easy to program.

The Internet Service Application Programming Interface (ISAPI) is a direct interface with IIS. Server objects can be accessed via ISAPI.

IIS 4.0 enables the creation of dynamic HTML pages or web applications via the use of Active Server Pages (ASP). The ASP technology provides a script environment at the server end. ASP pages are files which can contain conventional HTML tags as well as script commands. The related script commands are executed on the server and are used to generate HTML code. The dynamic and static HTML code is returned to the requesting browser in the form of an HTML page. The use of ASP pages enables the design of interactive contents for users. Database access can also be implemented using the ASP pages.

IIS 4.0 supports the following technologies in conjunction with the development of web contents:

Microsoft Script Debugger
Enables testing of ASP applications.

COM programming interface
Gives developers access to the COM components which access the protocol functions of the ISS.

Java Virtual Machine
Enables the creation and execution of Java components within a virtual machine.

IIS Admin objects
Give developers access to the components needed to create administration utilities.

Transactional ASP pages
Enable ASP pages and their components called to be part of a transaction

---

which must, however, be administered by the Microsoft Transaction Server (refer also to chapter 3.11.3.3).

Process isolation

This enables ASP and ISAPI applications (Internet Server-API) to be executed in separate processes. The processes are executed parallel to the server main process.

Loading and unloading of components

This means that web developers can dynamically load or unload components of a web application.

3.11.3.2 Authentication and security

The security model is the same for all NT server components. The same functions which are available to the file or database servers can also be used for the ISS. The existing domain users and groups can be used to assign tailored privileges and authorization. The IIS uses the same directory database as the other Windows NT servers. Users can be given restricted access to the network resources, such as HTML pages, web applications and files. The file system privileges of the NTFS can also be used for the fine-grained assignment of privileges.

The use of the Secure Sockets Layer (SSL) enables a method for the secure interchange of information between clients and server. It is also possible that the server checks or authenticates the client's identity and that the user does not need to logon at the server.

The integrated Certificate Server permits the establishment of a certification instance and the provision of the X.509 standard certification for clients.

3.11.3.3 Additional components of the Internet Information Server

Besides the core component of the IIS, Microsoft offers various components for extending the web server functionalities. The components described in the following also form part of the Windows NT Option Pack.

Microsoft Transaction Server (MTS)

The MTS is a transaction processing system for the development, implementation and administration of distributed server applications. Transaction processing can, for example, be used to implement distributed business applications.

Microsoft Script Debugger

The Microsoft Script Debugger is designed to support the identification of bugs in ASP files. The debugger can be executed in conjunction with the Internet Explorer and can be used for debugging.

Microsoft Index Server

The Index Server can be used as a search engine for Internet and/or intranet contents. The server can index the text contents of the contents stored which can

then be browsed by users using web forms. Besides pure HTML documents, the Index Server can also index Microsoft Word and Excel documents.

Microsoft Message Queue Server

The Microsoft Message Queue Server (MMQS) enables application programs to communicate asynchronously with other application programs by sending and receiving messages.

Microsoft Management Console

The Microsoft Management Console (MMC) enables the administration of the most varied tasks by different network administration programs. Administration of the servers is enabled by so-called "snap-ins" within the console.

3.11.4 Replacing migration

3.11.4.1 Apache

The Apache web server is an application which is widely used in practice on Linux-based systems. Accounting for more than 60% of the products installed, Apache is the most frequently used web server[56] world-wide. It is freely available subject to the Apache software license. The Apache web server is one of the most successful projects of the Open Source Community. The project was developed on the basis of the NCSA (National Center for Supercomputing Application, University of Illinois) server to which ever-growing numbers of patches were added ("A patchy web server") and which served as the basis for the first beta version in 1995. By now, it has been ported to almost all platforms. The Apache server is today the most commonly used web server on Linux/UNIX platforms, but it also runs on a whole range of other platforms, including, for example, Windows NT or Novell Netware.

Since version 2.0.35 from April 2002, the development series 2.0 of the Apache web server has been released as stable, and is also recommended by developers for productive use. Development series 1.3.x is currently being updated parallel to the new 2.0.x series, with version 1.3.27 as the latest version available.

Pursuant to the terms and conditions of its license and thanks to its high quality, the Apache web server is also used in commercial products. IBM, for example, supplies Apache as part of the Websphere product.

Functionality

The Apache web server consists of its kernel and a large number of modules which can be compiled and/or loaded as required for the specific applications. Thanks to its modular design, the Apache server can be easily upgraded and adapted to changing requirements. The standard software delivery already includes a large number of different modules which can be supplemented by further modules (own developments, for example). Apache modules are code

---

[56] http://news.netcraft.com/archives/2003/03/

segments which correspond to the Apachi API specification and which can be loaded into the Apache web server. Apache modules can be either statically permanently linked or loaded dynamically via the configuration file of the web server. This modular design enables the upgrading of web server functionalities and increases the flexibility of the system significantly. The efficiency and speed of the web server is increased if internal processes can be executed instead of external applications.

The many modules include authentication, security as well as interpreter modules for programming languages, such as PHP, Java, Python, Tcl and Perl. Two different options exist for the use of the modules:

In the case of the static compilation of the web servers, the modules can be statically linked.

The modules can be loaded dynamically during operation of the server. This so-called DSO (Dynamic Shared Objects) functionality eliminates the need for re-compilation in the case of a change in server configuration. A server restart is sufficient, with a graceful restart being possible without interrupting service.

Since no modules other than those actually needed are used, Apache is smaller than a standard version and requires less memory capacity. At the same time, fewer modules also mean less exposure, so that the security of the system is improved.

The table below shows a small selection of the modules available.

Table 17: Apache modules

Module	Function
Standard and additional modules	
mod_cgi	Execution of CGI (Common Gateway Interface) scripts.
mod_dav	Integrated DAV support (HTTP Extensions for Distributed Authoring – WebDAV). Editing files and directories directly via HTTP on the web server. DAV means "Distributed Authoring and Versioning".
mod_fastcgi	Integrated FastCGI support.
mod_frontpage	Integrated FrontPage support.
mod_iserv	Integrated Java servlet support.
mod_php3	Integrated PHP 3 support.
mod_php4	Integrated PHP 4 support.
mod_perl	Integrated Perl support.
mod_alias	Provides the alias and/or redirect statements.
mod_autoindex	Generates directory indexes.
mod_include	Required for Server-Sides Includes.
mod_mime	Ensures the generation of the corresponding MIME headers.
mod_log_config	For keeping one or more log files, with the possibility to adapt the contents to the corresponding requirements.
mod_deflate	Serves for compressing different file types prior to transfer to the browser. This is particularly useful in the case of limited bandwidth. The compression function must be supported by the browsers.

Module	Function
mod_proxy	Adds the functionality of a proxy and/or proxy cache to the Apache web server.
mod_rewrite	Enables the use of internal aliases and external redirects.
mod_speling	Corrects the users' typographic errors.
mod_ssl	Makes the SSL (Secure Sockets Layer) and TLS (Transport Layer Security) protocols available.
mod_usertrack	HTTP cookies are used to log user behavior.
mod_vhost_alias	Interesting for the bulk configuration of virtual hosts, especially for service providers.
Authentication modules	
mod_access	Access control on the basis of host names or IP addresses.
mod_auth	For configuring password-protected directories and documents. A very simple variant of an authentication module which should be used by a small number of users only.
mod_auth_digest	User authentication by MD5 Digest Authentication, with the passwords not being transmitted as plain text.
mod_auth-dbm	User authentication by Berkeley DB files, suitable for a larger number of users.
mod_auth_ldap	User authentication by LDAP.
mod_auth_kerb	User authentication by Kerberos, supports versions 4 and 5.
mod_auth_notes	User authentication by Lotus Notes Server.
mod_auth_oracle	User authentication by Oracle database; further modules are additionally available, for example, for MySQL and Postgres databases.
mod_auth_smb	User authentication by SMB server (Samba, Windows NT).

This list of modules available is not exhaustive. Instead, it is designed to show just some of the possibilities of the Apache web server.

However, not all the modules for the web server are free. More and more commercial companies offer native Apache modules. Some examples are:

Allaire with the Macromedia JRun Java servlet engine and the Macromedia ColdFusion application server

Sun Microsystems with its Active Server Pages module.

Related issues

The Apache web server can be supplemented by a program which enables the integration of a search functionality with a website. Different software units are available with the HTDig[57] search system being described in the following as an example of such units. HTDig permits indexing of complete websites. The lprogram uses a so-called robot in order to generate a search index which can be browsed by a suitable CGI script. The core functionalities of the software are outlined in the following points.

---

[57] http://www.htdig.org/

Generation of a search engine index (for one or more websites and/or for parts of a website)

Use of filters in order to limit the indexing function. Possible filter criteria are file types and specific URLs.

External additional programs can be used in order to index file formats (PDF, DOC, etc.).

Numerous query options exist, and different search algorithms can be used (words, word parts, synonyms, etc.).

The search page and the corresponding hit list can be adjusted using simple template files.

Umlauted vowels in the search strings are supported.

The robot used supports the standard for "Robot Exclusion" and the "Basic WWW Authentication" for indexing protected contents.

The HTDig distribution is subject to the GNU General Public License (GPL) and is hence freely available.

Administration

The configuration of the installed Apache is relatively simple because most configurations just require entries to be edited or added in a well-documented file. This is a simple text file which can be edited using any text editor. Some commercial and non-commercial projects related to the Apache GUI[58] exist already for administrators who prefer a graphic user interface.

Migration

The data and/or contents to be migrated must be discriminated within the scope of a migration project. Differentiation is possible in terms of:

HTML files

CGI programs (Perl, PHP, C, etc.)

Program modules using the ISAPI (Internet Server Application Programming Interface) of the Internet Information Server

Active Server Pages

HTML pages

Static contents, i.e. pure HTML pages, can be exported to the new web server without further adaptation, and are likely to cause the least number of problems and effort in conjunction with a change in web server.

Common Gateway Interface

Programs which were developed for the Common Gateway Interface (CGI) also use the specific CGI standard. This standard defines the way in which programs and web servers interact. This standard is not language-specific and is supported

---

[58] s.a. http://gui.apache.org/

by the Apache web server. Numerous options are available for the development of CGI programs. Perl is one of the most widely disseminated and most portable script languages. Perl is available on MS-DOS, UNIX/ Linux, OS/ 2, Macintosh and any Windows variant, to mention but a few. Perl also offers web developers a host of options for text and data manipulation. Applications which were developed in Perl can be very easily migrated to Apache. Apache includes the "mod_perl" module which represents the full Perl implementation. Furthermore, execution performance can also be achieved in many cases. The Perl modules embeds a Perl interpreter into the Apache web server, so that it is no longer necessary to start a separate process in order to execute the program code. Furthermore, speed can be increased tremendously. Porting of the Perl applications requires only minimum changes in program code.

PHP is one of the fastest-disseminating script languages, featuring a very good support of different database systems and a relatively simple syntax. PHP, like Perl, runs on many different systems. PHP applications which were developed for the Internet Information Server can be ported to the Apache web server with minimum effort.

ISAPI

Applications which use ISAPI can only remain in use in conjunction with Apache web servers if these are run on a system based on Windows NT or 2000. Apache includes full ISAPI compatibility as a standard functionality under Windows systems. The applications only have to be re-compiled in the new Apache environment. This means that no change in code is normally necessary. However, the ISAPI filters and the Microsoft extensions for asynchronous file operations are not supported.

ASP

Applications which are based on the ASP technology were normally designed for generating dynamic web contents. Different bases can be used, such as:

Visual Basic Script (VBScript)

JScript

and ActiveX Data Objects (ADO) for access to databases,

In order to execute ASP pages on the Apache web server, the complete Microsoft-compatible development environment (VBScript, JScript, ADO) is required. Sun Microsystems offers its "Sun One Active Server Pages 4.0" product[59] as a compatible environment for executing ASP pages within the Apache web server. The web server can run on an NT operating system and on a UNIX/Linux operating system as well.

The product supports:

ASP 3.0

VBScript 5.5

---

[59] Refer also to http://sun.de/Produkte/software/chilisoft/

JScript 5.5.

Migration to an Apache web server on a Linux system requires all the ASP files to be copied to the new target platform as the first step. In another step, the COM objects used within the ASP application must be identified and reconciled with the objects supported under Linux. Numerous objects are supported by Sun One ASP. If a necessary object is not supported, the COM-to-Java Bridge supplied can be used in order to implement the functionality using Java. Furthermore, changes with regard to the upper-case and lower-case notation must be checked under the ASP and/or Scripting Engine version. A detailed description is given in the related documentation. The issue of the necessary database migration is not discussed in this section. The "Databases" chapter contains detailed information.

Besides the option to leave the ASP applications unchanged in their existing form, the use of alternative technologies is, of course, also possible. This approach should be adopted if a higher degree of platform independence is a significant requirement. This will, however, require an increased migration effort because the implementation of applications in a new technology usually requires increased efforts. However, the migration process can also be used to consolidate and optimize contents and applications.

The use of the PHP technology can be a real alternative for many applications. Especially the combination of

Linux

Apache

MySQL

PHP

in recent years led to the development of a very popular platform (LAMP) for generating web contents. If conversion of the ASP applications to PHP is required, a look at the contents of the "ASP-to-PHP"[60] project may be helpful. The project offers an ASP-to-PHP converter on its homepage and offers support within the scope of its mailing list.

Besides this option, the use of Java-based technology can also be considered. Java-based web applications are an interesting alternative to web applications based on ASP. The at-present most commonly used Java applications are based on the Java 2 Standard Edition (J2SE) and Java 2 Enterprise Edition (J2EE) specifications by Sun Microsystems. The Java technology is based on an industry standard and offers the advantage of platform independence. J2SE web applications enable the development of dynamic contents using Java Server Pages (JSP) and Java servlets. Both technologies enable, for example, the development of personalized contents and access to external data sources. The Open Source Product "Tomcat"[61] can be used to execute the JSP pages and

---

[60] http://asp2php.naken.cc

[61] http://jakarta.apache.org/tomcat/index.html

servlets. The Tomcat project was developed in the context of the Apache Software Foundation (ASF). Tomcat offers a scalable execution environment for JSP pages and Java servlets and thus represents a very good alternative to ASP solutions in the case of applications that do not contain a complex business logic. Tomcat version 4.x supports the servlet 2.3 and the JSP 1.2 specification.

The standards of the Java 2 Enterprise Edition can be used for complex application scenarios which require extended functionalities. So-called Enterprise Java Beans (EJBs) enable the implementation of applications for complex business processes and rules which require simultaneous access to external systems. The J2EE environment needs an application server which executes the EJBs. The application server must be enabled to ensure the session management for the user. Furthermore, it must offer suitable interfaces with external applications and it must ensure the high degree of availability required (cluster, load-balancing, failover). Besides familiar, commercial products – such as IBM Websphere, BEA Weblogic, Oracle Application Server and several others – it is also possible to use an Open Source product. The "JBoss"[62] project offers a complete Java application server on an Open Source basis. The application server supports the J2EE specification. It comes with an integrated web server, a JSP and servlet engine, and it supports Enterprise Java Beans, as well as clustering and many other functionalities.

Detailed descriptions of the procedures for migrating ASP applications to Java-based technologies are also offered, for example, by SUN[63] and Oracle[64] so that no such description needs to be given at this point.

3.11.5   Continuing migration

3.11.5.1   Internet Information Server 5.0

New features

The Internet Information Server forms an integral part of the Windows 2000 Server. Its successor version, i.e. Internet Information Server 4.0, comes with several new functionalities. The most important of these new features are compiled in the table below.

Table 18: Extended functionalities of Internet Information Server 5.0

Function	Description
Data supply	
WebDAV	Support of the WebDAV standards for the joint editing of files and directories directly via HTTP on the web server.

---

[62] http://www.jboss.org

[63] http://developer.iplanet.com/docs/migration/webserver/IIS_50.pdf

[64] http://otn.oracle.com/tech/migration/asp/content.html

Technical description of the migration paths

Function	Description
Web directories	Support of web directories which serve users as conventional file directories on the web server and which are directly related to the WebDAV functionality.
Frontpage support	Enables development and administration of web contents using Microsoft Frontpage. The administrator can use the graphic frontend in order to create and edit web contents on the web server.
Support of multiple websites	Enables the hosting of multiple websites on one server and one IP address.
HTTP 1.1 compression	Enables HTTP compression during communication between the web server and the client system with compression capability. This feature is particularly helpful in the case of limited bandwidth.
PICS Rating	"Platform for Internet Content Selection"[65]-Rating is a technical standard for the use of a rating system for web contents of the W3 consortium. PICS enables the rating of contents and the filtering of websites according to certain features. This is achieved by adding a PICS code to the HTML header of a document which is not visible in the browser.
Web-based applications	
XML integration	An XML parser in Windows 2000 is implemented as a COM component and offers a complete XML basis for applications.
Windows script components	Developers can use the scripting technology in order to develop reusable COM modules for web applications.
Determination of the browser properties	The exact browser properties of the client systems can be determined using ASP.
Process isolation	The administrator can isolate individual application processes from the kernel processes and other application processes.
ADSI 2.0	Enables access to the objects, properties and methods of the active directory service interface. The integration of the web server and of the active directory enables the assignment of different websites on one web server to particular user domains.
Administration	
Management Delegation	Enables the delegation of management tasks.
Process Throttling	Enables the limitation of CPU time for a network application or website. This feature can be used to ensure that CPU time is available to other websites or non-web applications too.
DFS	The Distributed File System is a file system which enables the transparent distribution of files to multiple computers. This feature can be used for the document root as the place where the web contents are stored in the file system.
Authentication and security	
Kerberos	User identification is possible via Kerberos, whilst the old Windows logon using the Windows LAN Manager (NTLM) still remains possible.

---

[65] http://www.w3.org/PICS/

Function	Description
Encryption	Use of SSL 3.0 and TLS (Transport Layer Security) for encrypted data transmission.
Digest Authentication	Enables encrypted password transmission for authentication.
IP and domain restrictions	The administrator can permit and/or prohibit access to contents for computers and domains.
Certificates	Support of client and server certificates.

3.11.5.2 Internet Information Server 6.0

Windows Server 2003 comes with Internet Information Server 6.0 (IIS 6.0) which is, for the first time, fully disabled in the standard installation and not automatically integrated into the system. The administrator must explicitly initialize the installation process and activate certain server functionalities.

Of the combination of the following technologies of the Windows 2003 Server product group:

Internet Information Server 6.0

ASP.NET

ASP

COM+

Microsoft Message Queuing (MSMQ)

the possibilities of an application server will be offered in future.

Several new features were implemented for this new role as an Internet Information Server. These new features are briefly outlined in the following.

Changes were implemented within the processing architecture in order to improve reliability and scalability. This enables the automatic detection of errors and the restarting of processes when necessary. Parallel to this, the web server can receive incoming requests in a queue. IIS 6.0 is capable of monitoring the status of work processes, applications and websites. Furthermore, a new kernel mode driver was introduced with Windows 2003 Server designed to optimize the data throughput of the web server.

The IIS 6.0 can be integrated into the authorization framework of the Windows 2003 server. Furthermore, the authorization manager can be used for delegation and authorization actions. Administration of the IIS 6.0 is now implemented on an XML meta basis, enabling administrators to directly edit the configuration.

Another new feature is the integration of ASP.NET and IIS, which offers developers extended functionalities of the .NET Framework for creating applications. The Unicode standard can be used by developers and users in the interest of internationalization.

3.12   SharePoint Portal Server

3.12.1   Overview

This migration guide does not discuss the Share Point Portal Server under aspects of concrete migration. The system is primarily studied with a view to future use. One can conclude that the analysis of requirements clearly suggests that the SharePoint Portal Server may well be considered within the scope of a comprehensive concept for a portal solution or a document management solution.

3.12.2   Introduction

With the SharePoint Portal Server, Microsoft offers a platform for creating web portals with the following main functionalities:

Search

Document management

Group work

Microsoft has thus developed a product designed to fulfill the classic tasks of a company-wide intranet portal. The SharePoint Portal Server is strongly integrated into the desktop applications (Windows Explorer, Office applications, browser) for creating and administering company-wide contents. The SharePoint Portal Server constitutes a portal solution with integrated workflow and search functionalities.

Minimum system requirements are Microsoft Windows 2000 Server or Advanced Server as well as Internet Information Service 5.0 and the Simple Mail Transfer Protocol services. The active directory service is not mandatory for the SharePoint Portal Server. The server can be installed in a Windows NT or in an active directory domain.

SharePoint Portal Server 2001 is based on Microsoft's WebStorage system database. Administration of the server is carried out via the Microsoft Management Console (MMC). Work areas, security roles, timeout times and protocol settings can be determined here, to mention but a few. SSL encryption can be activated in order to enable the secure exchange of data via the Internet/extranet.

The SharePoint Portal Server is discussed and described in this context in order to underline the individual aspects relevant for portal design.

3.12.3   Dashboard site

When the SharePoint Portal Server is installed, a web portal called the "dashboard site" is automatically generated. The following functions can be made available to users of the web portal:

Search functionalities

Subscribing to new or modified contents

Checking documents in and out, including versioning

Publication of documents

The dashboard site uses Microsoft's Digital Dashboard technology in order to organize and display the information. A digital dashboard consists of so-called web parts which can represent information from external and internal sources within the portal. Other SharePoint Portal Server work areas, intranet or Internet sites, hierarchies of public folders of Microsoft Exchange 2000 and Exchange Server 5.5, Lotus Notes databases, local file systems and network file servers can be added to the external content sources. Web parts can be developed by users themselves or obtained from third-party manufacturers. However, standard web parts are also available, for example, for integrating Outlook incoming and outgoing mail, calendars and appointments. Web parts from third-party suppliers can be integrated in order to access further information systems (SAP, CAD system, archive system, etc.) via the portal.

Information and documents can be assigned to specific categories within the portal. These categories, for their part, can also be given a hierarchical structure.

Within the digital dashboard, every user can control the arrangement and presentation of the web parts. The dashboard site can be accessed by a web browser, such as Microsoft Internet Explorer or Netscape Navigator. Microsoft JScript or Netscape JavaScript must be activated in the browser as a precondition for the dashboard site to work.
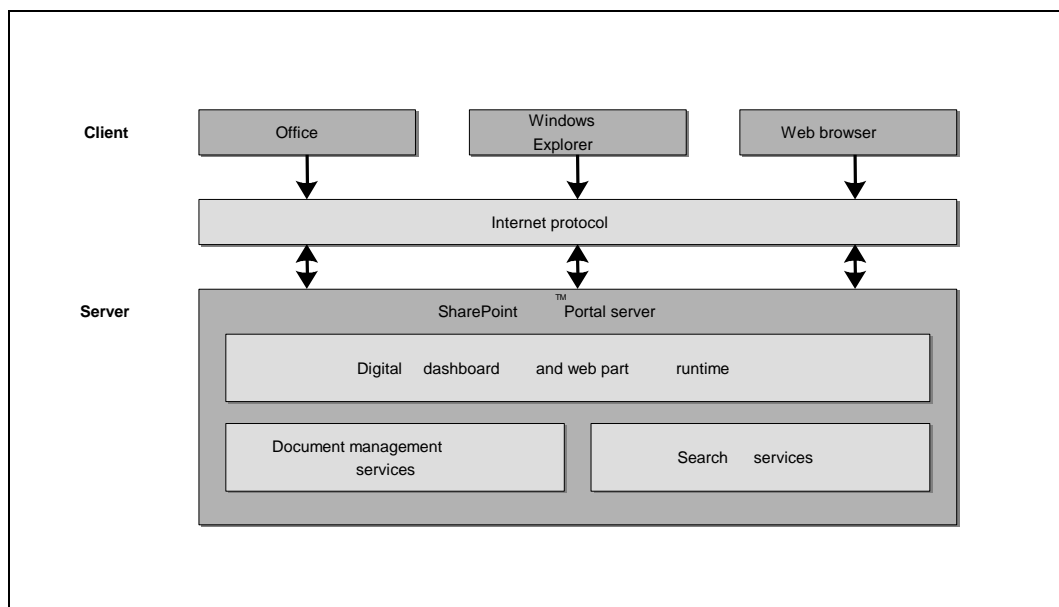
Fig. 28:   Architecture of the SharePoint Portal Server[66]

---

[66] Source: Einführung in Microsoft SharePoint Portal Server 2001 – Whitepaper März 2001

3.12.4   Document management system (DMS)

The integrated DMS functionalities represent another important module of the SharePoint Portal Server. The following standard functions are offered:

Document management

Version management

Authorization workflow

Checking in and out

Document profiles and document publication

Subscriptions

The document processing and management functionality (checking in and out) is fully integrated into the Microsoft Office suite. The SharePoint Portal Server also enables hierarchical document filing. The hierarchy is represented in the browser-based portal on the one hand and using so-called web folders via the Windows Explorer on the other. The so-called authorization propagation for new document versions is also supported. The version is not published until it has been checked and released.

3.12.5   Search functions

The SharePoint Portal Server offers a search function for the entirety of the information and documents in the portal. Different knowledge bases (internal and external content sources) can be covered by a search engine index and made available to users for full-text search. Users are also offered attribute search options (document profiles). The hit list displayed to a user contains only those documents which the user is also authorized to access.

So-called IFilters (index filters) are used for document indexing. When a document is checked in or when external content sources are added, the server automatically identifies the document type and starts the appropriate IFilter. The filters then ensure extraction of the document contents which are then added to the full-text index accordingly. IFilters are currently available for DOC, XLS, XML, RTF, PDF, MP3 and ZIP.

3.12.6   Conclusions

A comprehensive analysis of the ACTUAL and TARGET situation must be carried out in advance before an efficient, company-wide intranet platform is introduced. A precise and detailed concept is vital for the establishment of a company and/or staff portal. Portals must be adapted to the needs of the employees and the company in order to become a successful, new platform.

The requirements can usually be met by suitable portal solutions (including content management and document management solutions). However, one should not expect that the solutions – including the SharePoint Portal Server – are out-of-the-box solutions. All systems must be adapted to the previously defined requirements in a more or less complex process. Depending on the

desired outcome, extensive programming work may become necessary. A high degree of competence in analyzing and designing business processes is required for the introduction of the SharePoint Portals Server and for the introduction of complex DMS, archive and workflow solutions.

The SharePoint Portal Server may well be considered one possible solution depending on the results of an in-depth analysis of requirements.

3.13   Databases

3.13.1   Overview

The technical discussions related to database migration show that, besides MS SQL Server 2000 as a continuing Microsoft product, adequate OSS solutions are clearly available as alternative solutions which justify replacing migration. Important representatives of such OSS are MySQL, PostgreSQL, Firebird and SAP DB. Moreover, commercial products, such as Oracle and DB2, which are also available and already in use at many public agencies are not included in the technical discussions in this guide.

The OSS mentioned offer different functionalities, and their suitability must be analyzed from case to case against the background of the different requirements.

It must be noted that all OSS solutions mentioned here are platform-independent and that there are also Windows versions ready for installation which can be downloaded from the Internet. This means that these database systems can also be used in cases of selective migration.

3.13.2   Introduction

Database systems are used to keep, manage and store large amounts of data. Database systems store coherent data elements in one form and/or in grouped data records. Defined relationships can exist between the structures and groups. The use of a well-planned and structured database can help avoid redundant data elements.

The data from a database system is usually not directly made available to users. Access is more inclined to place via an application that accesses the data and offers it to users in an appropriate form. This means that suitable interfaces must exist between the database system and the application. A communication component ensures communication between the client and server systems. Applications which are executed on the client systems can access the database server via the network. The database servers must be capable of handling larger numbers of parallel client access. The task of the server is then to avoid logic problems due to parallel read and write access by the client systems.

Databases are usually made up of two components, i.e. the real physical database and the database management system (DBMS). The functions of the DBMS include the following:

Monitoring the data relationships within the database

> Monitoring and ensuring correct data storage, taking the data relationship rules into consideration

> Restoring consistent data in the case of a system error or similar events

The DBMS also defines the commands and applications which must be used in order to work with the data in the database. The most commonly used language for database systems is the Structured Query Language (SQL).

3.13.3   MS SQL Server 7.0

Microsoft SQL Server is an SQL-based, relational client/sever database. The database system consists of the real data storage medium and the database management system (DBMS).

3.13.3.1   Server architecture

The server is the component of the MS SQL Server which receives SQL instructions from the clients and performs the related actions.

The client systems send their queries using a protocol at the application level which is specific for the MS SQL Server and referred to as Tabular Data Stream (TDS). Versions 4.2 and 7.0 are supported. The respective packets are generated by the OLE DB provider and the ODBC-driver for MS SQL Server. The TDS packets are sent via the network protocol used to the server and, in the opposite direction, to the client. The Open Data Service on the MS SQL Server administers the data packets and calls the related function in the MS SQL Server.
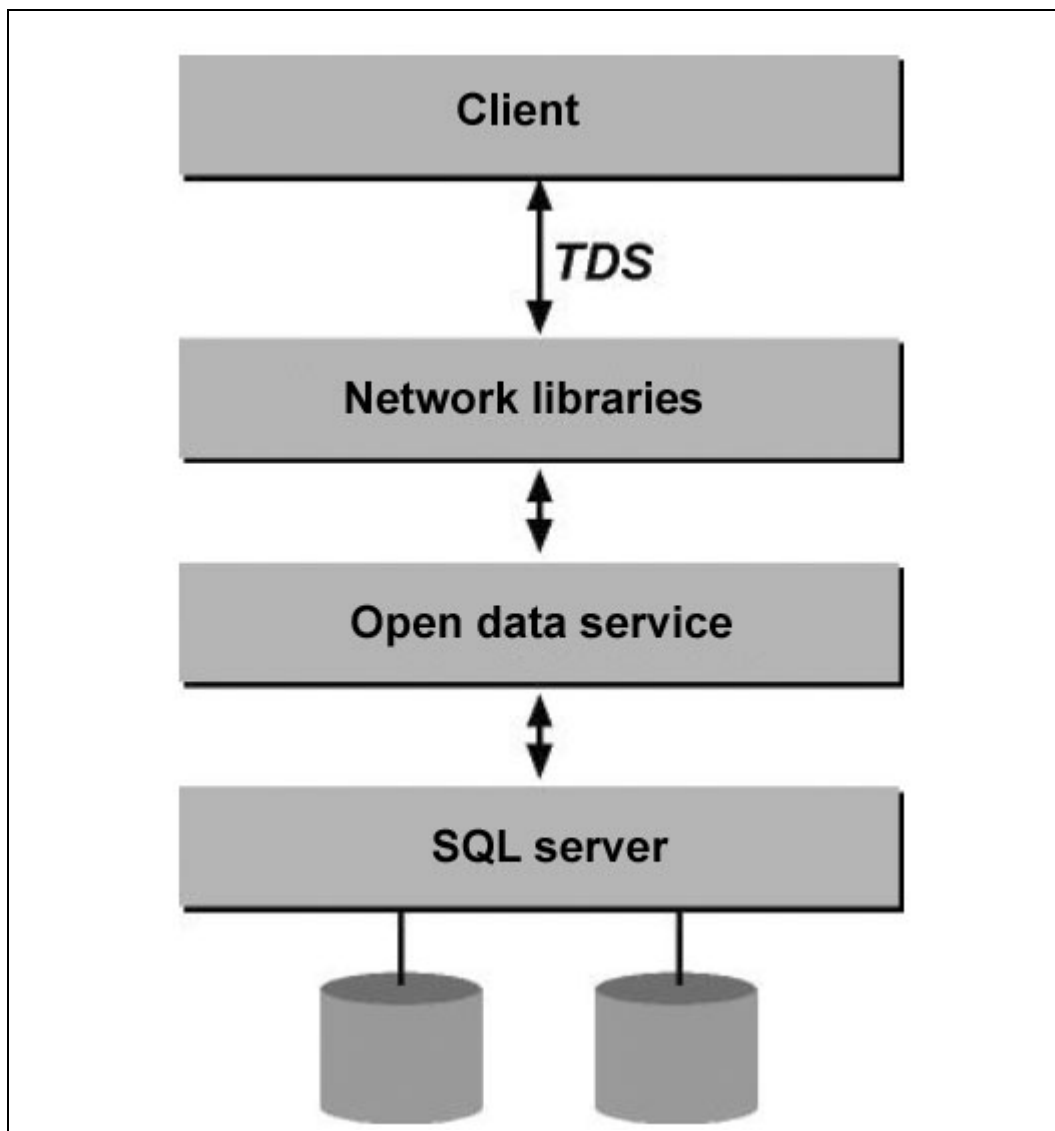
Fig. 29: Server architecture of the MS SQL Server

The real database server consists of two main components, i.e. the relational module and the storage module. The two modules communicate with each other via OLE DB-API.

The functions of the relational module consist of the analysis of the SQL queries, the optimization of the execution plan, and the execution of the operations laid down in the execution plan.

The tasks of the storage module include the following:

File and memory space management

Management of the data buffer and of the I/O operations

Administration of transactions and disabling transactions

Logging and restoring

Technical description of the migration paths

Implementation of the service functions (BACKUP, RESTORE, DBCC and bulk copying)

3.13.3.2 Database architecture

The data in a database is structured within logic components which, on their part, are physically stored in the form of files on the data volume. When working with the database, the user primarily uses the logic components (tables, views, stored procedures, etc.).

Every MS SQL Server installation includes several databases, i.e. a total of four system databases plus one or more user databases. Besides the system databases, the real content databases must be created after installation. These productive databases are organized in the form of different objects. The table below contains the most important components which exist as objects in MS SQL Server.

Table 19: Components that exist as objects in MS SQL Server

Components	Explanation
Tables	The real data of the database is stored in tables. The tables consist of columns and lines, with the lines containing the respective data records. Data types defining the way in which the data is stored in the columns can be defined for the columns.
User-defined data types	Besides the basic data types of MS SQL Server, users can create user-defined data types.
Views	Views are defined views of a virtual table or saved query. The database includes SELECT statements the result set of which forms the contents of the virtual table. Views fulfill the following functions: ● Restricting user access to specific lines or columns in the table ● Combined presentation of columns from multiple tables ● Summarizing information
Stored procedures	Stored procedures constitute a group of transact SQL statements which was compiled to form a single execution plan. The functions of stored procedures include, for example: ● Implementation of program-spanning program logic for the execution of frequently recurring tasks ● Increase in performance; the stored procedures are kept in the cache in compiled form ● User access to the tables can be prevented
Restrictions	Restrictions provide a method for securing the integrity of the database. Restrictions define the rules concerning the values permitted in the columns
Rules	Rules ensure downward compatibility; they sometimes have the same functions as the CHECK restrictions. Rules are used to restrict the values in a column.

Components	Explanation
Default values	Default values are the values used in the column if no value was entered in the column when a data record was added.
Triggers	Triggers are a special form of stored procedures. Triggers are executed automatically when an UPDATE, INSERT or DELETE statement was made for a table.
Table indices	An index which is linked to a table and accelerates the line query process.

3.13.3.3 Client components

Microsoft SQL Server is not directly accessed by the user. Special applications are used to access the data. The following can be used to access Microsoft SQL Server:

Utility programs of MS SQL Server

Programs from third-party suppliers

Programs developed within public agencies

MS SQL Server is accessed via the database API (Application Programming Interface) which consists of two parts as follows: the language statements which are passed on to the database, and a set of functions or object-oriented interfaces and methods which send the language statements to the database and process the results. The language statements used by MS SQL Server are **Transact-SQL**, with all statements of the entry level of SQL-92 and further SQL-92 features (from the intermediate and full levels) being supported. Furthermore, Microsoft-specific Transact-SQL extensions are also available.

MS SQL Server supports two main classes of database APIs:

OLE DB – The system-own provider supports applications written by means of OLE DB or APIs which use OLE DB (such as ActiveX Data Objects (ADO)). Furthermore, objects and components using OLE DB are also supported (such as ActiveX and Windows DAN applications).

ODBC – The driver supports applications and components written by means of ODBC.

Furthermore, MS SQL Server supports the DB Library and Embedded SQL.

3.13.3.4 Communication components

Several methods of communication between the client applications and the server are supported. The communication on a computer between server and application uses process-spanning technologies, such as Named Pipes or Shared Memory. Applications running on another client system use the network Inter-process Communication (IPC). IPC is based on the API and the network protocols. The following protocols are available:

TCP/ IP

Novell IPX/ SPX

Apple Talk

Banyan VINES.

3.13.3.5 Scalability

Microsoft SQL Server is designed for administering databases which can have a size of one terabyte or more. MS SQL Server includes certain features designed to boost the efficiency of the database system.

MS SQL Server maximizes the extent of parallel access to data by selecting a suitable locking level. Access is optimized by dynamic locking processes at the line and/or table levels.

The database system also supports VLDB (Very Large Database) environments with databases volumes of one terabyte or even more. The Transact-SQL BACKUP and RESTORE statements can write parallel to multiple backup media and create incremental backups.

An integrated query optimizer in MS SQL Server accelerates query handling processes. Parallel execution plans can be set up for the purpose of supporting multi-processor machines in order to distribute the SQL statements.

MS SQL Server supports distributed queries. Transact-SQL statements referring to heterogenous OLE DB database sources can be executed.

Data integrity during updates (changes) is ensured by the fact that updates always end in a consistent status. If this consistent status is not achieved, rollback to the starting point (i.e. to the last consistent status) takes place.

Furthermore, distributed transactions are possible, with a transaction manager then managing these distributed transactions.

3.13.3.6 Access control

MS SQL Server offers two kinds of user authentication:

SQL Server authentication
The appropriate logon accounts and passwords must exist in MS SQL Server – these stand in no relationship with the NT user accounts. Logon and password request take place directly at MS SQL Server.

Windows NT authentication
Although the Windows NT accounts and groups must be included in MS SQL Server, authentication itself takes place at the NT domain.

The administrator can decide whether authentication is to take place via Windows NT or in hybrid mode.

3.13.3.7 System integration

MS SQL Server supports the use of Windows NT users and domain accounts, so that Windows NT authentication is available to MS SQL Server. The users are

not authenticated by MS SQL Server, with the server making a trusted connection available to the client systems.

Besides integration into the NT user authentication system, MS SQL Server can be closely connected to the following products:

Data storage service for the Microsoft Internet Information Server which is normally used for generating dynamic web contents on ASP basis

As a data storage functionality for the Sites Server which is used for the administration of websites

3.13.3.8 Administration

Various tools are made available for the administration of MS SQL Server.

MS SQL Server Agent

This enables the preparation and planning of tasks to be executed once off or periodically. Warning messages for the administrator can be generated when certain system conditions occur.

MS SQL Server Profiler

This enables the monitoring and analysis of the network load during transmissions from and to a server.

MS SQL Server System Monitor – This enables integration into the Windows NT system monitor which monitors the performance of SQL Server and of the graphic presentation.

MS SQL Server Enterprise Manager

This makes a snap-in available to the Microsoft Management Console (MMC) for managing MS SQL Server.

Index Optimization Assistant

This enables the analysis of the use of indices of SQL statements.

Furthermore, the SQL Distributed Management Objects (SQL-DMOs) enable the integration of automation tasks within applications. Recurrent tasks can also be implemented as jobs.

3.13.4　Replacing migration

Databases or, more precisely, relational database management systems (RDBMS), have paved the way for the use of Linux in enterprise-critical areas of application. The Software Workgroup launched AdabasD as early as 1997 as a fully commercial (and at that time SAP-certified) RDBMS for Linux. Oracle and Informix followed suit in 1998, thereby boosting the credibility of Linux in the professional environment. The combination of Linux, Apache, MySQL and PHP which is known under the acronym "LAMP" has been one of the most popular infrastructures for webshops and dynamic websites since the beginning of the commercial use of the Internet. PostgreSQL, Firebird and SAP DB constitute a whole range of full-scale RDMBSs with transaction support, triggers and stored procedures even under Open Source licenses. There is certainly no lack of high-

quality options for the use of Linux and Open Source software in the field of database systems.

RDBMSs play a special role within the framework of a migration strategy in that they are always connected to applications where data is managed by RDBMSs. This means that a change also requires a change in data stocks on the one hand and possibly even in applications on the other.

Within an organization, the data ideally occurs in one database system only and in a normalized form (without redundancy). The query language (SQL) used by the applications on the database is ideally standardized, and every application should smoothly work with any RDBMS. Reality unfortunately shows that in most IT infrastructures several RDBMSs with sometimes redundant data are kept in different databases. This means that this data is queried by the different applications in different SQL dialects and with manufacturer-specific language extensions as well as via manufacturer-specific interfaces. Even if communication with the database via ODBC or JDBC is standardized, and even if no triggers or stored procedures are used, the ODBC/JDBC driver must be replaced at the client end in the case of database migration.

Against this background, migration offers the opportunity to consolidate software and data structures even though this is obviously not easy to achieve.

These initial considerations suggest that an alternative to continuing migration should be considered in the following cases only:

> The RDBMS which is currently running under Windows is also available for an Open Source operating system (such as Oracle on Linux). This means that the database system remains in place as commercial software. In a Linux-based server infrastructure, this variant also offers advantages from the administrator's point of view. However, a Linux version is unlikely to be launched for MS SQL.

> The applications are linked to the legacy RDBMS via ODBC or JDBC. In this case, the data can be exported to another database system and the client connection can be redirected to the new RDBMS by replacing the ODBC driver (at the system level with the client). However, the details are a problem in this case. If the application uses stored procedures or triggers, these must be ported too. (This is occasionally also possible without any changes in the client software).

> The application is a Microsoft Access application with file-based data storage. In this case, the data can be very easily imported into a central DBMS and the Access application can be changed to the ODBC interface.

> The client is available as source text and can be adapted to the new RDBMS within the framework of a migration project. Apart from the above-mentioned factors (i.e. triggers and stored procedures), the migration effort also depends on the programming interface used. If the database application was implemented directly via an interface of the manufacturer (such as embedded SQL), the migration effort will be significantly higher than in the case of an intermediate abstraction level, such as ActiveX Data Objects (ADO).

Another option is finally to cooperate with the manufacturer of an application as another way to achieve database migration. Many suppliers of commercial database applications also consider the fixed link to a particular RDBMS as a market disadvantage, so that it may well be assumed that there is a substantial and growing readiness for migration, especially towards an Open Source RDBMS.

If database migration is generally possible, a suitable RDBMS must be selected as the target system. This migration guide focuses on Open Source databases as potential target systems. The overview below shows the database systems currently available under an Open Source license:

Table 20: Database systems available under an Open Source license

Database	Version	License	Query	Trans-actions	Stored Procs
GDBM www.gnu.org	1.8.3	GPL	Hash		
Berkeley DB www.sleepycat.com	4.1.25	BSD Type	Hash	X	
SHORE www.cs.wisc.edu/ shore/	1.1.1	BSD	SDL/ODL		
ZOPE www.zope.org	2.6.1	Zope PL	DTML		
mSQL www.hughes.com.au	3.4	Hughes	MSQL		
MySQL www.mysql.com	4.0.12	GPL	SQL	X	
PostgreSQL www.postgresql.org	7.3.2	BSD	SQL	X	(X)
Firebird firebird.sourceforge.net	1.5	InterBase PL	SQL	X	X
SAP DB www.sapdb.org	7.4.03	GPL/ LGPL	SQL	X	X

The hash systems have no relational organization. The last four systems with SQL interface are the best candidates for migration. These four systems will be characterized in the following.

3.13.4.1 MySQL

MySQL is developed and distributed by the Swedish company of the same name. The database is subject to GPL and hence constitutes free software. Since the programming interfaces are also subject to GPL, programs linked to them must also be subject to GPL as soon as they are distributed and/or marketed for commercial purposes. Alternatively, MySQL AB also offers commercial licenses which enable suppliers of commercial applications to use MySQL without the

need to subject their own software to GPL. MySQL offers regular support and service agreements, training as well as consultancy services.

The manufacturers estimate the number of database installations at 4 million world-wide. Most popular is MySQL together with Linux, Apache and PHP for the creation of dynamic websites.

MySQL can use the same frontend (SQL Parser) on different backends for data storage. With innoDB as the backend, MySQL also offers transaction support. Stored procedures are at present not available from MySQL. According to the manufacturer, these will be available as of version 5.0.

MySQL can also be compiled using OpenSSL support – in which case client and server communicate via the Secure Socket Layer (SSL) protocol using X.509 certificates.

Files are typically stored in the file system with MySQL. The data structures do not use more disk capacity than is actually required for storing the contents. Allocation of disk space to a table or database is not necessary. A single, active database server can administer any number of database instances.

MySQL is generally very lean and extremely quick during all read access. It is typically used for small and medium data stocks and for simpler applications. However, MySQL AB's reference list shows that the database is also suitable for large applications and data stocks and that it can clearly compete with any fully commercial database system.

3.13.4.2   PostgreSQL

PostgreSQL has its origins in the Postgres database designed at UCB in 1986, and is subject to BSD copyright. In 1995, the database query was changed to SQL. Development is carried out by a large community spread all over the world applying purely open source methods. In line with the community model, various companies offer products and services related to PostgreSQL.

PostgreSQL enables users to define their own functions in different programming languages which can return both individual values as well as tupels or even complete tables. This means that these functions offer a wider range of options than user-defined procedures. Another special feature of PostGreSQL's concept is the control concept which extends beyond the functionality of mere triggers. Thanks to the broad-based community process, PostgreSQL comes with a rich functionality, is very flexible and thus suitable for the most varied applications, and constitutes a very secure system. PostgreSQL offers, for example, very powerful encryption both for authentication and for data communication on the basis of X.509 certificates.

Data is stored in the file system with PostgreSQL. Allocation of database or table space is not necessary; allocation to different memory areas is possible even retroactively. One database server can serve multiple database instances. PostgreSQL uses, in a manner similar to Oracle, a view system which in contrast to conventional locking mechanisms enables locking of the database even during

ongoing operation at high performance levels. The data backup system is consistent in this context.

PostgreSQL is lean and at the same time offers a powerful functionality. It is typically used for medium data stocks. A Windows-based administration tool can be used to link a Migration Wizard for Access databases, so that the import of data from Access can be automated to a very large extent.

3.13.4.3 Firebird

Firebird came up in mid-2000 as an independent project from the InterBase database, version 6.0 which Borland had released into the Open Source. A small, committed community is working on the further development of this database system. The documentation mainly consists of Interbase's PDF files. An update is at present not foreseeable. Some interfaces which exist solely for Interbase will be omitted during the course of further development. Firebird is not yet a suitable candidate as an RDBMS for professional use.

3.13.4.4 SAP DB

The SAP DB was launched as a university research project at Technische Universität Berlin. The early beginnings even date back to 1977. In the 1980s, the system was further developed and sold by Nixdorf under the name DDB/4. It then came via Siemens/Nixdorf to the Software Workgroup where it was continued under the name ADABAS D. In 1997, SAP acquired the unrestricted exploitation rights from the Software Workgroup and since then has continued developing the database under the name SAP DB. In 2000, the SAP DB was subjected to GPL, however, without reducing SAP's investment in its further development. The SAP DB is offered by SAP as a certified platform for almost all SAP solutions and is used as a core technology in several products. The functionality includes not just transaction support, but also trigger and stored procedures.

The main focus of the further development and quality assurance work was placed on the functionality required in conjunction with SAP solutions. Since the entire business logic runs in the SAP application server, the database system is primarily used for the performant supply and storage of relational data. Stored procedures do not play a role here. Accordingly, the SAP DB still lacks versatility and flexibility in this respect.

The SAP DB uses volumes for data storage which are created in the file system or on raw devices and which are in each case completely allocated to a database instance. The database is reorganization-free, with the possibility to make backups during ongoing operation without affecting performance.

The SAP DB is the heavyweight among the Open Source databases. It is a candidate as a migration target for Access databases in exceptional cases only.

3.13.4.5 Interim conclusions

A wide range of attractive migration targets are on offer in the Open Source area.

It is not possible to make a general, simple and clear-cut decision in favor of one or another system on the basis of its respective characteristic features.

Technical description of the migration paths

All four SQL database systems described are platform-independent. All four SQL database systems are, in particular, can be downloaded from the Internet as Windows versions ready for installation.

In order to support a detailed comparison of the possible target systems of a migration project, an exact comparison of the list of features is required with a view to the database functionalities that are actually used in the source system.

A good overview can be found at http://www.mysql.com/information/features.html.

The table below gives some additional assistance:

Table 21: Overview of SQL database systems

Feature	MySQL	PostgreSQL	Firebird	SAP DB
Lizence	GPL	BSD	Borland PL	GPL
Documentation from third-party suppliers	X	X	(Inter Base)	n.a.
TableSpace	unlimited	unlimited	unlimited	unlimited
SSL / Network Traffic Encryption		X		
Kerberos Authentication		X		
ODBC	X	X	X	X
JDBC	X	2.0		3.0
Perl	X	X		X
PHP	X	X		X
Python	X	X		X
Group/role concept		X		X
Online backup		X	X	X
Incremental backup				X
Extension of the DB space during ongoing operation	Via LVM	Via LVM	Via LVM	X
Raw devices	(X)			X
Namespaces		sheme.table		owner. table

3.13.4.6 Notes

When data is imported from data types that do not exist in an identical form in the target system, it is usually possible to identify a suitable type with a larger value range. However, both during the import of data and during the transition to an

ODBC connection, care must be taken to ensure that the ODBC interface has its own concepts and definitions of data types.

3.13.4.7 Recommendations in the interest of independence

In cases where replacing migration is currently not recommended, one can nevertheless give some recommendations concerning database programming in this context in order to facilitate future migration.

Stored procedures and manufacturer-specific extensions should not be used. If the business logic or functionality is to be moved from the client to the server, 3-layer architectures are today a very good means for this. In the sense of platform-independent implementation, a suitable candidate for this is Java both for the client and for the application server (Tomcat).

Standardized interfaces (ODBC, JDBC) should be used to connect the database, or an abstraction level should be added which can be optionally switched to ODBC, JDBC or other interfaces without any changes in the program code.

SQL statements must be isolated and modularized in the program code.

3.13.5 Continuing migration

3.13.5.1 Microsoft SQL Server 2000

New web functionalities were, in particular, integrated with MS SQL Server 2000. The further development focuses on XML capability and improved scalability. The most important new functionalities will be introduced in the following section.

Internet and intranet

The table below shows the most important extensions of MS SQL Server 2000 for the field of Internet and intranet solutions.

Table 22: Extended Internet and intranet solutions with MS SQL Server 2000[67]

Function	
XML	- Support of XML, Xpath, XLS and HTTP: - Display of and access to relational data by using XML views. - URL and HTTP access to data on the Internet. SQL, XML templates or Xpath can be embedded into URLs in order to generate queries. - SELECT statements can be returned in XML form. - XML can be edited by Transact-SQL and stored procedures.

---

[67] The extended functionalities of the Enterprise Edition are not discussed here. They are described in White Papers and related technical descriptions.

Technical description of the migration paths

Function	
Integrated data mining	Enables the analysis of relational and OLAP data ("Online Analytical Processing") for trend analyses and forecasts.
Support of multiple instances	Hosting of separate database instances for applications or customers.
Security	Support of SSL connection and Kerberos.

Administration and development

The table summarizes the most important new features concerning the administration and development options of Microsoft SQL Server 2000.

Table 23: Administration and development functionalities

Functions	
Active directory integration	Integration of the central MS directory service.
Wizard for copying databases and DTS	Moving and copying of databases and objects between servers. Data Transformation Services enable the importing and exporting of primary and external keys between supported database products.
User-defined functions and new triggers	Creation of reusable Transact-SQL functions. Extended triggers for code execution instead of or after a process.
Data types, indices and sorting	New data types (bigint, sql_variant, table) can be used, and indices can be defined in column types if the data is to be calculated in the columns of other columns. Sorting is enabled at column level. This enables the storing of objects which are subject to different sorting rules in the same database.
Analysis services virtual cubes and the MDX Generator	Analysis Services enable the development of OLAP, data warehousing and data mining solutions. The editor for virtual cubes enables editing of virtual cubes. The MDX Generator can be used to create multi-dimensional expressions.

3.14   Groupware

3.14.1   Overview

The technical discussions concerning the migration of groupware and messaging focus both on the performing of the functionalities of Exchange 5.5 by alternative solutions which can be used on Linux-based systems and on the continuation with Exchange 2000. With regard to replacing migration, the use in heterogenous system environments with Linux-based server systems and Windows-based client systems with MS Outlook remaining almost completely in use is one major aspect of the technical analysis.

The analysis suggests that two of the solutions studied are particularly suitable because they fulfill the requirement of realtime connection to a large extent. Realtime connection enables the conflict-free use of the group functionalities. The two solutions are Samsung Contact, a commercial solution based on HPOpenMail on the one hand, and Exchange4Linux on the other. The latter is a

solution with a server component which is available as free software and a proprietary outlook connector which is available as a commercial software module. Exchange4Linux scales a maximum of 500 users and is hence more suitable for smaller public agencies. Samsung Contact is particularly suitable for use in medium to large public agencies. Another OSS solution is Kroupware which can be connected to Outlook via the commercial Bynari Connector. Kroupware is currently still subject to the restriction that sufficient experience with real operation is not yet available.

The commercial OpenExchange product from SuSe can be used in cases where realtime connection is not an indispensable requirement.

Furthermore, realtime connection also ensures that the Exchange 5.5 functionalities are covered to the largest extent. One exception in all cases is the use of forms which is not covered by any of the solutions studied.

Besides use in heterogenous systems, use in purely Linux-based system environments also plays a central role and hence the question concerning client software which can serve as an alternative to MS Outlook. In this respect, Samsung Contact is the only solution which comes with a Java-based, platform-independent, integrated client. Although web clients exist for all the solutions studied, their use is, however, subject to more or less far-reaching functional restrictions. Offline use, in particular, is not possible with such web clients. However, the mail functionalities can be used with all mail clients which support POP 3 and IMAP.

Concerning continuing migration to MS Exchange 2000, one can summarize that this introduction is only possible in conjunction with the introduction of the active directory. This hence requires a fundamental strategic decision, so that the technical discussions of AD in chapter 3.7 should be referred to once again at this point.

3.14.2 Introduction

As already noted in chapter 2, it can be assumed that Exchange is used by most public agencies as the groupware solution. This is why the starting situation will be described first, followed by a discussion on different groupware solutions which can be used on Linux-based operating systems with a view to replacing migration. Both pure Open Source projects and commercial products will be discussed. Approaches, aims and target groups of the products are sometimes very different. A general distinction can, however, be made between purely web-based and classic client/sever solutions. In view of the large number of different solutions, it is not possible to discuss all the solutions available on the market. The solutions discussed were selected on the basis of different requirement scenarios.

MS Exchange 2000 and, to some extent, even MS Exchange 2003 will be discussed with a view to continuing migration.

3.14.3 The starting situation – Microsoft Exchange 5.5

The most important features and functionalities of the groupware solution from Microsoft will be described here with regard to version 5.5.

3.14.3.1 Basic infrastructure

Microsoft Exchange Server requires a Windows NT 4 domain structure as the basis which is used primarily for authentication.

3.14.3.2 Logic structure units

The largest structure unit of Microsoft Exchange Server is the organization. An organization can extend over several NT domains.

Furthermore, Exchange uses sites as a means for structuring. A site logically combines a group of Exchange servers that communicate with each other via a fast network connection. Exchange servers of a site serve each other the mails directly and replicate the directory information directly with each other. The routing of mails between sites must be explicitly configured. A site is an administration unit.

3.14.3.3 Basic components

Microsoft Exchange Server is made up of the following basic components

Exchange directory (Directory Service, DS)

Message Transfer Agent (MTA)

Information storage (Information Store, IS)

System Attendant (SA)

The **Exchange directory** saves all the information concerning users, resources and the organization in a database (dir.edb). This includes lists of the e-mail users registered on the server, as well as server names and server configurations. It is important to note that the complete configuration information is stored in the directory.

The **information store** consists of two databases, i.e. the "Private Information Store" (priv.edb) and the "Public Information Store" (pub.edb). The "Private Information Store" stores the messages and file attachment for the users whose mailboxes are located on the server in question. The "Public Information Store" stores the contents of replicates of the public folders.

The **Message Transfer Agent** (MTA) sends the messages to other servers, sites and external systems. In conjunction with the Exchange directory, the MTA decides about the routing of messages. The MTA passes incoming messages on to the information store. The MTA also converts messages to other formats.

The **system attendant** is the administration unit for the Exchange server. This component can be used, for example, to generate new e-mail users and to carry out monitoring and service tasks. The system attendant monitors the network connections to other Exchange servers and prepares routing tables.

The table below shows the corresponding components and describes their particular functions in concise form.

Table 24: Basic components of Exchange 5.5

Component	Functions
Directory	• Administration of the information concerning recipients, distribution lists, servers and messaging infrastructure. • The directory can be used by other components for information reconciliation purposes, for example, to reconcile addresses. • Within an organization, the replication of the directory information of all servers is carried out automatically.
MTA	• Forms the core component of the communication infrastructure of the Exchange server. • Transmission of messages to other servers, sites and systems. • Format conversion for other systems.
Information store	• Storing the messages sent to individual users. • Processing and storing the information in the public folders. • Private and public information is stored in two separate databases. • Informs the clients about new messages and also receives messages from the client.
System attendant	• Logging the messaging activities. • Monitoring of the message connections between the servers. • Preparation of routing tables. • Monitoring the directory replication processes and resolving conflicts. • Logging the message sending processes. • Generating e-mail addresses for newly created recipients.

3.14.3.4 Optional components

Optional, modular components, such as different connectors and the key management server, can expand the functionality of the Exchange server.

Connectors are used to transmit messages between different systems or sites.

Site connector and directory replication connector (connecting sites to form an enterprise-wide system)

Dynamic RAS connector (connects sites via asynchronous dial-up connections)

      Internet Mail Service (connects sites via SMTP or the Exchange system to the Internet)

      Internet News Service (connects Exchange via NNTP to Internet News)

      MS Mail Connector and Directory Synchronization (enables connection to MS Mail 3.x systems)

      Microsoft Schedule+ Free/ Busy Connector

      X.400 Connector (connects sites by dedicated bandwidth control or the Exchange system to external X.400 systems

      Connector for cc:Mail (connects Exchange to Lotus cc:Mail systems).

Internal and external connectors can be distinguished. Internal connectors connect two Exchange sites to each other and basically constitute logic objects which simplify administration tasks. External connectors are additionally also software components which enable the connection of the Microsoft Exchange server to other mail systems. Connectors ensure the correct conversion of message contents and address information. In this way, messages originating from Exchange can be read in external systems, and messages originating from external systems can be read by Microsoft Exchange users.

The **key management server** (KMS) can be used to manage keys that can be used for the encrypted transmission of messages and for attaching a digital signature to messages.

The **chat server** is another optional component. It enables the implementation of so-called "Internet Relay Chats" (IRCs) which, for their part, enable large numbers of users to simultaneously communicate with each other.

The so-called **Server Scripting Service** was also implemented effective as of version 5.5. This service ensures that scripts which were written in a script language, such as Perl, VB Script or JScript, can be filed in a public folder. The service ensures the execution of programs as soon as specific events occur. Scripts can be used to automate tasks.

3.14.3.5 Protocol support

Exchange supports a whole series of different protocols; the most important protocols are discussed in the following section.

The Simple Mail Transfer Protocol (SMTP) is a standard protocol for message transmission via the Internet.

The POP3 protocol is used for sending messages to client computers which are not permanently connected. This standard is designed for the exchange of information between e-mail clients and servers which are connected on a temporary basis only. Mail clients use POP3 to read messages whilst SMTP is used to send messages.

The IMAP4 standard which is supported by most e-mail products is based on a different approach. The major strength of IMAP4 compared to POP3 is the ability

to selectively load messages from the server. In this way, it is possible, for example, to download messages separate from any attachments.

Thanks to the integration of HTTP, documents in public folders can be accessed via the Internet. The use of Microsoft Internet Information Server (IIS) and of Exchange Server 5.5 enable Outlook Web Access (OWA) users to access functionalities which would otherwise be possible with the Outlook client only. The information is generated using the Active Server Pages, so that the HTTP support is primarily an extension of the Internet Information Server. HTTP hence also requires the existence of an Internet Information Server with ASP functionality. Users can, for example, view private and public folders, send and receive mails, and use further functions. However, use of the full functionality depends on the Microsoft Internet Explorer.

NNTP enables the world-wide spread of newsgroups. The contents of the newsgroups are sent from server to server via NNTP. The Exchange server can make the contents of newsgroups available in the public folders via the NNTP connection.

LDAP gives clients access to directory information from the Microsoft Exchange server directory.

3.14.3.6 Product variants

Exchange Server 5.5 is used in two different versions, i.e.

Standard Edition

Enterprise Edition

The Enterprise Edition supports an exchange cluster with two nodes based on the Windows NT 4 Enterprise Edition.

3.14.3.7 User functionalities

The following functionalities resulting from ownership of a mailbox are available to the user:

Receiving and sending e-mails

Task management

Calendar

Address lists (general address books and personal contacts)

Journaling and notes

This guide assumes Microsoft Outlook as a typical client software. Outlook is available in versions 97 (Ver. 8), 98 (Ver. 8.5), 2000 (Ver. 9) and 2002 (Ver. 10, XP).

Outlook and Exchange enable the offline storing and editing of data with the possibility to subsequently synchronize this data when a connection to the net is available (the typical case with notebooks).

Outlook itself offers the PIM (Personal Information Manager) functionality which enables the use of personal folders which are stored as files (*.pst).

Workflows or group mailboxes can be made available in public folders. The use of public folders enables the shared use of information. Users having the required access privileges can read and/or write the information stored in the folders.

3.14.3.8   Client-to-server communication

The communication between client and server in a typical LAN environment with Outlook clients takes place via MAPI (Messaging Application Programming Interface) and hence via RPC (Remote Procedure Calls).

Thanks to support of SMTP, POP3, IMAP and HTTP, the most varied communication scenarios can be implemented between client and server.

3.14.3.9   Server-to-server communication

The communication between Exchange servers can be controlled by the different connectors. Two servers located at the same site communicate via RPC.

3.14.3.10 Related issues

The use of mail systems means greater exposure to virus attack. Exchange permits third-party manufacturers to implement anti-virus software by using the anti-virus API which was specifically created for this purpose.

Integration of FAX solutions in Exchange environments is addressed by many third-party manufacturers.

Archiving of e-mails or displacing mail objects which have not been used for some time (hierarchical storage management, HSM) can be carried out by software from third-party manufacturers.

3.14.4   Replacing migration

The particular goal of replacing migration can vary from application to application. The requirements which a groupware product must fulfill must be precisely identified prior to migration. The list below contains some examples of criteria for selecting a groupware solution:

Which client systems must be supported?

- Web-based clients only

- Outlook clients (MAPI support)

- Linux-based client systems

- Clients in heterogenous system landscapes (Windows-based and Linux-based systems)

Which groupware functionalities must be supported by the new system?

Which scalability requirements must the systems fulfill?

And so forth.

Verification of the requirements for a new groupware product is a mandatory exercise which must be carried out prior to a project.

3.14.4.1 phpGroupware

The "phpGroupware"[68] solution which is subject to GPL is one representative of the purely web-based solutions. The generation of the dynamically created contents is based on the PHP script language. The contents are made available by a web server, whilst it is possible to use a MySQL database for data management and storage. However, other suitable database systems are PostgreSQL, Oracle and Sybase, with an LDAP directory being used for address management. Different technologies (SQL, SQL_SSL, LDAP, HTTP, NIS, PAM) are also available for user authentication.

Any mail servers supporting the SMTP and POP3/ IMAP protocols can be used for the e-mail functionality. Support of server-based filter rules and absence profiles is at present not possible.

phpGroupware is a modular system. Numerous modules are available for integration. Besides modules used for the implementation of classic groupware functionalities, many other modules are available.

Table 25: Selection of phpGroupware modules

Module	Function
Addressbook	Contact manager
Admin	Administration
Backup	Backup tool
Calendar	Calendar, including sending of invitations and access privileges
Cdb	Contact database
Email	E-mail client
Forum	News and discussion forum
Projects	Project management
Timetrack	Time recording
ToDo	Task management
TTS	Trouble Ticket System

Optional activation of the modules by administrative intervention is possible. The web interfaces are based on a template system, with three different types being available for the layout descriptions (XML, eTemplates, HTML). Colors, fonts and justification are defined using CSS (Cascading Style Sheets). A problem is the occasional use of Javascript within the web user interfaces because not all browsers are able to render the Javascript code free from errors. Furthermore, the use of Javascript is not permitted in many public agencies for security reasons.

---

[68] http://www.phpgroupware.org/

The use of a purely web-based solution offers many advantages:

Access via web browsers is possible, as well as secured access via HTTPS from outside.

Installation of a special client is not necessary.

Operating system independence offers advantages especially in heterogenous client landscapes:

Software is updated on the server only.

However, certain disadvantages must also be considered:

Access to data is not possible at times when users are offline and/or when users have to access to the corresponding network. This is a particular problem for field service staff.

Synchronization with mobile terminal units (PDAs) does not exist.

One can conclude that the solution presented is no alternative to the Outlook Exchange solution. However, the groupware product introduced here can be a favorable solution especially for smaller organizations with more moderate requirements concerning the relevant function depth. An advantage is the flexibility with which the individual modules can be adapted to the actual needs of the organization.

PHProjekt also offers a comparable solution.

Both projects have launched a live demo version[69] on the Internet, so that anyone interested can obtain a first idea of their functionalities.

3.14.4.2 Kroupware

The German Federal Office for Information Security (BSI) has commissioned a consortium of companies with the development of a free software groupware solution for use at BSI. This then means that the software can be used by all parties interested without having to pay any license fees. The project aims to create a platform-independent groupware solution that can be used both with GNU/ Linux and with Windows clients. The functionalities specified by BSI are comparable to the Outlook/ Exchange combination offered by Microsoft. The Outlook client system must be capable of working together with the new server[70] .

Server system

The central component is the Kolab server which, for its part, accesses several other free components. The table below shows the individual components.

---

[69]PHPGroupware :
  http://phpgw.de/modules.php?op=modload&name=phpGroupwareDemo&file=index

PHProjekt : http://www.phprojekt.com/demo.php

[70] http://www.kroupware.org/

Table 26: Kolab components

Components	Function
Cyrus IMAP	IMAP mail server
Cyrus SASL	Authentication
OpenLDAP	User administration
Postfix	Mail transfer agent (MTA)
Apache	Web server for WebDAV and web frontend
ProFTP	FTP server

The Kroupware solution is based on the classic client/sever approach which enables asynchronous use of the groupware functionalities by users. Users can, for example, use e-mail, appointments and personal to-do lists offline via the appropriate client software. The changes are reconciled by subsequent data replication. The Kroupware project is designed for installations with 1500 users on one server machine. Its scalability is based on the cluster capabilities of Cyrus IMAPD and OpenLDAP. Installations with large numbers of users are foreseen for both systems, so that their use by a large circle of users should be possible. The data restoring option is another crucial element for productive use. The architecture of the entire system simplifies recovery operations. The mailboxes are represented by individual directories in the file system and are hence easy to restore. The complexity is dependent upon the backup tools used. Besides complete mailboxes, it is also possible to restore individual mails and appointments.

Client systems

Access to the mail and groupware functionalities is possible both with a Windows and with a GNU/ Linux client. Microsoft Outlook 2000 was the reference client used in the development, with a connector from Bynari used to connect the Outlook clients to the Kolab server. Bynari's Insight Connector[71] is a commercial product which must be paid for and which must be additionally installed on the clients. The connector enables the exchange of Cal and collaboration data between the groupware server and the Outlook client. However, stability problems in conjunction with the connector were reported in practical use.

The connector from Konsec[72] might be a future alternative, but is at present still in the beta phase.

The GNU/ Linux client is the result of adapted versions of KMail, KOrganizer and other components of the PIM KDE project. The client fits very well into the KDE user interface and enables intuitive operation by users. The client supports the POP3 and disconnected IMAP4 protocols. Filtering of incoming e-mails (spam, etc.) at the client end is supported.

---

[71] http://www.bynari.net/index.php?id=7

[72] http://www.konsec.com/KON/de/konnektor.html

Technical description of the migration paths

The following list shows the most important functionalities of the groupware solution. The functionalities are supported by both client products.

Receiving and sending e-mails

Contact administration for the individual users

Global address book

Group calendar and appointments

Shared resources (public folders)

Notes and to-do lists

Free/busy lists

Absence confirmations

Read confirmations

Palm PDA synchronization.

Security

Developers paid special attention to the integration of security standards Communication between the client systems and the server can be fully encrypted (SSL/ TLS). Encrypted communication is possible using

IMAPS

SMTP via TLS

WebDAVS

The Linux client supports end-to-end security as well as electronic signatures on the basis of international standards (S/MIME, X.509v3) for which a corresponding plug-in[73] is available.

Administration

Special user groups with special privileges are set up for administration purposes. The different groups are the following:

Administrator

Maintainer

User

Administration in line with the different privileges can take place via a web frontend to a limited extent. Simple administrative tasks can be carried out via the web user interfaces. More far-reaching activities require adjustment of the corresponding configuration data.

---

[73] www.gnupg.org/aegypten

The following can, for example, be carried out via the web frontend:

 User and address book administration

 Administration of the public folders

 Administration of certain server services

 Absence confirmations

The web frontend primarily enables access to the directory service. Further adaptations are necessary at the corresponding components.

The individual user can change certain parameters directly. Users can, for example, modify their personal data and add mail addresses.

Migration

Practical experience from within migration projects is not yet available. However, the following mechanisms can in principle be used for migrating existing data:

 Exporting the directory information using LDIF and script-based adaptation of data

 E-mails should be migrated to the new client using POP3

 Transfer of data in the vCard or iCalender format.

Conclusions

Concrete statements concerning the suitability of the Kroupware solution for practical use are at present not possible. Experience from productive environments will be necessary for this. The Kroupware may certainly become an adequate groupware basis for smaller to medium-sized organizations. The advantage is the modular design of the entire system which was developed on the basis of tried-and-tested, scalable components.

The option of implementing the user administration function within the scope of a central directory service simplifies data administration. The directory service can also be used for administering data for other systems (such as Samba). Parallel support of Linux clients and Outlook clients renders this system particularly suitable for use in heterogenous client environments.

3.14.4.3 exchange4linux

The Bill Workgroup Data Exchange Server was developed at the German company Neuberger&Hughes GmbH. The server is released as GPL software and is continuously updated. The aim of the development was and still is to offer an alternative server system for the Microsoft Outlook client.

Future users of the product will have several options for implementing the groupware solution. The server system can be obtained as free Debian packages and purchased as a full-scale solution sold by Neuberger&Hughes. The all-in-one solution includes, in addition to the integrated groupware system, the "Easygate" access software. Easygate provides the most important infrastructure services (DHCP, DNS, file server, proxy server, Internet).

Technical description of the migration paths

Server system

The groupware functionalities are implemented by several software units that interact with each other. The table below shows the software packages needed to operate the groupware server. The server was implemented on the basis of the Python programming language and uses Corba (see below) in order to communicate with the Outlook clients.

Table 27: Exchange4linux components

Components	Functionalities
PostGRSQL	Central data storage
PyGreSQL Python interface	Interface between the database and the groupware server
Python 2.1	Programming language
Exchange4linux	Groupware server

It is also possible to implement the Bill server with a directory service. This option should be considered especially in conjunction with Samba and then enables central user administration for an NT domain and the groupware component. However, this solution cannot be implemented with the N&H complete package. Certain modifications of the Bill server must then be carried out by service providers.

Client systems

The Bill workgroup server is accessed by the Outlook client. The basis for the client's access to the workgroup server is a client MAPI driver developed by N&H which must be installed on the client system. The MAPI clients use Corba in order to generate the necessary Outlook commands on the Bill server. N&H's MAPI Service Provider is a commercial product and thus subject to a license with license fees.

The server supports the following functionalities in conjunction with the Microsoft Outlook client:

Receiving and sending e-mails

Address administration for the individual users

Global address book

Group calendar and appointments

Shared resources

Task management

Notes in private and public folders

Free & busy function

Invitations, with the possibility to accept or to reject

Absence confirmations

PDA synchronization via Outlook

Support of other client products is not yet possible. However, a web client for the most important groupware functionalities is planned for the next release.

Security

Encrypted data transmission using the SSL and TLS standards is possible between the systems. Incoming mails can be subjected to virus checking at the server end using third-party products. Server-based filter rules in order to ward off spam mail complete the security options.

Access privileges can be assigned as protection against unauthorized access within the public folders. So-called Access Control Lists (ACL) are used to implement the access rights.

Data storage within a database system also offers a relatively simple way of restoring data that has been deleted by mistake. The restore operation can be carried out using database tools.

Administration

A web-based frontend is used for administration in conjunction with the use of the all-in-one solution. Administration by default distinguishes between users and administrators only. Further differentiation is not foreseen. The web frontend of the all-in-one solution enables the administration of routine jobs. More complex administrative activities can be carried out using the conventional Linux on-board tools.

Migration

Different approaches towards data migration are proposed, depending on the starting scenario.

In the case of a very small migration project (up to around 10 users), a copy of the mailbox and other data should be saved in a personal folder on the client systems concerned. This data can then be imported to the newly created mailboxes of the new system. This method is very reliable, but also very time-consuming. In the case of migration of up to 250 users, other tools should be used in addition. Data of Exchange users can be exported using the Exchange Administrator Console and Microsoft's "exmerge.exe" tool. The information concerning the mailbox users is stored in a simple CSV file. The contents of the mailboxes can be saved as PST files in any user-defined directory. The same approach must also be adopted for the public folders. Thereafter, the CSV files can be imported to the Bill workgroup server using a migration tool supplied by N&H. Thereafter, the users can then use Outlook in order to import the saved mailboxes (PST files) to the server.

In the case of larger migration projects, further technical data transfer options exist which must be checked from case to case.

Technical description of the migration paths

Conclusions

The groupware solution presented offers very good support for Outlook clients because all important groupware functionalities are supported and are thus available to the users. The solution is at present optimized for application scenarios with several hundred (maximum of 500) users and is used in productive environments within this framework.

3.14.4.4   SuSE Linux OpenExchange Server 4

OpenExchange Server 4 is a further development of e-mail server 3.1 of the Linux SuSE workgroup. The groupware is an all-in-one solution which includes a complete operating system, databases as well as e-mail and web servers. The technology of the operating system is based on the SuSE Linux Enterprise Server. The system is designed for a completely new installation rather than as an upgrade for legacy systems. The distributor offers its customers an all-in-one solution with matching software packages.

Server system

No software packages other than those which are directly related to the groupware solutions are discussed here. The complete solution consists of different, modular software units that interact to implement the mail and groupware functionalities. The table below summarizes the central modules of the solution.

Table 28: Central components of OpenExchange Server 4

Components	Tasks
Postfix	Mail Transfer Agent (MTA)
Cyrus IMAPD	Implements the IMAP functionality
Comfire	Groupware functionalities
OpenLDAP	Central directory service for user administration
PostGRESQL database	Database for handling the groupware data
Apache – Tomcat	Implementation of the web frontend (mail, groupware)

One particular advantage of the modular architecture is its scalability thanks to the possibility to distribute components to different systems. The modular design also enables flexible upgrading of existing systems.

The server components offer a wide range of mail and groupware functionalities. Various functions are available to users as follows:

Receiving and sending e-mails

Calendar

Address management

Task management

Note functions

Document management (version management and folder structure)

Project management

Configurable knowledge database

Group-based discussion forum

The functionalities can be fully used via an integrated web portal page.

Client systems

The mail and groupware functionalities must be discriminated with a view to the support of different client systems. The mail functionalities can be accessed by any POP3 and IMAP-enabled clients. Furthermore, users can access their mails via a specially integrated webmail solution.

The groupware functionalities can be generally used in two different ways:

Browser-based access to the web portal contents

Limited access via the Outlook client

The comprehensive web interface gives users access to all the functionalities listed above. The LDAP-based address books, the possibility to assign privileges, and search functionalities are available to the users in all the function modules. If the appointment function is used, the server automatically analyses the resources available during the period in question. The web-based offers give users access to a wide range of group functionalities.

The second access option is to use the Microsoft Outlook client. This use is contingent upon the availability of additional replication software which must be installed on the client system. The replication process reconciles the data at the user's request and hence does not take place in realtime as in the case of a connector. The software enables integration of mail, contacts, tasks and personal appointments. In the case of conflict, the user must decide from case to case how to resolve these. Data replication is carried out using SOAP in conjunction with HTTP and enables the reconciliation of the server data with the data of the Outlook database. The use of Outlook also enables PDA replication. The MAPI interface of Microsoft is not supported for Outlook.

At present, Outlook does not permit group appointments because Outlook does not include additional functions of the OpenExchange server, such as the delegation of tasks. Furthermore, the global MAPI address book is at present not supported either. It is hence currently not possible to implement a real realtime application. According to the manufacturer, however, this option is under development.

Security

OpenSSL can be used for encrypted data transmission. OpenSSL implements the data encryption between applications and components. The secure transmission of IMAP and POP3 is possible via SSL tunnel and of SMTP via TLS.

A virus scanner can be retrofitted in order to boost the security of mail communications by identifying potentially infected mails and their attachments.

Technical description of the migration paths

The SIEVE mail filter can be used by default to filter spam mails. If necessary, the mail filter can also be used to restrict the size of mails and to apply further filters according to any user-defined criteria.

Administration

A web-based administration frontend is supplied for administrative tasks. The administrator can decide which data users are authorized to edit on their own. Users can change their passwords and generate absence notes via the web frontend. This reduces the system administrator's administrative workload. The administrator can use further administrative options for basic settings for groupware, mail and security components. Furthermore, the conventional means (command line command and configuration files) are available for system administration.

Migration

The SuSe Linux workgroup offers special support for data migration from Microsoft Exchange 5.5 to OpenExchange Server 4. Members of the SuSE Workgroup and/or SuSE partners analyze the system on site and prepare a migration offer on this basis. Microsoft programs and own developments are used for migration.

The following data can be migrated:

> User lists, including the related privileges
>
> Mails stored locally and globally
>
> Tasks
>
> Contacts
>
> Appointments
>
> Notes

Data for functionalities not supported by OpenExchange is not taken over during migration either. These functions include, for example, journals, recurring tasks, categories and user-specific sub-folders.

Conclusions

The groupware solution developed by the SuSE Linux AG constitutes a modular groupware system where the individual modules are largely based on tried-and-tested Open Source components. The commercial "Comfire" package was integrated as the groupware component offering users a wide range of groupware functionalities. The user can access the related groupware information either in a web-based manner or via the Outlook client. Users have browser-based access to the entire range of the OpenExchange solution. However, this function is limited for Outlook clients. Users are currently unable to access a realtime connection, nor do they receive real MAPI support either. This means that only a limited Outlook functionality is available to users.

3.14.4.5   Samsung Contact

Samsung Contact (SC) is a comprehensive groupware solution which was designed for use in enterprises of varying dimensions. The system enables the administration of several hundred to several thousand users on one server. The software functionality is largely compatible with the Microsoft Exchange product. All server components are available for Linux (RedHat, SuSE) and most commercial UNIX derivatives (AIX, HP-UX, Solaris). Several operating systems are supported at the client end. The SC Java client runs under both Linux and Windows. A web-based client enables access from any web-enabled platform. A MAPI provider is included and provides access to the full range of an existing Outlook functionality (98, 2000, XP).

Samsung Contact is based on the tried-and-tested *OpenMail* technology from Hewlett-Packard (HP). Samsung was established in Korea and has been in the market for more than 15 years. In November 2001, Samsung SDS took over all the rights for the further development of the product as well as the pertinent developer team from HP.

Server system

The illustration below explains the principles of the system architecture.

Technical description of the migration paths
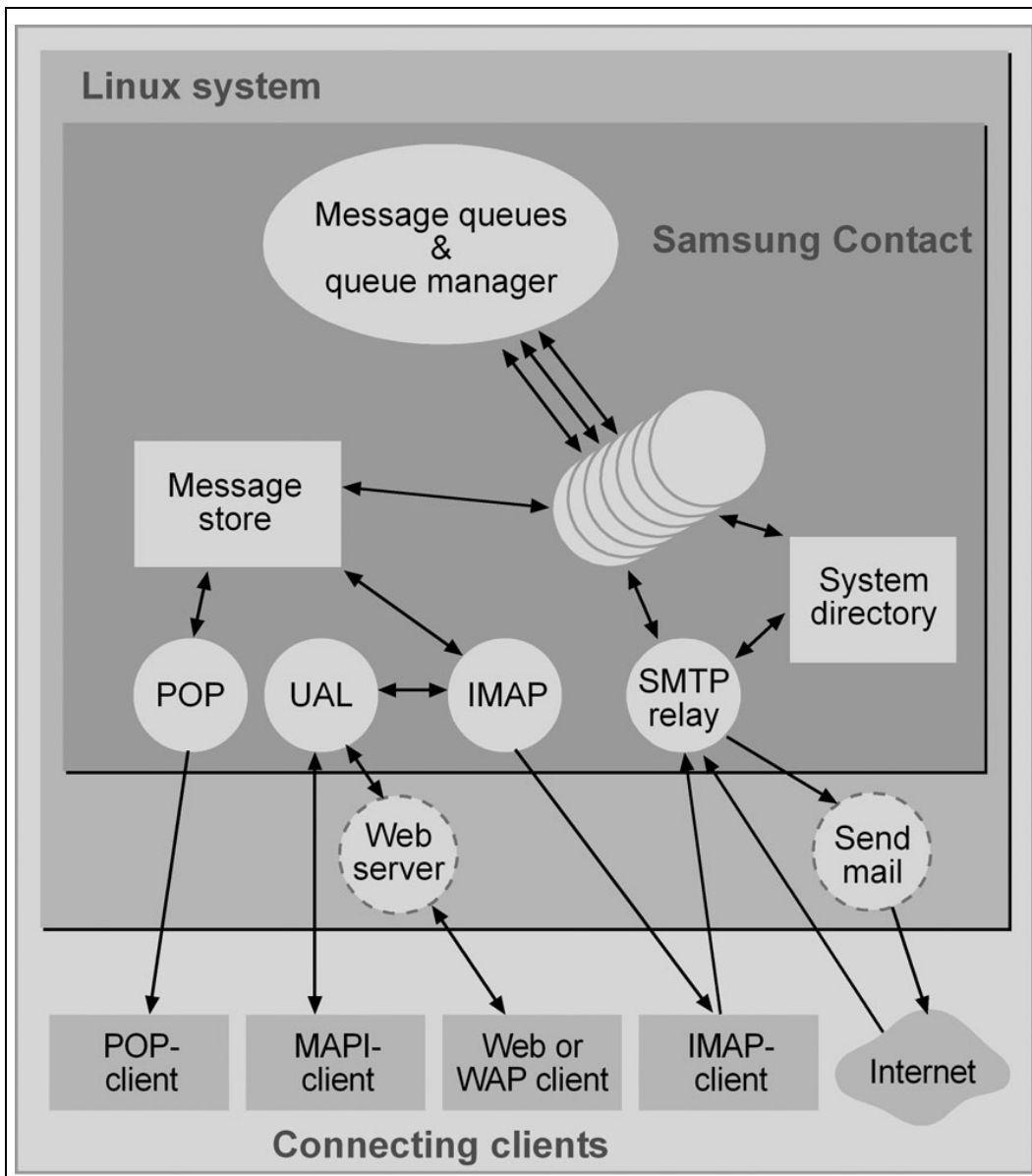
Fig. 30: Samsung Contact architecture

The server system consists of several independent components which can also be distributed to multiple servers in the sense of horizontal scaling. Furthermore, several completely independent instances can run on one server system. The table below gives a general overview of the server processes and their different tasks.

Table 29: Samsung Contact components

Components	Function
Service Router	Redirects a message to the service necessary to process the message. This includes the processing of rules at the server end for distributing or automatically answering messages.
Local Delivery	Delivers a message to a local mailbox.
Internet Mail Gateway	Converts a message to a MIME-conforming Internet

Components	Function
	mail.
Remote Client Interface	Connects mail clients via a network. This type of connection is used by the MAPI provider and the Java clients, for example. This connection is a single-socket connection between the client and the server process.
Test Service	This test service is used to check the mail routing which generates a simple reply mail.
Print Service	This service enables the printing of mails at the server end.
Request Service	This service is used for the script-driven processing of messages at the server end and can, for example, be used for handling mailing lists.
Directory Synchronisation	This service enables the synchronization of directories between several Samsung Contact servers.
Bulletin Board Service	This service is used to replicate bulletin boards (shared folders) between different Samsung Contact servers.
Background Search Service	This service is used for the asynchronous search for information in a message store.
Client Directory Access Service	This service processes the entries in the central directory, for example, in order to be able to make these available as a global address book in the Outlook client.
Application Link Service	This service enables the linking of external applications, such as fax gateways.
POP3 Service	This service makes the contents of a mailbox available via the POP3 protocol.
omscan Service	This service is used to check the consistency of the message store.
Directory Relay Service	This service is used to access directories on remote Samsung Contact servers.
Container Access Monitor	This service checks the rights to access the message store.
Notification Service	This service notifies client processes on the occurrence of an event (such as arrival of a new messages or a hit by the search service).
LDAP Service	This service exports the internal directory via LDAP in version 3. OpenLDAP serves as LDAP server.
Queue Manager	This central process ensures the secure administration of the message queues.
Item Delete Daemon	This background process is used to remove deleted messages from the message store.
IMAP Service	This service makes the contents of a mailbox available via the IMAP protocol.
SMTP Relay	This service is used to receive messages via SMTP. Prior to delivery to a mail node, the recipient is searched for in the directory. The SMTP gateway supports anti-spam mechanisms and SASL-based authentication.
SMS / Pager Service	This service enables the receiving and sending of SMS and/or pager messages.

Technical description of the migration paths

The mail transport agent (MTA) used by default is sendmail. The use of postfix is generally also possible. Apache is recommended as the web server for the web client and the administration frontend.

Samsung Contact supports both a single-server installation as well as distributed installations at several sites. However, the mailbox of a user is always assigned to one server node. This directory can be replicated on a site-spanning basis. The *Public Shared Folders* known from the *Microsoft Exchange* environment are implemented via bulletin boards (BB). These can also be replicated in a site-spanning manner which is particularly favorable in the case of narrowband connections between two sites.

A special API and the *Application Link Service* are available for linking external applications to the groupware solution. This interface is used, for example, by the company VIPcom (www.vipcomag.de) and by Ferrari (www.ferrari-electronic.de) in order to link a unified messaging system (voice, fax).

The system design of Samsung Contact was optimized with a view to its high-availability capability. Most system parameters can be changed without interrupting operation and without the need to restart the entire system. Operation of the system in an HA cluster is recommended as effective protection against hardware failure of a mail node. The HP solution in the form of the HP Service Guard product is traditionally recommended for this purpose. Any cluster software can in general be adapted to Samsung Contact as long as such software permits the taking over of a joint storage node (RedHat Advanced Server, Steeleye, Polyserve, Failsafe, Linux Heartbeat).

Clients

Samsung Contact offers a wide range of supported clients. Besides an MAPI provider for connecting Microsoft Outlook clients, a groupware client developed in Java and a corresponding web interface are also available. The client is by default connected via the UAL protocol. This is a simple socket protocol for which an open C and Java API exist. The Samsung MAPI provider and the web client use the C API, whilst the Java client uses the Java API.

Alternatively to the Samsung clients, the contents of the mailboxes and the standard POP3 and IMAP4 protocols can be requested. This means that any mail client with POP3 or IMAP support can be used to receive and send e-mails (Eudora, Evolution, Mozilla, Netscape, Outlook Express, K-Mail). A modified version of a web client exists for WAP access.

The Outlook clients can be used thanks to the MAPI implementation of Samsung Contact. All major functionalities of an Exchange server are represented. This also includes all important groupware features. SC enables the assignment of privileges to other users for accessing individual folders (mail, appointments, contacts, tasks). The public shared folders known from Exchange are made available in the form of bulletin boards. The definition of server-end rules concerning the distribution of incoming messages and the automatic generation of an absence message are also supported. A proxy can be defined for an absent

user, with the proxy having the user's access privileges during the absence period. Appointments for meetings are supported, in analogy to the Microsoft Exchange procedure, by a free-busy list which is managed in the directory of the Samsung Contact server. An offline folder synchronization feature was implemented in order to enable mobile use.

Security

Samsung Contact does not offer message encryption by default. However, solutions are offered by third-party suppliers which enable S/MIME-conforming end-to-end encryption (certificates) within Outlook (such as Entrust). Encryption of the connection between client and server (POP3 / IMAP) can be achieved via an upstream SSL tunnel (stunnel).

User authentication is implemented via a PAM architecture. This is used both by the server processes for the UAL/IMAP/POP3 protocol and by the command line tools for administration purposes. Besides authentication against the Samsung Contact directory, authentication against external instances is also possible. The present scope of delivery includes PAM modules for authentication against UNIX accounts as well as against external Radius and SMB servers (Samba). Samsung Contact enables a detailed definition of access rights for the following server resources in the form of so-called access control lists (ACLs):

> Bulletin boards (public shared folders)
>
> Directories
>
> Service processes
>
> Print server
>
> Scripts of the request service

The maximum size of the memory space which can be used by one user can be limited in the form of quotas.

No special backup software is necessary for the message store. Any product available for the respective server operating system can be used. The system design of Samsung Contact permits consistent backups during ongoing operations. A command line tool is available for the single-user backup/restore functionality. This means that a single user can be easily moved from one mail node to another.

Any SMTP-based antivirus gateway (MIME-Sweeper, Trendmicro Viruswall) can be generally used. The AHN antivirus product (www.ahnlab.com) is integrated at the server end. Besides virus protection, filtering of mails on the basis of user-defined mail filters is also enabled at the server end. These filters are configured via a web frontend. The SMTP relay supports antispamming according to RFC 2505.

Administration

Administration of a Samsung Contact mail node is possible in two different ways. A simple web frontend exists on the one hand for creating users, distribution lists

and directories, and a large number of command line tools are available for the administration of all components on the other. The web frontend is designed for daily routine use. The command line interface is primarily suitable for automating administrative tasks.

The administration of the system can be carried out by any user having administrative privileges. An additional entry in the system directory determines whether a user is authorized to act as an administrator.

Migration

Migration from an *Exchange* or Outlook environment to Samsung Contact is possible in different ways. If the number of users is not too large (< 100), the manual export of mailboxes, appointments, contacts and tasks into a local PST file, followed by a manual transfer to a folder structure at the server end can still be achieved with a reasonable effort. The mailboxes and users are then also created manually in such a case.

In larger system environment, manual migration is no longer reasonable from a cost and efficiency perspective. A commercially available migration tool should be used in environments of this kind. Depending on the particular manufacturer, fully automatic import of all data, including reconfiguration of the Outlook clients, is possible. The following information can be migrated at the server end:

Users (without passwords)

Calendar entries

Directory entries

Public distribution lists

Folder hierarchy, including all contents (mail, appointments, tasks, contacts)

Bulletin boards

Server-based rules

Access control lists

We recommend involving an external service provider having the required expertise to prepare such a migration project.

Conclusions

Samsung Contact is a full-scale replacement for a *Microsoft Exchange server* both for very large installations and for smaller ones. All groupware functionalities of an Exchange server are supported. Form applications are an exception. However, a third-party supplier is working on this issue.

The basic technology has been available on the market for more than 15 years. The product is in use in a large number of reference installations. The recent acquisition by Samsung ensures the further development of the projects for the coming years.

3.14.4.6   Summary

Some groupware solutions are currently available under Linux with a functionality similar to that of Microsoft Exchange. The solutions generally pursue two different strategies as follows:

Browser-based access to the groupware servers, dynamic processing of the data on the server

Access to the groupware server using special client software

The table below gives an overview of the most important functionalities of the different groupware solutions.

Table 30: Alternative groupware solutions

	phpGroup ware	Kroupware	exchange4 linux	SuSE Linux OpenExch ange Server 4	Samsung Contact
Outlook support					
Outlook connection	No	Connection via Bynari Insight connector	Connection via N&H MAPI Service Provider	Replication – no reconcilia- tion in realtime as in the case of connectors	MAPI connector
Global MAPI address- book	No	Yes	Yes	No	Yes
Mail	No	Yes	Yes	Yes	Yes
Contacts	No	Yes	Yes	Yes	Yes
Tasks	No	Yes	Yes	Yes	Yes
Appoint- ments	No	Yes	Yes	Yes	Yes
Other client systems					
Palm Pilot Synchron- ization	No	Yes, via KDE and Outlook client	Via Outlook	Via Outlook	Via Outlook
Groupware functionalities					
Web portal	Yes	No	No	Yes	Yes
Contact administra- tion	Yes	Yes	Via address adminis- tration	Yes	Yes
Calendar	Yes	Yes	Yes	Yes	Yes
Task manageme nt	Yes	Yes	Yes	Yes	Yes

Technical description of the migration paths

	phpGroup ware	Kroupware	exchange4 linux	SuSE Linux OpenExch ange Server 4	Samsung Contact
Notes	Yes	Yes	Yes	Yes	Yes

The functionalities described for the above-mentioned groupware solutions show that adequate Linux-based products are already available. The selection of a particular groupware solution is based on the following criteria:

Use of the Microsoft Outlook client

Use in heterogenous client environments, simultaneous use of Linux-based client systems and of the Outlook client

Use of a web-based solution

Use of Outlook

The Kroupware, SuSE OpenExchange and Samsung Contact products are generally the more suitable candidates for continued use of Outlook as the client system. The non-existent realtime connection of the SuSE OpenExchange product to Outlook at present still restricts the former's functionality, so that it will not become an interesting alternative for many users until the realtime connection to Outlook is implemented. The exhange4linux and Samsung Contact products presently offer the more profound Outlook support. The Kroupware solution introduced above may become an interesting alternative in future, especially in heterogenous system landscapes (see below). In view of the lack of results from the productive environment, it is not yet possible at this point to make any concrete statements concerning the practical suitability of this solution. For organizations with several hundred users, the exhange4linux server constitutes a stable groupware platform which has also demonstrated its value in practical use. Samsung Contact which has been on the market for a long time and which offers good Outlook support is a promising alternative, especially for larger organizations. Thanks to the good scalability of the system, it is even suitable for use in organizations with several tens of thousands of people. The acquisition of HP OpenMail by the Samsung group has also answered the question[74] concerning further development and support offers.

Heterogenous client landscapes

Organizations using different operating systems at the client end will be able to use Samsung Contact and, in future Kroupware, for example. Samsung offers an own Java-based client which offers the desired groupware functionalities independent of the operating system. In this way, Outlook and/or the Java client can be used on Windows-based systems and the Java client only on Linux-based systems. Kroupware will in future also implement a potential solution for hybrid

---

[74] Refer also to the feasibility study for a German Federal Ministry from 2001

system landscapes. The possibility to simultaneously use Outlook and the KDE client offers users the respective groupware functionalities even offline.

Web-based solutions

The phpGroupware solution which is subject to GPL and the commercial OpenExchange solution offer a very extensive functionality to organizations preferring a web-based approach. OpenExchange additionally enables connection to the Outlook client, however, subject to the restriction that realtime connection is not available.

3.14.5   Continuing migration

3.14.5.1   Exchange 2000

New features

The most far-reaching change in architecture in conjunction with the launch of Exchange 2000 compared to Exchange 5.5 is the shifting of the Exchange directory service to the Windows 2000 active directory (AD). This means that Exchange 2000 no longer includes a directory service of its own and hence requires an active directory as a mandatory feature. Furthermore, Exchange 2000 cannot be installed on Windows NT servers, but on Windows 2000 servers only.

The former Exchange 5.5 structure unit "Site" is subject to the following changes:

> The active directory is solely responsible for directory replication; the sites introduced there should not be mistaken for the sites from Exchange 5.5.

> Exchange serves are structured in "administrative groups" for administration purposes.

> Furthermore, Exchange servers are divided into routing groups which do not necessarily have to be identical to the "administrative groups".

Since the Exchange 2000 servers no longer contain a directory service, a service is necessary which provides comprehensive information beyond domain boundaries, i.e. the Global Catalog (GC). The GC can be made available on Windows 2000 domain controllers only. It contains information concerning all the objects of a Windows 2000 overall structure (forest), however, concerning selected attributes only. Modern clients (such as Outlook 2000 or 98 SP2) can receive information directly from the GC, whilst older client versions are served by the Exchange 2000 server which acts as proxy and passes the query on. In contrast to this, every Exchange server in Exchange 5.5 includes a directory service.

The distribution lists in Exchange 5.5 are replaced by e-mail-enabled groups in the active directory. Pure distribution groups and security groups exist in the AD. Security groups are also e-mail-enabled, so that redundancies can be prevented. Remember that the AD contains groups with different validity (visibility) areas: domains (global and local) and universal groups (in native mode of the domain only). Only the universal groups are visible beyond domain boundaries.

Technical description of the migration paths

In Exchange 2000, the draft is no longer determined by the administration model of the Exchange environment because servers can be organized separately by administrative groups and routing groups. However, this separation is only possible if Exchange 2000 itself is executed in native mode, i.e. if no 5.5 servers are or will be used any longer.

Exchange 2000 offers a guideline model for administration purposes. This model enables administrators to change options for one object group (such as user mailboxes, servers and public folders) in one operation.

Transport between the Exchange 2000 servers now takes place via SMTP (Simple Message Transport Protocol). Exchange 5.5 uses RPC. SMTP is already integrated into Windows 2000, just as much as NNTP.

The routing group connector of Exchange 2000 replaces the site connector.

The following connectors are available:

X.400 connector (no longer contained in the MTA of Exchange 2000)

Microsoft Mail Connector

CC:Mail Connector

Lotus Notes Connector

Novell Groupwise

Up to four storage groups with up to four databases can be created per Exchange 2000 server. This offers certain advantages, especially with a view to data backup and data recovery.

Indexing the Exchange database is now possible.

Exchange clusters can be operated in "active-active" mode.

Outlook Web Access (OWA) now supports WebDAV (Web Distributed Authoring and Versioning), a further development of HTTP 1.1. An advantage with regard to OWA is the fact that Exchange servers can be configured as frontend and as backend, so that OWA servers themselves do not contain any data stock.

Furthermore, installation of

chat services

and instant messaging services

is now possible.

The separate, new "Exchange 2000 Conferencing Server" product variant also enables audio and video conferences, for example.

The development environment of Exchange 2000 is upgraded by

the improvement of CDOs (Collaboration Data Objects)

extended workflow mechanisms

the introduction of XML

and the increased integration of IIS (Internet Information Server) and ASP (Active Server Pages).

Remarks concerning migration

Migration from Exchange 5.5 to Exchange 2000 is a complex process that requires intensive preparation, concept development, migration planning and production-near testing. Although this guide cannot address these tasks in an exhaustive manner, some important aspects of a migration project should nevertheless be mentioned.

First of all, however, some terms should be defined. An *Exchange 2000 upgrade* refers to the installation of Exchange 2000 on an Exchange 5.5 server. The term *operating system upgrade* of a server refers to the installation of Windows 2000 on a Windows NT 4 server.

The fact that Exchange 2000 can only be used if a Windows 2000 active directory exists leads to several technical boundary conditions, including the following:

The domain structure of the Windows 2000 active directory has stronger repercussions on Exchange 2000 than the domain structure under Windows NT on Exchange 5.5. The forest constitutes the boundaries of the Exchange organization because the domain-spanning collective information of the Global Catalog (GC) exists only once in a forest.

The OU structure chosen for the Windows 2000 domains has primarily no repercussions on the migration of Exchange 2000.

The introduction of Exchange 2000 requires a schema amendment of the active directory. This amendment can be carried out without the need to install Exchange 2000 itself (key word: forestprep). Furthermore, the domain concerned must be prepared (key word: domainprep).

The operating mode (native vs. mixed mode) of the Windows 2000 domains influences the availability of universal groups and hence the visibility of e-mail distributors.

An *Exchange 2000 upgrade* is only possible after a prior *operating system upgrade*. It is not possible to install Exchange 2000 on Windows NT 4. In contrast to this, Exchange 5.5 can run on Windows 2000.

An *operating system update* of an Exchange server requires careful analysis (service packs, etc.), especially in cases where additional third-party software (such as antivirus software) is installed.

Before the first *Exchange 2000 update* is carried out, the Exchange servers must be members of a Windows 2000 domain and/or of a forest.

Users must logon at an active directory if they wish to and/or are required to use Exchange 2000.

Technical description of the migration paths

The complexity of the complete portfolio of migration scenarios (complete NT domain models, several Exchange organizations, Exchange in resource domains, Exchange on domain controllers, distributed sites, Windows 2000 forest, etc.) is not addressed within the scope of this guide. However, some tools that can facilitate migration and/or coexistence should be mentioned here.

Active Directory Connector (ADC) enables replication of a hierarchy of directory objects between an Exchange server 5.5 directory and an active directory. ADC thus plays an important role for the migration of Exchange 5.5 to Exchange 2000. Note that there are two ADC versions (on the Windows 2000 CD and on the Exchange 2000 CD). With regard to migration to Exchange 2000, the latter version is the relevant one.

The Site Replication Service (SRS) enables Exchange 2000 servers to replicate the Exchange 5.5 configuration.

3.14.5.2   Exchange 2003

Exchange 2003 (code name: Titanium) is the successor to Exchange and is due to be launched before the end of 2003.

The number of new features compared to Exchange 2000 is relatively small. The main reason for the introduction of Exchange 2003 is the fact that the changes in Windows 2003 compared to Windows 2000 no longer enable the installation of Exchange 2000 on the Windows 2003 platform. This means that Exchange 2003 only can be installed under Windows 2003[75].

The compatibility matrix below gives an overview of the different combinations of Exchange 5.5, Exchange 2000, Exchange Server 2003 and Windows Server 2003 which are supported.

Table 31: Compatibility matrix – Exchange[76]

	Installation and execution of Exchange under		Active directory environments supported	
Exchange version	Windows 2000 SP3 or higher	Windows 2003 server	Windows 2000 SP3 or higher	Windows 2003 server
Exchange 5.5 SP3	Yes	No	Yes	Yes
Exchange 2000 SP2	Yes	No	Yes	Yes
Exchange 2000 SP3	Yes	No	Yes	Yes
Exchange 2003	Yes	Yes	Yes	Yes

---

[75] German Whitepaper "Microsoft Exchange Server – Kompatibilität mit Windows Server 2003"

[76] German Whitepaper by Microsoft "Microsoft Exchange Server – Kompatibilität mit Windows Server 2003" (http://www.microsoft.com/germany/library/resourcesmod/exchange+titanium+und+windows+server+2003.doc)

The illustration below outlines the possibilities of hybrid environments.
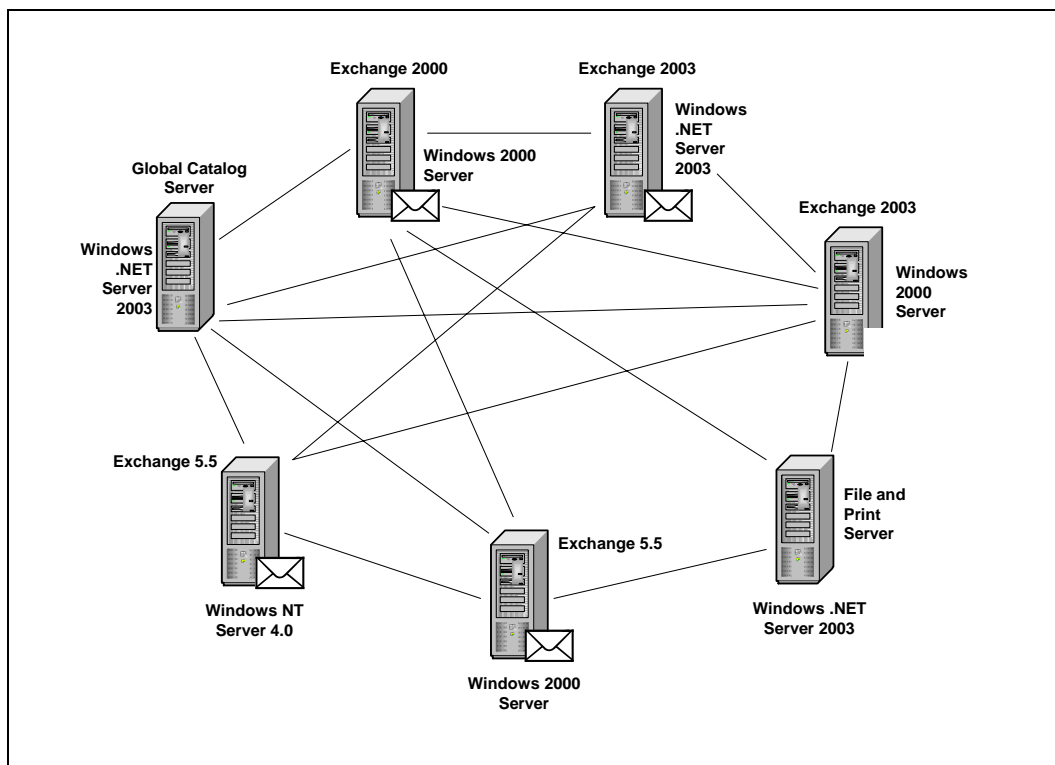
Fig. 31:   Hybrid environments – Exchange [77]

New features of Exchange 2003 include the following:

Outlook Mobile Access (currently Microsoft Mobile Information Server 2002) will be included in Exchange Server 2003. Outlook Mobile Access offers users or mobile devices access to their personal information.

In Exchange Server 2003, the Internet Information Server (IIS version 6 in Windows 2003) enables a new form of communication between Outlook and Exchange, which is referred to as "RPC via HTTP". In this way, Outlook users can directly synchronize their data with an Exchange Server 2003 via a HTTP connection in a secure manner.

Clustering support in Windows 2000 Advanced Server is limited to two nodes or four nodes if the Windows 2000 Server DataCenter Edition is used. Windows 2003 and Exchange 2003 now enable the implementation of clusters with up to eight nodes with at least one passive node if Exchange Server 2003 and Windows Server 2003 Enterprise Edition are used.

---

[77] Source: German Whitepaper "Microsoft Exchange Server – Kompatibilität mit Windows Server 2003"

Exchange 2003 uses under Windows 2003 the volume shadow copy service and thereby enables shorter backup and recovery times for Exchange environments.

3.15 Office / desktop

3.15.1 Overview

With a view to replacing MS Office 97 or Office 2000, it will certainly make sense to await the launch of MS Office 2003 and first experience with MS Office 2003, all the more so since the launch of MS Office 2003 has been announced for summer 2003. Besides the pure cost aspects, technical considerations play a particularly important role with regard to the anticipated changes in document format. Microsoft plans to establish XML as the main format for Office documents with MS Office 2003. In this context, one cannot rule out that the present problems of compatibility with the alternative OpenOffice.org OSS solution and StarOffice as its commercial counterpart will be reduced or even eliminated. Given a positive outcome of the compatibility check concerning the exchange of documents between MS Office 2003 and OpenOffice 1.1 or StarOffice 6.1, respectively, one would have to analyze the actions and costs resulting from the import of existing Office documents to MS Office 2003. In another step, these actions and costs would then have to be compared to the actions and costs which are today already largely known for migration to OOo/SO.

Only then should a decision in favor of MS Office 2003 or OOo/SO be made.

The substitution of the Microsoft desktop will eventually be determined to a significant extent by the question as to whether MS Office can be replaced by OOo/SO on the one hand and whether necessary Windows applications will be available in the long term as Linux applications on the other and how good these applications can in the meantime be made available as Windows applications on the Linux desktop. This must, however, be examined from case to case.

3.15.2 Introduction

The desktop is the interface visible to users, providing them with the tools and applications which they need for their day-to-day work. Work with the Microsoft Office package (MS Office) stands in the foreground in this context. However, various other standard tools are also available to users the functionalities of which remain available even after migration. Furthermore, various specialist applications exist in addition which are more or less integrated into the desktop and which are often Windows applications which cannot be directly executed under Linux. The technical discussion in the following is thus divided into five sections as follows:

MS Office: the starting situation

Replacing migration of MS Office

Continuing migration of MS Office

Further desktop applications

Windows applications under Linux.

3.15.3   MS Office: the starting situation

MS Office is available in different packages and versions. In contrast to the operating system, one does not have to assume that a particular MS Office version is used by the majority of public agencies. One can, however, assume that versions older than Microsoft Office 97 are hardly in use any more and that Microsoft Office XP is not yet very widely used. Most public agencies probably use Microsoft Office 97 or 2000. The following discussions will thus be based on these two versions as the starting basis for migration. Most of the new features of Microsoft Office XP compared to Office 2000 concern the user interface as well as the team work areas, with part of the additional functions in the team work area covering groupware functionalities which are already covered by other applications. Furthermore, Microsoft integrates the two areas, i.e. Office and SharePoint Services, stronger than before[78]. This will, however, mean only minor changes for day-to-day work. The new functionalities of Office XP will thus be addressed in selected contexts only.

Besides the versions, the different Office packages play an important role with a view to migration. These packages usually differ in terms of the individual applications which they comprise. Taking the Office 2000 Professional package as the basis, the sections on

> Replacing migration of MS Office and

> Continuing migration of MS Office

will discuss

> Word

> Excel and

> Powerpoint

as individual applications. Outlook will be discussed in chapter 3.11 as part of a groupware and messaging solution. Access will be analyzed and evaluated in conjunction with the migration of databases. Internet Explorer and PhotoEditor will be discussed in the section on "Further desktop applications" together with other desktop tools. The authors also briefly address MS Project in the same section.

3.15.3.1   Functionalities

A list of all functionalities available in Word, Excel and PowerPoint would go beyond the scope of this section. Instead, the following two chapters will explain the most important differences between the starting situation and possible future alternatives with a view to migration.

One aspect to be considered first is the sometimes intensive use of agency-specific software solutions which supplement the functionalities of MS Office.

---

[78] For details concerning the new features compared to earlier versions, refer to
   http://www.microsoft.com/germany/ms/officexp/prof/vergleich.htm

This means on the one hand that the programming environment available with MS Office is used by many public agencies and other organizations to create document-specific scripting solutions (macros) in order to largely automate work processes with MS Office. This even includes the implementation of department-spanning workflows. On the other hand, public agencies also use a number of external software solutions that are more or less integrated into Office. This is why the programming environment of MS Office will be briefly addressed in the following.

3.15.3.2   *The MS Office programming environment*

The programming environment of Microsoft Office is based on the BASIC programming language. The Microsoft-dominated world currently refers to this language as Visual Basic. This family of languages currently includes several dialects as follows:

Visual Basic (Visual Studio, Vollversion)

Visual Basic for Application (VBA)

Visual Basic Scripting Edition (VBS).

Although all the dialects have the same basic vocabulary, they differ in terms of functionality and execution environment.

The programming environment of MS Office includes Visual Basic for Application (VBA). VBA is available under a Microsoft license, so that third-party manufacturers can integrate VBA into their products.

The use of the Office 97 package is assumed as the starting point for the purposes of this guide. Earlier versions provided different programming environments for the different products (Word Basic, Excel VBA, Access Basic). Office 97 standardized the programming environment as VBA version 5. The table below shows the VBA versions vs. the different Office versions.

Table 32: VBA versions

Office versions	VBA versions
95	Word Basic, Excel VBA, Access Basic
97	5
2000	6
XP	6.3

VBA will be primarily discussed in the following and especially the variants of Visual Basic (full version and Scripting Edition) for differentiation purposes.

VBA basic concepts

VBA is an interpreter language that can be executed in Office applications only. VBA is based on the COM (Component Object Model) which is a further development of the OLE (Object Linking and Embedding) technology.

Office itself is not just capable of using COM objects, but even offers COM objects itself. Office 97 comes with more than 550 own COM objects, Office 2000 with more than 600. Via COM, it is also possible to use external functionalities in Office. VBA enables the use of external programs (such as the operating system) in the form of DLLs (Dynamic Link Libraries)[79].

The illustration below once again shows the possibilities of VBA to use functionalities.
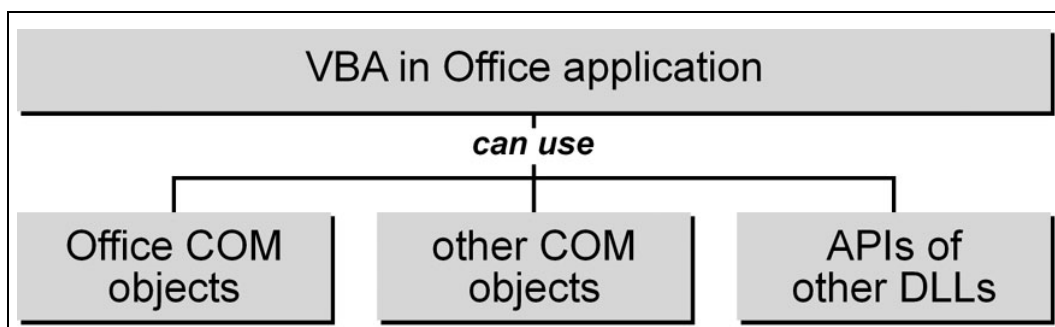
Fig. 32:   VBA in the Office application

In VBA, the individual module types are differentiated further in terms of

Modules

Class modules

Forms

Modules contain "normal" program code. Class modules can be used to create own objects as well as their properties and methods.

These modules enable the expansion of functionalities existing in MS Office, the automation of sequences of function calls, as well as the implementation of additional functionalities. Amendments, automated functions and additions are referred to as macros and scriptings. In order to integrate these macros in MS Office, the menu bars and buttons of the symbol bars can, in particular, be modified in order to facilitate their use.

Special procedure names (such as AutoOpen, AutoNew) identify the program code which us executed automatically when Office files are opened. This feature is often used in templates and involves the **risk of so-called "macro-viruses"**.

Macros and scriptings can be activated and integrated in the following forms in Office:

---

[79] Visual Basic Script (VBS) does not yet permit such integration.

as add-ins

in templates

as wizards

Add-ins can be further distinguished as follows, depending on their use:

COM add-ins and

application-specific add-ins

COM add-ins are compiled DLL or EXE files which are generated by Visual Basic (full version). These add-ins can be used in an application-spanning manner.

Application-specific add-ins are generated by the integrated programming environment of Office and can be used within Office only. Add-ins are typically used where the program code must be permanently available in the application, so that the user does not have to start any templates.

The illustration below once again gives an overview of the expandability options in MS Office by user-specific programming.

Office expandability options by user specific programming							
Add-ins		Wizards		Templates			
COM add-ins	application-specific add-in	Power-point	Word	Access	Excel	Power-point	Word
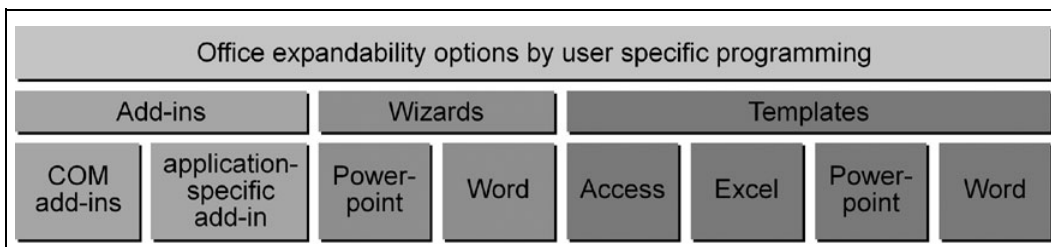
Fig. 33: Expandability options of Office

Developer environment

With VBA version 5, a uniform development environment was integrated within the Office application. Although the so-called IDE (Integrated Development Environment) is started in a separate window, it runs in the same memory area of the Office application.

IDE comes with:

an editor with syntax check and color highlighting

a project explorer

an additional properties window

debugger tools

an object browser

conditional compilation

protection mechanisms against changing or copying of the code programmed

and IntelliSense (completion, drop-down selection, syntax information)

Besides this editor, a macro recorder can also be used in the application in order to generate the simple program code.

Remote control

Since Office itself consists of a large number of COM objects, remote control of Office, i.e. COM automation, is possible.

Windows Scripting Host (WSH) or PerlScript can, for example, be used for remote control.

3.15.4   Replacing migration

3.15.4.1 Introduction

A whole range of Office software packages or sub-applications (such as word processing) are available as free or proprietary software for the Linux operating system. Some examples of these packages are listed below:

OpenOffice

StarOffice

Koffice,

GnomeOffice

ThinkFree Office

and many more

All experts agree that, from today's point of view, only the OpenOffice.org (OOo) package and the StarOffice (SO) package based on it are a real alternative to the MS Office suite. This guide will hence discuss these two packages only in detail with a view to migration.

OpenOffice is currently available as version 1.0.3, the equivalent being StarOffice 6.0. Both versions can also be used for the Windows NT, 2000 and XP operating systems. OOo/SO features the same functionality and the same file format on all operating systems supported and hence facilitates "gentle" migration in that only the Office package is replaced during the first step. The new versions 1.1 (OOo) and 6.1 (SO) are already available as beta versions, and are scheduled to be released as the final version in July 2003.

Differences between OpenOffice and StarOffice

The basic technology of the two Office suites is developed on the basis of OpenOffice.org. In 2000, Sun Microsystems migrated the source text of the then StarOffice 5.2 Office package to the OpenOffice.org Open Source project. The OpenOffice.org project is subject to the double license of GPL and SISL (GNU Public License or Lesser GNU Public License, respectively, and Sun Industrie Source License). The double license permits the commercial products to be derived from OpenOffice.org on the one hand. On the other hand, it guarantees that the specifications of the API and of the file format are binding upon and uniform for OpenOffice.org and all derivatives.

Technical description of the migration paths

Sun has developed and/or added new components for StarOffice and compiled a product package which includes professional quality assurance, comprehensive documentation, support and training offers. Some of the Sun components are:

TrueType fonts similar to those of Microsoft (refer to Fig. 34:   MS   Office OOo/SO fontmapping

)

An own spell-check function and thesauruses, with OpenOffice typically using MySpell (LGPL)

Additional templates and a picture gallery

the ADABAS database.

Furthermore, Sun offers bug patches or service packs for the different product versions. At present, a new StarOffice service pack with improved security aspects, bug fixes or improvements in import filters is released every three months. In contrast, OpenOffice.org contains these components in its latest version only[80].

Fig. 34:   MS Office OOo/SO fontmapping[81]

Unlike the free OpenOffice.org suite, the StarOffice suite is available against payment only. Support services must usually be paid for with both variants. StarOffice support is offered directly by Sun and other suppliers, whilst support for OpenOffice.org is available from third-party suppliers only.

Constituent parts of OOo and SO

OOo and SO, just like MS Office, consist of several sub-applications. These include:

Word processing (Writer)

---

[80] For further details concerning the differences, please refer to:
http://marketing.openoffice.org/conference/presentationspdf/thu1500/SOvsOOo.pdf

[81] Source: SunMicrosystems

Spreadsheet (Calc)

Presentation (Impress)

Formula editor[82] (Math)

Drawing[83] (Draw)

Database[84] (Adabas)[85].

The following discussion will, however, focus on the first three of these modules only.

The three Office suites are identical in their most important functionalities, especially those which are used by the majority of all users. Most users typically use the same small set of functions out of the overall functionality which is available. The following chapters will address the most important differences between MS Office and OOo/SO in detail. This guide initially focuses on the word processing, spreadsheet and presentation modules. Chapter 3.13 discusses a potential replacement of the MS Access module with another database system in more detail. Chapter 3.15.6 describes further modules of the MS Office suite and other applications of the MS desktop.

3.15.4.2 File format differences compared to MS Office

Every Microsoft Office version uses its own binary file format to store text, attributes, embedded pictures, meta data and layout elements as OLE-structured data.

In contrast to this, OpenOffice.org and StarOffice 6.0 (OOo/SO) use an XML-based file format which stores contents as plain text and which can hence be directly read and processed further without OOo/SO required to read and decode. The format is publicly documented and available as a free format as part of the OpenOffice.org project.

The XML-based file format of OOo/SO stores contents, layout and formatting information of every document as a separate set of XML streams or sub-documents.

In order to enable the user-friendly use of the different documents and XML streams – besides the pictures and external data (if any) embedded in binary form – such documents and XML streams are stored in the familiar, compressed ZIP format. However, files generated by OOo/SO have different extensions for

---

[82] With Microsoft, the functions which Math offers are integrated via a specific editor which can be opened via Insert/Object/New/Microsoft formula editor.

[83] With Microsoft, the functions which Draw offers are currently integrated via the "Drawing" symbol bar.

[84] Not in OpenOffice.org

[85] Not directly comparable to Access under Windows.

different sub-applications, just like MS Office, rather than the ".zip" extension (refer to table 33).

Table 33: File extensions of the most important Office applications

Document type	MS Office application	Ex-tension	OOo/SO application	Extension
Text	Word	doc/dot	Writer	sxw/stw
Spreadsheet	Excel	xls/xlt	Calc	sxc/stc
Presentation	Power Point	ppt/pot	Impress	sxi/sti

Furthermore, OOo/SO additionally includes the Draw and Math sub-applications which form part of the three above-mentioned main applications in MS Office and which cannot be directly assigned to a specific application. Draw can be used to create drawing documents (sxd/std), Math being used for mathematical formulas (sxm/stm). Draw and Math objects can be linked to other OOo/SO document types where they can then be edited.

Since OOo/SO are ZIP files, they can be unpacked by any UNZIP program.
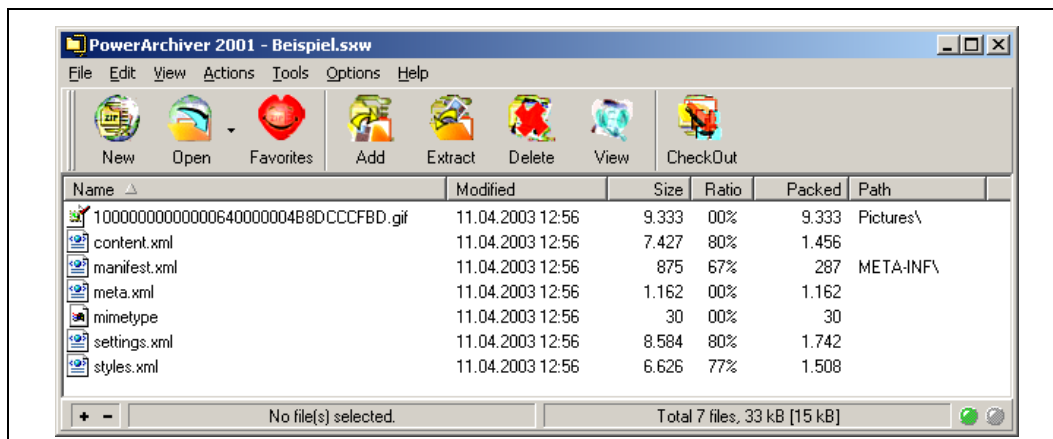
Fig. 35:   Contents of an OOo/So file as presented by a ZIP file viewer

Embedded pictures or objects, if any, are stored in the "Pictures" or "Objects" directory, respectively. These directories then include a reference (href-link) to the corresponding subordinate files.

A typical OOo/SO document which does not contain any embedded objects or pictures consists of 5 XML streams as follows:

content.xml
Stores the main contents of the document, including text tables and graphic elements. If embedded pictures or objects exist, these are then stored in the Pictures or Objects directories, with a reference (href-link) then referring to the corresponding subordinate files.

styles.xml

Stores the properties and attributes of all character, paragraph, page, object and numbering styles used in the document.

meta.xml

Stores general information concerning the document, including title, type, position, user, time saved last, and so forth. The contents of this file refer to the information entered in the File/Properties mask.

settings.xml

Saves application-specific document and view settings for the present document, as well as pre-selected printer properties and print options, zoom level and window size.

manifest.xml

Saves additional information concerning the XML files, such as MIME type and encryption method. This file, just like bitmap files and object files, is also saved in its own directory.

If the document also includes macros, the package contains further XML streams[86].

3.15.4.3 Restrictions concerning the conversion (import) filter

OOo/SO comes with several file format converters (filters) which enable the opening and editing of MS Office documents in OOo/SO and the subsequent storing of such documents as MS Office documents again. Furthermore, it is also possible to import and edit MS document templates. Files can be stored either in the MS Office 97/2000/XP format or in the OOo/SO format.

The conversion quality is generally acceptable unless complex documents containing macros and special format features are involved. MS Office features certain layout properties and formatting attributes which OOo/SO does not support or treats differently. This means that a converted document must be manually re-edited to a certain extent in order to obtain a format which corresponds to that of the original document. A 100% conversion success should not be expected especially in the case of complex and very product-specific document properties, such as indices, fields, frames and tables. Furthermore, differences between the original document and its converted counterpart can also occur after conversion of basic attributes and formatting instructions, such as page margins and blank spaces between paragraphs.

The table below shows the MS Office properties which may require manual re-editing after automatic conversion.

---

[86] For further information concerning the XML format of OOo/SO, please refer to http://xml.openoffice.org (general), http://xml.openoffice.org/xml_specification_draft.pdf (technical details) and http://xml.openoffice.org/package.html (Zip file format).

Technical description of the migration paths

Table 34: Problematic MS Office properties with a view to conversion OOo/SO

Application	Properties

Microsoft Word	AutoShapes
	Revision marks
	OLE objects
	     Certain control and form fields
	     Indices
	     Tables, frames and multi-column formatting
	     Hyperlinks and bookmarks
	     WordArt pictures
	     Animated text

Microsoft Excel	AutoShapes
	     OLE objects
	     Certain control and form fields
	     Pivot charts
	     New chart types
	     Content-depending formatting
	     Certain functions and formulas

Microsoft PowerPoint	AutoShapes
	     Spaces between tabs, lines and paragraphs
	     Background picture of the master
	     Grouped objects
	     Certain multi-media effects

3.15.4.4 Functional differences

At a concept level, there is no fundamental difference between MS Office and OOo/SO. Both systems are based on a 3-layer architecture consisting of the application itself, the document templates and the documents. The lowest layer is the application layer containing the tools and the properties for creating documents and templates. The next layer is the template layer which can contain large numbers of objects, macros, formatting instructions and settings which simplify the creation of new documents. This concerns the documents which, at the top layer, can also contain further objects, macros, formatting instructions and user settings which supplement the functionality of the templates.

The difference between the two Office suites lies in the features and functions which they offer and support. In many cases, these differences concern the design selected and the different object models underlying the applications. In most cases, the two suites already include equivalent properties corresponding to the individual features and functions of the other product.

The table below (table 35) gives an overview of the template and format types available in MS Office and OOo/SO for the different applications.

Table 35: Comparison of template and format types available

Type	MS Word	OOo/SO Writer	MS Excel	OOo/SO Calc	MS Power Point	OOo/SO Impress
Standard document template	normal. dot	hardcoded	bOOok.xlt sheet.xlt	hardcoded	blank.pot	hardcoded
Document template	Various	Various	Various	Various	Contents/ design templates	Contents/ design templates
Format templates	N/a Paragraph Character List[88] N/a Table[90]	Page Paragraph Character Number-ing Frame[89] Table	Page/ sheet Cell	Page/ sheet Cell	N/a[87] N/a	Picture templates Presen-tation

The table below (Table 36: Differences in the key functionalities) summarizes the differences in the key functions. The "StarOffice 6.0 Migration Guide"[91] gives a detailed description of further functional and other differences.

Table 36: Differences in the key functionalities

Feature	Remarks
Macro recorder	MS Office comes with a macro recorder. Neither OpenOffice 1.01 nor StarOffice 6.0 have a macro recorder. The macro recorder is planned for the successor version, and is already implemented in the beta version which is currently available.
Document-based macros	OOo/SO does not support any VBA macros because of the differences between the two object models. VBA macros must be (manually) converted in order to be reused. However, OOo/SO documents can contain macros in their own programming language (StarBasic). However, VBA macros are not lost during import or export.

---

[87] PowerPoint provides a pre-defined color and amination pattern which is valid for the complete presentation. In contrast to this, Impress uses styles for defining the graphic layout and for the presentation of individual objects.

[88] MS Office XP only.

[89] Frames are embedded objects which are surrounded by an invisible box.

[90] MS Office XP only.

[91] http://uk.sun.com/software/staroffice/pdf/somigrationguide.pdf

Technical description of the migration paths

Feature	Remarks
3D graphics	MS Office uses the "Escher 3D Graphic-Engine" which is not identical to the OOo/SO 3D-Engine. This means that minor differences may occur in the rendering of 3D objects if 3D objects are imported from MS Office.
	The filters available in OOo/SO do not support the export of 3D objects to the Escher 3D format.
Table (MS Word)	OOo/SO and MS use different table models, so that minor differences may occur in the rendering of tables. OOo/SO does not support the following MS features:
	New page within a line
	Background patterns in cells
	The rendering of frames can differ after conversion because OOo/SO does not support all the MS Word line types.
Character formats (MS Word)	Word permits the selection of different formats for the list characters and for the list contents. This feature is implemented in Writer by assigning a dedicated character format for the list character.
Character and space metrics (MS Word)	Inter-character spaces are normally slightly smaller in Word than in Writer. The two applications use different metrics for vertical spacing (Word = points, OOo/SO = Inch). This means that the number of lines can vary from application to application within the same document.
Worksheet size (MS Excel)	The maximum capacity of a single worksheet in Calc is limited to 32,000 lines. Excel, in contrast, has a limit of 65,536 lines. When an Excel sheet with more than 32,000 lines is imported, Calc distributes the entries to several worksheets.
Pivot charts (MS Excel)	Excel supports pivot charts for complex data analyses.
	Calc includes a comparable tool called "Datapilot", however, with fewer analysis functions and without support for dynamic chart creation.
	When an Excel document making much use of pivot charts is imported, functionalities will get lost.
Chart types (MS Excel)	The Chart Engine in Calc is by far less powerful than in Excel. Various chart types in Excel have no equivalent in Calc[92]. When documents of this kind are imported, Calc tries to select a chart type as similar as possible.
Optional parameters	In contrast to Calc, Excel supports functions with missing optional parameters. During conversion, OOo/SO generates an error message in order to confirm this condition. A valid standard value must be manually added in the functions concerned in the place where the optional parameter is missing.
Timeline (MS PowerPoint 2002)	PowerPoint 2002 uses the timeline functionality which enables animation of objects with precise timing. OOo/SO does not have a comparable feature.
	Furthermore, PowerPoint XP enables the definition of different time intervals for different objects. The current Impress version enables just one time interval to be determined for all objects.

---

[92] For details, refer to the "StarOffice 6.0 Migration Guide", pages 56-59.

Feature	Remarks
Merge documents (MS Word)	Both Writer and Word support the use of so-called "merge documents" being a combination of Excel worksheets with a Word document, for example. The implementation of this functionality in Word is somewhat different than in Writer and the filters available do not support this functionality. Although the corresponding documents are imported along with the linked fields, the link must be made manually in the data file.
VBA macros	Macros created in MS Office cannot be executed in OOo/SO. If these macros are to be reused following conversion, they must be created anew in OOo/SO or adapted to StarBasic. New macros can be created under OOo/SO using a corresponding development environment which is accessed via Tools/Macros and the "Edit" button. However, MS Office documents can be opened, read, edited and saved with OOs/So in a hybrid environment (MS Office – OOo/SO) without existing VBA macros getting lost or being destroyed.

3.15.4.5 Important stock-taking criteria

Before a fundamental decision in favor of or against migration and subsequent detailed planning is possible, the following questions must be answered within the scope of stock-taking:

What is to be migrated?

Is migration possible?

Which efforts/costs will be involved?

During stock-taking, the documents should be analyzed and, if necessary, categorized with a view to the following criteria:

Availability of the documents

- Documents which may have to be processed/edited further
  Conversion can make sense in the case of these documents.

- Documents which are to be read again only, if at all.
  It should be considered whether these documents should be archived and/or converted to PDF in the case of migration. The migration effort is reduced by this.

Complexity of documents

- Simple documents
  These documents do not contain any macros, proprietary graphics (such as WordArt), vector graphics, complex formatting instructions or elements like footnotes, tables or indices. These documents are most easily converted in a batch process (refer to the section on "conversion methods" in chapter 3.15.4.7).

- Complex documents
  These documents contain macros, shared components, paragraph

and page formatting instructions, proprietary and vector graphics, many links and cross-references, OLE objects, frames, text boxes, footnotes, active components, form fields, form controls, forms or charts, i.e. a host of different formats and elements. These documents normally require additional planning and should be evaluated and converted individually.

Complexity of templates

- Simple templates
  Simple templates consist of generic text and the corresponding formatting which serve as the starting point or rough models for new documents. Good examples of this are model letters, general reports or minutes. The same conversion options are available for simple templates which also exist for simple documents.

- Complex templates
  Complex templates contain form fields and macros which are not always easy to convert and which must be created anew using the OOo/SO development environment or which even require reengineering.

Use of external data sources
External data sources must usually be re-linked. This is normally possible without any major problems. Data sources of this kind are, for example, databases and Excel documents.

Integration of external software
In these cases, the extent of the integration project and the number of applications concerned must be checked on the one hand, and the availability of the source text must be determined with a view to integration in OOo/SO. If external software uses MS Office via the OLE/COM automation interface, it is then also possible to link OOo/SO via this interface. The MS Office functions called must be converted to the corresponding OOo/SO calls.

3.15.4.6 *Preparing conversion*

Word documents

Many layout differences following conversion are due to "incorrect" formatting. In order to increase document layout fidelity, measures should be taken to ensure that the original text is and/or was formatted "correctly". The following advice should be followed during day-to-day work even if migration is not yet to take place immediately.

Use character and paragraph format templates rather than direct formatting.

Remove unnecessary (hard) returns between list entries in order to create additional free space between individual bullets. During conversion, these returns generate additional bullets without contents (blank list entries).

Do not use multiple tabs in order to create table columns. Define tabs in such a manner that only one tab separates the text between two columns. A table

creation tool can be used as an alternative. If multiple tabs are used, it may happen that a table is "out of range" after conversions because the two applications use different default tabs.

Make sure that the page format in the document is identical to the printer page size. OOo/SO does not adjust the page format automatically in order to ensure correct printer output.

Excel documents

Large and complex spreadsheets must be carefully checked with a view to special formatting techniques used and logic (formulas, add-ins) contained in the spreadsheets in order to ensure their correct conversion. This is especially important in the case of third-party and standard Excel add-ins.

Some of the aspects concerned will be briefly presented and explained in the following:

Check the settings for data sources of charts. Excel is generally much more flexible than Calc with regard to the data ranges of charts. OOo/SO stipulates, for example, that the labels be always located in the first line or column. Otherwise the charts are usually imported without labels.

Does a password protection system for documents exist? Calc is unable to open Excel spreadsheets that are protected by a password. This means that the protection must be disabled prior to conversion.

Avoid array constants in formulas. Unlike Excel, Calc does not support any array constants in formulas (such as {1,2;3,4}), but only cell areas which specify an array (such as {A1:B2}).

Avoid the use of special characters in the names of worksheets. Excel supports more special characters than Calc in the names of worksheets.

Avoid worksheets with more than 32,000 line entries and spreadsheets with more than 256 worksheets because Calc does not support more entries at present (refer also to 0).

Avoid different view settings for different worksheets which are supported by Excel. Calc enables such settings only globally for the complete document.

Check the cell size with regard to right-justified text. If the cell is too small, right-justified text is not extended to the left beyond the cell boundaries.

PowerPoint documents

Simple PowerPoint presentations are usually accepted by Impress correctly and without any problems. Presentations with extended layout functions and effects normally lead to a different rendering in the converted document.

The measures listed below are designed to help preserve the original formatting:

Avoid, remove or modify shadow objects which are not supported by Impress. Impress does not support all the shadow formats of PowerPoint. The illustration (Fig. 36: Shadow objects in PowerPoint and Impress

Technical description of the migration paths

) shows the conversion of shadows from PowerPoint to Impress.

Avoid, remove or modify the object attributes.

- Three-color color merge

- Margins with two and three lines

- Rounded corners

These features are not supported by Impress. Prior to conversion, these features should be changed to:

- two-color color merge

- margins with one line.

Rounded corners are automatically converted to square corners.

Missing information in the document properties.
In contrast to PowerPoint, Impress does not store the date of last access. Furthermore, the PowerPoint document properties are not imported to the converted document. If necessary, macros can be used to compensate or avoid these two shortcomings.

Random selection with multiple transition effects
Impress does not support random selection in conjunction with the use of multiple transition effects. It is important that these multiple effects are changed to simple effects prior to conversion. Otherwise these multiple effects are automatically converted to vertical line effects during conversion. Also note that Impress uses different names for certain transition effects and sometimes a slightly different behavior than PowerPoint.

Lacking support of the "record narration" function
In contrast to PowerPoint, Impress does not support the "record narration" function. Impress enables a separate soundfile to be created for every slide. In order to reuse the recordings made in PowerPoint, these must be either re-recorded or converted in a splitting process[93] .

---

[93] Refer to the "StarOffice 6.0 Software Migration Guide" page 47 "Re-record or split narration".
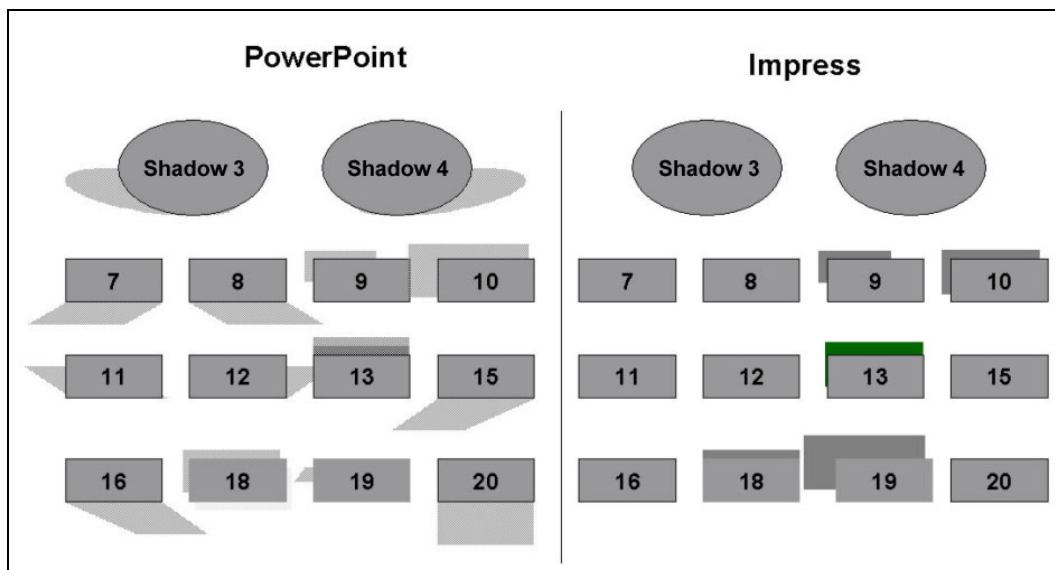
Fig. 36: Shadow objects in PowerPoint and Impress[94]

3.15.4.7 Conversion process

Conversion methods

MS Office documents can be converted to OOo/SO by the software either as a single conversion or as a batch conversion process.

Single conversion
The MS document is opened in OOo/SO and stored as an OOo/SO document.

Batch conversion
The documents concerned are copied into a separate directory (which should be specifically created for this purpose). The OOo/SO function "File/Autopilot/Document converter" can then be used to initiate the batch process. In a first step, the source format (MS or OOo/SO) is selected (refer to Fig. 37: Document converter: selecting the source format

). This is followed by the definition whether documents or templates are to be converted and in which source directory these can be found. Furthermore, the target directory in which the converted documents are to be stored must be selected (refer to Fig. 38: Document converter: selecting the source and target directories

). Thereafter, all the MS documents in the source directory are converted and stored as OOo/SO documents in the target directory.

---

[94] Source: „StarOffice 6.0 Migration Guide"

Technical description of the migration paths
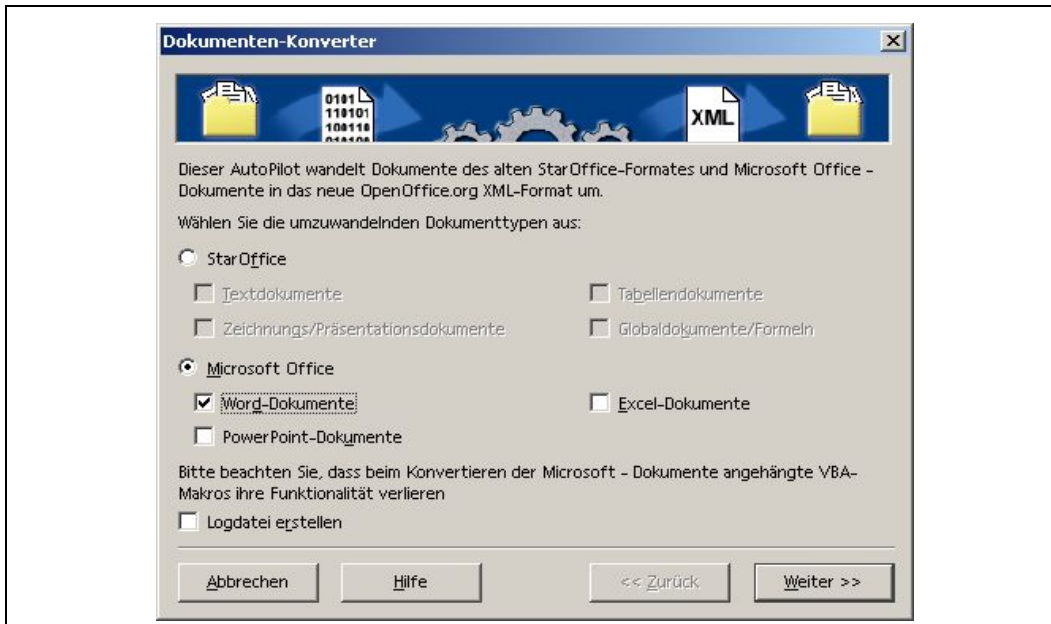
Fig. 37: Document converter: selecting the source format

Fig. 38: Document converter: selecting the source and target directories

As the illustration above (**Fig. 38: Document converter: selecting the**) shows, the document converter can discriminate between documents and document templates. The important difference is that the MS Office template is also stored as an OOo/SO template.

The particular type of converter which is the more favorable option at a given time depends on the complexity of the documents or templates (refer to chapter 3.15.4.5).

Furthermore, a situation where macros, OLE/COM control or integration of

external applications is concerned must be examined in more detail. These must then be created anew.

Conversion options

As a means for optimizing batch or individual conversion operations, OOo/SO enables compatibility settings within the scope of the options[95].

Checking the converted documents

Following conversion, the documents should be checked in order to make sure that the following settings were converted correctly:

Character size

Margins

Tabs

Indents

Line length (characters per line)

Line spacing within paragraphs

Spacing between paragraphs

Tables

Header and footer lines

Lists

Pictures

Other conversion measures

Besides the general conversion of existing documents and templates, it may be necessary to import into the new system existing autotext entries and user dictionaries which were developed over a longer period of time.

The export of autotext entries from existing templates to OOo/SO can be automated[96].

Both MS Office and OOo/SO support the creation and administration of user dictionaries. Although the dictionaries have the extension ".dic" in both applications, they are not compatible with each other. MS Office stores its dictionaries as simple text files, whereas the dictionaries in OOo/SO are stored in a proprietary format. An automated migration routine does not exist so far.

3.15.4.8 Integration of external applications

In the case of external applications, their degree of integration into the MS Office suite plays an important role with a view to a potential migration to OOo/SO. Many of the specialist and standard applications which are today in use at public

---

[95] Refer to "StarOffice 6.0 Software Migration Guide" pages 49 - 51

[96] For a detailed description, please refer to the "StarOffice 6.0 Migration Guide", pages 69 –71.

---

agencies are specifically designed for use in a system environment dominated by MS Windows and strongly depend on proprietary Windows API modules, such as:

MAPI

COM

DDE

...

The degree of integration into the Windows environment can vary strongly from case to case. A simple and still quite unproblematic integration is the use of the MAPI interface in order to access the standard e-mail client from within an application. A much higher degree of integration is obviously given if an external application permits certain MS applications only and/or if MS applications are even mandatory in order to be able to use the full functionality of a given application.

These differences in the degree of integration of external applications into Windows and the MS Office suite require careful examination as to whether migration is technically feasible and which effort is required for this. If the source code of the external application is available, it must be examined from case to case to see whether integration into OOo/SO is possible via the UNO[97] (Universal Network Objects) interface made available by OOo/SO[98].

3.15.4.9   Migration of macros and OLE/COM control

Macros and OLE/COM are methods which are intensively used to extend Office functionalities and for Office automation under Windows (refer to chapter 3.15.3.2). Uses even include the automation of complete workflows between individual departments of an organization. Since the macros and scriptings are primarily based on VBA, they cannot be executed under OOo/SO. Support for automated migration to OOo/SO is not offered at present. This means that existing macros and OLE/COM applications must be manually migrated or created anew if they are to be used further. Depending on quantity, the degree of complexity and the quality of the documentation, this can mean substantial migration effort and hence also considerable costs. On the other hand, this also enables a consolidation of the macro and OLE/COM applications as well as a reorientation of the IT strategy for office automation.

Note**:** In order to become more independent of a particular Office package in future, the modules necessary for automation purposes should be implemented as Java or C++ components.

---

[97] For further details concerning UNO, please refer to
  http://udk.openoffice.org/common/man/uno.html .

[98] The "StarOffice 6.0 Migration Guide", page 73, outlines integration into OOo/SO in 5 steps.

3.15.4.10 Programming environment of OOo/SO

OOO/SO, just like MS Office, comes with an API[99]. The OOo/SO API is designed independent of a programming language or an operating system. OOo/SO can at present be programmed in the Java, C++ and StarBasic programming languages and under Windows via OLE/COM control. All the programming languages use the same API,. so that the same tasks are possible. Furthermore, both Java and C++ enable the development of components which can perform the most varied functions as plug-ins in OOo/SO:

New chart types

New Calc functions

Wizards

Additional functionality for the user

StarBasic upgrade

StarBasic is the integrated, modular script language in OOo/SO and follows the same principles as VBA. Both languages feature a very similar structure and syntax in many respects, so that skilled VBA programmers will not have any major difficulties migrating VBA macros.

Besides the API, OOo/SO just like MS Office offers an integrated development environment (IDE) with a user interface which is very strongly oriented towards the development environment of MS Office[100].

3.15.4.11 Compatibility with MS Office

The previous chapters have shown that 100% compatibility with MS Office is not given. What does this mean with regard to the exchange of documents between users of OOo/SO and users of MS Office? This question must be answered under two aspects.

1.   The purpose of the exchange of documents must be considered.

2.   The complexity of the documents to be exchanged must be considered as well.

Documents are exchanged for purely informative purposes

The complexity of the documents to be exchanged does not play a role in this case. The documents to be exchanged should be converted to PDF format. Free PDF Reader copies are available to all users and can be downloaded from the Internet at no cost. The PDF format has been recommended to Federal Agencies as the document exchange format for some time already.

---

[99] For the relevant information in this context, please refer to http://api.openoffice.org/ (online documentation). The specification of the interface can be found at the URL http://udk.openoffice.org/.

[100] For further details concerning the use of the programming and development environment, please refer to the "StarOffice 6.0 Migration Guide", pages 79 –90.

Technical description of the migration paths

Documents are exchanged for the purpose of common processing

As the explanations in the foregoing have shown, the complexity of the documents plays a very important role in this case.

1.   Simple documents can be jointly processed without any major problems. The editing functions in OOo/SO and MS Office are interoperable.

2.   However, significant restrictions are inevitable in the case of complex documents to be jointly processed.

   ● As far as word processing and spreadsheet functionalities are concerned, joint processing can be recommended solely at the contents level. Formatting responsibilities should be clearly assigned to one party, and formatting should not take place until the contents have been completed. Both parties must be in agreement with regard to the procedure.

   ● As far as spreadsheet documents are concerned, the charts cannot be generated until the data contents are completed due to the differences in the chart engines. If the charts are to be generated using Calc, the label creation restrictions (see above) must be taken into consideration.

   ● Joint processing of Pivot tables is not possible because these are not supported by Calc.

   ● Joint processing of complex presentations cannot be recommended.

In the case of joint processing or editing of documents under OOo/SO and MS Office, the following rules should be observed:

   Agree to one document format. If the choice is between OOo and SO, the use of MS Office formats is mandatory because MS-Office does not include any OOo/SO filters. If there is a format which both versions are able to master – such as RTF – this should be used.

   Avoid so-called "round-trip" conversion.

   Format only at the last stage/instance because mapping between OOo/SO and MS Office does not work one-to-one.

   Do not edit any documents in mixed mode which:

   ● are to be jointly used by many and

   ● which may include automatic functions.

   Convert the final documents to PDF format.

3.15.5   Continuing migration

With regard to continuing migration, migration from Office 97 to Office XP (2002) is the main point of interest because the changes relevant for a migration study take place between these two versions. In the case of a change from Office 2000 to Office XP, the changes to be considered are less far-reaching or were already

implemented and will be considered in conjunction with a migration from Office 97 to Office XP. MS Office versions older than Office 97 are not considered any further in this guide.

Microsoft also uses mainly Office 97 as the reference basis in its documents dealing with migration to Office XP[101] and in its descriptions of the differences compared to earlier versions[102].

Furthermore, a short outlook at the new features likely to result from a change to Office 2003 should also be given.

3.15.5.1   Office 97 to Office XP

Converting existing documents

The document formats were left largely unchanged. These can be simply opened by the respective Office XP applications. However, reliable experience is not yet available to confirm that this really works perfectly for all formats, templates, macros and scriptings. Evidence exists that Office 97 documents and templates could not be converted without difficulty in some cases.

Just as much as Ooo/SO, Office XP also enables batch conversion by means of the "Batch Conversion Wizard". Microsoft also offers an "Office Converter Pack" in addition to the standard conversion filter[103].

Compatibility with earlier versions

The file formats of Office 97, 2000 and XP are compatible. All documents can generally be opened, edited and stored in each version. It may, however, happen that certain new functions and formatting options of Office XP have no counterpart in Office 97. However, according to the Whitepaper titled "Microsoft Office XP and File Sharing in a Heterogeneous Office Environment"[104] these are not lost during editing with Office 97 and can be reused when the document is opened the next time in Office XP.

Migration of macros, scriptings and integration of external applications

The main difficulty when migrating to Office XP lies in the changes within the programming environment of Office. The change in the "Object Model" requires particular attention in this context.

With the change from VBA version 5 to version 6 (Office 2000) and version 6.3 (Office XP), it is especially the change in the method used to link objects that has repercussions on compatibility with earlier versions and hence on migration. One can generally assume that Office applications (macros, scriptings, external applications) which were developed in the programming environment of Office 97

---

[101] Microsoft Office XP Deployment Planing Blueprint, March 2001 (XPBluePrint), and "Office XP Migration Blueprint", Jerry Honeycutt, February 2003 (magrionblueprint)

[102] "Microsoft Office Version Comparison" (Compare)

[103] http://www.microsoft.com/office/ork/xp/appndx/appa09.htm

[104] http://www.microsoft.com/office/techinfo/deployment/fileshare.asp

---

can also be used in an Office XP environment without any problems and without any need for adaptation. However, despite the generally existing downward compatibility, Microsoft does not rule out that there may be exceptions which require adjustment[105].

The opposite situation is much more difficult. It means that newer applications which were developed for Office XP can hardly be used without problems in an Office 97 environment. This applies, first and foremost, to macros and must be considered if no complete change or a gradual change is carried out in an organization which uses both Office versions at the same time.

In view of the uncertainty as to whether the continued use of all Office applications remains ensured or whether applications need to be adapted, careful stock-taking of the existing macros, scriptings and external applications is necessary in much the same manner as in the case of replacing migration.

Differences in functionalities

With regard to functional changes, the introduction of so-called smarttags[106] and the extended functionalities for the joint processing, editing and use of documents stand in the foreground.

Smarttags are another means of automation that offers users context-sensitive support. A smarttag triggers a function in response to an input (for example, a particular word or a known number). Simple smarttags and COM-based smarttags can be distinguished. Simple smarttags[107] are administered in XML lists which are stored at a central, defined point in the computer network and which are then available to all users. COM-based smarttags[108] are used as so-called smarttag add-ins. However, smarttags do not seem to offer any paramount benefits. Suitable smarttags can certainly support inexperienced users by hinting to the functionalities and formatting aids available, when necessary. It may as well, however, lead to complete confusion if an inexperienced user does not understand the functionalities offered. In order to avoid this, greater training efforts will be necessary in conjunction with a change.

With a view to the future, smarttags are another application-specific automation gadget that correspond to none of the open standards and which can only be used in conjunction with MS Office. The increased use of smarttags will eventually require even greater effort when it comes to replacing MS Office or may even prevent this replacement for economic reasons.

The so-called "SharePoint Team Services" are at the heart of the extended functionalities for the joint processing and use of Office documents. These should not be mistaken for the SharePoint Portal Server which is introduced in chapter

---

[105] "Microsoft® Office Resource Kit, Technical Article (whitepaper), Microsoft Office 97 to Microsoft Office XP Migration Issues" (Xpdelta).

[106] Einführung in Smarttags auf den Microsoft Web-Seiten

[107] http://www.microsoft.com/germany/ms/officexp/developer/smarttags/einfuehrung.htm

[108] http://www.microsoft.com/germany/ms/officexp/developer/smarttags/comsmarttag.htm

3.12[109].   The   website   http://www.micro-soft.com/sharepoint/server/evaluation/overview/technologies.asp gives a brief overview of the major differences and interactions. The SharePoint Team Services are, in principle, the light version of the portal server and are nothing but a very simplified content management functionality. They make joint documents of workgroups available on a web platform to all the members of a workgroup via the intranet or Internet. Due to their simple design, SharePoint Team Services are particularly suitable for small organizations and for ad-hoc workgroups, even working beyond the boundaries of organizations using the Internet. However, the potential security risks of this application must also be taken into consideration.

The authors of this migration guide see the most promising approaches especially at this point with regard to the joint preparation and publishing by workgroups of documents independent of proprietary document formats, in a simple, web-based manner and on the basis of XML (separation of contents and presentation). Especially in the case of cooperation beyond the boundaries of organizations, one cannot always assume that everybody uses the same tools. In order to remain open for any form of cooperation, generally accepted standards, such as XML, should be used. It seems that Microsoft has also understood this and will in future intensify the use of this standard with the Office 2003 product.

3.15.5.2 Outlook to Office 2003

With Office 2003 scheduled to be launched before the end of this summer (June 2003), Microsoft plans to focus its Office package more on the use of XML. Information so far available comes from experience reports on the beta 2 version of MS Office 2003[110] and from technical descriptions and articles published by Microsoft[111] . Most of the information relates to the use of XML within Word 2003.

This information suggests the following.

Although Microsoft has oriented its XML towards the XML standard of the W3C (World Wide Web Consortium), it modified it for its own purposes.

This modified XML will become the standard file format in Office 2003. However, the old file formats can be used parallel to this.

A separate, Word-specific XML schema (Word ML) exists for Word.

Furthermore, Word files can be additionally stored in so-called "pure XML" format. The user is informed that formatting information may be lost in this case.

If external XML documents are to be opened in Word, a valid schema file for this external document must be made available at the same time.

---

[109] The website http://www.microsoft.com/sharepoint/server/evaluation/overview/technologies.asp gives a brief overview of the major differences and interactions.

[110] http://xml.coverpages.org/microsoftXDocs.html

[111] Microsoft Office Word 2003 Beta 2 Preview (Part 1 of 2), Microsoft Office Word 2003 Beta 2 Preview (Part 2 of 2), Beitrag aus TechNet Datenbank and others.

Own stylesheets (XLST file) can be assigned to external documents.

During storing in Word-specific XML format, however, only a single file is generated which contains everything.

The situation will be similar with Excel 2003.

Office 2003 comes with an XML parser which generates error messages, for example, when the syntax used is incorrect or if a document does not match the specified schema file.

However, this information does not constitute a sufficient basis for any statements concerning compatibility between "standard XML" and "Microsoft XML". The main question in this context is which repercussions will the XML extensions implemented by Microsoft have with a view to the exchange of documents between different platforms, and will Microsoft disclose its amendments?

3.15.6 Further desktop applications

Besides the Office packages discussed in the foregoing, there is still quite a number of further desktop applications which have become vital for day-to-day work. In the following, adequate alternative applications on the Linux desktop, including the key facts, will be described for the most important desktop applications available on the Windows desktop.

3.15.6.1 MS Project

A solution comparable to Microsoft Project is at present not available under Linux. Although some projects (such as Mr. Project[112] and Gantt Project[113]) are working on this, they do not offer even a fraction of the functionalities MS Project has to offer.

3.15.6.2 Desktops

Most Linux distributions offer users ready-made desktops integrating the most important applications in a manner similar to the Windows desktop. The two most important representatives are KDE and GNOME.

The graphic user interfaces of the desktops are implemented via the X-Window system and various Window managers.

Discourse: the X-Window system and Window Manager

The X-Window system[114], also simply referred to as "X", is a window system with network capability which is especially used in conjunction with UNIX. X is based on the client/server principle, with the server providing the screen, keyboard and mouse resources and the client, being an application program, communicating with the server via the X protocol. Server and client can run on separate

---

[112] http://mrproject.codefactory.se/

[113] http://ganttproject.sourceforge.net/

[114] For further information, please refer to http://www.x.org/

machines or on the same machine. This is the rule when Linux is used on PCs. Its network capability renders X particularly suitable for the use of thin clients.

The "look and feel" of the graphic user interface is determined by the toolkit used (such as Xt, Athena Widgets, OSF/Motif, Tk, Qt, Gtk+, etc.) and the respective window manager (such as IceWM) rather than by X itself.

The window manager is an X client responsible for managing the layout, size etc. of the program windows, as well as their "dressing", i.e. the color tables and many other features available. A large number of window managers are available for user-defined desktop design[115]. The desktops described in the following come with their own window managers.

KDE

KDE is a transparent and modern desktop environment for Linux and UNIX workstation computers. KDE is the acronym for the "K Desktop Environment" Open Source project.KDE offers a "look and feel" similar to that of Windows and Mac desktops (refer to Fig. 39: KDE desktop – example 1

). This look and feel can, however, be modified in any manner the user wishes (refer to Fig. 40: KDE desktop – example 2).

Practically everything can be changed in principle. Different color themes, frames and icon sets can be chosen, in part as a function of the underlying window manager that can also be freely selected. All X11R6 window managers can be used. These flexible design and layout options enable the creation of a uniform desktop adapted to the specific requirements of a public agency or department. At the same time, the individual users can be given any degree of freedom with regard to the layout of their personal desktops.

---

[115] http://www.plig.org/xwinman/intro.html
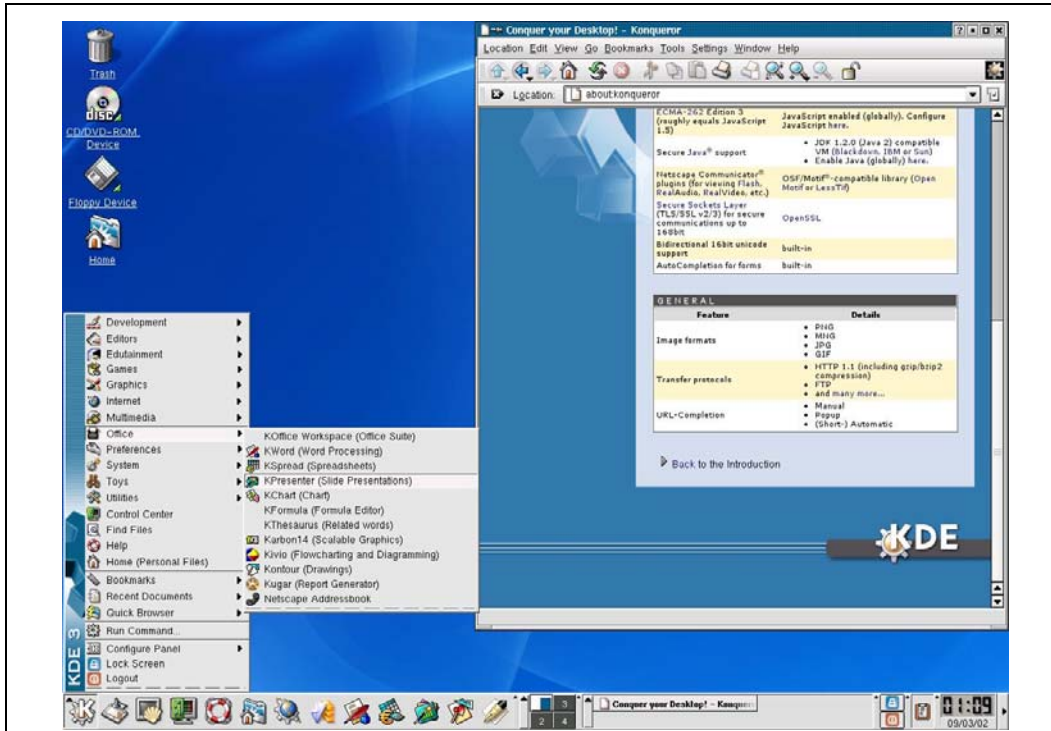
Fig. 39:   KDE desktop – example 1[116]
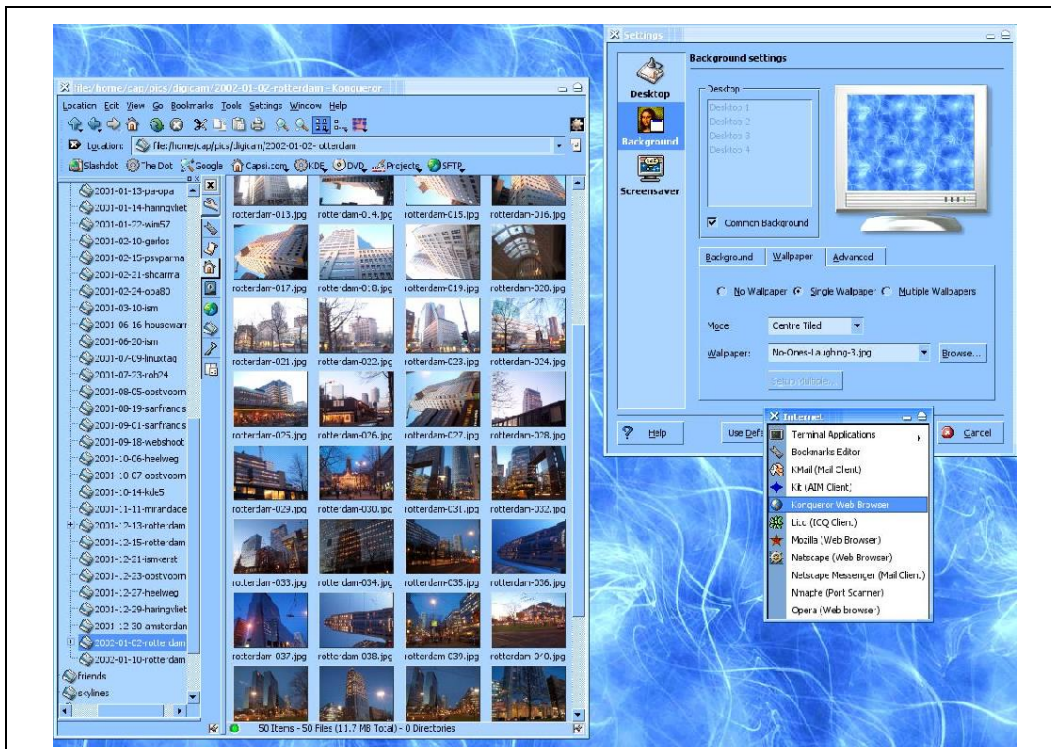
Fig. 40:   KDE desktop – example 2[117]

---

[116] Source: http://www.kde.org/screenshots/

[117] Source: http://www.kde.org/screenshots/

KDE comes with its own "Koffice" office package. Further desktop applications for KDE are the following:

The "Konqueror" file manager and browser (refer to chapter 3.15.6.3 and 3.15.6.4)

The "KMail" mail client (refer to chapter 3.15.6.5)

The "Kroupware" groupware developed for the German Federal Office for Information Security (BSI) (refer to chapter 3.11)

The "Noatun" MediaPlayer

Further important features are the various administration tools and the integrated development environment. The complete documentation is available at http://docs.kde.org/.

Furthermore, all "non-KDE applications" can also be made accessible via KDE.

GNOME

GNOME[118] is part of the Open Source GNU project[119]. GNOME means "GNU Network Object Modell Environment". In terms of layout, GNOME is as flexible as KDE (refer to Fig. 41: GNOME desktop – example 1

and Fig. 42: GNOME desktop – example 2

).

GNOME also comes with its own office package and a development environment. Some of the familiar applications are:

The "GNOME Commander" and "Nautilus" file managers (refer to chapter 3.15.6.3)

The "Balsa" mail client

The "galeon" browser (refer to chapter 3.15.6.4)

The "GnomeZip" packer

A largely complete list of the GNOME applications available can be found at http://www.gnome.org/softwaremap/.

---

[118] http://www.gnome.org/

[119] http://www.gnu.org/
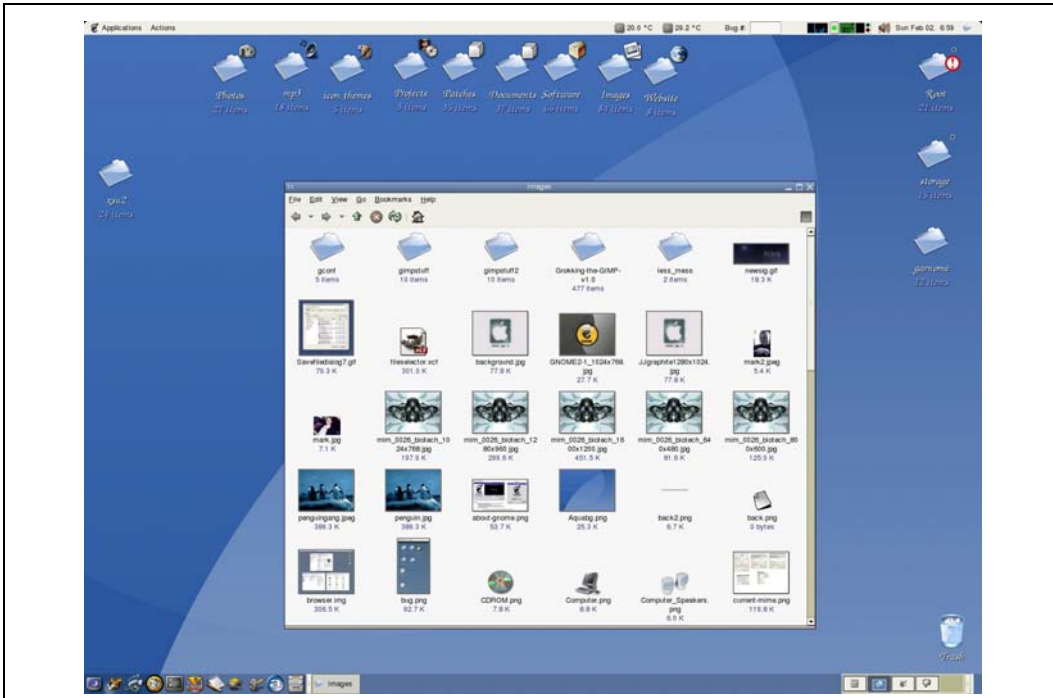
Fig. 41:   GNOME desktop – example 1[120]
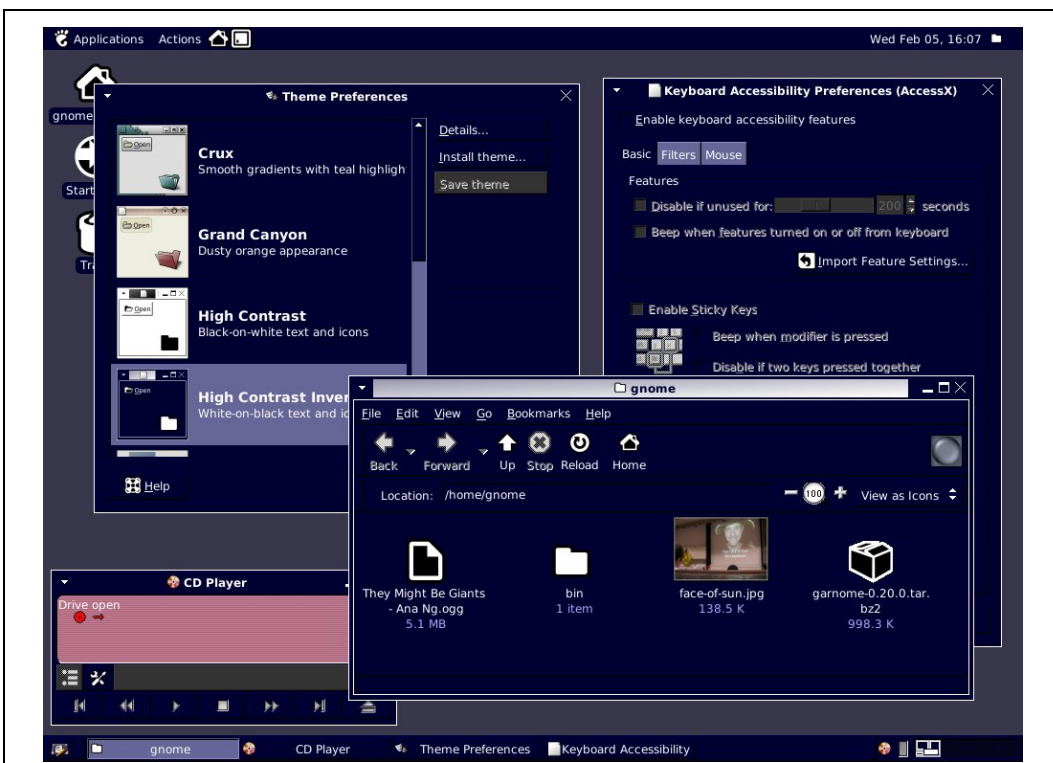
Fig. 42:   GNOME desktop – example 2[121]

---

[120] Quelle: http://vhost.dulug.duke.edu/~louie/screenshots/2.2/

[121] Quelle: http://vhost.dulug.duke.edu/~louie/screenshots/2.2/

3.15.6.3   File managers

Konqueror

Nautilus

GNOME Midnigtcommander

3.15.6.4   Web browsers

Linux offers users a whole range of different browsers which can be selected as desired or required. The most important web browsers are:

Galeon
Galeon[122] is a GNOME web browser which is based on the "Gecko" Mozilla rendering machine. Galeon is a lightweight with a basic functionality only. It is, however, fast and compatible with all standards.

Beonex Communicator
Beonex Communicator is an Open Source browser subject to GPL license. The browser is available for all known Linux distributions and also for other platforms. Beonex Communicator is considered to be one of the most secure browsers.

Konqueror
Konqueror[123] can be used not just as a file manager (see above), but also as a web browser under KDE. In a manner similar to the Explorer and the Windows desktop, Konqueror is fully integrated into the KDE desktop. Konqueror is also subject to GPL license.

Mozilla
Mozilla[124] is an Open Source browser; its source code is available under four licenses, i.e. MPL ("Mozilla Public License"), NPL ("Netscape Public License"), LGPL and GPL and under the so-called "tri-license", i.e.[125] MPL/LGPL/GPL.

Netscape
Netscape version 7.x is based on the Mozilla browser and comes with additional functions.

Opera
Opera[126] is a very fast browser which is available for a whole number of platforms[127]. Opera is a commercial product subject to a fee unless the user

---

[122] http://galeon.sourceforge.net/

[123] http://www.konqueror.org/

[124] http://www.mozilla.org/

[125] http://www.mozilla.org/MPL/

[126] http://www.opera.com/

[127] http://www.opera.com/download/index.dml?custom=yes

can accept the integrated advertising banners. In this case, Opera is available as a free download.

All of the above-mentioned browsers are largely HTML 4-conforming and have their specific advantages and disadvantages, for example, with regard to support of Java and XML. As already mentioned, Beonex is considered to be one of the most secure browsers, whilst Galeon and Opera are very fast browsers. The table below summarizes the browsers once again.

Table 37: OSS web browser overview

Browser	Version[128]	Mail client POP3/IMAP	News client	HTML 4 conforming
Galeon	1.2.10			x
Beonex	0.8.2	x/x	x	x
Konqueror	3.3.1[129]			x
Mozilla	1.3	x/x	x	x
Netscape	7.0	x/x	x	x
Opera	7.1	x/x		x

3.15.6.5   Mail clients

Numerous mail clients (including those which are integrated into the browsers) are available for a Linux desktop. Two of them will be briefly presented in the following, i.e. K-Mail and Sylpheed.

KMail (with Ägypten)

KMail[130] is the KDE mail client which, however, can also be used on any other Linux environment. KMail is hence also a free software. KMail offers public agencies a significant advantage compared to other mail clients under Linux:

A SPHINX-conforming plug-in is available for the encryption and signing of e-mails with KMail. This plug-in was developed on behalf of the German Federal Office for Information Security (BSI) within the scope of the Open Source "Ägypten"[131] project and is subject to ongoing further development. SPHINX conformity ensures, for example, interoperability between the different SPHINX-conforming solutions based on the "TeleTrust e.V. MailTrusT Version 2" protocol. This means that users at public agencies can use "Ägypten' in order to exchange S/MIME-encrypted and signed e-mails with users in other organizations, no matter whether these use, for example, Outlook with the SPHINX-conforming Secude plug-in or LotusNotes with the MailProtect plug-in.

---

[128] At the time of writing this guide.

[129] KDE version

[130] http://kmail.kde.org/

[131] http://www.gnupg.org/aegypten/

Apart from this, KMail also forms part of the "Kroupware" groupware solution (refer to chapter 3.11).

KMail supports the following protocols:

POP3

IMAP

SMTP

SMTP AUTH.

SSL/TLS support is also available for POP3, IMAP and SMTP.

Sylpheed

The Sylpheed[132] mail client is also an Open Source Project (GPL). It is worth mentioning because Sylpheed features the "look and feel" of Outlook and because it is a fast e-mail client and news reader. Sylpheed supports the following protocols:

POP3

APOP

IMAP4

SMTP

SMTP AUTH

NNTP.

3.15.6.6 Further tools
The list below contains some alternative OSS tools for selected tool categories:

Image manipulation

- Gimp http://www.gimp.org/

Video players

- MPlayer http://www.mplayerhq.hu/

- XTheater http://xtheater.sourceforge.net/

Audio players

- SnackAmp http://snackamp.sourceforge.net/

- MPEG123 http://www.mpg123.de/

- XMMS http://xmms.org/

Packers

- gzip http://www.gzip.org/

- karchiver http://perso.wanadoo.fr/coquelle/karchiver/

---

[132] http://sylpheed.good-day.net/

- gnozip http://www.geocities.com/SiliconValley/9757/gnozip.html

- gnochive/gnomera http://gnochive.sourceforge.net/index.html

3.15.7 Integration of Windows applications in conjunction with Linux clients

Almost every public agency runs one or more specialist or standard applications which are vital for its work and which are unfortunately available as Windows applications only. If these applications cannot be made available under Linux, migration to a Linux environment may fail because of this.

The long-term aim of migration to Linux must also be to eventually make the above-mentioned applications available as Linux applications. As far as standard applications are concerned, public agencies depend on the manufacturers' development policy and this is where it is often not foreseeable when a particular application will be launched for the one or other Linux platform. One can only hope that manufacturers will in the medium term make their applications available for Linux as use of Linux and open source software (OSS) by public agencies increases.

In the case of the specialist applications, which were developed as individual applications for one or more public agencies, the public agencies would have to commission a new development as a platform-independent solution or the porting of this to a Linux platform. However, this cannot be achieved within the scope of migration because such a project would require unreasonable amounts of time and money and would hence no longer be economically justifiable.

This means that an interim solution must be found enabling public agencies to continue using the above-mentioned applications under Linux until new development or porting are technically justified and economically reasonable on the one hand and until a standard application is also available under Linux on the other.

Solutions which enable the use of Windows applications even on Linux-based workstations have been available for a long time. These products can be divided into three groups:

Solutions which directly enable the execution of Windows applications without the need to buy Windows licenses. Products of this kind are WINE and Crossover Office.

Solutions which can emulate a PC in which Windows can be executed, so that the parallel execution of Windows and Linux applications on the same computer is possible. Products of this kind are, for example, VMware and Win4LIN.

Server-based products where Windows applications are executed on a Windows-based application server and presented and operated on the Linux client, such as Citrix and Microsoft Terminal Services.

It must, however, be carefully checked from case to case in order to determine which particular solution is the best for which of the given applications, requirements and environments. The features of the individual solutions as well as the costs vary significantly.

In the following, the above-mentioned solutions will at first be analyzed with a view to their technical and functional properties. One particularly interesting parameter is the degree of integration depth with which the individual solutions can be integrated into the overall system.

3.15.7.1   VMware

Workstation 4

VMware enables, for example, the execution of other operating systems in a virtual machine under Linux. To this effect, VMware emulates a virtual computer with:

> harddisks
>
> floppy drive
>
> several interfaces and
>
> other infrastructure components.

The software ensures that the guest operating system can be executed in the virtual machine parallel to the real operating system (i.e. the host operating system) of the computer.

Operating systems supported

Thanks to the complete emulation of a computer, VMware achieves a very high degree of compatibility with many operating systems. The following guest operating systems are supported:

> All known Microsoft operating systems
> (Windows Server 2003, Windows XP, Windows 2000, Windows NT 4.0, Windows ME, Windows 98, Windows 95, Windows 3.1, MS-DOS 6)
>
> The known Linux distributions, including Red Hat, SuSE, and Mandrake
>
> FreeBSD
>
> Novell NetWare 6.0 and 5.1 .

VMware Workstation 4.0 is available for all usual Linux distributions. The program consists of an extension of the Linux kernel and an application program. The kernel extension is supplied as source code, so that it can be theoretically ported to any kernel versions.

Executable programs

Depending on the particular operating system, most of the applications supported can be executed without any restrictions. Minor restrictions only exist with regard to multimedia programs.

Technical description of the migration paths

VMware Workstation is hence particularly suitable for the use of specialist applications as well as Office and Internet applications. However, the main field of application is today software development because developers can test the development of multi-platform applications on the same machine parallel under different operating systems.

Restriction

Complete emulation of a computer still puts high demands on the hardware of the machine used for this emulation. Many programs are hence significantly slower under VMware than on a comparable real computer.

Integration depth

VMware presents the Windows desktop in a separate window on the Linux computer used for emulation. The relevant Windows applications can then be activated from within this window. The exchange of data between Linux and Windows takes place via an emulated network. This requires Samba to be set up during the installation of VMware in order to enable access to the home directory of the Linux computer.
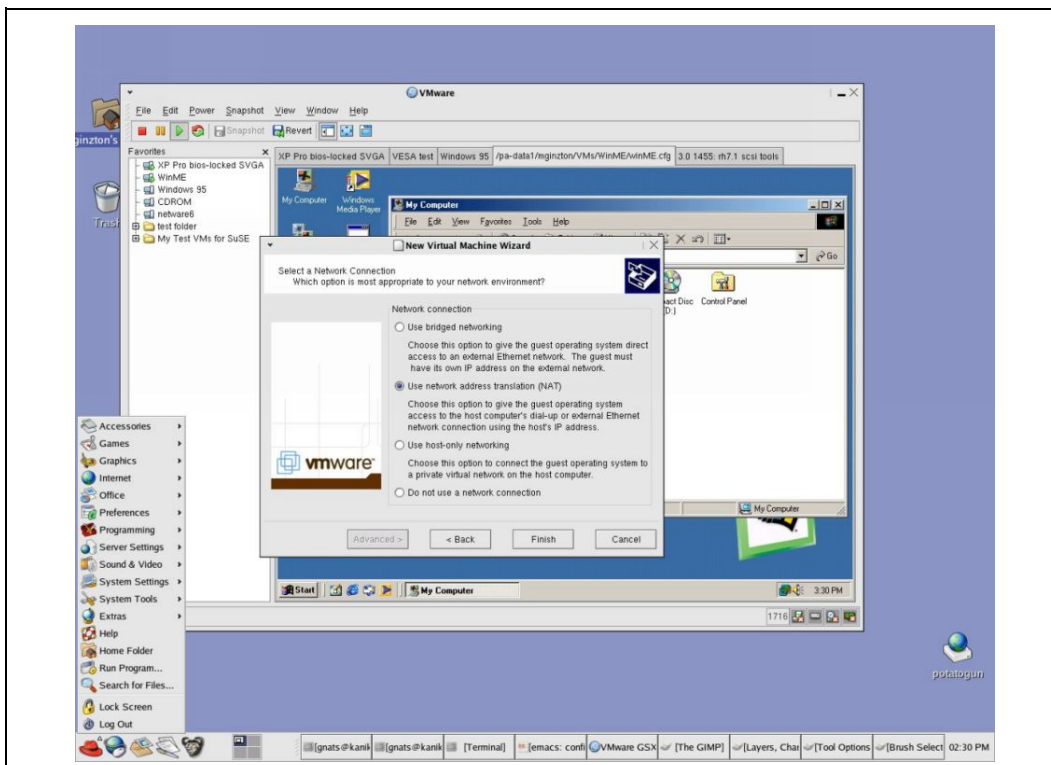
Fig. 43: Windows desktop under Linux using VMware[133]

Altogether, however, integration into the Linux workstation is only rudimentary. Furthermore, the presentation of the Windows application via the Windows desktop must be classified as not very ergonomic.

---

[133] Source: VMware http://www.vmware.com/products/desktop/ws_screens.html

Costs

VMware is a commercial product subject to a fee[134]. Furthermore, Windows licensee fees are payable as a precondition for the use of Windows applications. The additional requirements of VMware also mean increased hardware costs.

Making Windows applications available with VMware under Linux is hence a relatively costly exercise.

Evaluation

The real strength of VMware is probably, as already mentioned, that it constitutes a good development platform for multi-platform applications rather than making Windows applications available under Linux. VMware should be used for these purposes in exceptional cases only.

GSX Server 2.5

VMware GSX Server is based on the same technology as VMware Workstation. GSX Server enables virtual machines to be executed as background processes, to be remote-controlled by Windows or Linux computers, and to be remote-administered via a web interface and a special scripting API. This also enables the simultaneous execution of multiple server operating systems on Intel hardware and the consolidation of server landscapes in this way.

What was said in conjunction with the workstation variant also applies with regard to the "operating systems supported", "executable programs", "restrictions", "integration depth", "costs" and "evaluation"[135].

3.15.7.2   Win4Lin

Win4Lin 4.0 – Workstation Edition

Win4Lin[136] enables execution of the DOS-based Windows versions 95, 98 and ME under Linux. In this case, Win4Lin just like VMware does not emulate a PC, but provides the system services necessary for Windows in the form of a number of kernel modules. During installation, the files of the Windows operating system are modified in such a manner that the Windows operating system avails itself of the corresponding services of the kernel modules rather than executing these services itself. This means that applications under Win4Lin are normally much faster than under VMware.

Win4Lin presents, just as VMware, the Windows desktop in a separate window. After the program has started, it opens a window in which Windows is then booted. The user can now start and use the Windows applications (refer to 44: Windows desktop on Linux using Win4Lin

---

[134] For more details, refer to http://www.vmware.com/vmwarestore/ pricing.html

[135] The prices for the server license can be found at http://www.vmware.com/vmwarestore/ pricing.html

[136] Manufacturer: Netraverse http://www.trelos.com/

).

Win4Lin does not impose any special hardware requirements. The software runs on any normal PC[137].

Operating systems supported

Win4Lin can run on any common Linux distributions using a kernel from the 2.4.x version family.

As already mentioned, Win4Lin enables the use of the following Windows versions under Linux[138]:

95

98

ME

Executable programs

Win4Lin 4.0 typically enables the use of Office, Internet and database-based applications on a Linux workstation.

Restrictions

Restrictions exist with regard to the following aspects:

Supported Windows versions
One must soon expect that execution of many newer applications will no longer be possible.

Patching of Windows modules
Loading Windows patches from Microsoft must be handled with care because it cannot be ruled out that files changed by Win4Lin are exchanged, so that the system enters an inconsistent state.

Available memory space
Since version 4.0, a maximum RAM capacity of 128MB can be made available to Windows applications running under Win4Lin.

The virtual memory is limited solely by the available memory capacity of the disk partition containing the user's "$HOME/win" directory.

Interface support
The DirectX and USB interfaces are not supported.

Integration depth

Win4Lin presents, just in the same manner as VMware, the Windows desktop in a separate window in which the Windows applications can be called.

---
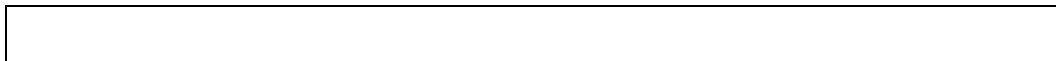
[137] Hardware requirements according to the manufacturer:
http://www.netraverse.com/products/win4lin40/requirements.php

[138] For details, please refer to
http://www.netraverse.com/support/docs/400_relnotes.html#install_winver

---
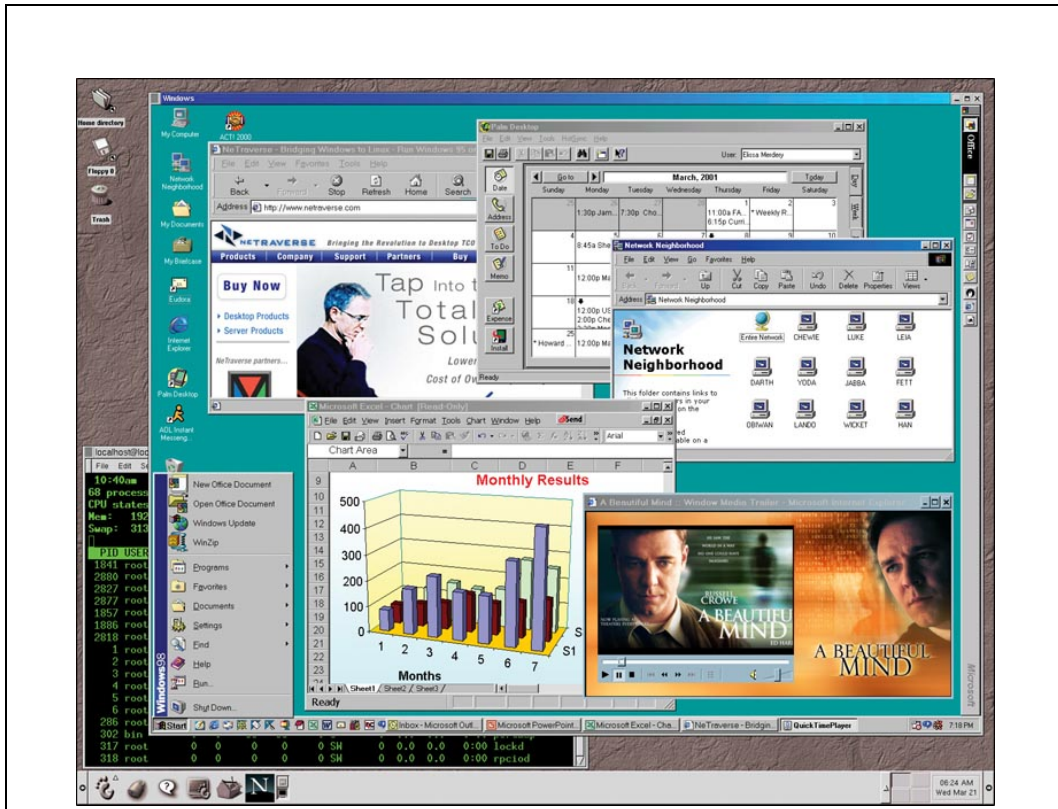
Fig. 44:   Windows desktop on Linux using Win4Lin [139]

However, the exchange of data between Linux and Windows applications is simpler than in the case of VMware. Win4Lin enables Linux directories to be simply presented as drives under Windows.

However, the individual applications are not really integrated in this case either. After the program has started, it opens a window in which the user can watch Windows booting before the user can then start and use applications in this window.

Costs

Win4Lin is also a product subject to a fee. However, the license fees[140] are substantially lower than for VMware. However, in just the same way as in the case of VMware, Microsoft licenses must be additionally acquired, however, at a reasonable cost for the operating systems concerned. This means that Windows applications under Linux can be run under Win4Lin at a significantly lower cost than with VMware.

Evaluation

---

[139] Source: Netraverse http://www.netraverse.com/products/win4lin40/fullsizescreen shot.jpg

[140] License fees for Win4Lin 4.0 Workstation Edition;
http://www.digitalriver.com/dr/v2/ec_Main.Entry?SP=10007&SID=40113&CID=0&CUR=840&DSP=0&PGRP=0&CACHE_ID=0

Technical description of the migration paths

Despite certain technical restrictions, Win4Lin is today often a feasible way of using individual, simple Windows applications under Linux. This is particularly the case if such an application is required on a few workstations only. If such an application is required on a larger number of workstations, the use of Win4Lin Terminal Server which is briefly outlined below may be a feasible approach.

Win4Lin Terminal Server 2.0

With Win4Lin Terminal Server, Netraverse uses the network capability of the X protocol in order to use Win4Lin from within another system. This is possible because this protocol enables the Win4Lin window to be displayed on the Linux desktop.

With Win4Lin Terminal Server, a separate program session is then executed on a Linux server for every user of Win4Lin. These sessions are then transferred via the X protocol to the clients.

The main advantage of this is that central installation and administration is possible for both Lin4Win and the Windows operating system as well as the required applications.

WINE

WINE is a free software project[141] which has been persistently pursuing and enhancing Windows/Linux integration at the application level. WINE uses a fundamentally different principle than the other solutions described so far in order to make Windows applications available under Linux.

WINE makes a free implementation of the Windows API available for use under Linux and X-Windows. When a Windows application is started, WINE, in exactly the same manner as Windows itself, loads this application into the computer's RAM, links it to the libraries made available by WINE and is thereby capable of making the applications work under Linux. This means that, strictly speaking, WINE is not a Windows emulator.

The greatest challenge now involves making the existing Windows libraries available as free implementations to the largest extent possible, so that as many Windows applications as possible can run under Linux. WINE already implements the Windows libraries with the most important functions, so that no problems arise when a Windows application accesses the standard functionality (of the Windows operating system) only and includes all the other functions in itself already. The situation is more difficult if a Windows application accesses mainly newer functions of Windows libraries, which have not been implemented yet, or libraries of other applications. It should also be mentioned in this context that application manufacturers usually try to support even older windows versions. In order to achieve this, they use newer features only seldom and on an optional basis only, so that this does not necessarily lead to practical problems.

---

[141] WINE project homepage: http://www.winehq.com/

WINE already supports a large number of applications (refer to the following section on "WINE is available for practically every Linux system, and forms part of most distributions.

") and features[142].

Operating systems supported

WINE is available for practically every Linux system, and forms part of most distributions.

Executable programs

WINE enables the execution of practically all Windows applications on condition that the required libraries are available.

Programs for which this is certain include, for example, WinWord, Excel and PowerPoint from the Office 97 and 2000 packages as well as the Internet Explorer. In individual cases, practical suitability must be tested in advance. For this purpose, the WINE application database (http://appdb.winehq.com/) should be examined first.

Restrictions

One problem with WINE is the still very complex configuration of the program which requires much expertise.

Integration depth

WINE enables optimum integration of Windows applications into the Linux desktop. The programs are started directly by the window manager of the Linux desktop in a separate X-Window rather than from a desktop of their own.

---

[142] A list is available at
http://www.winehq.com/?page=wine_features;winehq=d35c3404fe39283bf96bb1dd54b14c8d.
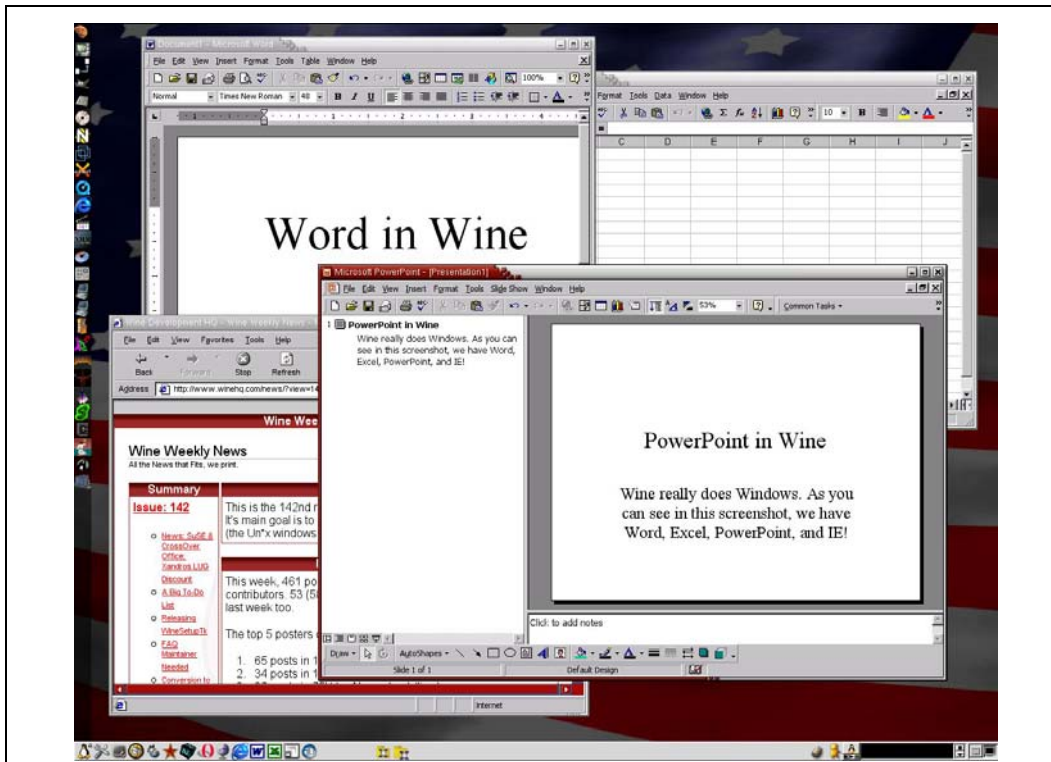
Fig. 45: Windows applications on the Linux desktop using WINE[143]

Costs

No costs other than the license fees for the respective Windows application are incurred. However, the administration effort exceeds that necessary for the other solutions.

Evaluation

This approach offers two major advantages:

There are no costs for Windows operating system licenses.

No additional operating system is necessary which would increase the workload of the resources available. The Windows applications can theoretically be executed with the same speed as under Windows and require the same memory resources.

If the required libraries are available for an application in WINE, the use of WINE should be clearly preferred.

WINE could be one way to enable the execution of MS Project on the Linux desktops because an alternative Linux application is at present not available. However, no positive entry can so far be found in the application database.

---

[143] Source: http://www.winehq.com/?ss=1

Crossover 0ffice

Crossover Office (CO) is a product from Code Weavers[144]. CO is based on WINE and compensates the disadvantage of WINE's complex configuration in that CO supplements WINE by a user-friendly installation program as well as scripts for creating users and installing the Windows applications.

Executable programs

Crossover Office currently supports Microsoft Word, Excel and PowerPoint (from Office 97 and 2000). Other applications, such as Outlook 2000, IE 5.5 and Notes R5, are executed in a relatively stable manner.

Costs

Besides the license fees for MS Office, license fees are also payable for Crossover Office[145].

Evaluation

What was said in conjunction with WINE applies here too. Users looking for a more user-friendly installation and configuration procedure should choose CO WINE.

Crossover Office Server Edition

The Crossover Office Server Edition enables the central installation of Windows applications on a Linux-based application server from where they are then made available to client systems via the X protocol. This offers the advantage that central provision and administration of the Windows applications is possible.

WineX

WineX is another variant of WINE in which the company Transgaming[146] has concentrated on enhancing DirectX support. WineX enables a number of sophisticated Windows games to be played under Linux. This is also why WineX is not discussed in more detail. It is mentioned for the sake of completeness only.

WineX is not free software.

3.15.7.3 Citrix Metaframe

The functionalities are described in chapter 3.16.5.

Operating systems supported

(Refer to chapter 3.16.5)

Executable programs

Any Windows applications that can be used under Windows NT or Windows 2000 can be executed.

---

[144] Code Weavers homepage http://www.codeweavers.com/home/

[145] Price information for Crossover Office http://secure.codeweavers.com/store/

[146] Transgaming homepage http://www.transgaming.com/

Restrictions

The only restriction concerning the execution of Windows applications is that applications with a substantial graphic component (see above) should not be executed via Citrix Metaframe.

Integration depth

Just like VMware and Win4Lin, the Windows desktop can be opened in a separate window on the Linux desktop, with the Windows applications being executed in this window. Data can be exchanged via the network only. The integration depth is thus very limited in this case.

Costs

The costs depend on the specific functionality of the desired metaframe and must be analyzed from case to case. In general, however, the full Microsoft license fees must be paid in addition to the Citrix licenses.

Evaluation

Citrix Metaframe cannot be recommended as an interim solution for the execution of Windows applications on a desktop until such applications are available under Linux because Citrix Metaframe is, first and foremost, too expensive and too complex.

Citrix Metaframe should, however, be considered if it is foreseeable that certain Windows applications must remain in use for a longer time to come.

The major advantage of Citrix Metaframe is the central installation and administration of applications as well as central data storage. Citrix Metaframe is also a suitable system in an environment with thin clients or diskless clients.

3.15.7.4   Windows Terminal Server

The functionalities are described in chapter 3.16.5.

Operating systems supported

(Refer to chapter 3.16.5)

Executable programs

All Windows applications running under Windows 2000 can be executed.

Restrictions

(Refer to chapter 3.16.5)

Integration depth

Refer to the comments on Citrix Metaframe.

Costs

Compared to Citrix, no costs other than fees payable to Microsoft are incurred.

Evaluation

This variant can be assessed just like the Citrix Metaframe solution. It is, however, slightly more favorable. However, the disadvantage compared to Citrix Metaframe is that experience with Windows Terminal servers is still limited compared to Citrix Metaframe, especially with regard to larger and more complex environments. This is, however, of minor importance in the search for a solution to the problem at hand.

Summary

The VMware, Win4Lin, WINE and Crossover Office solutions should only be regarded as an interim solution or as a solution for individual, smaller applications on individual workstations. A corresponding platform-independent application which can be executed under Linux will be required in the medium term.

Otherwise one can examine whether Citrix Metaframe can be an economically feasible solution, even though this is more likely to be a strategic decision.

Under these conditions, one can conclude the following:

Given a limited number of Windows applications, the use of WINE is worthwhile (if necessary, with additional development effort).

If many Windows applications are concerned, it is very unlikely that all the applications can be executed using WINE. The possibility of using Win4Lxn must then be examined (executable under Windows 95, 98 or ME).

If the number of Windows applications concerned is very large, the general question arises as to whether migration will make sense (with the need to check from case to case where the limit is).

Platform-independence of applications must be a requirement in future.

3.15.8   Evaluation

On the basis of the previous discussion, the option of replacing Office 97 and/or Office 2000 either with Office XP or by Office 2003 or with OOo/SO will be evaluated in the following. The results of this evaluation will form the basis for an evaluation of the possibility of replacing the Microsoft desktop with a Linux desktop.

3.15.8.1   *Replacing Office 97/2000*

Migration to Office XP

A migration from Office 97 and/or 2000 to Office XP must at present be re-considered for the following reason.

Migration always costs time and money, so that migration is always targeted towards the latest and most advanced technology rather than towards older technology which still exists. In the case of Office XP, it is foreseeable that this will be replaced by Office 2003 with a more advanced and innovative technology before the end of 2003. If, as announced, a first full version of Office 2003 is launched in summer 2003, one can expect that a first, relatively stable and bug-free version will be available by the beginning of 2004.

Migration to Office 2003

The only technical argument against migration to Office 2003 is that no experience whatsoever with productive use is at present available with Office 2003.

Considering the stronger orientation towards XML in Office 2003 and the present experience with the beta 2 version, one may expect that the cross-platform exchange of documents with Office 2003 will be facilitated. This alone is reason enough to postpone a migration of the Office package until a relatively stable and bug-free version of Office 2003 is available and until more experience is available with regard to its day-to-day use and the exchange of documents between different platforms.

Migration to OOo/SO

Migration to OOo/SO can from today's point of view only be recommended if a public agency or an organization

> never or seldom shares documents with other public agencies or organizations which use MS Office (up to XP) or

> shares only simple documents, i.e. documents without macros and without special formatting, with other public agencies or organizations which use MS Office (up to XP).

If complex documents have to be jointly created with other public agencies and organizations which use Office 97, 2000 or XP, one will have to expect that this cooperation will become too complex and difficult.

Furthermore, migration to OOo/SO is not recommended from a technical perspective if external applications which are strongly integrated into MS Office and which are definitely needed cannot be integrated into OOo/SO.

A statement on this issue is at present not possible because sufficient experience with the exchange of documents between MS Office 2003 and OOo/SO, then in their versions 1.1 and 6.1, is not yet available.

3.16   Terminal servers and thin clients

3.16.1   Overview

The decision in favor of the use of terminal servers and thin clients can also be made within a migration project and is hence also one of the subjects of this migration guide. This is, however, not a classic migration subject because terminal server environments are usually not migrated. The use of the systems discussed in the following primarily concerns a decision within the overall IT strategy of a public agency. However, the solutions presented are meant to give an insight into the general issue and to illustrate the technological potential.

The technologies discussed can be used in the most different areas:

Linux-based servers and client systems with the Linux Terminal Server Project

NX Terminalservices with Linux-based server systems and client systems for Windows and Linux

Windows Terminal Server with primarily Windows-based client systems

Citrix's Metaframe solution with various client systems (DOS, Windows, Unix, Linux, etc.).

The systems discussed cover a wide range of different technical solutions (server and client systems) and must be analyzed in more detail from case to case. Besides technical differences and options, the systems also vary strongly with regard to licensing models and costs.

3.16.2 Introduction

Administration and service of workstation computers are very labor-intensive jobs, especially in cases where the computers are fitted with different hardware and software. Furthermore, increasing complexity of the hardware and software used can render workstation computers more susceptible to failure and thereby boost administrative requirements. The list below gives an overview of the tasks related to system administration:

Installation – including configuration work on site, if necessary

Adaptation to user requirements

Administration of software upgrades – preparation and updating of installation packages and distribution thereof

Fault diagnosis and trouble-shooting, support

Spare-parts management

The tasks can be generally automated given adequate support by suitable administration tools and system management applications. Although automation is a way to reduce the general work requirement, this requirement nevertheless usually still remains very high. Furthermore, not every organization has the funds necessary for the sometimes very expensive system management software. This is, in particular, the case with smaller organizations.

The use of terminal servers can reduce these problems significantly. Also with a view to future migration projects, it is worthwhile thinking about the future use of terminal servers and the related thin clients. In a conventional, distributed IT landscape, programs are usually installed and executed on the workstation computers. The main purposes of the server structure are central data management, data backup as well as control of access privileges. In the case of a terminal server solution, one or more powerful central computers, i.e. the real terminal servers, ensure site-independent access to the necessary data and applications. The terminal servers offer users direct access to the graphic user interface of the operating system via the network. On the terminal server, every

logged-on user has his own session and access to all the available resources of the operating system. In contrast to conventional, distributed workplace architectures, not just data, but also applications are made available on central servers. Access to the applications and data of the terminal servers must take place via special terminal programs and so-called thin clients.

The table below gives a short overview of the advantages resulting from the use of terminal servers and thin clients.

Table 38: Advantages of terminal servers and thin clients

Advantages	Explanations
Central administration	Operating system and applications are kept in a simple, centralized form on the terminal servers. Centralized software upgrading (patches, updates) is possible now. Work on the client systems is no longer necessary. The administration of applications is centralized, fault diagnosis and trouble-shooting are simplified. Increased productivity for users and administrators. ● Simplified administration accelerates the provision of applications for users. ● Elimination of labor-intensive trouble-shooting operations on site drastically reduces administrative workloads.
Reduced hardware requirements	The client systems require fewer hardware resources (network card, graphic card, keyboard, mouse). Regular upgrading of client hardware in response to increased requirements on the part of operating systems and applications is no longer necessary. Existing hardware can be used for a longer time.
Enhanced security	The use of thin clients (without harddisks) mans that data storage is possible on the central servers only [this being equally applicable to fat clients]. This reduces the risk of data loss and prevents unauthorized individuals from accessing data as a result of manipulation of theft of client systems.
Independence from the client	Workplace computers can be quickly replaced because no personal data or settings are stored on the clients any longer. Most importantly, users can easily change their place of work without having to miss "their" familiar environment.

Besides these advantages, however, certain disadvantages should also be considered when deciding whether to use terminal servers or not.

Table 39: Selected disadvantages of terminal servers and thin clients

Disadvantages	Explanation
Dependence	User sessions are aborted when the terminal servers fail. Work cannot be resumed unless the problem on the terminal server is fixed. This disadvantage can be minimized by the use of a server farm. An abort of a user session can lead to loss of data.

Disadvantages	Explanation
Increased resource demand	The terminal servers must feature significantly increased resource capacities, especially memory capacities. However, in relation to the total demand (servers and clients), fewer resources are required because certain operations need to be carried out on a server only once for all users rather than separately on every single client.
Increased network load	The server and client systems communicate via the network level, with the differences in contents during screen refresh or instructions for screen displays being transmitted. Certain applications (such as graphic programs, etc.) can lead to a significant increase in network load. However, in the case of other applications (word processing, for example), network communication can even be reduced because changes only (keyboard entries and screen changes) are transmitted during saving rather than complete files.
Adaptation of existing applications	Not all applications can run on a terminal server without problems. Especially in the Windows area, applications may exist which open system files for writing, so that these files are then locked for other users. These problems can often be resolved by administrative intervention.

Different client types can be used for communication with terminal servers.

Fat clients

A fat client is a full-scale workstation computer. It uses special terminal server/client software in order to access the terminal server.

Technical description of the migration paths
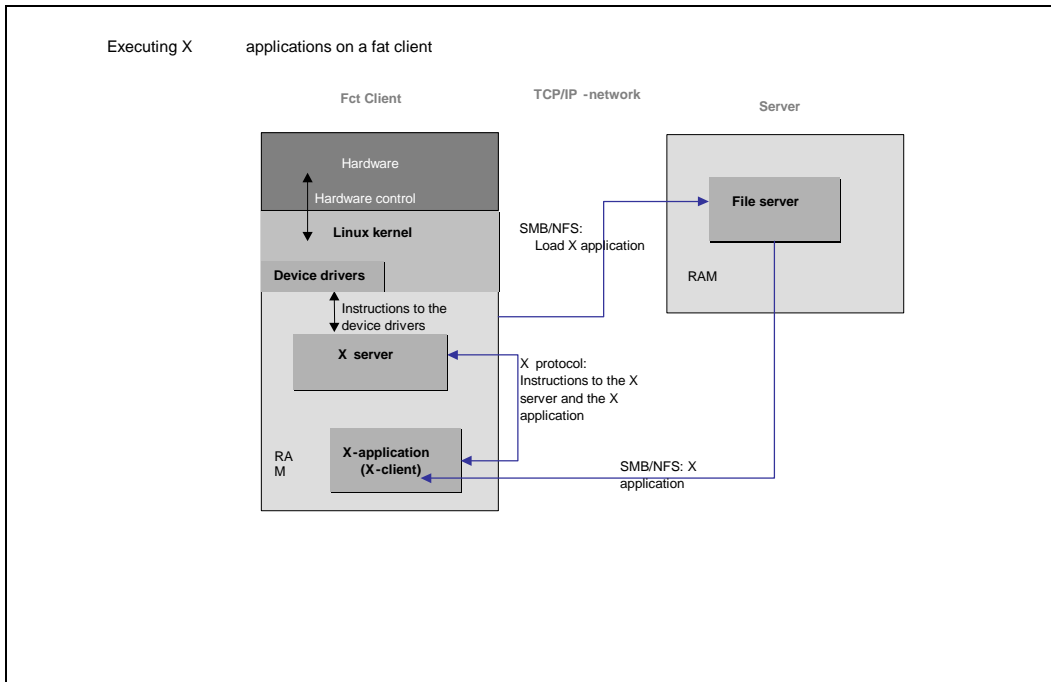
Fig. 46:   Executing X applications on a fat client

Thin clients

Thin clients are computer systems with minimum hardware resources. The clients take their operating system either from a flash EPROM or they are booted via the (pxe, tftp, nfs) (refer to Fig. 48:   Booting a Linux system via network
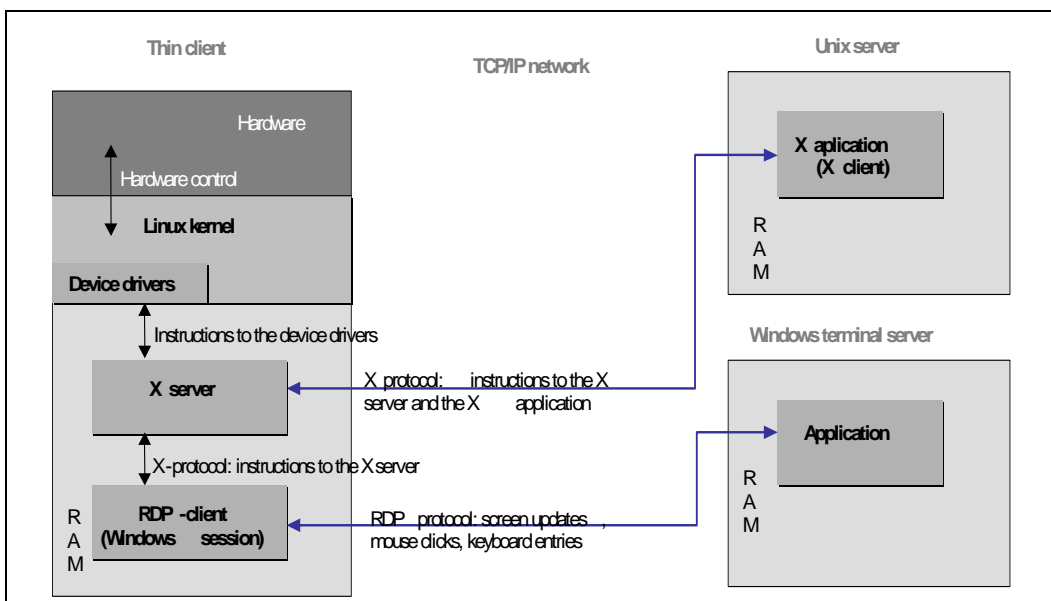
Fig. 47:   Executing X and Windows applications on a thin client
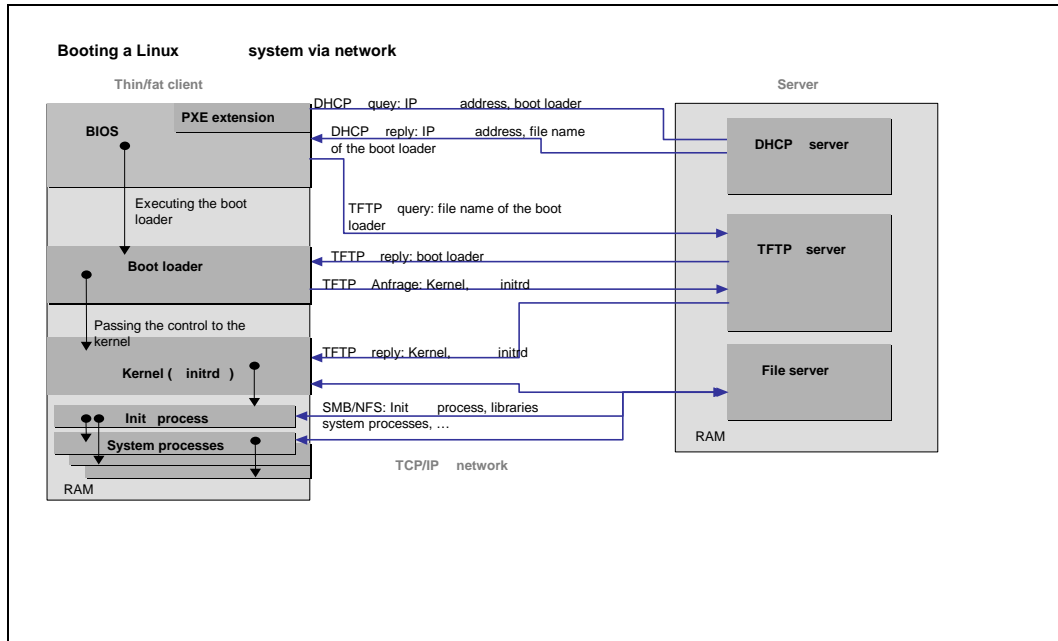
Fig. 48:   Booting a Linux system via network

Some selected approaches towards the implementation of terminal environments will be briefly presented in the following.

3.16.3   Linux Terminal Server Project

The Linux Terminal Server Project (LTSP)[147] uses the excellent options which Linux and X-Window offer in order to have client systems booted by server systems. The required applications are subsequently executed on the server system. The graphic outputs of the applications running on the server are sent to the terminals via the X protocol. The configuration of the client systems is implemented via simple text files and enables various options, from the use of local printers right through to the local execution of programs. The LTS project enables low-cost workstation computers to act as terminals using a Linux or other UNIX server, whilst the clients can work both in text-based mode or with a graphic user interface.

The client systems are booted by the server via the network. The client systems are fitted with special boot ROMs to this effect which can be installed in most modern network adapters. User and/or account data is administered using the normal GNU/Linux on-board functions.

Two examples based on the LTSP approach are described below.

---

[147] http://www.ltsp.org/

3.16.3.1   The GOto concept

The GOto concept[148] was used within the framework of the migration project at the Mariensee Institute for Animal Science and Animal Husbandry. The company GONICUS has developed the GOto concept and made its constituent parts available as free software.

The major difference compared to the LTSP approach is the simplified management on an LDAP basis. All configurations and user profiles are stored centrally on the servers using LDAP (Lightweight Directory Access Protocol). This ensures that every user at every workplace has access to his specific profile, as well as his particular applications and data. Administration can be carried out using the Gosa web frontend which provides access to the required LDAP structures and their administration. Both solutions are released under GPL.

The GOto concept also enables the complete booting of thin client systems by the respective servers via the network. The boot process was extended for the standardized PXE protocol because the related boot options today form part of the standard functionality of many network cards, so that not even a boot ROM is required in many cases. Both thin and fat clients are supported. Administration of the fat clients can be carried out in a manner equivalent to that used for thin clients. Once the fat clients are installed, they can be automatically kept at the latest level.

3.16.3.2   Desktop server

The univention_ desktop server[149] is a commercial, integrated and scalable Linux-based server solution with a module for the implementation of thin clients and an extended version of the OpenLDAP directory service as a backend for user and configuration administration.

Just like the GOto concept, it differs from the LTSP in that the support of the system start is not only via BOOTP, but also via PXE. Furthermore, special tools are available for monitoring user sessions in order to avoid "process corpses" when clients are switched off. Furthermore, access to local devices – such as CDROM, floppy, sound card or printer – which are connected to the thin client is enabled (even though this access can be restricted by administrators). The entire user and configuration management system is contained in an LDAP directory. Furthermore, the administration fits into the administration of Windows-based or Linux-based fat clients.

The integrated load-balancing functionality ensures good scalability and it is possible to easily integrate further boot or application servers into the system, when necessary.

---

[148] http://www.gonicus.de/

[149] http://www.univention.de/

3.16.4   NX terminal services

The NX product from the Italian company Nomachine[150] represents a relatively new Linux-based terminal server technology. NX is a commercial product. After several years of development, the developers successfully implemented an extremely efficient compressor for the X-Window protocol. Remember that the X-Window system features a network-transparent design. This means that the output of any application is possible on a remote screen. However, the protocol used is unfortunately not very bandwidth-optimized. This is why the use of the X-Window protocol so far made sense within the LAN only. Despite attempts to improve the WAN capability by caching events and bitmaps and/or by compressing the protocol (Low band X), the results were not yet sufficient.

The NX has meanwhile reached a compression factor which approximately corresponds to that of Citrix. The NX server runs on one or more Linux servers and, besides the X-Window protocol, is also capable of efficiently transmitting the Microsoft RDP and the frame buffer protocol of the VNC viewers to the NX client. The NX client runs under Linux, Windows, as well as on iPAC and Zaurus PDAs.

Besides the efficient transmission of screen contents, the NX technology also enables access to the local file system and the transmission of audio data. Redirecting the serial interface is not yet possible. In technological terms, the system is mainly based on Open Source components. All compression components were released under GPL. Communication is fully encrypted via an SSH tunnel. Similar to Citrix Metaframe, it is possible to "publish" the windows of a single application only. This enables very flexible integration between the Windows and Linux application worlds. It is possible to present Windows applications on the Linux desktop or Linux applications on the Windows desktop. The separation of application server and compression nodes enables an extreme degree of scalability. The application server is not additionally burdened by the data compression job. Version conflicts between application and compression server cannot occur.

The licensing model is interesting in that it is dependent upon the number of server nodes rather than the number of clients. This makes the product significantly cheaper than other products on the market.

3.16.5   Windows Terminal Services and Citrix

The entire application logic is provided centrally by the servers, so that a bandwidth of around 10 to 20 kbps is required between client and server. The separation of the application logic from the user interface on the terminal servers means an increased workload on the backbones compared to conventional client/server environments during access to file, print and database servers, etc.

The servers on which the applications are installed are a key component of the terminal server technology. The terminal server enables parallel client access by

---

[150] http://www.nomachine.com/

several users in sessions during which the users can execute the applications in a protected memory area. Since in the non-configured state, all users have all privileges, the system must be protected against unintended and unauthorized user intervention. For this purpose, the familiar instruments known from NT administration – such as server-based profiles, policies and settings of NTFS security – can ensure the required security for files and directories.

Furthermore, application tests are particularly important in a terminal server environment in order to ensure the optimum server size. It is hence essential to know

the processor performance requirement and

the RAM capacity requirement of an application,

how many users access the program at the same time,

whether the program is a 16-bit or a DOS application,

whether the application is multi-user enabled at all.

The Windows Terminal Services are offered for Windows NT 4 in a separate product variant ("Terminal Server Edition", TSE). With Windows 2000, this service is included in each of the product variants.

Unless Metaframe from Firma Citrix is used, communication between the terminal server and the terminal server client is based on the IP-based Remote Desktop Protocol (RDP). Windows NT 4 TSE supports RDP version 4, Windows 2000 the extended RDP 5.

Microsoft offers terminal server clients (RDP clients) for all Windows operating systems (including 16-bit systems). Third-party manufacturers offer additional RDP clients for other runtime environments (such as Java).

A disadvantage of a purely Microsoft-based terminal server solution is that users must connect themselves to a particular server. This leads to problems if

the server is not available

the server is overloaded.

The Metaframe product from Citrix offers a solution to this. Metaframe enables several terminal servers to be logically combined to form a server farm. The user (client) is then faced with so-called published applications rather than a single server to which he connects. A mechanism within the server farm then decides the server on which the user's applications will be executed.

It should be noted at this point that these explanations merely outline the underlying technological principles rather than even scratching the surface of the complexity of the entire Citrix concepts and its options. This outline is, however, absolutely sufficient at this point in order to illustrate the general option of using Citrix Metaframe in order to execute Windows applications on the Linux desktop.

In order to ensure this functionality, Metaframe includes the so-called ICA (Independent Computer Architecture) protocol. The necessary ICA client exists for

all Windows operating systems

DOS

Java

a large number of UNIX derivatives (including Linux)

and hand-held systems.

At the server-end, the above-mentioned Microsoft operating systems (Windows NT 4 TSE and Windows 2000) are primarily supported. However, variants for UNIX are also available (such as Metaframe for Solaris).

Citrix currently offers two Metaframe product variants, i.e.

Metaframe 1.8

Metaframe XP

The XP version must be considered to be the strategic variant because 1.8 is due to be phased out in the near future..

Metaframe can be found in large environments with large numbers of servers because these environments call for intelligent load management (load balancing). If several terminal servers are combined to form a so-called server farm, a load balancing function can be implemented for the servers.

The illustration below outlines the principles of a server farm under Metaframe XP.
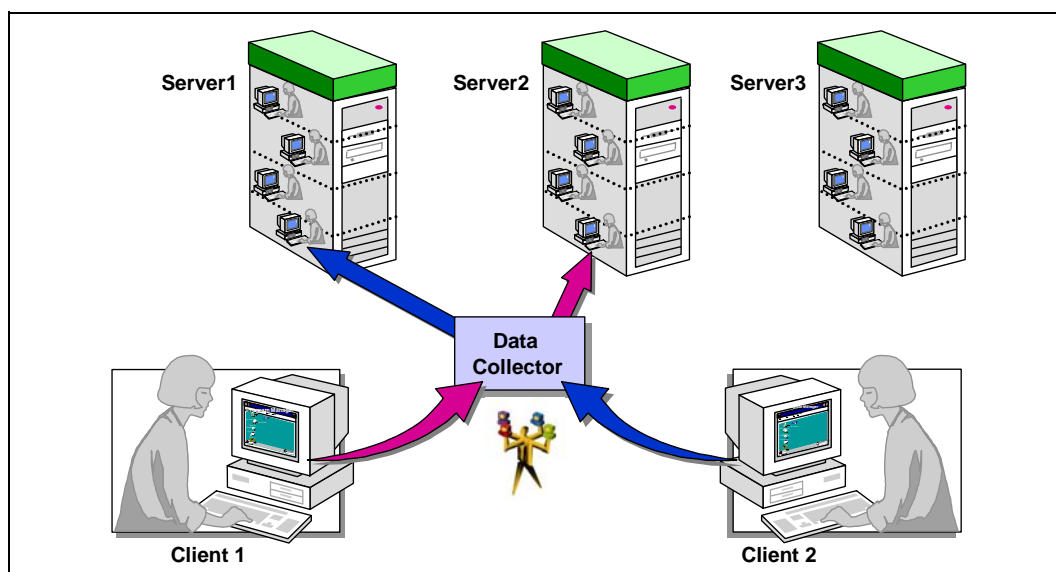
Fig. 49:   Server farm under Metaframe XP

Load balancing supports the performance and application availability in the entire system because no users are assigned to a server that is not available. Once a load evaluation program is assigned to the servers, the workload of the server is reported under Metaframe XP to the data Collector and stored there for the purpose of handling connection requests. When a published application is requested via the ICA client, the data collector identifies and selects the server offering the highest performance at this time and notifies the client of this. The client then connects to this server.

In the case of server farms consisting, for example, of 1-processor and 2-processor machines, different management rules can be set for the different servers. The standard user application load for the 2-processor machine reaches, for example, 100% load when 50 users are connected, whilst a 1-processor machines reaches this full-load level when 25 users are logged on. This "tuning" functionality enables hardware differences to be leveled out.

The following technical aspects should be considered with regard to the terminal server technology.

Server farms need a Windows domain (logon).

Server farms use server-based profiles in order to support roaming users (stable file services).

Windows terminal servers print via RPC on Windows print servers in order to reduce the workload of the terminal servers.

The user account in the Windows domain is supplemented by additional terminal-server-specific parameters.

Not every Windows application runs on terminal servers (feasibility study, integration efforts/costs).

3.17 High availability

The field of application must be characterized as a precondition for determining whether high-availability requirements can be fulfilled using Open Source software.

3.17.1 Aims

High-availability installations provide services in such a manner that their downtimes, minimum capacity, data throughput and further parameters do not fall below certain limits. This requirement can be due to several reasons.

The services are urgently needed for internal purposes. They are, for example, the basis for many activities by many users and the economic damage of a failure would be enormous.

The services are security-critical. Failure can affect national interests.

The services should be available to citizens or companies without failure or on an ongoing basis.

With its eGovernment initiative, the government of the Federal Republic of Germany has taken up the challenges for a modern, efficient country. This means on the one hand, that backend systems (such as databases) can be permanently accessed or that new applications can be received on a permanent basis and any loss must be prevented. However, the related, longer service times also mean new requirements for the frontend systems on the other. Costs must be cut and processing time reduced, and the image of the public administration can be significantly enhanced by initiatives of this kind. Non-availability of services would, however, undermine these aims.

3.17.2   The "five new" and reality

High-availability systems (HA systems) are categorized, amongst other parameters, by the percentage of the time during which they provide services. The table below illustrates what this means for an HA system which must be available around the clock.

Table 40: Requirements for an HA system

Availability	Maximum downtime per month	Maximum downtime per year
99.5%	3 hours, 39 minutes	43 hours
99.7%	2 hours, 12 minutes	26 hours
99.9%	44 minutes	8 hours
99.99%	4 minutes	1 hour
99.999%		5 minutes

However, these much-quoted figures are not realistic. Most service level agreements (SLAs) specify defined waiting times during which the service is not available although this time is not counted as downtime. This means that high availability is usually categorized as *non-scheduled downtime*.

The specification for an SAP database, for example, can stipulate that the database is available at 99.99% during office hours from 7:00 a.m. to 7:00 p.m. If it is possible to work outside these times, then these requirements can be fulfilled much easier and hence at a lower cost than in the case of an unrealistic specification of a maximum downtime of 5 minutes per year with 24x365 operation.

3.17.3   The approach

High availability is achieved with redundant resources and monitoring of their functionality. When a component fails, a standby component automatically steps in. From this time on, however, redundancy is affected or even does not exist any longer, so that repair must start immediately. HA systems require substantial administrative effort and do not work alone. The mean time to repair (MTTR) rather than the mean time between failure (MTBF) is an important quality measure in this context.

Technical description of the migration paths

Redundancy can be achieved on all levels:

Table 41: Summary of abstraction levels

Abstraction level	
User and/or administration environment	Disaster recovery
Application	Distributed applications
Middleware	Clustering
Operating system	Resource monitoring, restart, failover
Hardware	Duplicating components

Today, redundant harddisks are already standard (mirroring, RAID1; the use of RAID5 is today hardly justifiable any longer) and available on all platforms. The situation is, however, more difficult in the case of the other hardware components. Network cards with redundant configuration capability are only seldom supported. Support of hardware redundancy by the operating system is at the heart of these discussions. In this field, the proprietary UNIX systems and, of course, also mainframes offer significant advantages which, in the authors' opinion, are unlikely to be achieved by Open Source systems in the nearer future.

Redundancy at the operating system level is achieved by monitoring resources and their swapping to another computer in the case of a failure (failover).

Certain middleware components (such as databases or transaction monitors) also permit treating a large number of systems as a single one. Some applications do not require this feature because they are distributed to multiple computers anyway, so that failure of one computer does not cause any problems.

If high availability can be provided at one abstraction level, this is theoretically sufficient for all the other abstraction levels below that level. In practical use, the robustness and hence the reliability of an HA system are boosted by implementing redundancy measures on as many levels as possible – remember that even an HA subsystem may fail at some time and can then be compensated for by another redundant component.

And finally, the most serious source of error should not be overlooked: man, in his capacity as system administrator or programmer. Administration or programming errors are often taken over by the system, so that all redundant services or components are subsequently faulty. If, for example, an administrator has deleted several hundred GB by mistake, no mirroring and no service redundancy can help – the data is deleted from all components. This is why good backup and restore policies and, if necessary, also disaster recovery practices in the interest of business continuity planning are elementary components of an HA solution.

3.17.4 Categories of HA systems

Whilst the underlying principle of high availability is always redundancy, this redundancy can be achieved in different ways.

Failover:

This is the "classic" architecture of an HA system, i.e. two to three machines which initially try to restart a service that has failed. If this attempt fails, the service is transferred to another machine and started there.

Application clustering

A few applications are already cluster-enabled and hence capable of working on multiple machines which then present themselves as a single system to the outside world and which can cope with a failure of individual machines in a transparent manner. The best-known example of this architecture is Oracle 9*i* with the Real Application Cluster (RAC) option.

Server farms

This approach has become popular especially for web servers. A *load balance*" distributes incoming requests to a set of machines. This method is particularly suitable for services which have no status. It is often used for frontend implementations whilst backends are operated on a failover system.

Another mechanism frequently used for databases is redo log shipping for disaster recovery. With this method, redo logs are generated for all transactions and sent to the backup computer where their processing then generates the latest database status on the backup system too.

This categorization approach helps identify existing high-availability solutions and to determine where the use of Open Source products makes sense.
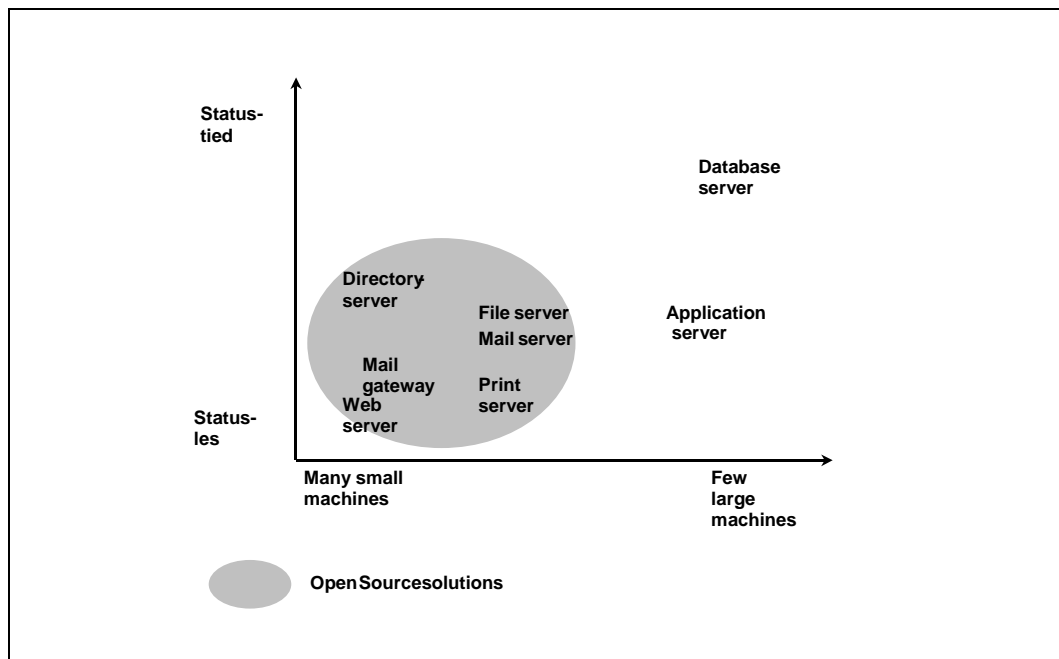
Fig. 50: HA solutions

Technical description of the migration paths

The insufficient implementation of the cluster types which work with a few large, fully redundant machines is primarily due to the special hardware used for which the operating system often offers insufficient support.

Open Source software can chiefly be used in the field of server farms, ideally in conjunction with systems without major session states. Typical applications are web servers, e-mail gateways, file and print servers.

There are only few Open Source applications with application servers. There they can be used if the SLA requirements are not too high (such as 99.9% during office hours, etc.). Although high availability is then typically ensured via a failover architecture, clustering possibilities also exist at the middleware level (with JBoss, for example).

High-availability Open Source databases do not exist. It is, however, possible in this respect to plan the use of proprietary software (such as Oracle RAC) on Linux, making it possible to achieve substantial hardware cost savings in certain cases.

3.17.5   Proprietary HA software

HA software is a domain of the UNIX and mainframe world. Windows DataCenter is usually not regarded as being sufficient for mission-critical applications.

At the operating system level, each of the large UNIX manufacturers offers an HA solution based on failover architecture. Following the merger with Compaq, HP even offers two; only the survivor will be discussed here.

Table 42: Overview

	IBM	HP	Sun
Operating system / HA package	AIX HACMP	HP-UX MC/Serviceguard	Solaris Sun Cluster
File system	JFS2	HFS	UFS with Sun VM
Cluster-wide file system	Yes	No	Yes
Maximum number of machines	32	16	8
Support of multiple application instances	Yes	Yes	Yes
Partitioning	Yes	Yes	Yes
Failover of existing TCP connections	No	Yes	Yes
Storage technology	Ultra3 SCSI Fiberchannel	Ultra3 SCSI Fiberchannel	Ultra3 SCSI Fiberchannel
Disaster recovery options	HAGEO GeoRM	CampusCluster Metrocluster Continental cluster	Storage Data Network replicator

		Continuous Access XP	
Management	GUI integrated in SMIT	Separate GUI	GUI integrated in SUNMC

As already mentioned, Oracle RAC is an important option in the database area when it comes to achieving high availability even at middleware level. This solution is available for the proprietary UNIX systems, Linux and Windows Server.

3.17.6   Open Source HA software

The world of Open Source tools is subject to extremely rapid development. The following section provides an overview of existing Open Source HA software that is already widely used and tried-and-tested in many existing applications. With regard to concrete HA projects, however, this overview can only give an indication of potential use. The specific architecture for every single project must be determined and the suitability of the related tools must be checked from case to case. The authors of the study hence urgently recommend involving seasoned experts in the respective projects.

Many of the tools to be mentioned in the following are, of course, also offered by companies. In Germany, almost all Linux-based tools are available from SuSE. Support and project assistance are offered by many companies, including EDS, for example.

3.17.6.1   Disk subsystems

Since Linux Kernel 2.4 which is used in all current distributions, Linux has been supporting disk mirroring using the Multi-Disk (md) kernel module. This subsystem also supports multi-path access, i.e. the simultaneous connection of disk subsystems to different computers. This feature is required for data and application disks in a failover architecture. System disks must always be connected to exactly one computer.

LVM is a functioning volume manager. ext3 is becoming the standard file system with journaling properties (refer also to chapter 3.2.3).

3.17.6.2   Failover via heartbeat
A failover architecture using heartbeat can be implemented for Linux systems. heartbeat supports the definition of resource groups (services, file systems and IP addresses) which can be started on another server after a failure. The application status of existing sessions is not taken over in this case.

Since Linux does not support the multi-path configuration of network cards, the service availability can be checked via different communication channels (serial and network).

Fully automatic booting of the device is often required in the case of a service failure. The "watchdog" solution which is the most widely documented solution is error-prone and leads to unnecessary reboots. A new module with the name "hangcheck-timer" is said to be superior in many situations. The selection of the

concrete module should be left to the consultants planning the concrete HA architecture for the given application.

Every HA project should be aware of the restrictions of the Open Source failover solution: There is no cluster-wide file system; the maximum number of machines in a failover cluster should not exceed three; logic partitioning of existing machines (assignment of hardware resources, such as CPU and disk space to resource groups) is not supported, and disaster recovery options do not exist either.

heartbeat is a widely used module; according to the Linux HA project, several thousand installations are in productive use world-wide. It is the key element of the HA solutions offered by leading Linux manufacturers (SuSE, Conectiva, Mandrake). A well-known user in Germany is the Bayerischer Rundfunk TV and radio station which used heartbeat in order to implement the 2002 Olympic Games website of the German Association of TV and Radio Stations (ARD) under Linux.

Within the scope of a migration project based on heartbeat[151] , a reliable high-availability solution was successfully implemented for the office of the Federal Data Protection Commissioner. The illustration below gives an overview of the solution used and its architecture.
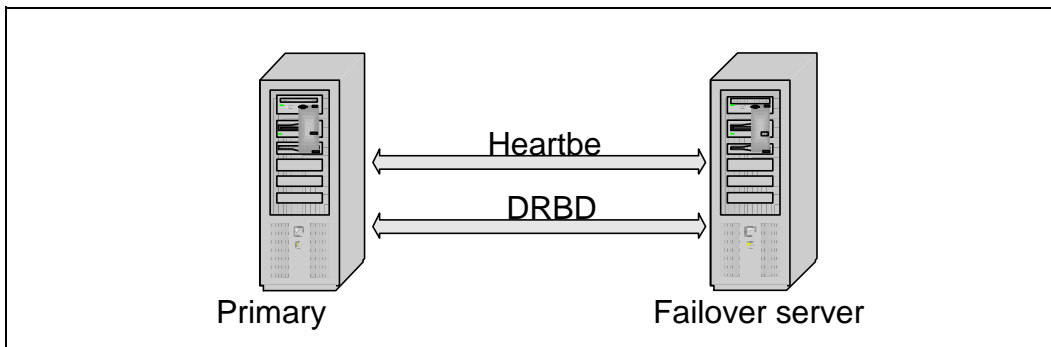
Fig. 51:   Solution with heartbeat and DRBD

The program combination used, consisting of heartbeat and DRBD[152] (Distributed Replicated Block Device), implements a high-availability solution for the file and print services, for the mail services, the web server, the domain services (DNS, DHCP) and the directory service. The server nodes are monitored by heartbeat. For this purpose, the machines were connected using a crossover Ethernet and a serial null modem cable. If the active server can no longer be accessed via these communication lines, the failover server automatically takes over the virtual IP address and the corresponding services. Besides high availability, the DRBD program implements Raid-1 mirroring of the partitions and/or logical volumes.

---

[151] http://linux-ha.org/heartbeat/

[152] http://www.complang.tuwien.ac.at/reisner/drbd/

This means that any data that has been written is available to the second system at the very moment the active server fails. DRBD can constitute a cost-effective alternative to external SAN systems for certain scenarios.

3.17.6.3 Server farms

The Linux Virtual Server (LVS) provides the infrastructure for a server farm. A load balancer under Linux distributes incoming requests to a set of real systems. These real systems are hidden to the end user to whom the entire installation seems to be a single, large server. Typical applications include, for example, web, e-mail or media servers.

The Linux Virtual server is often combined with a failover architecture for the load balancer. The UltraMonkey project or the Open Source Piranha project from Red Hat exist for the simple combination of these two technologies.

LVS is in productive use in many companies. Very large websites, such as `linux.com` and `sourceforge.net`, use LVS in order to secure their high-availability websites. Real Networks uses LVS for a cluster of media servers.

3.17.6.4 Application clustering

The leading Open Source application servers offer application clustering.

> Tomcat is the low-level application server used to implement Java servlets and Java server pages (JSPs). Its load balancing feature supports clustering. Tomcat is just as widespread as Apache.

> JBoss is one of the stars of the Open Source world, a full-scale application server that implements the J2EE standards. In 2002 alone, more than 2 million downloads were recorded from the reference site, with an abounding number of implementations in productive use. Its functionality also includes application clustering.

Open Source databases do not provide any high-availability solutions. One of the major problems in most cases is the fact that no online backup functionality is available. However, Oracle offers its RAC option for Linux systems, enabling substantial savings in the hardware and service areas.

3.17.6.5 Compute clusters

For the sake of completeness, the HA solutions in high-performance computing should also be mentioned at this point even though this application is certainly of limited interest for public administrations. Beowolf was the first compute-cluster implementation under Linux and is still today the most frequently used solution. Job scheduling within a cluster is ensured by the portable batch system (PBS) or the MAUI scheduler.

4 Evaluation of economic efficiency

4.1 Introduction

As the discussion on studies currently available on the TCO[153] subject in conjunction with the use of OSS and COLS products[154] shows, evaluating the economic efficiency of IT projects is generally a very difficult task which is almost impossible to resolve in light of the often multi-dimensional models of economic efficiency.

A broad-based and multi-faceted analysis – which is definitely the case when comparing the costs of Microsoft and OSS/COLS platforms – must ensure comparability of the subjects analyzed and the appropriate extent of the analysis as major requirements. Too narrow a discussion of isolated aspects would mean that the results cannot necessarily be applied to the overall picture. This does, for example, become apparent from the IDC study "Windows 2000 vs. Linux für Unternehmensanwendungen" [Windows 2000 vs. Linux for Enterprise Applications] which was commissioned by Microsoft. Since the study restricts itself to the costs of servers for infrastructure functions where the ratio between software license costs and total costs differs from that of client applications, for example, it is not possible to directly derive analogous statements concerning economic efficiency in the application or desktop areas.

Another aspect to be considered in a study is user structures. The size of organizations and the different starting scenarios for an IT environment are particularly relevant aspects when the economic efficiency of a migration project is considered. One common observation is that smaller public agencies (in the communal sector, for example) use IT infrastructures that can be set up and operated with simple means and without intensive user training. In contrast to this, the reliable operation of infrastructures or computer centers for large and/or specialist public agencies and data centers with service level agreements requires higher user training levels, organizational rules for downtimes and emergencies, as well as different hardware in many cases.

Taking this reference framework into consideration, a multi-dimensional approach is necessary in order to analyze the economic efficiency of information and communication systems. Even before IT costs are analyzed, a substantial increase in economic efficiency can be achieved by suitable personnel-related, organizational and streamlining measures at public administrations. In addition to this, a suitably designed IT strategy can also provide a major contribution towards boosting economic efficiency.

The overall economic efficiency of IT systems is significantly influenced by the following parameters.

---

[153] TCO = Total Cost of Ownership

[154] OSS = Open Source Software, COLS = Commercial Linux Software

The degree to which low-cost standard products cover the required functions.

Quality, modification flexibility and development capability of the standards, technologies and products used

Efficient introduction and system management

Smooth and consistent integration of components and systems into a process-oriented value chain

A good (internal or external) service organization as well as high-quality expertise

Economic lifecycles of products

Costs and efficiency of the purchasing/sourcing process

Competition in the field of products and services

Optimum interaction of all these factors over an extended observation period is a prerequisite for establishing and controlling economic efficiency. This means that a simplified analysis of individual cost items normally fails to correctly reflect the overall picture.

Besides the identification and comparison of costs, the evaluation of the possible utility values is another important aspect of an evaluation of economic efficiency. Especially in this area, strategic considerations and forecast benefits play an important role in order to enable an integrated evaluation of both the starting situation and prospects. Example: In a strategic context, higher costs of an individual component can still lead to a significantly better total result thanks to manufacturer independence and hence a better position in software license fee negotiations.

Both the method and the result can thus merely serve as an aid in determining an organization's own economic efficiency and hence the development of its own IT strategy.

4.2 Methodological principles

Although it is generally possible to compare items which differ in functional or qualitative terms, this requires a cost-to-benefit analysis which also confronts the anticipated *increase in productivity* with the anticipated *additional costs*.

However, a productivity analysis in the IT value chain is not possible within the framework of this migration guide because the necessary unbiased long-term studies are not available, especially in public administrations. On the basis of today's experience and especially with a view to the fact that both Linux/UNIX and Microsoft platforms are mature products with a long development history, such an analysis would probably lead to a balanced result. This is why the evaluation of economic efficiency in this migration guide will focus on a direct, *simplified monetary* analysis and a *benefit* analysis.

4.2.1 Monetary analysis

The net present value method is used to determine the monetary effects of the projects. As a dynamic method, it evaluates investment projects on the basis of their net present value, i.e. by realistically describing money flows (revenue and expenditure, budget-relevant and not budget-relevant) with a focus on a common reference time. Revenues and expenditures which can be related to the project can be planned for five years ahead. The current market value of future values is determined by discounting, using an interest rate determined by the Federal Ministry of Finance.

4.2.2 Benefit analysis

The benefit analysis is applied if the decision has to additionally consider other effects which cannot be measured in monetary terms. The benefit analysis evaluates individually and independently weighted target criteria that are subsequently included in a final evaluation. Evaluation scales are used in order to quantify the so-called "soft" factors.

We recommend evaluating the results in two steps as follows.

1. Priority must be given to the results of the monetary evaluation of economic efficiency. Costs and savings resulting from a project are expressed by an ROI ratio which is reflected by a positive net present value.

2. The results of the benefit analysis lead to urgency and strategy ratios. Within the framework of the migration projects, they should be treated with lower priority.
   This second step is mainly designed for handling cases in which an evaluation of economic efficiency according to monetary aspects is neither generally sufficient nor enables a clear profitability assessment. Urgency and/or strategy criteria can always require a high implementation priority for a project, irrespective of monetary criteria.

4.2.3 IT-WiBe 21 (recommendations on economic efficiency assessments for IT systems)

Evaluations of economic efficiency in the federal administration are subject to section 7 of the Federal Budget Code (§ 7 BHO) and the administrative regulations enacted under this which, since 1995, have mainly considered economic methods. In order to adapt these regulations to the specific requirements of information technology, the Co-ordinating and Advisory Agency of the Federal Government for Information Technology in the Federal Administration (KBSt) already issued an administrative directive in 1992 titled "Empfehlung zur Durchführung von Wirtschaftlichkeitsbetrachtungen beim Einsatz der IT in der Bundesverwaltung (IT-WiBe) (recommendations on economic efficiency assessments for IT systems)". A completely revised edition was issued in 1997. The IT-WiBe includes three major steps as follows.

Identifying influence variables (selecting criteria)

Gathering/evaluating data

Determining ratios
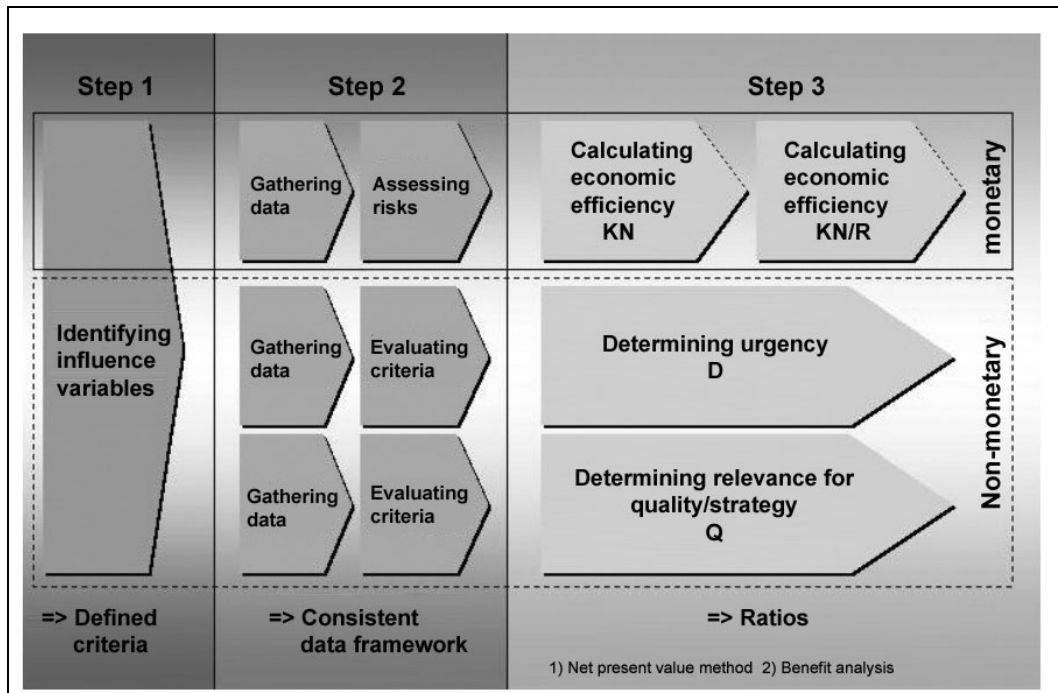
Fig. 52:   IT-WiBe methodology

IT-WiBe is a method which, unlike the TCO method, also considers possible savings rather than the cost aspect alone.

4.2.4   Migration cost matrix

Since the IT-WiBe method is generally well-suited for evaluating the economic efficiency of a given project, but often too complex and (due to the lacking budget figures required) not feasible, a simplified method – the *migration cost matrix* – is adopted in order to analyze the monetary dimension.

This approach does not require that costs and savings be determined according to selected criteria but instead summarizes them in three categories, i.e. hardware, software and manpower. Acquisition[155] and follow-up costs as well as possible savings are recorded over a period of five years for these categories. A complete view gives an overview of all years and categories. Furthermore, an ROI analysis supplies, similar to the WiBe21 method, a net present value discounted to the reference time.

---

[155] The "acquisition" and "follow-up costs" sectors as well as the savings category include the following sub-sectors: server infrastructure, database applications, messaging/groupware, web applications, Office/desktop and miscellaneous.

This gives planners in public agencies an instrument for simple and quick assessment of project cost volumes, including follow-up costs and savings, as well as for ROI assessment[156].

4.2.5   TCO

The fundamental principle of the TCO analysis is to divide all costs of an IT system into two large groups, i.e. direct and indirect costs. Direct costs are all costs which can be budgeted. One feature which all direct costs have in common is that they can be directly measured in monetary units. The second large group includes the indirect costs that cannot be budgeted. This group includes the downtimes during which the systems under review are not available for use for scheduled or non-scheduled reasons. These times can be measured, but not directly in monetary units. This requires a sometimes controversial conversion via wages paid "in vain" or loss of revenues. Indirect costs also include any "non-productive" end user activities, such as self-help, mutual assistance, formal and informal learning, data administration and backup, games, surfing, etc.

This method would, in principle, also be suitable for determining the costs of migration projects. Since only the cost aspects are considered here and because an ROI analysis is also lacking, and all the more so since all of the above-mentioned cost aspects can also be addressed by the WiBe 21 method and the migration cost matrix, the TCO approach is not used to evaluate the economic efficiency of migration projects.

4.2.6   Comparability

The evaluation of economic efficiency is carried out for two scenarios in order to ensure the comparability of the different evaluations.

Migration of individual or several migration objects[157] (partial migration) in the case of clearly definable products or product groups[158]

Complete migration, i.e. migration of a complete IT environment – servers, clients, infrastructure, special applications

Migration is generally possible in two ways:

Replacing migration – i.e. migration to a completely new, Open Source-based software environment using open source software (OSS) and/or Commercial Linux Software (COLS) or

Continuing migration – i.e. migration within the framework of the products already in use towards newer versions

---

[156] Refer to the "Monetary dimension", chapter, diagram "migration cost matrix"

[157] Refer to the definition of objects in the "Approach" chapter

[158] Desktop applications as migration objects with word processing, spreadsheet analysis, graphics and Internet browser as products.

A reduced catalog of criteria which is specifically tailored to partial migration cases is used for migrating migration objects. This catalog includes criteria for introduction and operation[159].

The general evaluation criteria of the IT-WiBe method must be adopted in cases of complete migration. Because this often involves migration of special applications too, development work for such specific applications will also be necessary in addition to the migration activities for standard products.

These rules are generally also applied to cases of "internal" migration. If individual products or product groups only (such as MS Office) are migrated, we once again refer to migration objects and apply the specific catalog of criteria. In contrast to this, the complete WiBe catalog of criteria is applied in the case of a more complex scenario (such as MS products for communication and office, special applications, etc.).

Another aspect is that a comparative analysis of economic efficiency only makes sense if the different alternatives are comparable in technical and functional terms. The following applications of OSS and Microsoft technology can be considered to be comparable for the purposes of this migration guide:

Infrastructure services

- File server

- Print server

- Logon server

- Networks

Messaging and groupware systems

Office packages

Database and web application server

The aspect of IT security is today not considered to be comparable in view of the clearly higher exposure of Windows systems. Even with increased effort and at a higher cost, it is not possible to ensure comparable security levels of the systems, so that a comparison of economic efficiency is not carried out for the security area.

4.2.7 New introduction vs. migration of systems

A cost analysis with a view to the introduction of new technologies must generally differentiate between new introduction and migration of processes and systems. As a general rule, one can say that a new introduction is usually simpler and cheaper than migration where different, sometimes historically grown architectures must be replaced and data migrated without disrupting operations to a larger extent and without losing data of the former application.

---

[159] In contrast to the general catalog of criteria, the criteria for development are taken out and replaced by criteria for introduction.

Evaluation of economic efficiency

As any migration method is always dependent on its starting situation, it is hardly possible to make any generally valid and all-encompassing statements concerning its cost. Whilst migration is in some cases possible without any problems and almost without any additional cost, the existence of user-developed applications to be migrated, the transfer of legacy data, special user and access privilege structures or other special features may generate substantial project costs which must be evaluated from case to case, also taking criticality aspects of the particular public agency concerned into consideration.

4.2.8 Full cost approach

For these reasons, the evaluation of economic efficiency focuses on the determination and analysis of the full costs for the general alternatives contemplated in this migration guide, i.e.

Open source software (OSS)

Commercial Linux software (COLS)

Microsoft software (MS)

The results of the analysis give a fundamental outlook on the long-term development of costs with the different alternatives from today's perspective. Thereafter, the costs of migration must be determined in order to complete the basis for a decision in favor of or against a potential change and migration. Thanks to a large number of companies offering their services in this sector, such an estimate can be obtained directly in the form of a migration offer both from internal and from external service providers, and can then be compared to the potentials identified.

The method used to this effect considers the non-homogenous structure and different sizes of public agencies by a differentiated analysis of data. The full costs of the individual alternatives are determined in several steps as follows:

Definition of the applications to be studied

Determination of cost factors in the applications studied

Determination of values of the cost factors for:

- small public agencies

- medium public agencies

- large public agencies

Determination of the costs for rationalization tools (system management tools)

Determination of the cost structure of the alternatives studied

Determination of the qualitative and technical comparability

Scenario analysis in the case of a change to:

- OSS   Open source software

- COLS   Commercial Linux software

The direct potential of OSS/COLS in the purely monetary dimension primarily results from savings in license costs (further potentials resulting from the strategic assessment). The result of the evaluation of economic efficiency is hence the analysis of long-term potentials by determining the software license costs compared to the full costs of the infrastructures studied.

4.3   The monetary (operative) dimension

4.3.1   Applications

In order to obtain a sensible result, the analysis is carried out within an overall context that encompasses several applications. The overall evaluation of the costs to be studied includes the following fields:

Server infrastructure

- File services

- Print services

- Logon services

- Network services

Desktop infrastructure

- Office

- Web

Messaging/groupware

DB and web applications

This list is certainly not exhaustive, but constitutes a common denominator for cost infrastructure areas of public agencies.

4.3.2   Cost categories

Ensuring comparability and standardizing the results of the cost analysis require a uniform and at the same time unambiguous cost model for all applications. The methodology adopted in this migration guide is based on the concept that no productivity assessment is carried out (refer also to chapter 4.2), which means that no separate analysis of downtime-related productivity influences or outsourcing calculations are carried out either.

For these reasons, three major cost categories were defined for the common cost model as follows:

Hardware

- Comparison of hardware requirements

Software

Evaluation of economic efficiency

- Software license costs

- Software maintenance costs

- Additional costs for directory systems
- Additional costs for system management and security

Manpower

- Administration

- Support

- Software maintenance

- Training

Agency - Description - Number of - Number of sites - Number of - Start [1] 2003		To tal		Ha rd wa re		So ft wa re		Ma np ow er	
1st year -	Quantity unit [2]	**Total** Total [4] cost		**Hardware** Total [4] cost		**Software** Total [4] cost		**Manpow** Total [4] cost	
Balan		**0**		**0**		**0**		**0**	
Costs (acquisition +		**0**		**0**		**0**		**0**	
Acquisition costs		0		0		0		0	
Server		0		0		0		0	
-		0		0		0		0	
- Workstation		0		0		0		0	
- Network		0		0		0		0	
Database applications		0		0		0		0	
Messaging/groupware		0		0		0		0	
Web applications		0		0		0		0	
Office / desktop		0		0		0		0	
Miscellan		0		0		0		0	
		0		0		0		0	
Follow-up		**0**		**0**		**0**		**0**	
Savings		**0**		**0**		**0**		**0**	

Fig. 53: Migration cost matrix with cost categories and applications

The following should be noted with regard to downtime: The experience so far available, especially from computer centers, suggests a higher availability of Linux systems compared to MS Windows systems and hence a higher productive yield under Linux [160].

4.3.3 Features of applied categories of public agencies

The following sections briefly address the features of different types of public agencies. Considering the sometimes large differences in terms of IT equipment and organization of the different public agencies, these can only serve as a very general orientation guideline with regard to the relevant study criteria.

---

[160] IDC also confirms this in its study "Windows 2000 vs. Linux für Unternehmensanwendungen" [Windows 2000 vs. Linux for Enterprise Applications], 2002, which was commissioned by Microsoft

4.3.3.1   Small public agency

Users: up to 250

Hardware: typically small and low-cost Intel platform

Backup and recovery: low-cost backup mechanisms, use o tape drives or RAID systems

Personnel: usually one administrator with a universal profile, one deputy

IT organization: individuals, sometimes groups, low degree of specialization

Security and availability: usually low to medium requirements

System management: individual tools (MS) or scripts (Linux)

4.3.3.2   Medium public agency

Users: between 250 and 1000

Hardware: small and large server systems, Intel and RISC platform, both distributed and central architectures being possible

Backup and recovery: dedicated backup and archive servers available, the use of RAID technology being the rule

Personnel: several administrators working 8 hours a day, specialization, standby duty

IT organization: IT department

Security and availability: usually medium to high requirements

System management: software distribution tools, thin clients, network and system monitoring and supervision

4.3.3.3   Large public agency / computer center operation[161]

Users: more than 1,000 (up to 100,000)

Hardware: low-cost Intel clusters, large server solutions, distributed architectures, central mainframe systems

Backup and recovery: central backup / disaster recovery servers with Robot or Jukebox hardware

Personnel: several administrators working 8 hours a day, specialization, standby and emergency duty

IT organization: computer center, local administration groups, if necessary

Security and availability: high to very high requirements, use of comprehensive SAN solutions

---

[161] It may be necessary to combine medium and large public agencies and to analyze computer centers as a separate type of public agency.

System management: software distribution tools, thin clients, network and system monitoring and supervision

4.4   Strategic dimension

Besides the direct monetary analysis of the full costs of the different alternatives, a strategic analysis (or *dimension* in the WiBe terminology) must be included.

The need for a strategic analysis results from the direct monetary repercussions of "manufacturer dependence" as a strategic factor. This is relevant both from a macroeconomic and from a microeconomic point of view.

4.4.1   Macroeconomic discussion

Competition-related aspects play the key role in this discussion. Major advantages of functioning competition are the following:

Better product quality

Lower product prices

Higher innovation rate

Although all software manufacturers usually claim to ensure both higher product quality and technological innovation, a statement of general validity can seldom be made in reality. Especially the development of the World Wide Web shows that Microsoft, for example, long "overslept" this the most important innovation of recent decades.

Despite the fundamental nature of the macroeconomic discussion, the readers of this migration guide cannot directly influence the macroeconomic aspect which is hence not discussed in more detail in this document. The European Commission is currently addressing the issue of Microsoft's monopoly-type position in the field of operating systems. The results and conclusions, if any, are yet to be communicated.

4.4.2   Microeconomic discussion

An analysis of an agency's dependence on suppliers of products and services is the important issue in this context. Although this dependence is substantially fostered and made apparent through the existence of monopolies or quasi-monopolies, excessive dependence on suppliers can occur and cause economic disadvantages even in an environment of functioning competition. These disadvantages can take the form of higher product prices, as well as shorter product life cycles and additional introduction costs in the case of continuing migration.

Under extreme conditions, this dependence can lead to a situation where no reasonably priced, acceptable alternatives for action exist any longer. In contrast to this, a situation based on a strategic equilibrium leads to a better negotiating position with access to alternatives should problems arise.

4.5   Overall results of the evaluation of economic efficiency

Most of the studies related to this topic use the full cost approach in their analysis and agree that a substantial share of the costs is related to personnel costs in conjunction with introduction and operation rather than to software license costs. Due to different assumptions – chiefly concerning the administration capabilities of systems – the studies come to opposing conclusions with regard to the economic benefits of the different alternatives.

The studies favoring Microsoft state the lower personnel costs due to a lower training standard and hence lower basic salaries of administrative personnel as the most important (albeit not exclusive) reason for the lower TCO calculated for Microsoft platforms[162]. Another advantage – however, based on very questionable assumptions – is seen in the field of IT security which is said to be generally easier to implement for Microsoft-based platforms.

The Microsoft-skeptical studies come to a generally different result. Although these studies also find a difference in basic salaries, this is more than offset by better administration capabilities, especially in computer center operations.

The studies carried out within the scope of this migration guide hence refer to three important factors of the TCO analysis which is necessary with regard to the introduction of Linux/OSS:

1. Percentage of the software license costs in total costs

2. Degree of specialization of candidate IT systems and infrastructures

3. Degree of automation of candidate IT systems and infrastructures

The share of software license costs in total costs of IT systems and processes ranges from 20% to 50%. This is hence also the range for the direct and indirect potential of the OSS and COLS alternatives in purely monetary terms on condition that the work results which can be achieved are comparable.

Besides a statement concerning the share of software license costs in total IT costs, another two factors should be considered in order to evaluate the actual degrees of freedom for IT decision-makers. These are the index of costs which can be directly influenced on the one hand and the analysis of the budget-relevant costs on the other.

Cost types that can be directly influenced include the following:

1. Software acquisition costs:
    Lower purchasing prices mainly thanks to a change to lower-priced products or thanks to negotiation

2. Software maintenance costs:
    Mainly by consolidating (reducing product variety) software products or omitting update cycles

---

[162] Refer to the IDC study "Windows 2000 vs. Linux für Unternehmensanwendungen" [Windows 2000 vs. Linux for Enterprise Applications], 2002

3. Hardware acquisition costs:
   Thanks to a change to lower-cost hardware platforms

4. Hardware maintenance costs:
   By consolidating (reducing the product variety) hardware or extending life cycles

Unlike hardware and software costs, personnel costs as the largest complex of IT expenditure are usually not costs that can be directly influenced. This is due to the fact that the introduction and operation of IT infrastructures and systems are firstly related to a base load that is determined less by individual license models and more by requirements concerning service intensity, availability and security of the platforms used. Reducing existing personnel numbers or outsourcing and consolidation are usually not alternatives which can be implemented in the short term.

The analysis of IT costs which can be directly influenced shows that license costs (software acquisition, maintenance, updates) account for the largest part and hence offer the largest freedom for action.

4.6 Migration recommendations based on the evaluation of economic efficiency

The migration recommendations concern the following scenarios:

- ❍ Complete migration (for large, medium and small public agencies)
- ❍ Continuing migration (for large, medium and small public agencies)
- ❍ Partial migration (selective migration and partial migration at the server end)

The examples discussed[163] will largely neglect the hardware aspect. Migration of modern hardware (not older than 2 to 3 years) is possible without modification of the hardware. In the case of older hardware, replacement and/or supplementary investment may become necessary in any case irrespective of the direction of migration (Open Source or Microsoft)[164].

The monetary analysis is based on a term of use of five years for assets which is typical for public agencies. Reinvestment is expected only after this time. This concerns both migration towards Linux and Microsoft-internal (continuing) migration. Follow-up costs are not assumed during the four years following acquisition.

The calculations are based on price assumptions typical for public agencies. The calculations mainly include once-off purchasing prices. Lease variants are additionally calculated for the Windows and Office products.

---

[163] Refer to chapters   - 4.8.6.7,

[164] In order not to render the calculations too complex, the "hardware" factor was omitted from the analysis of migration costs.

A comparison of user-related migration costs for complete and continuing migration shows clear cost advantages in the case of migration towards the OSS environment[165] .

Table 43: Comparison of user-related migration costs for complete / continuing migration

Type of public agency	Complete migration	Continuing migration
Small	€500[166]	€850[167]
Medium	€340[168]	€730[169]
Large	€180[170]	€600[171]

The costs of continuing migration are around twice as high as those of complete migration.

The cost advantage of complete migration is mainly due to software cost savings (between 92% and 95% for small to large public agencies). The comparison of personnel costs, in contrast, shows differences in favor of continuing migration. In the small/medium/large types of public agencies, the personnel costs of this migration variant are around 14.0% / 6.5% / 2.2% more favorable.

One trend is approximately identical for both migration variants: costs increase as the size of the organization decreases!

[165] Migration to the OSS environment is referred to as "complete migration".

[166] Refer to the chapter on "Complete migration", sub-chapter "Small installation".

[167] Refer to the chapter on "Continuing migration", sub-chapter "Small installation".

[168] Refer to the chapter on "Complete migration", sub-chapter "Medium installation".

[169] Refer to the chapter on "Continuing migration", sub-chapter "Medium installation".

[170] Refer to the chapter on "Complete migration", sub-chapter "Large installation".

[171] Refer to the chapter on "Continuing migration", sub-chapter "Medium installation".

Evaluation of economic efficiency

Migration cost development
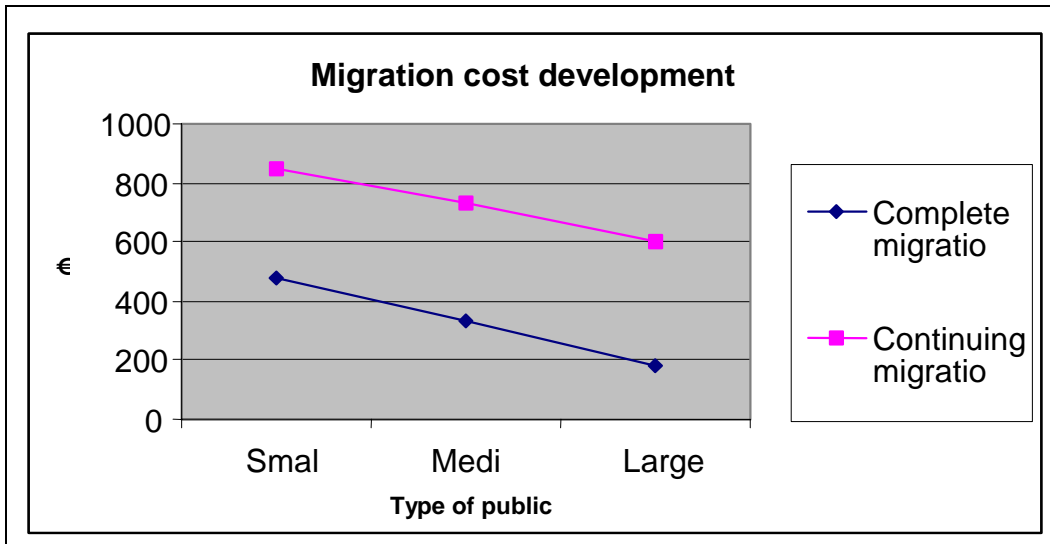
Fig. 54:   Migration cost development

4.6.1   Complete migration

The calculation examples generally indicate a dominant personnel cost share in the order of 90% (around 87% to 93%). The migration costs range within the percentage bandwidths indicated below for the different types of public agencies.

Table 44: Distribution of costs in the case of "complete migration" in public agencies

Type of public agency	Software	Personnel
Small	Up to 7%	Up to 93%
Medium	Up to 10%	Up to 90%
Large	Up to 13%	Up to 87%

The savings calculated in this model represent the expenditure necessary for migration to the Windows 2000 environment.

Table 45: Total migration costs[172] per user in the case of complete migration

Type of public agency	Acquisition basis (once-off price)
Small	€500
Medium	€340
Large	€180

---

[172] The total migration costs include all expenditures related to the migrated systems for the five-year period analyzed. All figures are approximate values.

Complete migration means a superproportional savings effect in large public agencies. Savings in conjunction with migration from Windows NT to Linux compared to migration to Windows 2000 reach an order of magnitude which exceeds three times the expenditure.

Personnel costs in conjunction with the change were of a comparable size, so that license cost savings account for most of the savings.

The savings effects shown suggest migration to the Open Source environment.

The scenario for medium and small public agencies is generally comparable to that for large public agencies. Migration to Open Source is strongly recommended for these types of public agencies too.

4.6.2 Continuing migration

In the case of this type of migration, no savings can be identified and hence cannot be set off either. This is why the scenario-related cost volumes only are shown.

Table 46: Total migration costs[173] per user in the case of continuing migration

Type of public agency	Acquisition basis (once-off price)	Acquisition basis, or annual lease in certain cases
Small	€850	€1,860
Medium	€730	€1,740
Large	€600	€1,600

The economic efficiency of migration increases with increasing user numbers. A change from acquisition to lease prices[174] is not justified in the case of the model used here.

4.6.3 Partial migration

4.6.3.1 Selective migration

This form of migration concerns the permanent replacement of a selected system component within a complete IT structure. This case will be illustrated by a change from Exchange 5.5 to Samsung Contact. On condition that the full required functionality is ensured in the particular case, this form of migration can

---

[173] The total migration costs include all expenditures related to the migrated systems for the five-year period analyzed. All figures are approximate values.

[174] Lease prices were available for the MS Windows and MS Office products – hence the annotation "in certain cases"

be recommended for all types of public agency because it offers a measurable cost advantage compared to Microsoft-internal migration[175].

Table 47: Total migration costs per user in the case of selective migration

Type of public agency	Acquisition basis (once-off price)
Small	€99
Medium	€153
Large	€39

Samsung's graduated price range leads to the migration cost bandwidths per user shown in the table above.

Table 48: Migration cost distribution

Type of public agency	Software	Personnel
Small	Up to 35%	Up to 65%
Medium	Up to 21%	Up to 79%
Large	Up to 56%	Up to 44%

The software and personnel cost distribution oscillates around the 50% mark. This share can vary, depending on the labor intensity of the change processes. The costs taken here are assumed to equal those for a migration to Exchange 2000. However, experience suggests that this cost share is lower, so that the realistic personnel cost share of a migration is likely to be less than 50%.

4.6.3.2 *Partial migration at the server end*

This partial migration corresponds to that part of complete migration at the server end. As an alternative to complete migration, this form of change ensures relatively high efficiency with regard to urgency and quality/strategy criteria because the relevant part of the migration project takes place in the server area with regard to these aspects.

The costs are around €120 per user below those for complete migration (refer to the box below "Comparison of costs for complete migration and partial migration at the server end").

This migration alternative is recommended not just for cost reasons but also because it enables a gentle transition to the OSS world with minimum repercussions on users.

---

[175] The costs of migration to SamsungContact are set off by the costs of migration to Exchange2000 as savings. The result is in all cases positive capital values which indicate the corresponding cost advantages.

Table 49: Total migrations costs[176] per user with partial migration at the server end[177]

Type of public agency	Acquisition basis (once-off price)
Small	370 €
Medium	220 €
Large	65 €

Although in this case the migration costs concern the server platform only, they nonetheless correlate to the number of users in the type of public agency concerned for the purpose of comparison with the other costs.

Table 50: Comparison of costs for complete migration and migration at the server end

Type of public agency	Complete migration	Partial migration at the server end	Client share in complete migration
Small	€500	€370	€129
Medium	€340	€220	€120
Large	€180	€65	€116
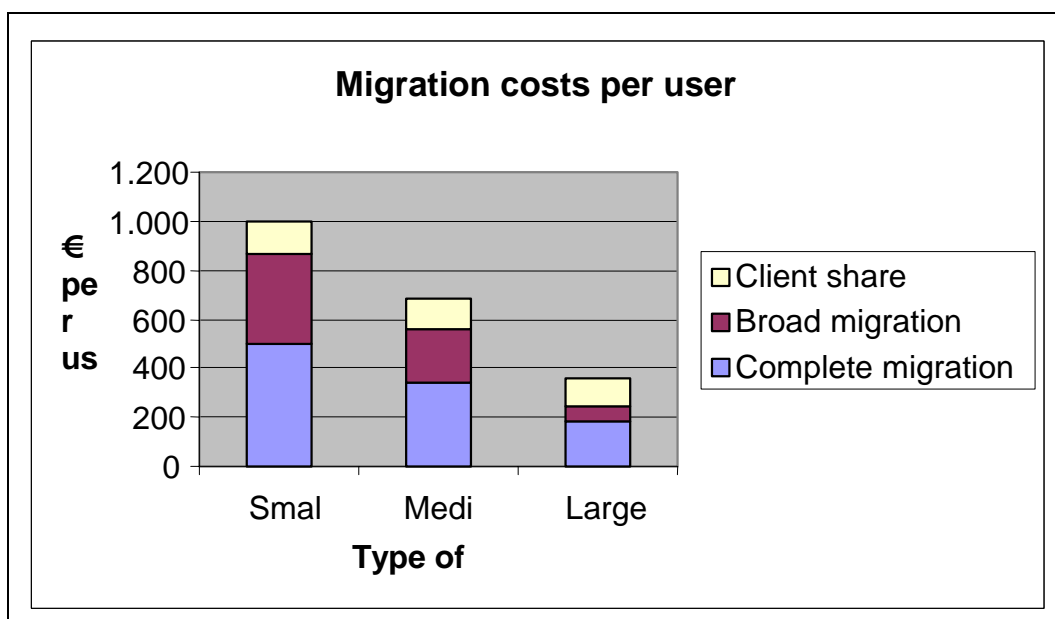
Fig. 55: Migration costs per user

---

[176] The total migration costs include all expenditures related to the migrated systems for the five-year period analyzed. All figures are approximate values.

[177] All figures are approximate values.

The cost development in the case of broad migration confirms the trend of decreasing costs with increasing organization size already identified.

Compared to complete migration, the share of change costs at the client end is relatively constant.

4.7 Conclusions

A comparison of economic aspects of the different types of migration shows clear advantages of partial migration at the server end. If a public agency decides to generally migrate its systems to Open Source, this approach is recommended from a commercial perspective. Broad migration at the server end (as a variant and/or precursor stage of complete migration) pays special tribute to a public agency's interests at the client end and thereby contributes towards more efficient and more sustainable implementation of the new IT platform.

If a public agency decides to retain its Microsoft-oriented systems, continuing migration is the appropriate procedure.

The methods of complete and selective migration are less-than-optimum approaches from an economic perspective. In the case of specific requirements and/or decisions in a public agency, these methods can nevertheless turn out to be the better approach[178].

4.8 Expenditures with different migration scenarios

4.8.1 General assumptions concerning migration expenditures

The total costs of the migration scenarios discussed here are generally made up of the following components:

- ❍ Hardware costs
- ❍ Software costs
- ❍ Personnel costs

This chapter discusses potential bandwidths for personnel expenditure. The hardware aspect will be disregarded[179], with the software costs being included in the respective examples[180].

In this migration guide, any estimate of expenditure is inevitably a rough estimate only, because neither the starting situation nor the desired target scenario are (can be) known exactly. This is why three different migration scenarios will serve as examples. The three scenarios are categorized in accordance with the

---

[178] Cases are, for example, conceivable in which migration of certain special applications is not possible, thereby forcing a public agency to retain its Microsoft systems. In other cases, server and client conditions may call for a complete change.

[179] Refer to the chapter on "Migration recommendations ..."

[180] Refer to the chapter on "Recommended assessments" and following chapters

examples of public agencies[181] already described here. These three environments will be roughly outlined in the following.

The following assumptions are applicable to all the environments:

❍ The change of the servers is accompanied by a replacement of hardware (new server hardware).

❍ The workstation computers are Windows NT 4 devices throughout (so that no group guidelines need to be designed for the workstation computers).

❍ The legacy environment is in a "good" condition and the primary purpose of introducing Windows 2000 is not to get rid of historical burdens. This primarily implies that so-called "in-place migration" (updating an existing NT domain) is not rejected.

❍ Consistent technical systems management is in place with products which are also suitable for Windows 2000.

❍ A documented operating concept exists which can be updated.

❍ The environments are completely administered by a sovereign organization which mainly acts as a central organization.

❍ Friction losses due to internal and political inconsistency and limited funds are minimal.

Furthermore, the following boundary conditions must be considered:

❍ A change of workstation computers to Windows 2000/XP is not discussed in this document.

❍ A change of Windows Terminal Services is not discussed either.

❍ A change or introduction of DFS does not have to be considered.

❍ A change of application servers, such as MS Exchange, MS SQL, MS SNA Server, MS Proxy or applications from third-party manufacturers or clustered NT servers (Enterprise Edition) with external storage units (harddisk subsystems or SAN) is not considered.

The model studied consists of six phases and can be briefly outlined in key words as follows.

❍ **Workshop** (kick-off, involving specialist departments and IT disciplines concerned, identifying any relevant issues, setting priorities, identifying decision-making needs, determining approach and project plan, detailed estimate of expenditures, defining sub-projects and setting up workgroups)

---

[181] Small, medium and large public agency

Evaluation of economic efficiency

○ **Stock-taking** (application landscape, communication lines, network infrastructure, central services, operating procedures, future requirements)

○ **General concept** (preparing performance specifications, refining the project plan and defining work packages, technical feasibility, implementation of an integration and test environment, description of the remaining production environment, application integration, hardware selection and evaluation)

○ **Detailed concept** (detailed definition of the range of functions, integration into the remaining IT environment, development of installation procedures and software distribution, integration into operations, rollout planning, pilot planning, training of IT personnel)

○ **Pilot** (feature stop, supplying a representative user group, load tests, integration of the UHD (user help desk), first sizing check, feedback to detailed concept)

○ **Rollout** (setting the installation procedures into operation, duplicating the server systems, user information and training, support by the project team, transition to regular operation)

Project management is additionally required.

4.8.2 Costs of migration from Windows NT to Windows 2000

The expenditure necessary for migration from Windows NT 4 to Windows 2000 on the basis of the following specifications is analyzed in the following.

○ Logon services

○ Network services

○ File services

○ Print services

Migration to Windows 2000[182] including the active directory can, just like other migration projects, be divided into different phases which contain different work packages. The table below describes the scenarios considered in key words.

Table 51: Description of scenarios for migration from Windows NT to Windows 2000

Category	Number of users	Starting situation	Target scenario
Small	Up to 250	One NT domain with 2 DCs which additionally provide WINS, DNS and DHCP One site Two file servers	One Windows 2000 domain One site Two file servers Two print servers

---

[182] The migration from Windows NT to Windows 2000 will be referred to as "continuing migration" in the following.

Category	Number of users	Starting situation	Target scenario
		Two print servers	
Medium	More than 250 and up to 1000	Three NT domains trusting each other, each with user and computer accounts DCs additionally provide WINS, DNS and DHCP Three sites of comparable size (number of users) All three domains, each with two file servers and two print servers	**One** Windows 2000 domain Three sites Furthermore, two file servers and two print servers per site
Large	More than 1000	11 domains with single-master domain model (1 account domain and 10 resource domains) DCs additionally provide WINS, DNS and DHCP 10 sites 10 domains, each with 2 file servers and 2 print servers	**One** Windows 2000 domain Ten sites Furthermore, two file servers and two print servers per site

The target scenarios described for large and medium environments include a consolidation of the number of domains to one.

It is assumed for all three environments that at least one legacy domain is upgraded (in-place upgrade). This assumption can be considered as anticipating the target and migration concept, but also means a simplification of the migration path in that it eliminates additional migration work related to user accounts (key words: cloning, SID history, assigning new privileges (ReACLing)).

The following requirements expressed in man-days (MD) are estimated for the different environments and phases.

Table 52: Man-day requirements in the case of continuing migration

Requirement in MD		Environment			
Phase	**Sub-package**	**Small**	**Medium**	**Large**	**Remarks**
Workshop		5	10	10	Flat share
Stock-taking	Logon network	2	6	22	2 per domain
	File	1	5	21	1 for first domain 2 for every further resource domain (ResDom)
	Print	2	6	20	2 for every ResDom
	Processes	2	4	12	2 for first domain 1 for every further resource domain (ResDom)
	Requirements	1	3	10	1 per site

Evaluation of economic efficiency

Requirement in MD		Environment			
Phase	**Sub-package**	**Small**	**Medium**	**Large**	**Remarks**
General concept	Performance specifications	2	4	6	Flat share
	Project plan	1	3	10	1 per site
	Setup of test environment	3	5	7	Flat share: 2 plus additional sites/domains
	Hardware selection	5	5	5	Flat share
Detailed concept	Concept of active directory (including network services)	5	8	15	5 for single target domain plus 1 per site
	File concept	1	11	51	1 for target domain plus 5 per additional ResDom
	Print concept	3	5	13	Flat share: 3 plus 1 per additional ResDom
	Installation method	3	3	3	Flat share
	Migration method	3	13	13	3, flat share plus complexity factor
	Systems management (backup, virus protection, disaster recovery, monitoring)	4	8	8	4 for central 4 for distributed
	Operating concept	10	20	40	Flat share
	Planning	2	6	20	2 per site
Pilot		10	25	25	10 central 15 distributed
Rollout		5	25	105	5 for first target domain 10 for ResDom
Total		**70**	**175**	**416**	

An additional flat share of another ten percent must be considered for project management.

The estimated expenditures shown here should be interpreted as the lower limits. Substantial time requirements can be defined for each of the sub-packages if the requirements specifications are laid down and amended accordingly. One

example to be mentioned in this context is the preparation and/or updating of an operating concept.

The estimated man-days concern both internal and external inputs. In the case of the Windows migration described here, the ratio is in the order of around 20% internal and around 80% external inputs.

4.8.3 Expenditure on migration from Windows NT to Linux

The table below describes the scenarios considered in key words[183].

Table 53: Description of the scenario for migration from Windows NT to Linux

Cat.	Number of users	Starting situation	Target scenario 1	Target scenario 2
Small	Up to 250	One NT domain with 2 DCs which additionally provide WINS, DNS and DHCP One site Two file servers Two print servers	One Windows 2000 domain One site Two file servers Two print servers	One Samba domain One site Two file servers Two print servers
Medium	More than 250 and up to 1000	Three NT domains trusting each other, each with user and computer accounts DCs additionally provide WINS, DNS and DHCP Three sites of comparable size (number of users) All three domains, each with two file servers and two print servers	**One** Windows 2000 domain Three sites Furthermore, two file servers and two print servers per site	**One** Samba/LDAP domain Three sites Furthermore, two file servers and two print servers per site
Large	More than 1000	11 domains with single-master domain model (1 account domain and 10 resource domains) DCs additionally provide WINS, DNS and DHCP 10 sites 10 domains, each with 2 file servers and 2 print servers	**One** Windows 2000 domain Ten sites Furthermore, two file servers and two print servers per site	**One** Samba/LDAP domain Ten sites Furthermore, two file servers and two print servers per site

The target scenarios described for large and medium environments include a consolidation of the number of domains to one.

---

[183] This form of migration will be referred to as "replacing migration" in the following.

Evaluation of economic efficiency

It is assumed for all three environments that at least one legacy domain is upgraded (in-place upgrade). This assumption can be considered as anticipating the target and migration concept, but also means a simplification of the migration path in that it eliminates additional migration work related to user accounts (key words: cloning, SID history, assigning new privileges (ReACLing)).

The following requirements expressed in man-days (MD) are estimated for the different environments and phases.

Table 54: Man-day requirement for replacing migration

Requirement in MD		Environment			
Phase	Sub-package	Small	Medium	Large	Remarks
Workshop		5	10	10	Flat share
Stock-taking	Logon network	2	6	22	2 per domain
	File	1	5	21	1 for first domain 2 for every further resource domain (ResDom)
	Print	2	6	20	2 for every ResDom
	Processes	2	4	12	2 for first domain 1 for every further resource domain (ResDom)
	Requirements	1	3	10	1 per site
General concept	Performance specifications	2	4	6	Flat share
	Project plan	1	3	10	1 per site
	Setup of test environment	3	5	7	Flat share: 2 plus additional sites/domains
	Hardware selection	5	5	5	Flat share
Detailed concept	Concept of OpenLDAP Directory (including network services)	4	7	14	4 for single target domain plus 1 per site
	File concept	1	11	51	1 for target domain plus 5 per additional ResDom
	Print concept	3	5	13	Flat share: 3 plus 1 per additional ResDom
	Installation method	3	3	3	Flat share
	Migration method	3	13	13	3, flat share plus complexity factor (Although the processes

Requirement in MD		Environment			
Phase	Sub-package	Small	Medium	Large	Remarks
					are in this case less standardized than in the case of continuing migration, only relatively limited additional inputs should be expected with regard to the detailed concept).
	Systems management (backup, virus protection, disaster recovery, monitoring)	6	9	9	6 for central 3 for distributed (Legacy solutions must be partially replaced. Many of the legacy systems can be used with OSS as well.)
	Operating concept	15	25	50	Flat share (Additional requirements must be expected here in the case of OSS migration. However, OSS migration does not mean a new development of the operating concept.)
	Planning	2	6	20	2 per site
Pilot		15	30	30	20 central 30 distributed (In the case of OSS migration, increased efforts for integrating the components and a certain share of individual development work should be expected.)
Rollout		10	35	125	5 for first target domain 10 for ResDom 5/10/20 for uncertainty (Once everything is planned and tested, rollout costs and efforts are not significantly higher. However, the uncertainty factor is larger and the error tolerance is smaller compared to continuing migration.)
Total		86	195	451	

An additional flat share of another ten percent must be considered for project management with both scenarios.

Evaluation of economic efficiency

The estimated expenditures shown here should be interpreted as the lower limits. Substantial time requirements can be defined for each of the sub-packages if the requirements specifications are laid down and expanded accordingly. One example to be mentioned in this context is the preparation and/or updating of an operating concept, where requirements can be almost unlimited.

4.8.4 Expenditure on migration from Exchange 5.5 to Exchange 2000

The expenditure necessary for migration from Microsoft Exchange 5.5 to Exchange 2000 is estimated in the following.

The following requirements expressed in man-days (MD) are estimated for the different environments and phases of the migration project.

Table 55: Man-day requirements for migration from Exchange 5.5 to Exchange2000

Requirement in MD		Environment			
Phase	**Sub-package**	**Small**	**Medium**	**Large**	**Remarks**
Workshop		2	3	3	Flat share
Stock-taking	Logon and network	1	1	1	Flat share
	Exchange environment	2	3	6	1 for organization 1 per 2 Exchange server
	Processes	2	4	4	Flat share
	Requirements	1	3	3	Flat share
General concept	Performance specifications	2	4	4	Flat share
	Project plan	1	3	3	1 central 2 distributed
	Setup of test environment	3	5	7	Flat share of 2 plus additional sites/ domains
	Hardware selection	5	5	5	Flat share to be doubled in the case of clustering
Detailed concept	Exchange concept	5	10	10	5 central 5 distributed
	Server design	5	5	5	Flat share
	ADC tests	5	10	10	5 flat share plus complexity factor
	Installation method	3	3	3	Flat share
	Migration method	2	12	12	2 flat share plus complexity factor
	Systems management	5	10	10	5 for central 5 for distributed

Requirement in MD		Environment			
Phase	Sub-package	Small	Medium	Large	Remarks
	(backup, virus protection, disaster recovery, monitoring)				
	Operating concept	10	15	25	Flat share
	Planning	2	6	20	2 per site
Pilot		5	10	10	5 central 5 distributed
Rollout		3	9	30	3 per Exchange server
Total		**64**	**121**	**171**	

An additional flat share of another ten percent must be considered for project management.

The estimated man-days concern both internal and external inputs. In the case of the Exchange migration described here, the ratio is in the order of around 25% internal and around 75% external inputs.

4.8.5 Expenditure on migration from Exchange 5.5 to Samsung Contact

The expenditure necessary for migration from Microsoft Exchange 5.5 to Samsung Contact is estimated in the following.

The following assumptions are applicable to all environments (on a Samsung Contact basis).

All the Samsung Contact servers are based on Linux or UNIX OS systems.

Consolidation of multiple MS Exchange servers is possible.

The number of users is solely dependent on CPU performance. There are no mailbox restrictions, and the message store can have a capacity of up to several terabytes.

Migration to ADS is not necessary.

The system is not resource-critical, so that the existing hardware can be reused after migration (Linux).

Migration of public folders, calendar and contacts is possible.

Table 56: Man-day requirements for migration from Exchange 5.5 to Samsung Contact

Requirement in MD	Environment	

Evaluation of economic efficiency

Phase	Sub-package	Small	Medium	Large	Remarks
Workshop					
Stock-taking	Logon and network	0.2	0.2	0.2	
	Exchange environment	0.2	0.5	1	
	Processes	0.2	0.5	1	
	Requirements	0.2	0.5	1	
General concept	Performance specifications	1	2	3	
	Project plan	0.5	1	1	
	Setup of test environment	1	2	5	
	Hardware selection	0.3	0.3	0.5	
Detailed concept	Contact concept	0.5	1	2	
	Server design				
	ADC tests	0.5	0.5	1	
	Installation method	0.5	0.5	1	
	Migration method	0.2	0.3	1	
	Systems management (backup, virus protection, disaster recovery, monitoring)	1	1	2	
	Operating concept	1	2	2	
	Planning	0.5	0.5	1	
Pilot		1	2	5	
Rollout		2	3	7	
Total		**10.8**	**17.8**	**34.7**	

4.8.6 Recommended assessments concerning products / product groups

4.8.6.1 General assumptions

❍ Solely the cost/benefit drivers are considered in the calculations of the example scenarios of migration objects, i.e.:

- Hardware costs

- Software costs

- Data import costs (= personnel costs)

❍ Against this background, any other cost types existing besides the above-mentioned cost types are considered to be neutral, i.e.

- Compatibility costs

- Training costs

- Administration costs

❍ Migration projects typically offer minor intrinsic savings potentials (software costs) only. The economic efficiency of a project is thus only seldom based on this factor. Since migration projects generally focus on the decision whether to migrate within Microsoft or to an OSS platform, a "cross analysis" will be carried out in the following examples. For this purpose, the comparable differential costs of Microsoft-internal migration which are not needed are considered as savings within the scope of the analysis of a migration to OSS.

❍ An average daily rate of €1,000.00 is assumed for external personnel costs.

❍ The information for supreme federal authorities[184] will be used here as a basis for assessing personnel costs. The cost estimate is based on salary grade IVa (supreme federal agencies, €36.98 per hour, 462 minutes per day).

❍ The personnel costs stated in the examples for large, medium and small public agencies are distributed to external and internal resources at a ratio of 80 to 20.

❍ The interest rate specified by the Federal Ministry of Finance (BMF)[185] (at present 6%) is used for discounting future savings.

❍ The software licenses for public agencies cost around 50% of the normal list prices[186]. These terms and conditions are granted by suppliers almost throughout.

The following examples are presented in two different structures in order to illustrate the different options described for an evaluation of economic efficiency in practical applications. These two different structures are:

❍ Structure according to WiBe21 on the basis of the defined catalogs of criteria

❍ Structure of IT cost categories on the basis of the three major cost factors, i.e. hardware, software and manpower, according to the migration cost matrix.

4.8.6.2 Examples according to the WiBe21 structure

Migration example: server infrastructure – small public agency

---

[184] Refer to "Personalkostensätze für Kostenberechnungen/ Wirtschaftlichkeitsberechnungen" by the Federal Ministry of Finance dated October 29, 2002.

[185] Refer to "Personalkostensätze ... " by the Federal Ministry of Finance dated October 29, 2002.

[186] Different prices are used in the calculations in individual cases if such different prices reflect the real situation of a particular public agency better.

Evaluation of economic efficiency

Table 57: Migration example: server infrastructure – small public agency

Migration object:	Migration from Microsoft Windows NT to the OSS environment on Linux – servers and clients
Scenario:	Small public agency, 250 users
Success factors:	Software costs, change costs
Assumptions:	Cost/benefit drivers are the following three criteria: ● License costs ● Change costs ● Training costs Against this background, any other cost types existing besides the above-mentioned cost types are considered to be neutral, i.e. no cost/benefit drivers other than those mentioned above are considered in the model calculation. The example considers the difference in the costs with a change from MS Windows NT to Linux which are not incurred as savings. This concerns both software licenses and change costs. Software licenses: The Windows license, as the difference with the free Linux system, is considered as savings. Change costs: The difference between the man-day requirements for MS-internal migration and migration to Linux is valued with the average external personnel rate of €1,000.00 and is calculated as savings. Internally saved man-days are valued using the rates specified by the Federal Ministry of Finance (BMF). Training costs for users are assumed to be almost identical for both platforms (Windows 2000 and Linux), and are hence assumed to be negligible. Administrator training is planned for 2 administrators, each of whom with 5 days (altogether around €2,000.00, including value-added tax). The ratio between external and internal expenditures is assumed as 80% (external) to 20% (internal).
Break-even	The project already breaks even during the first year.

Table 58: WiBe example 1, server infrastructure [Windows NT / Linux], small public agency

Criterion (costs/savings) Values in euro Year 1 = 2001		Quantity unit	Qty.	Year 1	Total benefit	Total cash (calc.int. =6%)
Number of years studied			5			
Calculated interest = 6%			6%			
Quantities (small agency)						
- Number of		Users	250			
1. Introduction costs/benefits						
1.1.2.2.1 Software acquisition (once-off or annual licenses)					4,500	4,245
> Windows 2000		Savings				
- of which budget-relevant (br)		Basis	1	435.00	0	0
- of which budget-relevant (br)		per user	250	18.00	4,500	4,245
- of which non-budget-relevant (nbr)					0	0
> Linux		Costs				
- of which budget-relevant (br)		per user	250	0.00	0	0
- of which non-budget-relevant (nbr)					0	0
1.1.3.3 Import of data stocks				2,569.49	0	0
> Windows 2000 migration savings		Savings				
- of which budget-relevant (br)		MD	28	1,000.00	28,000	26,415
- of which non-budget-relevant (nbr)			7	284.75	1,993	1,880
> Linux migration costs		Costs				
- of which budget-relevant (br)		MD	28	1,000.00	-28,000	-26,415
- of which non-budget-relevant (nbr)			7	284.75	-1,993	-1,880
1.1.3.4 Initial training for users and IT specialists				2,000.00	-4,000	-3,774
Cost/benefit balance					500	
Not present value cost/benefits for 5 year(s) **- Break-even after 1 year**						472
br					500	472
nbr					0	0

The above WiBe example shows a positive net present value on condition that the external change support does not exceed 28 man-days and the necessary internal support 7 man-days.

Migration example: server infrastructure – medium public agency

Table 59: Migration example: server infrastructure – medium public agency

Migration object:	**Migration from Microsoft Windows NT to the OSS environment on Linux – servers and clients**
Scenario:	Medium public agency, 1,000 users
Success factors:	Software costs, change costs
Assumptions:	Cost/benefit drivers are the following three criteria: • License costs • Change costs • Training costs Against this background, any other cost types existing besides

	the above-mentioned cost types are considered to be neutral, i.e. no cost/benefit drivers other than those mentioned above are considered in the model calculation.
	The example considers the difference with the costs of a change from MS Windows NT to Linux which are not incurred as savings. This concerns both software licenses and change costs.
	Software licenses:
	The Windows license, as the difference with free Linux system, is considered as savings.
	Change costs:
	The difference between the man-day requirements for MS-internal migration and migration to Linux is valued with the average external personnel rate of €1,000.00 and is calculated as savings.
	Internally saved man-days are valued using the rates specified by the Federal Ministry of Finance (BMF).
	Training costs for users are assumed to be almost identical for both platforms (Windows 2000 and Linux), and are hence assumed to be negligible.
	Administrator training is planned for 2 administrators, each of whom with 5 days (altogether around €2,000.00, including value-added tax).
	The ratio between external and internal expenditures is assumed as 80% (external) to 20% (internal).
Break-even	The project already breaks even during the first year.

Table 60: WiBe example – server infrastructure [Windows NT / Linux], medium public agency

Server infrastructure [Windows NT -> Linux] - medium agency

Criterion (costs/savings)) Values in euro Year 1 = 2001	Quantity unit	Qty.	Year 1	Total benefit	Total cash values (calc.int. =6%)
Number of years studied Calculated interest = 6% Quantities (medium agency)		5 6%			
- Number of	User	1,000			
1. Introduction costs/benefits					
1.1.2.2.1 Software acquisition (once-off or annual licenses)				18,000	16,981
> Windows 2000	Savings				
- of which budget-relevant (br)	Basis	1	435.00	0	0
- of which budget-relevant (br)	per user	1,000	18.00	18,000	16,981
- of which non-budget-relevant (nbr)				0	0
> Linux	Kosten				
- of which budget-relevant (br)	per user	1,000	0,00	0	0
- of which non-budget-relevant (nbr)				0	0
1.1.3.3 Import of data stocks			2,569.49	-12,854	-12,127
> Winows 2000 migration savings	Savings				
- of which budget-relevant (br)	MD	64	1,000.00	64,000	60,377
- of which non-budget-relevant (nbr)		16	284.75	4,556	4,298
> Linux migration costs	Savings				
- of which budget-relevant (br)	MD	76	1,000.00	-76,000	-71,698
- of which non-budget-relevant (nbr)		19	284.75	-5,410	-5,104
1.1.3.4 Initial training for users and IT specialists			2,000.00	-4,000	-3,774
Cost/benefit balance				1,146	
Net present value costs/benefits for 5 year(s) - Break-even after 1 year(s)					1,081
br				**2,000**	**1,887**
nbr				**-854**	**-806**

The above WiBe example shows a positive net present value on condition that the external change support does not exceed 76 man-days and the necessary internal support 19 man-days.

Migration example: server infrastructure – large public agency

Table 61: Migration example: server infrastructure – large public agency

Migration object:	Migration from Microsoft Windows NT to the OSS environment on Linux – servers and clients
Scenario:	Large public agency, 10,000 users
Success factors:	Software costs, change costs
Assumptions:	Cost/benefit drivers are the following three criteria: • License costs • Change costs • Training costs Against this background, any other cost types existing besides

Evaluation of economic efficiency

	the above-mentioned cost types are considered to be neutral, i.e. no cost/benefit drivers other than those mentioned above are considered in the model calculation. The example considers the difference with the costs of a change from MS Windows NT to Linux which are not incurred as savings. This concerns both software licenses and change costs. Software licenses: The Windows license, as the difference with the free Linux system, is considered as savings. Change costs: The difference between the man-day requirements for MS-internal migration and migration to Linux is valued with the average external personnel rate of €1,000.00 and is calculated as savings. Internally saved man-days are valued using the rates specified by the Federal Ministry of Finance (BMF). Training costs for users are assumed to be almost identical for both platforms (Windows 2000 and Linux), and are hence assumed to be negligible. Administrator training is planned for 2 administrators, each of whom with 5 days (altogether around €2,000.00, including value-added tax). The ratio between external and internal expenditures is assumed as 80% (external) to 20% (internal).
Break-even	The project already breaks even during the first year.

Table 62: WiBe example – server infrastructure [Windows NT / Linux], large public agency

Server infrastructure [Windows NT -> Linux] - large agency

Criterion (costs/savings) Values in euro Year 1 = 2001	Quantity unit	Qty.	Year 1	Total benefit	Total cash values (calc.int. =6%)
Number of years studied Calculated interest = 6% Quantities (large agency)		5 6%			
- Number of users	User	10,000			
1. Introduction costs/benefits					
1.1.2.2.1 Software acquisition (once-off or annual licenses)				180,000	169,811
> Windows 2000	Savings				
- of which budget-relevant (br)	Basis	1	435.00	0	0
- of which budget-relevant (br)	per user	10,000	18.00	180,000	169,811
- of which non-budget-relevant (nbr)				0	0
> Linux	Costs				
- of which budget-relevant (br)	per user	10,000	0.00	0	0
- of which non-budget-relevant (nbr)				0	0
1.1.3.3 Import of data stocks			2,569.49	-174,818	-164,922
> Umstellungsersparnis Windows 2000	Savings				
- of which budget-relevant (br)	MD	84.8	1,000.00	84,800	80,000
- of which non-budget-relevant (nbr)		21.2	284.75	6,037	5,695
> Linux migration costs	Costs				
- of which budget-relevant (br)	MD	248	1,000.00	-248,000	-233,962
- of which non-budget-relevant (nbr)		62	284.75	-17,654	-16,655
1.1.3.4 Initial training for users and IT specialists			2,000.00	-4,000	-3,774
Cost/benefit balance				1,182	
Net present value costs/benefits for 5 year(s) **- Break-even after 1 year(s)**					1,115
br				**12,800**	**12,075**
nbr				**-11,618**	**-10,960**

The above WiBe example shows a positive net present value on condition that the external change support does not exceed 248 man-days and the necessary internal support 62 man-days. With 66 days of external support, a net present value which is not yet budget-relevant is achieved.

Migration example: Office / client desktop

Table 63: Migration examples: Office / client desktop

Migration object:	**Migration from Microsoft Office to the OSS environment on Open Office – servers and clients**
Scenarios:	Small public agency up to 250 users Medium public agency up to 1,000 users Large public agency more than 1,000 users
Success factors:	Software costs, change costs
Assumptions:	At the time of migration to OpenOffice, the Linux operating system is available on servers and clients. Cost/benefit drivers are the following three criteria:

	• License costs • Change costs • Training costs Against this background, any other cost types existing besides the above-mentioned cost types are considered to be neutral, i.e. no cost/benefit drivers other than those mentioned above are considered in the model calculation. In the example, the Microsoft Office license, as the difference with the Open Office, is considered as savings. Training costs for users are assumed to be almost identical for both platforms (Windows 2000 and Linux), and are hence assumed to be negligible. Administrator training is planned for 2 administrators, each of whom with 5 days (altogether around €2,000.00, including value-added tax). The examples calculated here are based on the following quantitative assumptions[187]: • Number of documents per user 13 • Number of macros per user 0.07 • Change time per document 0.2 h • Change time per macro • Small public agency 0.91 h • Medium public agency 5.54 h • Large public agency 6.94 h
Break-even	The project already breaks even during the first year for all categories of public agencies.

The following examples were, amongst other things, calculated with the intention to identify an upper limit for the time required for the migration of macros. The times stated in the assumptions represent the respective upper limits. Up to this value, no negative net present value will occur under c.p.[188] conditions.

Furthermore, this analysis provides an overview of the expenditure in the case of Microsoft-internal migration. This expenditure is considered as savings, and is stated in the "net present value, br" (br = budget-relevant).

The costs of migration to Open Office are largely not budget-relevant because this migration is carried out by own personnel.

However, the costs of external support must in any case be added to the expenditure considered here. These costs of external support can be budgeted at almost identical levels for both migration paths.

---

[187] Identifal for all types of public agency

[188] c.p. = ceteris paribus; i.e. "all other conditions left unchanged". This means that all the other general parameters and their correlations were left unchanged in these different examples.

Table 64: WiBe example – Office / client desktop [MS Office / Open Office], small public agency

Criterion (costs/savings) Values in euro Year 1 = 2001	Quantities	Quantity unit	Qty.	Explanation		Year 1	absolut	Total benefit	discounte	Total cash values (Calc.int.. =6%)
Number of years studied			5							
Calculated interest = 6%			6%							
Quantities (small agency)										
- Number of user		User	250	Total						
- Number of documents per user		Documents	13.00	3,250						
- Number of macros per user		Documents	0.07	18						
- Change time per document		Hours	0.20	650.0						
- Change time per macro		Hours	0.91	15.9						
1. Introduction costs/benefits										
1.1.2.2.1 Software acquisition								28,625		27,005
> Office 2000		Savings								
- of which budget-relevant (br)		Basis	1			241.00		0		0
- of which budget-relevant (br)		per user	250			114.50		28,625		27.005
- of which non-budget-relevant (nbr)								0		0
> Open Office		Costs								
- of which budget-relevant (br)		per user	250			0,00		0		0
- of which non-budget-relevant (nbr)								0		0
1.1.3.3 Import of data stocks						1,321.73		-24,625		-23,231
> Open Office migration costs										
- of which budget-relevant (br)		Hours		Hours				0		0
- of which non-budget-relevant (nbr)			665.9			36.98		-24,625		-23,231
1.1.3.4 Initial training for IT specialists						2,000.00		-4,000		-3,774
> Open Office										
- of which budget-relevant (br)		Training	2 per admin 1 week			2,000.00		-4,000		-3,774
- of which non-budget-relevant (nbr)								0		0
Cost/benefit balance								0		
Net present value costs/benefits for 5 year(s)										0
- Break-even after 1 year										
br								24.,625		23,231
nbr								-24,625		-23,231

Evaluation of economic efficiency

Table 65: WiBe example – Office / client desktop [MS Office / Open Office], medium public agency

Office / client desktop [Microsoft Office -> Open Office] - medium agency

Criterion (costs/ savings) Values in euro Year 1 = 2001	Quantity unit	Qty.	Explanation	Year 1	Total benefit	Total cash values (Calc.int. =6%)
Number of years studied Calculated interest = 6%		5 6%				
Quantities (medium agency)						
- Number of	User	1,000	Total			
- Number of documents per user	Documents	13.00	13.000			
- Number of macros per user	Documents	0.07	70			
- Migration time per document	Hours	0.20	2,600.0			
- Migration time per macro	Hours	5.54	388.1			
1. Introduction costs/benefits						
1.1.2.2.1 Software acquisition **(once-off or annual licenses)**					114,500	108,019
> Office 2000	Savings					
- of which budget-relevant (br)	Basis	1		241.00	0	0
- of which budget-relevant (br)	per user	1,000		114.50	114.500	108.019
- of which non-budget-relevant (nbr)					0	0
> Open Office	Costs					
- of which budget-relevant (br)	per user	1,000		0,00	0	0
- of which non-budget-relevant (nbr)					0	0
1.1.3.3 Import of data stocks				1,321.73	-110,500	-104,245
> Open Office migration costs						
- of which budget-relevant (br)	Hours		Hours		0	0
- of which non-budget-relevant (nbr)		2988.1		36.98	-110,500	-104,245
1.1.3.4 Initial training for IT specialists				2,000.00	-4,000	-3,774
> Open Office						
- of which budget-relevant (br)	Training	2	per admin 1 week	2,000.00	-4,000	-3,774
- of which budget-relevant (br)					0	0
Cost/benefit balance					0	
Net present value costs/benefits for 5 year(s)						0
- Break-even after 1 year						
br					**110,500**	**104,245**
nbr					**-110,500**	**-104,245**

Table 66: WiBe example – Office / client desktop [MS Office / Open Office], large public agency

Office / client desktop [Microsoft Office -> Open Office] - large agency

Criterion (costs/savings) Values in euro Year 1 = 2001	Quantity unit	Qty.	Explanation	Price	Year	absolut	Total benefit	disconte	Total cash value (calc.int. =6
Number of years studied		5							
Calculated interest = 6%		6%							
Quantities (large agency)									
- Number of	User	10,000	Total						
- Number of documents per user	Documents	13.00	130,000						
- Number of macros per user	Documents	0.07	700						
- Migration time per document	Hours	0.20	26,000.0						
- Migration time per macro	Hours	6.94	4,854.5						
1. Introduction costs/benefits									
1.1.2.2.1 Software acquisition							1,145,000		1,080,18
(once-off or annual licenses)									
> Office 2000	Savings								
- of which budget-relevant (br)	Basis	1		241.00			0		
- of which budget-relevant (br)	per user	10,000		114.50			1,145,000		1,080,18
- of which non-budget-relevant (nbr)							0		
> Open Office	Costs								
- of which budget-relevant (br)	per user	10,000		0.00			0		
- of which non-budget-relevant (nbr)							0		
1.1.3.3 Import of data stocks				1,321.73			-1,141,000		-1,076,41
> Open Office migration costs									
- of which budget-relevant (br)	Hours		Hours				0		
- of which non-budget-relevant (nbr)		30,855		36.98			-1,141,000		-1,076,41
1.1.3.4 Initial training of IT specialists				2,000.00			-4,000		-3,77
> Open Office									
- of which budget-relevant (br)	Training	2 per admin 1 week		2,000.00			-4,000		-3,77
- of which non-budget-relevant (nbr)							0		
Cost/benefit balance							0		
Net present value costs/benefits for 5 year(s)								0	
- Break-even after 1 year(s)									
br							**1,141,000**		**1,076,41**
nbr							**-1,141,000**		**-1,076,41**

Migration example: from Windows/ Microsoft Office to Linux/ Open Office

Table 67: Migration example: from Windows/ Microsoft Office to Linux/ Open Office

Migration object:	Migration of Microsoft Office, including Windows, to the OSS environment with Linux/ Open Office
Scenario:	Medium public agency, 500 users
Critical success factors:	Migration of existing data - Documents and macros
Assumptions:	Cost/benefit drivers are the following two criteria: • License costs • Change costs Against this background, any other cost types existing besides the above-mentioned cost types are considered to be neutral, i.e. no cost/benefit drivers other than those mentioned above are considered in the model calculation. The objects to be migrated are distinguished in terms of documents and macros. Change times for documents are usually short. Macros require strongly varying migration times depending on the complexity of the macro in

	question.
	The medium price level (level 2 of 3) of the skeleton agreement between Microsoft and the Federal Ministry of the Interior is assumed for the purpose of assessing the costs related to the Microsoft applications. Payment is not effected immediately in one sum, so that no discount is considered.
	35 complex macros to be migrated are considered for the entire public agency[189].
Bandwidth (threshold values) of the critical success factors:	
Break even after 3 years:	Given a maximum number of around 6,500 documents to be migrated and 500 users (corresponding to around 13 documents per user) as well as 35 macros for the entire public agency, break even is possible after 3 years.
Break even after 5 years:	Given a maximum number of around 12,500 documents to be migrated and 500 users (corresponding to around 25 documents per user) as well as 35 macros for the entire public agency, break even is possible after 5 years.

Table 68: WiBe example – Windows / Office to Linux / OpenOffice; break even after 3 years

Criterion (costs/savings) Values in Yearr 1 =	Qu ant itie	Quantity unit	Qty.	Supplem	Pr ce	ab s s val	Total benefi	Total		Net pre se	Total cash
Number of years			3								
Discount factor =			6					of			
Quantitie											
-Number		User	500.0								
- Number of		Document	13.0	Total=6500							
- Number of		Document	0.0	Total=35							
- Migration time per		Hours	0.4								
- Migration time per		Hours	40.0								
- Price for Windows + Office		Euro	116.0								
		%	8.00								
								br	nbr		
1. Introduction											
1.1.2.2.1 Software (once-off or annual							160,08	160,08	0		142,63
1.1.3.3 Import of data stocks							-	0	-		-
Costs/benefits							12,16	**160,08**	-		
Net present value cost/benefits - **Break-even after 3**											**3.08** -

[189] Refer to further quantity and price assumptions in the example calculated after the break-even discussion.

This project breaks even after three years. Office and the Windows environment are migrated to Open Office, including Linux environment. 6,500 documents are migrated.

No costs are incurred for the Open Source software. Annual license fees of around €160,000 payable to Microsoft are saved. This value is considered as savings in the recommendations on economic efficiency assessment (WiBe) and is budget-relevant.

Migration is carried out by own personnel, so that the costs of around €148,000 are not budget-relevant.

The net present value method is applied to discount the amounts to today's date, so that savings now total around €142,000 over the three years (Microsoft license fees no longer payable). Parallel to this, discounting of the migration costs for one year corresponds to an amount of around €139,000. The net present value hence amounts to €3,085. This project is hence economically efficient.

The risk analysis (probability of the occurrence of savings and migration costs) can be disregarded here because the savings represent the current license fee payments which will be omitted in future. The times required for migration were estimated in the higher rather than lower range in this context.

The best practice applied to the quantities assumed here is Gartner's[190] analysis which was adapted to reflect the interests of public administrations.

Table 69: WiBe example – Windows / Office to Linux / OpenOffice; break even after 5 years

Criterion (costs/savings) Values in Year 1 =	Quantities	Quantity unit	Qty.	Suppleme	Prices	abs val ue	Total benefit	Total		Net pres. val	Total cash
Number of years			5					of			
Discount factor = 6%			6%								
Quantities											
- Number of		Users	500.0								
- Number of documents		Documents	25.00	Total=12500							
- Number of macros		Documents	0.07	Total=35							
- Migration time per		Hours	0.40								
- Migration time per		Hours	40.00								
- Price for Windows + Office license		Euro	116.0								
-		%	8.00%								
								br	nbr		
1. Introduction											
1.1.2.2.1 Software acquisition (once-off or annual							266,80	266,80	0		224,77
1.1.3.3 Import of data stocks							-	0	-		-
Cost/benefit							30,12	266,80	-		
Net present value cost/benefits for 5 - Break-even after 5											1,496

---

[190] Refer to "The Cost and Benefits of Moving to Sun's StarOffice 6.0", July 1, 2002.

Evaluation of economic efficiency

This project breaks even after five years. The following should still be noted with regard to the example of a break-even period of 3 years.

The only differences are that the number of documents to be migrated was increased to 12,500 (corresponding to around 25 documents per user). The monitoring period was increased to 5 years.

The calculation method remains unchanged. A positive net present value of €1,496 is obtained after 5 years.

For the risk analysis and quantities assumed, see above.

Migration example: messaging/ groupware – small public agency

Table 70: Migration example: messaging/ groupware – small public agency

Migration object:	Migration of Microsoft Exchange 5.5 to the OSS environment under Linux on Samsung Contact, servers and clients
Scenario:	Small public agency, 250 users
Success factors:	Software costs, change costs
Assumptions:	Cost/benefit drivers are the following three criteria: ● License costs ● Change costs ● Training costs Against this background, any other cost types existing besides the above-mentioned cost types are considered to be neutral, i.e. no cost/benefit drivers other than those mentioned above are considered in the model calculation. The example considers the difference with the costs of a change from MS Exchange 5.5 to Exchange 2000 which are not incurred as savings. This concerns both software licenses and change costs. Software licenses: The difference between the Contact license and the Exchange license is considered here as savings. Change costs: The difference between the man-day requirements for Samsung and Microsoft is valued with the average external personnel rate of €1,000.00 and is calculated as savings. Training costs for users are assumed to be almost identical for both platforms (Exchange and Contact), and are hence assumed to be negligible. Administrator training is planned for 2 administrators, each of whom with 5 days (altogether around €2,000.00, including value-added tax). The ratio between external and internal expenditures is assumed as 75% (external) to 25% (internal).
Break-even	On the basis of the assumptions made, this project is highly profitable. The project already breaks even in the first year. The most important factor is savings of external support for Microsoft-internal migration. On the basis of a best-case and worst-case analysis within the framework of a positive net

present value, a bandwidth of 5 to 20 days of external support by Samsung for this project example is obtained.

Table 71: WiBe example – messaging/ groupware [Exchange 5.5 to Contact], small public agency

Messaging / groupware [Exchange 5.5 -> Samsung Contact] - small agency

Criterion (costs/savings) Values in euro Year 1 = 2001	Quantity unit	Qty.	Year 1	Total benefit	Total cash values (calc.int. =6%)
Number of years studied		5			
Calculated interest = 6%		6%			
Quantities (small agency)					
- Number of	User	250			
1. Introduction costs/benefits					
1.1.2.2.1 Software acquisition (once-off or annual licenses)				-5,500	-5,189
> Upgrade to Exchange 2000	Savings				
- of which budget-relevant (br)	Basis	1	2,420.00	0	0
- of which budget-relevant (br)	per user	250	12.50	3,125	2,948
- of which non-budget-relevant (nbr)				0	0
> Samsung Contact	Costs				
- of which budget-relevant (br)	per	250	34.50	-8,625	-8,137
- of which non-budget-relevant (nbr)				0	0
1.1.3.3 Import of data stocks			2,569.49	9,708	9,159
> Exchange 2000 migration savings	Savings				
- of which budget-relevant (br)	MD	28	1,000.00	28,000	26,415
- of which non-budget-relevant (nbr)		11	284.75	3,132	2,955
> Samsung Contact migration costs	Costs				
- of which budget-relevant (br)	MD	20	1.000.00	-20,000	-18,868
- of which non-budget-relevant (nbr)		5	284.75	-1,424	-1,343
1.1.3.4 Initial training of users and IT specialists			2,000.00	-4,000	-3,774
Cost/benefit balance				208	
Net present value costs/benefits for 5 year(s) **- Break-even after 1 year(s)**					197
br				-1,500	-1,415
nbr				1,708	1,612

In the above example, the upper threshold value for external support for Contact was determined for small public agencies. This value is in the order of 20 man-days. This means that the net present value (187) is still positive and the project is still profitable. The net present value is higher if less external support is needed.

The risk analysis (probability of the occurrence of savings and migration costs) can be disregarded here because the savings represent license fee payments which will be omitted in future. Furthermore, the times required for migration were estimated in the higher rather than lower range in this context.

Evaluation of economic efficiency

Migration example: messaging/ groupware – medium public agency

Table 72: Migration example: messaging/ groupware – medium public agency

Migration object:	Migration of Microsoft Exchange 5.5 to the OSS environment under Linux on Samsung Contact, servers and clients
Scenario:	Medium public agency, 1,000 users
Success factors:	Software costs, change costs
Assumptions:	Refer to the examples concerning a "small public agency". Furthermore: Extent and costs for administrator training do not change with the number of users – these parameters remain unchanged (around 2 x €2,000.00 including value-added tax).
Break even	On the basis of the assumptions made, this project is highly profitable. The project already breaks even in the first year. The most important factor is savings of external support for Microsoft-internal migration. On the basis of a best-case and worst-case analysis within the framework of a positive net present value, a bandwidth of 10 to 35 days of external support by Samsung for this project example is obtained.

Table 73: WiBe example – messaging/ groupware [Exchange 5.5 to Contact], medium public agency

Messaging / groupware [Exchange 5.5 -> Samsung Contact] - medium agency

Cirterion (costs/savings) Values in euro Year 1 = 2001	Quantity unit	Qty.	Year 1	Total benefit	Total cash values (calc.int. =6%)
Number of years studied Calculated interest = 6% Quantities (medium agency)		5 6%			
- Number of	User	1,000			
1. Introduction costs/benefits					
1.1.2.2.1 Software acquisition **(once-off or annual licenses)**				-20,500	-19,340
> Upgrade to Exchange 2000	Savings				
- of which budget-relevant (br)	Basis	1	2,420.00	0	0
- of which budget-relevant (br)	per user	1,000	12.50	12,500	11,792
- of which non-budget-relevant (nbr)				0	0
> Samsung Contact	Costs				
- of which budget-relevant (br)	per user	1,000	33.00	-33,000	-31,132
- of which non-budget-relevant (nbr)				0	0
1.1.3.3 Import of data stocks			2,569.49	25,669	24,216
> Exchange 2000 migration savings	Savings				
- of which budget-relevant (br)	MD	56.75	1,000.00	56,750	53,538
- of which non-budget-relevant (nbr)		20.25	284.75	5,766	5,440
> Samsung Contact migration costs	Costs				
- of which budget-relevant (br)	MD	34	1,000.00	-34,000	-32,075
- of which non-budget-relevant (nbr)		10	284.75	-2,847	-2,686
1.1.3.4 Initial training for users **and IT specialists**			2,000.00	-4,000	-3,774
Cost/benefit balance				1,169	
Net present value costs/benefits for 5 year(s) **- Break-even after 1 year(s)**					**1,102**
br				**-1,750**	**-1,651**
nbr				**2,919**	**2,753**

In the above example, the upper threshold value for external support for Contact was determined for medium public agencies. This value is in the order of 34 man-days. This means that the total net present value (1,102) is still positive and the project is still profitable.

Assuming the value of external support for Contact at medium public agencies to be in the realistic order of up to 5 days, this then means a relatively large positive net present value which suggests a good profitability of the project.

The risk analysis (probability of the occurrence of savings and migration costs) can be disregarded here because the savings represent license fee payments which will be omitted in future. Furthermore, the times required for migration were estimated in the higher rather than lower range in this context.

4.8.6.3   Migration example: messaging/ groupware – large public agency

Table 74: Migration example: messaging/ groupware – large public agency

Migration object:	Migration of Microsoft Exchange 5.5 to the OSS environment under Linux on Samsung Contact
Scenario:	Large public agency, 10,000 users
Success factors:	Software costs, change costs
Assumptions:	Refer to the examples concerning the "small and medium public agency".
Break even after 1 year:	On the basis of the assumption of a headcount of up to around 6,200, this project turns out to be profitable. The net present value turns negative when the headcount and/or the external support days increase. The savings due to the non-utilization of external support for internal Microsoft migration to be set off are effective up to this headcount only.

Table 75: WiBe example – messaging/ groupware [Exchange 5.5 to Contact], large public agency

Messaging / groupware [Exchange 5.5 -> Samsung Contact] - large agency

Criterion (costs/savings) Values in euro Year 1 = 2001	Quantity unit	Qty.	Year 1	Total benefit	Total cash values (calc.int. =6%)
Number of years studied Calculated interest = 6% Quantities (large agency)		5 6%			
- Number of	User	10,000			
1. Introduction costs/benefits					
1.1.2.2.1 Software acquisition (once-off or annual licenses)				-95,000	-89,623
> Upgrade to Exchange 2000	Savings				
- of which budget-relevant (br)	Basis	1	2,420.00	0	0
- of which budget-relevant (br)	per user	10,000	12.50	125,000	117,925
- of which non-budget-relevant (nbr)				0	0
> Samsung Contact	Costs				
- of which budget-relevant (br)	per user	10,000	22.00	-220,000	-207,547
- of which non-budget-relevant (nbr)				0	0
1.1.3.3 Import of data stocks			2,569.49	99,589	93,952
> Exchange 2000 migration savings	Savings				
- of which budget-relevant (br)	MD	111.25	1,000.00	111,250	104,953
- of which non-budget-relevant (nbr)		30.75	284.75	8,756	8,260
> Samsung Contact migration costs	Costs				
- of which budget-relevant (br)	MD	17	1,000.00	-17,000	-16,038
- of which non-budget-relevant (nbr)		12	284.75	-3,417	-3,224
1.1.3.4 Initial training for users and IT specialists			2,000.00	-4,000	-3,774
Cost/benefit balance				589	
Net present value costs/benefits for 5 year(s) - Break-even after 1 year(s)					556
br				-4,750	-4,481
nbr				5,339	5,037

In the above calculation example, 17 man-days were assumed for external support for Contact. This means savings of around 111 man-days for Microsoft services. The number of users was selected as 10,000. This calculating environment leads to a positive net present value.

4.8.6.4   Migration examples according by IT cost categories

The assumptions made in chapter 4.8.6 are applicable to this case too.

The examples calculated refer to the products shown in the table below.

Evaluation of economic efficiency

Level		Usual current scenari	Recommended future Migration types / products				
			Complete migration		Continuing migratio	Partial	
			larg	medium-	small-medium-	Selective	Broad
Client	Infrastruct	MS-NT WS	**Linux** Distribution Suse,	**Linux** Distribution Suse,	MS 2000		
	Deskto	MS-NT WS	**KDE,**	**KDE,**	MS 2000		
	Office	MS-Office	**Open** Štaroffic ,	**Open** Štaroffic ,	MS Office	**Open** Štaroffic ,	
Server	Infrastructure	MS NT 4.0	**Linux**	**Linux**	MS 2000		**Linux**
	Infrastructure -	MS NT 4.0	**Web server**	**Web server**	MS 2000		**Webserver**
	Infrastructure file	MS NT 4.0	**XFS**	**XFS**	MS 2000		**Samb**
	Infrastructure – print	MS NT 4.0	**CUPS**	**CUPS**	MS 2000		**CUPS,**
	Infrastructure -	MS NT 4.0	**BIND,**	**BIND,**	MS 2000		**BIND,**
	Database mgmt	MS SQL	**SAP** , Oracle,	**SAP DB, MY** **pŏstgreSQ**	MS SQL Server		**SAP DB, MY** **pŏstgreSQ**
	Messaging/	MS 5.5	SamsungConta	SamsungContact **Kroupwar**	MS 2000	SamsungContac Exchange4lin	Samsung Exhange4lin
	Directory	--	Sun	**OpenLDA**	--	Sun One**OpenLDA**

Note: Products **boldface** are available for free.

Fig. 56:   Migration types / products

A comparative analysis of the migration alternatives is carried out in this model on the basis of the given environment. A Microsoft-based platform serves as the starting scenario. Continuing migration is the only variant that does not yield any real savings which might thus be calculated. All the other variants lead to a complete or partial change in platform and hence include expenditures not made which are thus considered as savings compared to continuing migration.

The prices and conditions used in the model calculations lead to a liquidity drain during the first project year. As the calculations are based on purchasing prices, savings thus also occur during the first year only.

4.8.6.5   Complete migration

Complete migration means superprortional savings effects for all types of public agency. In contrast to migration to Windows 2000, migration from Windows NT to Linux generates savings which exceed expenditure many times over.

Large installation

Personnel costs in conjunction with the change were of a comparable size, so that license cost savings account for most of the savings.
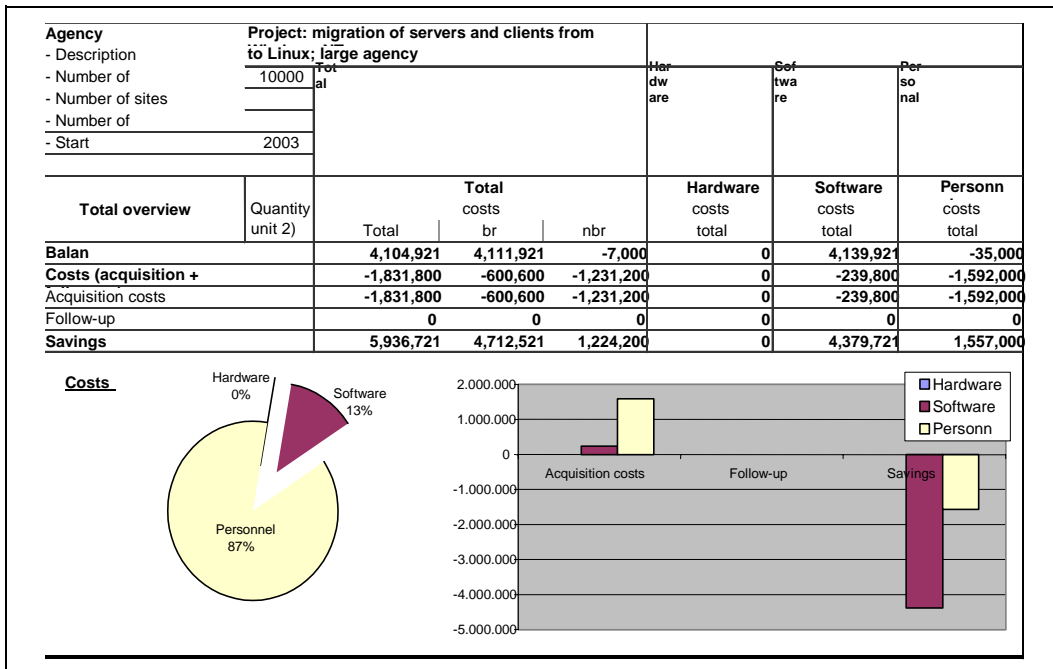

Fig. 57: Example of an economic efficiency calculation of migration from Windows NT to Linux, large public agency, analysis of project costs

The profitability analysis of this variant also yields a positive net present value and hence a profitable outcome of the project.

Evaluation of economic efficiency

Agency	Project: migration of servers and clients from to Linux; large agency			Ha rd wa re	So ft wa re	Pe rs on ne	
- Description							
- Number of	10000	To tal					
- Number of sites							
- Number of					annu all	annu all	annu all
-	2003						
Percentage for	6.00%						

Profitabilit	Total			Hardware	Software	Personnel	
	Total	br	nbr	total	total	total	
Cost/benefit	4,104,92	4,111,92	-7,000	0	4,139,92	-35,000	
Costs	-	-	-	0	-	-	
Acquisition costs	-	-	-	0	-	-	
Follow-up	0	0	0	0	0	0	
Savings	5,936,72	4,712,52	1,224,20	0	4,379,72	1,557,00	
Profitability	3,872,56	3,879,17	-6,604	0	3,905,58	-33,019	
Costs	-	-	-	0	-	-	
Acquisition costs	-	-	-	0	-	-	
Follow-up	0	0	0	0	0	0	
Savings	5,600,68	4,445,77	1,154,90	0	4,131,81	1,468,86	

Fig. 58: Example of an economic efficiency calculation of migration from Windows NT to Linux, large public agency, analysis of net present value

Medium installation

The scenario for medium and small public agencies is generally comparable with that for large public agencies. Migration to Open Source is strongly recommended for these types of public agencies too.

Agency	Project: migration of servers and clients from Windows to Linux; medium agency				Har dw are	Sof twa re	Per so nal	
- Description								
- Number of	1000	al						
- Number of sites								
- Number of								
- Start year	2003							

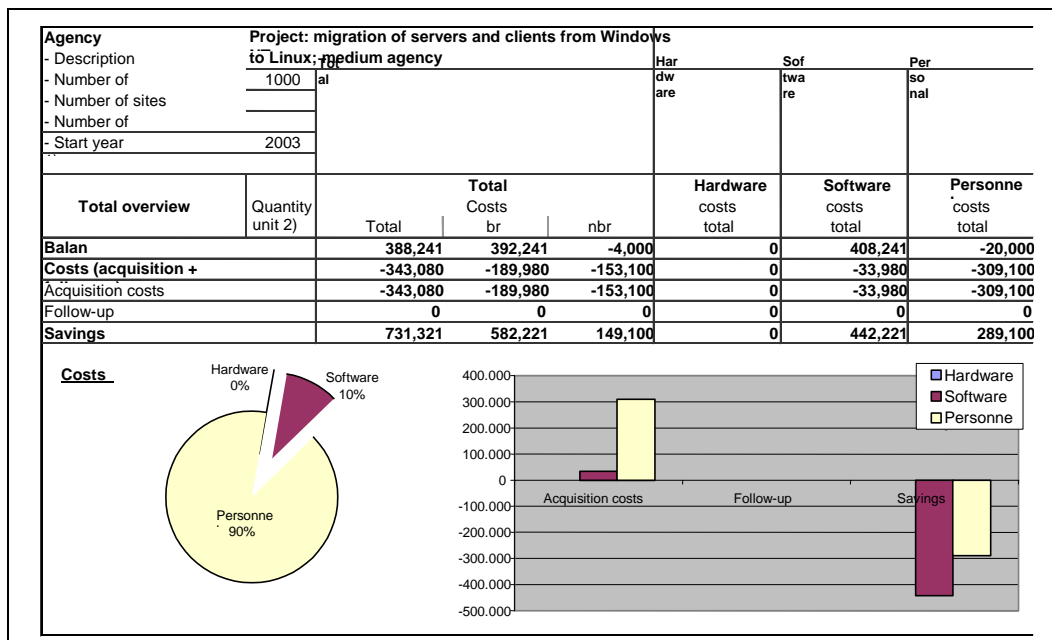| Total overview	Quantity unit 2)	Total Costs			Hardware costs	Software costs	Personne costs	
		Total	br	nbr	total	total	total	
Balan		388,241	392,241	-4,000	0	408,241	-20,000	
Costs (acquisition +		-343,080	-189,980	-153,100	0	-33,980	-309,100	
Acquisition costs		-343,080	-189,980	-153,100	0	-33,980	-309,100	
Follow-up		0	0	0	0	0	0	
Savings		731,321	582,221	149,100	0	442,221	289,100	

Fig. 59: Example of an economic efficiency calculation of migration from Windows NT to Linux, medium public agency, analysis of project costs

The comparative analysis of the migration variants shows a positive net present value for this type of public agency too.

Agency -Description	Project: migration of servers and clients from [Windows NT] to Linux; medium					
- Number of	1000	Tot al		Ha rd wa re	Sof tw are	Per so nn el
- Number of						
- Number of						
-	2003					
Percentage for	6.00					

Profitabilit	Total			Hardware	Software	Personal
	Total	br	nbr	total	total	total
Cost/benefit	**388,24**	**392,24**	**-**	**0**	**408,24**	**-**
Costs	**-**	**-**	**-**	**0**	**-**	**-**
Acquisition costs	-	-	-	0	-	-
Follow-up	**0**	0	0	**0**	**0**	**0**
Savings	**731,32**	582,22	149,10	**0**	**442,22**	**289,10**
Profitability	**366,26**	**370,03**	**-**	**0**	**385,13**	**-**
Costs	**-**	**-**	**-**	**0**	**-**	**-**
Acquisition costs	-	-	-	0	-	-
Follow-up	**0**	0	0	**0**	**0**	**0**
Savings	**689,92**	549,26	140,66	**0**	**417,18**	**272,73**

Fig. 60: Example of an economic efficiency calculation of migration from Windows NT to Linux, medium public agency, analysis of net present value

Small installation

The examples of medium and large public agencies are also applicable in this case.

Agency - Description	Project: migration of servers and clients from Windows to Linux; small agency					
- Number of	250	Tot al		Har dw are	Sof twa re	Per so nn el
- Number of sites						
- Number of						
- Start year	2003					

Total overview	Quantity unit 2)	Total			Hardware	Software	Personne
		Total	costs br	nbr	costs total	costs total	costs total
Balan		**88.976**	**92.176**	**-3.200**	**0**	**104.976**	**-16.000**
Costs (acquisition+		**-123.645**	**-77.920**	**-45.725**	**0**	**-9.120**	**-114.525**
Acquisition costs		-123.645	-77.920	-45.725	0	-9.120	-114.525
Follow-up		**0**	**0**	**0**	**0**	**0**	**0**
Savings		**212.621**	**170.096**	**42.525**	**0**	**114.096**	**98.525**

Costs

Hardware 0%
Software 7%
Personne 93%

Hardware
Software
Personne

Acquisition costs — Follow-up — Savings

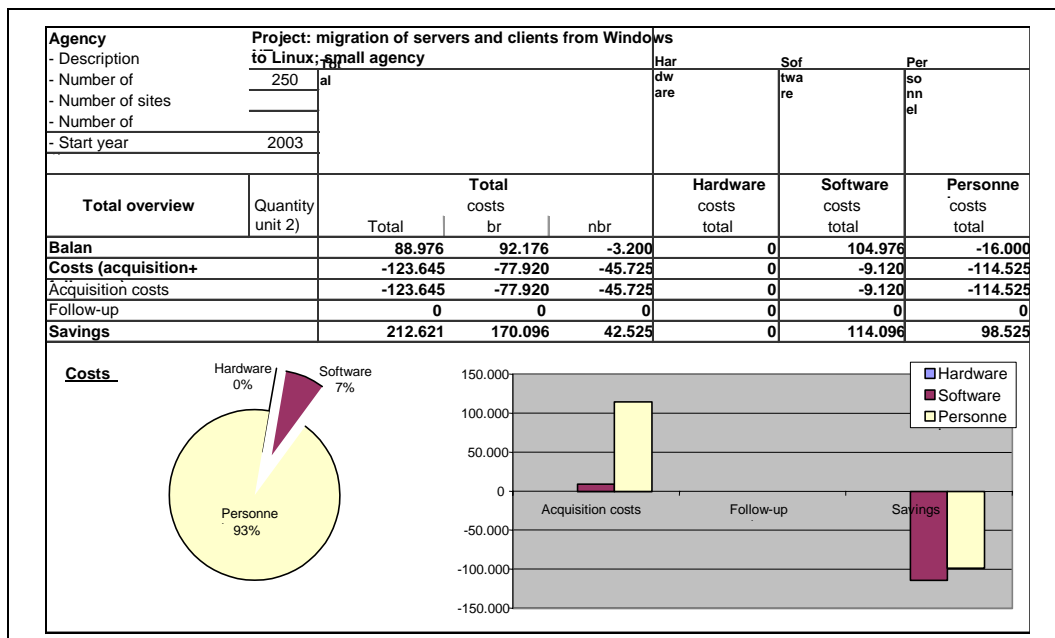150.000
100.000
50.000
0
-50.000
-100.000
-150.000

Fig. 61: Example of an economic efficiency calculation of migration from Windows NT to Linux, small public agency, analysis of project costs

Evaluation of economic efficiency

Agency	Project: migration of servers and clients from to Linux; small agency				Har dw are		Sof twa re		Per so nn el	
- Description										
- Number of	250	Tot al						ja nu all		ja nu all
- Number of							ja nu all			
- Number of										
-	2003									
Percentage for	6.00									

Profitabilit	Total			Hardware		Software		Personne	
	Total	br	nbr	total		total		total	
Cost/benefit	88,97	92,17	-	0		104,97		-	
Costs	-	-	-	0		-		-	
Acquisition costs	-	-	-	0		-		-	
Follow-up	0	0	0	0		0		0	
Savings	212,62	170,09	42,52	0		114,09		98,52	
Profitability	83,93	86,95	-	0		99,03		-	
Costs	-	-	-	0		-		-	
Acquisition costs	-	-	-	0		-		-	
Follow-up	0	0	0	0		0		0	
Savings	200,58	160,46	40,11	0		107,63		92,94	

Fig. 62: Example of an economic efficiency calculation of migration from Windows NT to Linux, small public agency, analysis of net present value

4.8.6.6 Continuing migration

In the case of this type of migration, no savings can be identified and hence cannot be set off either. This is why the scenario-related cost volumes only are shown.

Once-off purchasing prices are generally assumed. Parallel to this, the results are shown under the assumption of annual lease payments for upgrade versions of the Windows and Office products.

The calculations are carried out for large, medium and small installations.

The leased version is the significantly more expensive solution in all the variants analyzed (additional costs of around €250,000 for small migration projects, around €1m for medium migration projects and up to around €10m for large migration projects). The cost increase is caused solely by software follow-up licenses.

All the personnel costs shown represent external personnel costs.
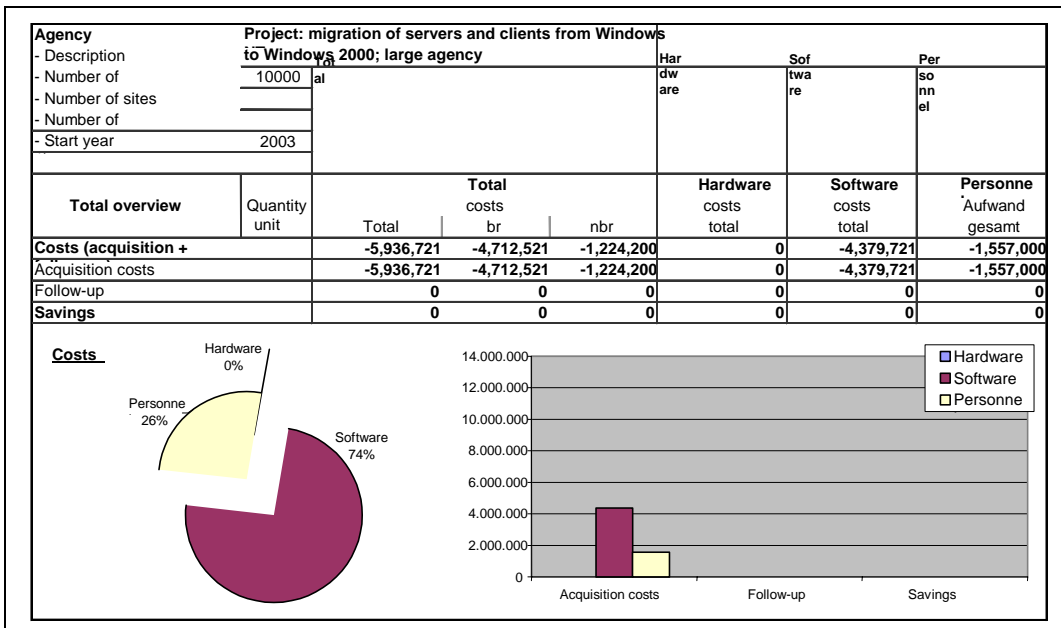
Large installation

Fig. 63:   Example of project cost calculation, migration from Windows NT to Windows 2000, large public agency
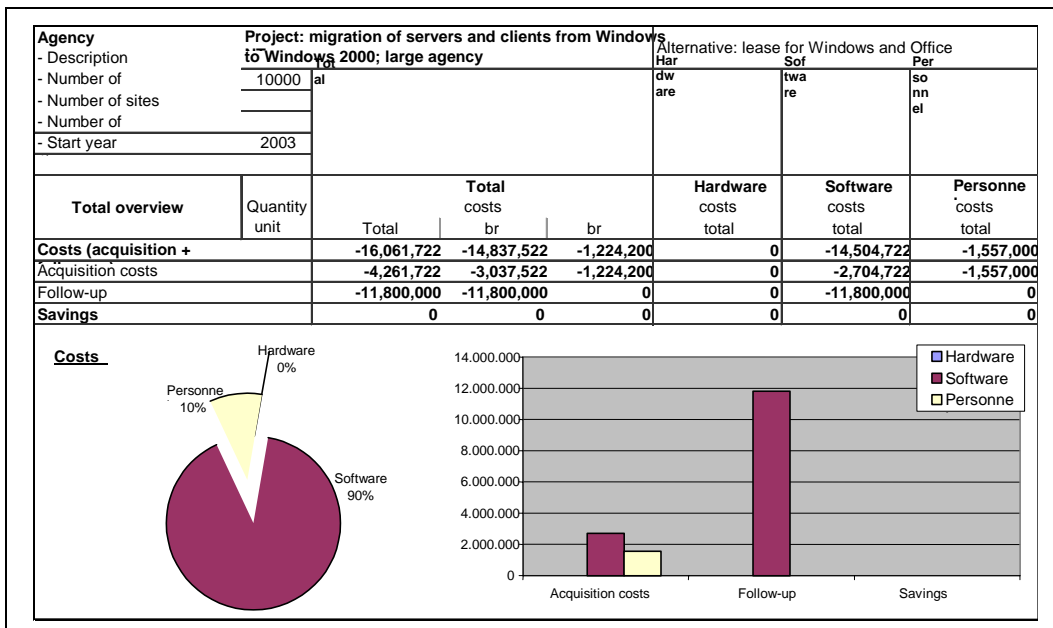

Fig. 64:   Example of project cost calculation, migration from Windows NT to Windows 2000, large public agency, alternative: lease of Windows / Office

Evaluation of economic efficiency
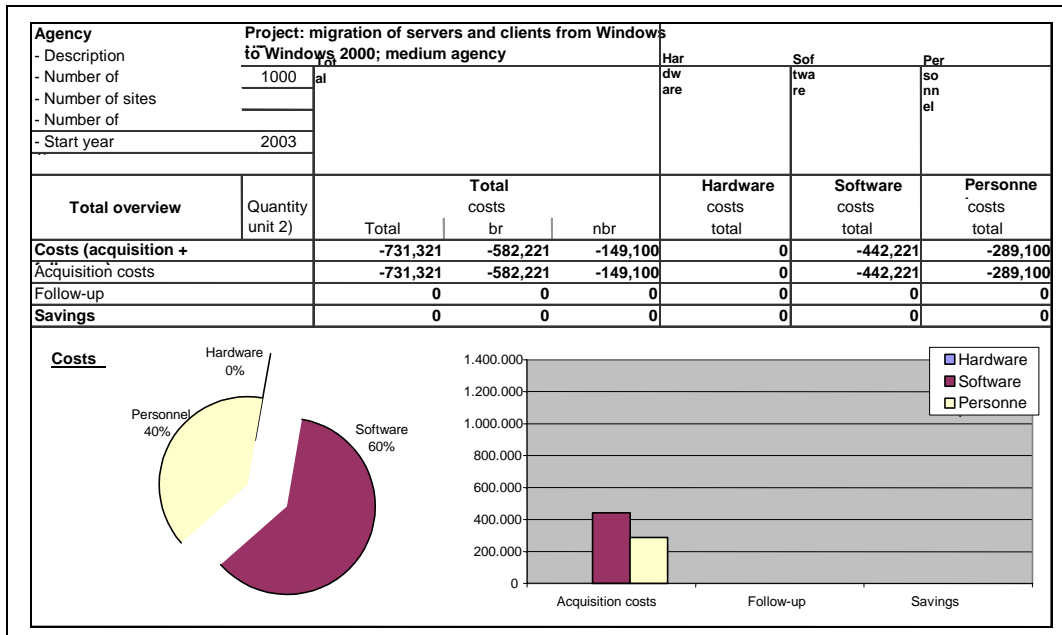
Medium installation

Fig. 65: Example of project cost calculation, migration from Windows NT to Windows 2000, medium public agency
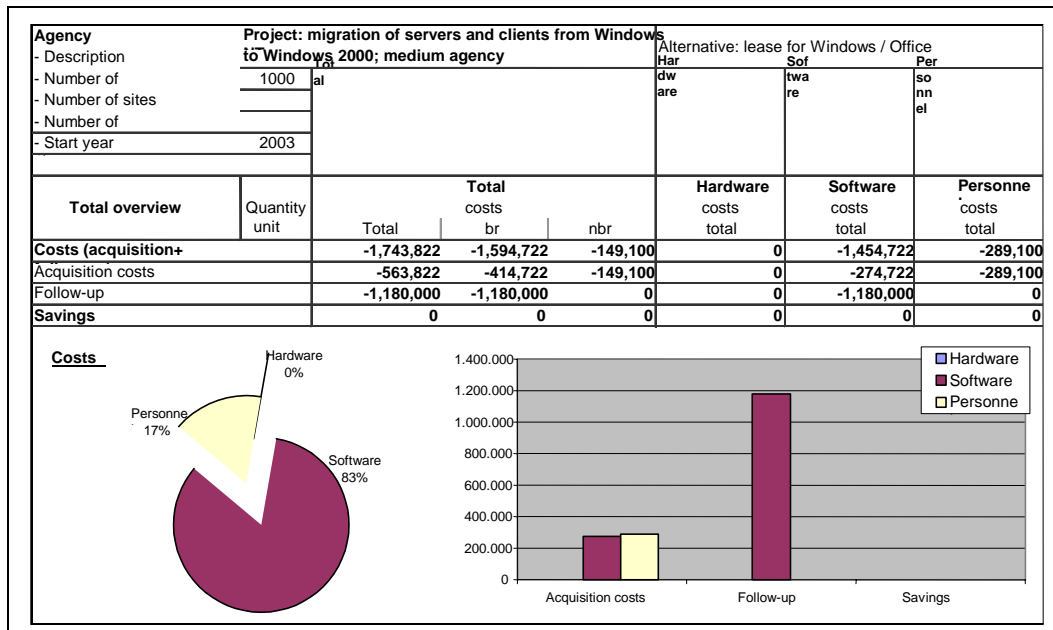

Fig. 66: Example of project cost calculation, migration from Windows NT to Windows 2000, medium public agency, alternative: lease of Windows / Office
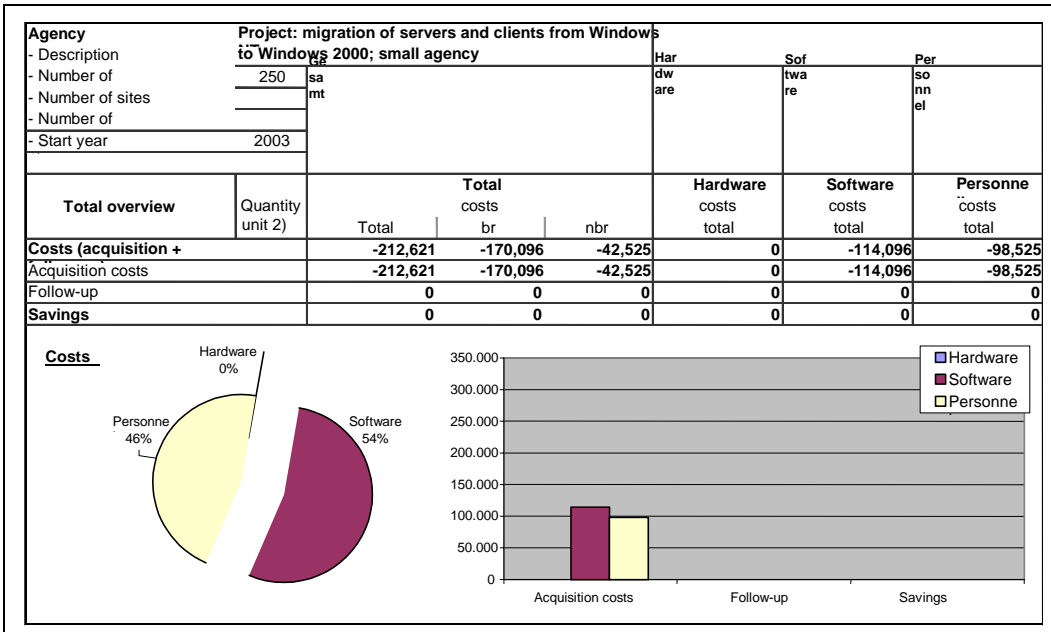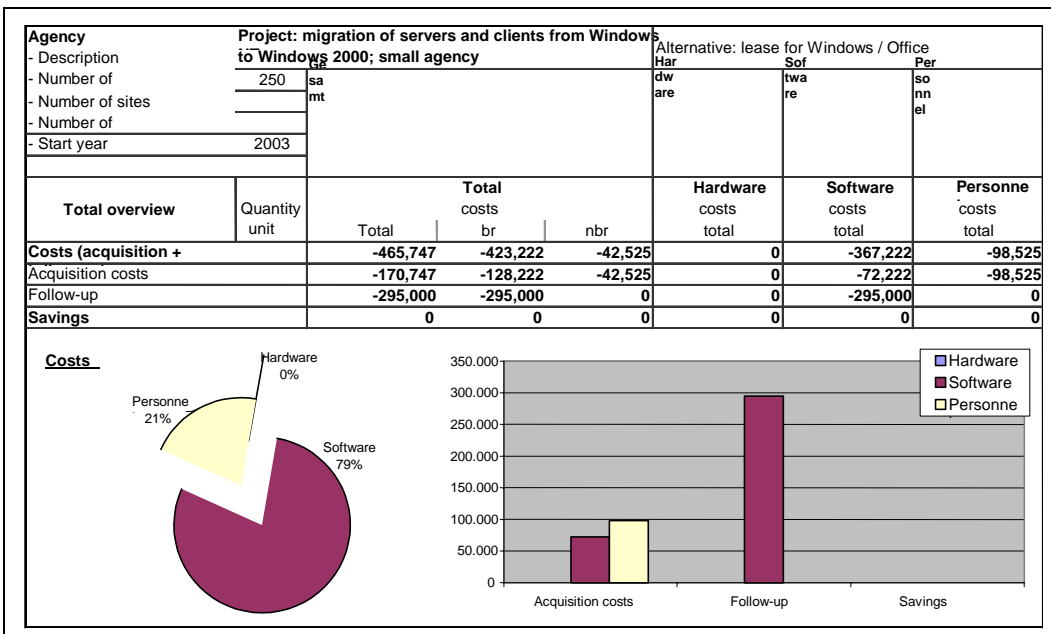
Small installation

Agency	Project: migration of servers and clients from Windows to Windows 2000; small agency					
- Description				Har dw are	Sof twa re	Per so nn el
- Number of	250	sa mt				
- Number of sites						
- Number of						
- Start year	2003					

Total overview	Quantity unit 2)	**Total** costs			**Hardware** costs total	**Software** costs total	**Personne** costs total
		Total	br	nbr			
Costs (acquisition +		-212,621	-170,096	-42,525	0	-114,096	-98,525
Acquisition costs		-212,621	-170,096	-42,525	0	-114,096	-98,525
Follow-up		0	0	0	0	0	0
Savings		0	0	0	0	0	0

Fig. 67: Example of project cost calculation, migration from Windows NT to Windows 2000, small public agency

Agency	Project: migration of servers and clients from Windows to Windows 2000; small agency			Alternative: lease for Windows / Office		
- Description				Har dw are	Sof twa re	Per so nn el
- Number of	250	sa mt				
- Number of sites						
- Number of						
- Start year	2003					

Total overview	Quantity unit	**Total** costs			**Hardware** costs total	**Software** costs total	**Personne** costs total
		Total	br	nbr			
Costs (acquisition +		-465,747	-423,222	-42,525	0	-367,222	-98,525
Acquisition costs		-170,747	-128,222	-42,525	0	-72,222	-98,525
Follow-up		-295,000	-295,000	0	0	-295,000	0
Savings		0	0	0	0	0	0

Fig. 68: Example of project cost calculation, migration from Windows NT to Windows 2000, small public agency, alternative: lease of Windows / Office

Evaluation of economic efficiency

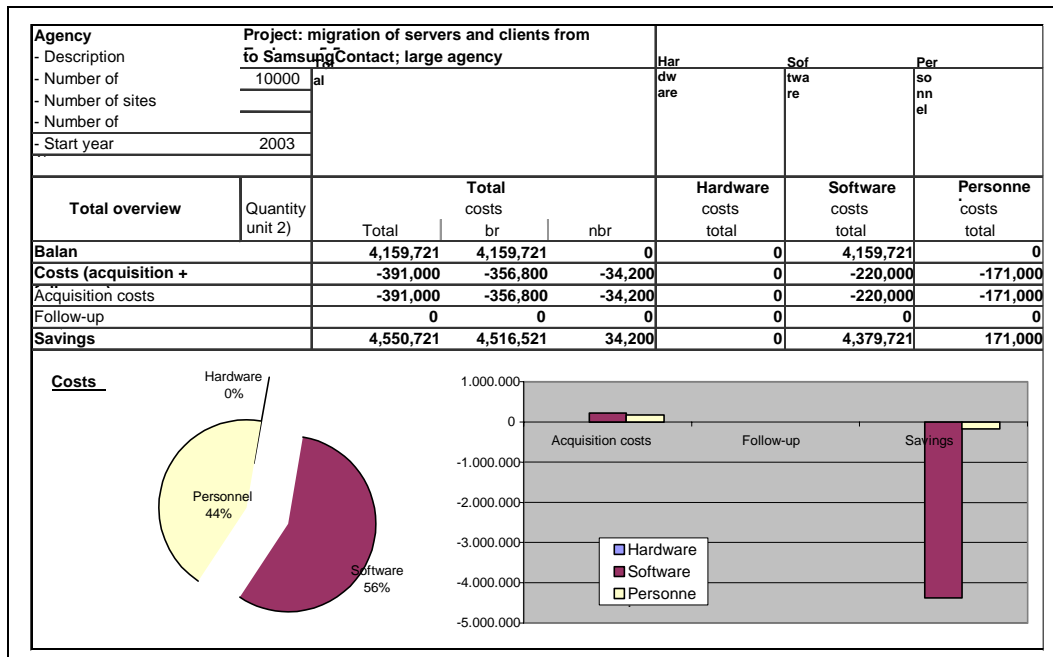## *4.8.6.7 Partial migration*

Selective migration

Agency	Project: migration of servers and clients from to SamsungContact; large agency			Har dw are	Sof twa re	Per so nn el
- Description						
- Number of	10000	al				
- Number of sites						
- Number of						
- Start year	2003					

Total overview	Quantity unit 2)	Total costs			Hardware costs total	Software costs total	Personne costs total
		Total	br	nbr			
Balan		**4,159,721**	**4,159,721**	**0**	**0**	**4,159,721**	**0**
Costs (acquisition +		**-391,000**	**-356,800**	**-34,200**	**0**	**-220,000**	**-171,000**
Acquisition costs		-391,000	-356,800	-34,200	0	-220,000	-171,000
Follow-up		**0**	**0**	**0**	**0**	**0**	**0**
Savings		**4,550,721**	**4,516,521**	**34,200**	**0**	**4,379,721**	**171,000**

Fig. 69: Example of project cost calculation, migration from Exchange 5.5 to Samsung Contact, large public agency

Agency	Project: migration of servers and clients fro, to SamsungContact; medium agency			Har dw are	Sof twa re	Per so nn el
- Description						
- Number of	1000	al				
- Number of sites						
- Number of						
- Start year	2003					

Total overview	Quantity unit 2)	Total costs			Hardware costs total	Software costs total	Personne costs total
		Total	br	nbr			
Balan		**410,221**	**410,221**	**0**	**0**	**410,221**	**0**
Costs (acquisition +		**-153,000**	**-128,800**	**-24,200**	**0**	**-32,000**	**-121,000**
Acquisition costs		-153,000	-128,800	-24,200	0	-32,000	-121,000
Follow-up		**0**	**0**	**0**	**0**	**0**	**0**
Savings		**563,221**	**539,021**	**24,200**	**0**	**442,221**	**121,000**

Fig. 70: Example of project cost calculation, migration from Exchange 5.5 to Samsung Contact, medium public agency

Agency	Project: migration of servers and clients from to SamsungContact; small agency				Hardware	Software	Personnel
- Description							
- Number of	250						
- Number of sites							
- Number of							
- Start year	2003						

Total overview	Quantity unit 2)	Total costs			Hardware costs total	Software costs total	Personne costs total
		Total	br	nbr			
Balan		105,471	105,471	0	0	105,471	0
Costs (acquisition +		-72,625	-59,825	-12,800	0	-8,625	-64,000
Acquisition costs		-72,625	-59,825	-12,800	0	-8,625	-64,000
Follow-up		0	0	0	0	0	0
Savings		178,096	165,296	12,800	0	114,096	64,000

Costs — Hardware 0%, Software 12%, Personnel 88%

Bar chart: Acquisition costs, Follow-up, Savings (Hardware, Software, Personne)

Fig. 71: Example of project cost calculation, migration from Exchange 5.5 to Samsung Contact, small public agency

Partial migration at the server end

Agency	Project: migration of servers only from Windows NT to Linux; large agency				Hardware	Software	Personnel
- Description							
- Number of	10000						
- Number of sites							
- Number of							
- Start year	2003						

Total overview	Quantity unit 2)	Total costs			Hardware costs total	Software costs total	Personne costs total
		Total	br	nbr			
Balan		-225,080	-218,080	-7,000	0	-190,080	-35,000
Costs (acquisition +		-645,800	-555,600	-90,200	0	-194,800	-451,000
Acquisition costs		-645,800	-555,600	-90,200	0	-194,800	-451,000
Follow-up		0	0	0	0	0	0
Savings		420,721	337,521	83,200	0	4,721	416,000

Costs — Hardware 0%, Software 30%, Personne 70%

Bar chart: Acquisition costs, Follow-up, Savings (Hardware, Software, Personne)

Fig. 72: Example of project cost calculation, migration from Windows NT to Linux at the server end, large public agency

Evaluation of economic efficiency

Agency	Project: migration of servers only from Windows NT to Linux; medium			Har dw are	Sof twa re	Per so nn el
- Description						
- Number of	1000	al				
- Number of sites						
- Number of						
- Start year	2003					

Total overview	Quantity unit 2)	Total costs		Hardware costs	Software costs	Personne costs
		Total	br	nbr	total	total	total
Balan		-42,760	-38,760	-4,000	0	-22,760	-20,000
Costs (acquisition +		-222,480	-183,480	-39,000	0	-27,480	-195,000
Acquisition costs		-222,480	-183,480	-39,000	0	-27,480	-195,000
Follow-up		0	0	0	0	0	0
Savings		179,721	144,721	35,000	0	4,721	175,000

Fig. 73: Example of project cost calculation, migration from Windows NT to Linux at the server end, medium public agency

Agency	Project: migration of servers only from Windows NT to Linux; small agency			Har dw are	Sof twa re	Per so nn el
- Description						
- Number of	250	al				
- Number of sites						
- Number of						
- Start year	2003					

Total overview	Quantity unit 2)	Total costs		Hardware costs	Software costs	Personne costs
		Total	br	nbr	total	total	total
Balan		-18,650	-15,450	-3,200	0	-2,650	-16,000
Costs (acquisition +		-93,370	-76,170	-17,200	0	-7,370	-86,000
Acquisition costs		-93,370	-76,170	-17,200	0	-7,370	-86,000
Follow-up		0	0	0	0	0	0
Savings		74,721	60,721	14,000	0	4,721	70,000

Fig. 74: Example of project cost calculation, migration from Windows NT to Linux at the server end, small public agency

4.9 Example of evaluation of urgency and quality / strategy

The evaluation example includes the calculation of urgency, D, and of the quality/strategy factors, Q, according to IT-WiBe 21 (recommendations on economic efficiency assessments for IT systems). It considers the situation of

public agencies in general and represents a rough estimate of today's discussion concerning the evaluation of legacy systems. The pros and cons leading to the different ratings are outlined in general terms. The description is oriented towards the degrees of target fulfillment according to the catalog of criteria.

The example evaluation for the **urgency** of migration projects yields a value of > **59** < . The projects are hence generally supported from this perspective.

The **quality/strategy** example evaluation of migration projects yields a value of > **66** <. This means that the projects make sense under these aspects as well.

4.9.1   Urgency criteria

These criteria (group 3 of the catalog of criteria) refer to the urgency to replace an existing system on the one hand and to compliance with administrative rules and laws on the other.

4.9.2   Quality/strategy criteria

Group 4 of the catalog of criteria contains the quality and strategy criteria of IT projects. They refer to the priority of an IT project, to internal quality improvements within public agencies and to the repercussions on employees and "customers" of public administrations (citizen orientation) as well as the general market availability of the software and IT security. The strategic "feasibility" of a given IT project is checked against the criteria. This means that the legacy system is no longer the focus of attention, but the IT project has to be checked on the basis of the factors referred to in the criteria.

4.9.3   Benefit analysis

The criteria for urgency and quality/strategy cannot be quantified in monetary terms. Instead, they form part of a benefit analysis. This requires a qualitative description of the repercussions of these criteria. This description, for its part, must be translated to a score for every criterion. A scale from 0 to 10 is available for this purpose. The points are multiplied by the applicable weighting factor and added up for the individual criteria groups. A value greater than 50 means that an IT project can be classified as "recommended for implementation" with regard to the area analyzed.

Evaluation of economic efficiency

MG item	Calculation	Weighting	Score	Result	Criterion
	Original system: NT or Unix				Migration objects>
					Explanation: Data must be gathered for the criteria marked by an x. The weighting of the criteria is determined once (total = 100). The score must be awarded per criterion and product (0-10).
B				**59**	**Dimension: urgency of the IT project**
3	Total	100	38	590	Urgency criteria
3.1					Urgency to replace the old
3.1.1	Wtd. score	20	8	160	Continuity of support for old system
3.1.2					Stability of old
3.1.2.1	Wtd. score	20	7	140	Bugs, errors and downtime
3.1.2.2	Wtd. score	20	3	60	Service problems, personnel
3.1.3					Flexibility of old
3.1.3.1	Wtd. score	10	8	80	Limits of expansion/upgrading
3.1.3.2	Wtd. score	10	9	90	Interoperability, interface problems at present / in
3.1.3.3	Wtd. score	20	3	60	User-friendliness
C				**66**	**Dimension: qualitative/strategic relevance of the IT project**
4	Total	100	61	663	Quality/strategy criteria
4.1					Priority of the IT project
4.1.2	Wtd. score	5	6	30	Integration into the IT landscape of federal administration in
4.1.3	Wtd. score	10	7	70	Follow-up effects for communication
4.1.5	Wtd. score	20	8	160	Manufacturer-
4.4					Staff-related effects
4.4.1	Wtd. score	5	6	30	Attractiveness of working conditions
4.4.2	Wtd. score	2	3	6	Quality assurance/enhancement
4.4.3	Wtd. score	3	2	6	Dissemination/availability of training
4.5					Effects related to citizen
4.5.4	Wtd. score	2	6	12	Image improvement
4.6				0	Dissemination/availability of software
4.6.1	Wtd. score	5	7	35	Market penetration
4.6.2	Wtd. score	5	6	30	Independent support
4.6.3	Wtd. score	5	5	25	Software certification available
4.6.4	Wtd. score	5	5	25	Admin tools for the software available
4.7				0	IT security
4.7.1	Wtd. score	6	7	42	Communication security
4.7.2	Wtd. score	6	6	36	Application security
4.7.3	Wtd. score	6	7	42	Failure safety
4.7.4	Wtd. score	6	7	42	Security management
4.7.5	Wtd. score	9	8	72	Investment and planning safety

Fig. 75:   Evaluation model for urgency and quality for migration projects

The table below describes the individual criteria.

Table 76: Example: benefit analysis for urgency factors

WiBe item	Criterion/ explanation	Weighting factor/ points	
3	**Urgency factors**		
3.1	Urgency to replace the legacy system		
3.1.1	Support continuity for the legacy system	G	20
	Support for the MS Windows NT operating system is no longer ensured as of 2003.	P	8

WiBe item	Criterion/ explanation	Weighting factor/ points	
3	**Urgency factors**		

| | Microsoft has already discontinued deliveries of service packs for eliminating security-relevant system bugs. Support of new features, such as USB, etc. is no longer ensured. | | |

3.1	Urgency to replace the legacy system		
3.1.2	Stability of the legacy system		
3.1.2.1	Bugs, errors and downtime	G	20
	The error-susceptibility of the legacy system is still within tolerable limits.	P	7
	The introduction of new administrative tools will increase error susceptibility because the software developers use new program libraries which are difficult to integrate into the Windows NT architecture.		

3.1	Urgency to replace the legacy system		
3.1.2	Stability of the legacy system		
3.1.2.2	Service problems, personnel bottlenecks	G	20
	The external support for system support will decrease even further in future because the manufacturer no longer ensures this support and because the manufacturer has already launched the second successor product to the operating system platform.	P	4

3.1	Urgency to replace the legacy system		
3.1.3	Flexibility of the legacy system		
3.1.3.1	Limits of expansion / upgrading	G	10
	Implementation of upgraded functionalities, such as USB, etc. is no longer ensured.	P	8
	Tools which support interoperability with new systems are no longer developed.		
	Changing architectures mean that interface problems with other IT systems will increase in future.		

3.1	Urgency to replace the legacy system		
3.1.3	Flexibility of the legacy system		
3.1.3.2	Interoperability, present/future interface problems	G	10
	Adaptation of the legacy system to up-to-date needs is becoming difficult.	P	9

| 3.1 | Urgency to replace the legacy system | | |

Evaluation of economic efficiency

WiBe item	Criterion/ explanation	Weighting factor/ points	
3	**Urgency factors**		

WiBe item	Criterion/ explanation	Weighting factor/ points	
3.1.3	Flexibility of the legacy system		
3.1.3.3	User-friendliness	G	20
	Hardly affected at present.	P	3

Table 77: Example: benefit analysis for quality/strategy factors

WiBe item	Criterion/ explanation	Weighting factor/ points	
4	**Quality/strategy factors**		

WiBe item	Criterion/ explanation	Weighting factor/ points	
4.1	Priority of the IT project		
4.1.2	Integration into the IT landscape of the federal administration in general	G	5
	The specifications issued by the Co-ordinating and Advisory Agency of the Federal Government for Information Technology in the Federal Administration (KBSt) with regard to the use of Open Source projects with a view to a realistically implementable system environment with all relevant facettes to be considered (administration, file conversion, etc.) can only be implemented conditionally using the given products and dependencies.	P	5

WiBe item	Criterion/ explanation	Weighting factor/ points	
4.1	Priority of the IT project		
4.1.3	Follow-up effect for communication partners	G	10
	In contrast to the present situation, an ideal communication basis will be created within the framework of the orientation towards the use of OSS products in order to simplify communication between different public agencies.	P	7

WiBe item	Criterion/ explanation	Weighting factor/ points	
4.1	Priority of the IT project		
4.1.5	Manufacturer-independence	G	20
	Considering the heterogenous structure comprising OSS and Microsoft products, a high degree of manufacturer-independence is aimed at through determined orientation towards the use of OSS products.	P	8

WiBe item	Criterion/ explanation	Weighting factor/ points	
4.4	Staff-related effects		
4.4.1	Attractiveness of working conditions	G	5
	Two separate effects will have to be considered in this	P	6

WiBe item	Criterion/ explanation	Weighting factor/ points	
4	**Quality/strategy factors**		

	context:		
	In the administrative area, the additional effort due to significantly more demanding activities resulting from the use of OSS products will clearly expand personal qualification profiles.		
	In the area of IT users, solutions are aimed at which will enable a distinct simplification of the currently sometimes still very limited product-spanning processing possibilities in the field of office communication software.		

4.4	Staff-related effects		
4.4.2	Increase/expansion of qualifications	G	2
	Effects leading to increased qualification can be expected in future. In the administrative area, these effects result from a more interesting portfolio of tasks and from training. In the user area, these effects result from enhanced knowledge due to the use of different office communication systems.	P	3

4.4	Staff-related effects		
4.4.3	Dissemination / availability of training	G	3
	There are no problems with a view to training and experience required for the use of the systems currently in use. However, given an increasing demand for OSS products, it may become more difficult in future to find adequately trained personnel. However, since one may assume that existing staff will be trained accordingly, this effect can be neglected in the medium term as far as the public administration is concerned.	P	2

4.5	Effects related to citizen orientation		
4.5.4	Image improvement	G	2
	Migration projects are also designed to integrate the heterogenous server and client worlds into everyday work.	P	6
	The gradual transition to an OSS environment enables gentle migration and will serve as a practical demonstration that the political goal to introduce OSS can be implemented.		
	In the medium and long term, the entire administration sector and citizens will benefit from significant added value as a result of the migration projects.		

4.6	Dissemination / availability of software		

Evaluation of economic efficiency

WiBe item	Criterion/ explanation	Weighting factor/ points	
4	**Quality/strategy factors**		

4.6.1	Market penetration	G	5
	○ The products to be used are available on the market without any problems.	P	7

4.6	Dissemination / availability of software		
4.6.2	Independent support	G	5
	Not just manufacturers, but also numerous independent companies offer support for the products used.	P	6

4.6	Dissemination / availability of software		
4.6.3	Available software certification	G	5
	Relevant references or even certifications exist for the products to be used.	P	5

4.6	Dissemination / availability of software		
4.6.4	Availability of administration tools for the software	G	5
	Administration tools are available to a sufficient extent.	P	5

4.7	IT security		
4.7.1	Secure communication	G	6
	Communication with internal and external partners is well ensured.	P	7

4.7	IT security		
4.7.2	Application safety/security	G	6
	The applications are mature.	P	6

4.7	IT security		
4.7.3	Failure safety	G	6
	The systems to be used are becoming increasingly fail-safe.	P	7

4.7	IT security		
4.7.4	Security management	G	6
	The systems to be used include safety and security mechanisms which are documented and which can be made available to all those concerned.	P	7

4.7	IT security		

WiBe item	Criterion/ explanation	Weighting factor/ points	
4	**Quality/strategy factors**		

4.7.5	Investment and planning safety	G	6
	The investment to be made is safe. The products will remain available even in future for a period of five years typical for public agencies. The systems to be used are stable and the processes based on these systems can be safely planned.	P	8

5   Migration recommendations

5.1 General statements

5.1.1   The decision-making path

The results of an evaluation of economic efficiency with a long-term perspective are crucial for a recommendation in favor of migration or further development recommendation. Even if complete or partial migration is possible without any restrictions from a technical perspective, economic considerations may suggest that migration does not make much sense under the given conditions. In view of the diverse correlations and interactions between the individual components and systems of an infrastructure and the application world, a long-term perspective is always required in the decision-making process.

In this context, the analysis from the point of view of an introduction of Open Source software does not differ from the customary evaluation analyses in the field of IT, for example, in the context of hardware or software consolidation. The following strategies are usually pursued in both public administrations and business alike.

System and application platforms closely adapted to each other on the basis of open standards and specifications, if necessary, with the help of dedicated integration products.

System and application platform closely adapted to each other on the basis of manufacturer-specific interfaces and specifications (not disclosed at all or disclosed to a limited extent only), if necessary, with the help of manufacturer-specific integration products.

 (Historical) use of isolated solutions for selective specialist methods and applications.

Since Open Source software is, due to its origins, often connected to the use of open standards, it constitutes another variant in this field:

System and application platforms adapted to each other on the basis of open standards and specifications using the open (reusable) source code.

Whilst a decision in favor of the selective introduction of a widely used, open-source product, such as the Apache web server, can usually be made in a very pragmatic manner and quickly, the decision in favor of a wide-spread, general introduction of Open Source software and the replacement of proprietary island requires a methodical approach because of its long-term repercussions. The fundamental milestones of such an approach are the following:

Development of an overall IT strategy, taking the given financial, organizational, innovation-related and personnel objectives into consideration

Definition of the future Open Source platform strategy, taking the long-term calculations of economic efficiency into consideration with a view to the use of

free and commercial standard products (OSS vs. COLS model, refer to section 5.1.2)

Identification of all the standards necessary to ensure internal and external reusability as well as interoperability in a blueprint catalog

Selection of the products meeting the requirements

Definition of the project, including the pertinent time schedule, list of actions, as well as ensuring a budget process

As the illustration below shows, methods and tools already in use at public administrations can be used for the different phases.
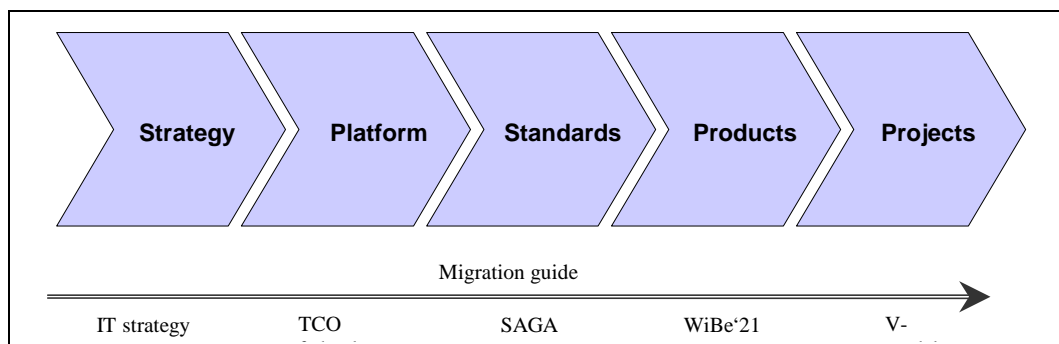
Fig. 76: Decision-making process for the introduction of OSS

5.1.2 General recommendations

In view of strongly varying starting situations (including isolated solutions), generally valid statements concerning the economic advantages of the platform strategies are only seldom possible. One can, however, generally say that economic efficiency increases the greater the degree of integration of the products of a platform. This is due to several reasons:

Higher productivity in the case of products correctly adapted to each other (without system inconsistencies)

Increasing reusability of components and solutions which were developed on the basis of the same middleware technology

Savings due to standardized purchasing and maintenance processes as well as service agreements, if any.

Furthermore, an increasing degree of standardization on the basis of open standards also boosts economic efficiency as a whole. This is due to several reasons as follows:

Beginning competition of products and solutions

Reduced manufacturer-dependence

Generally broader service markets.

Migration recommendations

In particular (however, not exclusively), the adoption of SAGA (Standards and Architectures for e-government Applications) and internal standardization within public administrations have increased the investment safety for commercial suppliers of Linux software. This is reflected by a growing supply of both basic components and specialist methods and makes the scenario of complete migration possible which was still difficult until recently.

On this basis, the following general recommendations can be developed for the use of open-source products.

Recommendation for adopting economic efficiency as an overall aim of the entire IT strategy, taking the innovation and organization factors adequately into consideration

Recommendation for the use of the Linux operating system as the basis of the IT platform for all fields of application if the preconditions for full or partial migration are fulfilled (refer to sections 5.2 and 5.4)

Recommendation for the use of open standards which are equally recognized by both the IT industry and the Open Source Community alike as a basis for the selection and integration of software products in order to avoid cases of extreme manufacturer-dependence

Recommendation concerning the implementation of a project-related evaluation of economic efficiency within the scope of the decision-making process related to the use of open and commercial Linux products (refer to chapter 4)

Migration to the OSS/COLS platform can generally turn out as the economically more reasonable (more profitable) variant compared to continuing migration to a new Microsoft version.

Omission or reduction of license costs can lead to direct (monetary) savings, for example, in the following cases:

Partial migration at the server end in conjunction with hardware and software consolidation of UNIX know-how and UNIX systems is already available

Selective replacement of members of the former backoffice family (today: .NET Enterprise Server), such as Exchange or SQL Server, especially with larger or increasing numbers of users and hence licenses

Partial migration of MS Office products at the client end unless the use of Office as the runtime environment for macros or applications prevents replacement

In many other application scenarios, the strategic dimension must be additionally considered in order to assess the savings. The chapter titled "Evaluation of economic efficiency" discusses this strategic dimension in detail.

Training costs as an economic aspect must be considered in any case both with the migration of today's platforms to the Linux world or to a new Microsoft level. As such costs are realistically incurred in either of the cases, this cost segment

can be considered to be largely neutral within the scope of a direct comparison of the alternatives. Furthermore, the costs of migrating specialist applications which may exist must also be considered in any case, i.e. for both alternatives[191].

Since the general recommendations cannot address the requirements and frames of reference of a concrete starting situation, further recommendations will be given with regard to different scenarios. Section 5.2 discusses the case of complete migration, section 5.3 addresses the scenario in which the existing platforms are left in place, and section 5.4 deals with a hybrid environment (partial migration).

5.2   Completely "replacing migration"

Complete migration as defined in this migration guide means that Linux is introduced as the operating system on all components of the IT infrastructure. A complete replacement of operating systems usually also involves replacement with SAGA-conforming products at the integration and application levels because the necessary Java products, in particular, have not yet reached the degree of dissemination that had been hoped for[192].

Two software variants which are often combined with each other are generally available for complete migration:

OSS: open source software (oder freie Software)[193]: open-source, free software developed by the OSS Community

COLS: COmmercial Linux Software: commercial, open-source or proprietary software for Linux offered by the software manufacturers.

Since many areas of the public administration intensively use specialist, Windows-based applications developed by the administrations themselves as well as ERP-based application systems, Open Source software can be expected to cover all requirements in the field of infrastructure only in the foreseeable future. In view of the positive promotion of Linux thanks to the availability of large application systems from manufacturers like SAP or Oracle, the use of commercial software and the growing supply of Linux software can be seen to be generally positive for the further development of the Open Source platform and will lead to further momentum for the advancement of this platform.

The specific features of the possible and recommended system and software architectures vary as a function of size, IT intensity and the degree of

---

[191] This cost segment is disregarded within the scope of this migration guide. It usually requires very specific analyses at the different public agencies concerned which cannot be covered by a migration guide. Dimensions shown within the framework of an evaluation of economic efficiency can vary from case to case if the migration costs determined for specialist applications are included in the analysis.

[192] In this case, the web applications of the (L)AMP model which are also quite commonly used under Windows are not affected by the need for a migration.

[193] Refer to the definition in chapter 2.

specialization of public agencies. The scalability and availability of individual components on the one hand and the input necessary for introduction on the other play a decisive role in this context.

This is why the focal aspects will be discussed separately, i.e. for <u>large</u> and <u>medium</u> as well as for <u>specialist</u> and <u>small</u> public agencies. A general and hence generic model for infrastructure tasks will be initially introduced as an introduction.

5.2.1 Architecture model

Given a consistent use of Linux as the platform for client and server applications throughout, two types of client architectures can be distinguished analogous to the usual UNIX and Windows architectures: fat clients and thin clients.
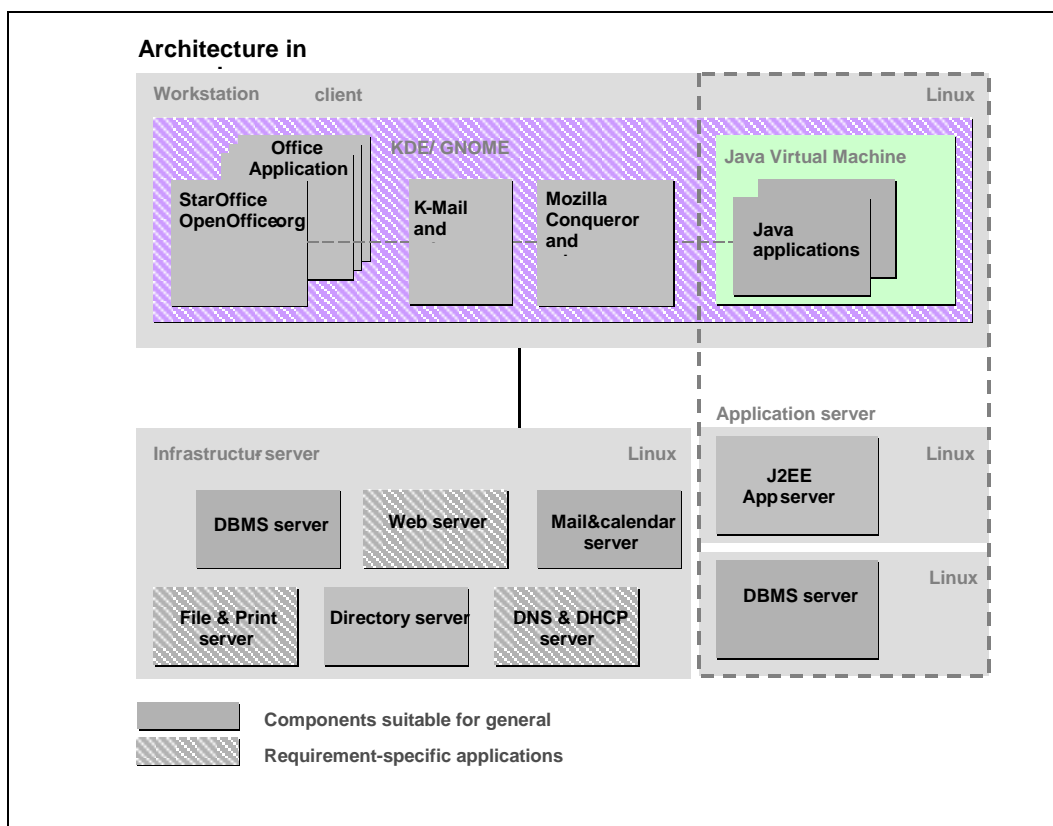
Fig. 77: System architecture with a Linux-based fat client

The configuration shown in System is representative of workstation computers with multi-function capability in a distributed architecture with a commercially available PC (fat client). The server platform covers the usual infrastructure functions, with an application server completing the picture of a 3-layer architecture.

The components selected cover various applications, including, for example, the following:

Workstation computers (desktop and Office)

Groupware (mail & calendar server)

Database systems (DBMS server)

Web server

File server

Print server

Authentication services

Network services (including, but not limited to, DNS & DHCP server).

The hatched areas in   System   can be used irrespective of the size and degree of specialization of the public agency concerned. The other system components will be discussed in the following sections against the background of their different application scenarios. These are:

Large and medium public agencies

Specialized public agencies with an IT service function

Small public agencies

Note: Certain restrictions must be generally considered with regard to the migration scenarios analyzed here.

The technical analysis shows that – with just a few exceptions – alternative solutions from the field of OSS and/or COLS products are available for replacing migration away from Microsoft products which form part of the starting situation considered here (refer to chapter 2.2.1). Critical points are:

Compatibility between OpenOffice.org/StarOffice and MS Office is not fully given. This affects especially those users who often have to create documents together with other users. If both Office variants are used in cases like this, formatting problems are usually encountered.

The Chart Engine of OpenOffice.org and StarOffice is not as powerful as the MS Excel Chart Engine. This is especially true with regard to the creation of charts on the basis of Pivot charts.

An adequate alternative to certain products, such as MS-Project or Visio, is not yet available.

A migration from Microsoft products to OSS solutions and COLS products may, however, be prevented by economic rather than functional reasons. This especially concerns the migration of the desktop.

MS Office
The scope and complexity of the macros, scripts, templates and documents can mean that migration to OpenOffice.org or StarOffice is not economical.

MS Office Professional
An analogous conversion problem exists in the case of MS Access and the

Access applications to be migrated which are often used for simple process automation applications.

Specialist   applications
Depending on the degree of use of native Windows specialist applications, replacing migration can, under worst-case conditions, be prevented until alternative products are available. (Refer to chapter 5.3) This is also valid for applications which were created on the basis of MS Exchange and which use MS Exchange as the runtime system.

5.2.1.1   Workstation computers

Operation of the workstation computers is based on Linux. It is not possible at this point to recommend a particular distribution (refer to 0). The decision depends on the circumstances of the particular case and the specific requirements of the public administration concerned. Both OpenOffice and StarOffice can be recommended for the Office area. The decision in favor of one product or the other depends on the specific requirements of the public agency concerned. Just as much as Microsoft Office, StarOffice and OpenOffice include the applications necessary for day-to-day work (word processing, spreadsheet analysis, presentation) and fulfill the functional requirements. For the StarOffice Suite, which is available as a COLS product, Sun has developed and/or added additional components (truetype fonts, own spell-checker, additional templates and a picture gallery, ADABAS database). OpenOffice.org, in contrast, is a member of the OSS family and available as a free product. The functional and technical differences between the two Office packages are only marginal.

The real desktop system is another important user interface. Within the Linux distributions, complete desktops are usually implemented for the users which, like the Windows desktop, cover the most important applications. KDE and GNOME are the two most important representatives of desktop systems. The selection of the particular desktop system is primarily a matter of personal taste and the user's preferences for certain applications.

5.2.1.2   Web server

The Apache web server (refer also to chapter 3.11.4) is at present the benchmark for the provision of Internet and intranet contents. Its flexibility thanks to its modular design and the number of modules available has made the Apache web server the market leader in the web server sector. The features of this component include its many years in use in large, productive environments, its stability, comprehensive security functionalities and readily available and freely selectable, professional support.

5.2.1.3   File system

The tried-and-tested Network File System (NFS) is recommended for the file services in a Linux-based system landscape. NFS is traditionally used as a network-based file system in UNIX networks. NFS is the standard protocol if directories are to be shared by different UNIX systems. Users can access the

required directory areas via central or distributed servers. The exported directory trees are automatically linked on the user's corresponding workstation computer.

The XFS and EXT3 file systems are recommended for the physical storage of data on the disk systems of the real servers. Both systems support journaling functionalities, quotas and the assignment of access privileges at file and directory levels.

5.2.1.4 Print services

The "Common UNIX Printing System (CUPS)" is the only system recommended for the provision of print services. CUPS is established on practically all UNIX systems and constitutes the de-facto standard of all major distributions (SuSE, Debian, RedHat, etc.). The CUPS print service offers all the functionalities required to provide a print infrastructure. CUPS supports a large number of different print devices and is capable of making the specific print options available to the respective users. CUPS is based on the Internet Printing Protocol as the new standard defined for printing both in local area networks (LAN) and in wide-area networks (WAN, Internet).

5.2.1.5 Network services

Due to their UNIX origin, the infrastructure-forming services for TCP/IP-based networks form, by default, an integral part of open source software. BIND (Berkeley Internet Name Domain) is recommended as the reference implementation for the domain name system. With regard to DHCP, also refer to the reference implementation of the Internet Software Consortium.

5.2.2 Medium and large public agencies

Medium and large public agencies feature special IT architectures, and the migration recommendations for certain applications may differ from those for smaller administrations. As of a certain size, public agencies typically operate both distributed and centralized IT architectures. The former are normally used for central operations (ERP, cost/output analysis) of public agencies. The individual system components which form the basis for the implementation of the centralized processes must meet with particularly demanding requirements with a view to IT safety and security, performance and scalability. The internally defined quality standards require a high degree of availability and call for intensive support for central components and users. This requires intensive use of system management platforms, especially for network and system monitoring.

Distributed architectures are found primarily in the fields of office communication, document processing/editing and special applications in public administrations. Distributed database, mail and file systems, for example, are often used on department level. Distributed systems require special replication mechanisms and distributed system administration.

Besides the components mentioned in chapter 5.2.1, components which are specifically adapted to the particular requirements of large environments are

recommended for the implementation of the specific technical and architectural requirements.

Concerning the recommendations of the evaluation of economic efficiency in the case of replacing migration for large and medium public agencies, refer to chapters 4.6.1 and 4.8.6.5.
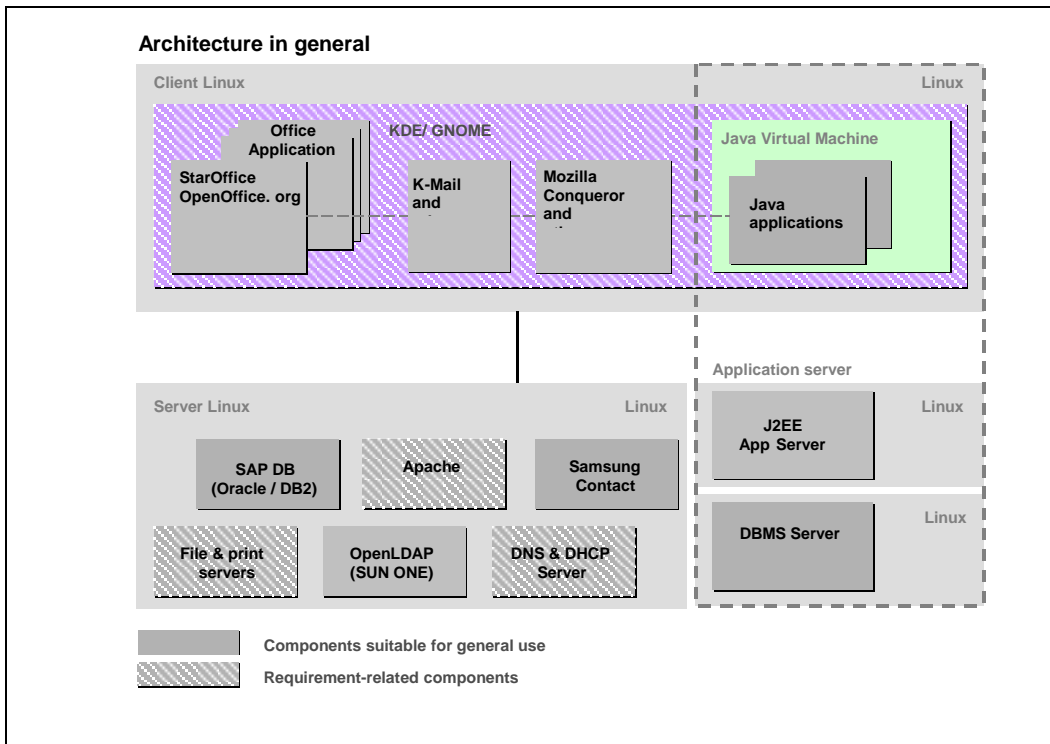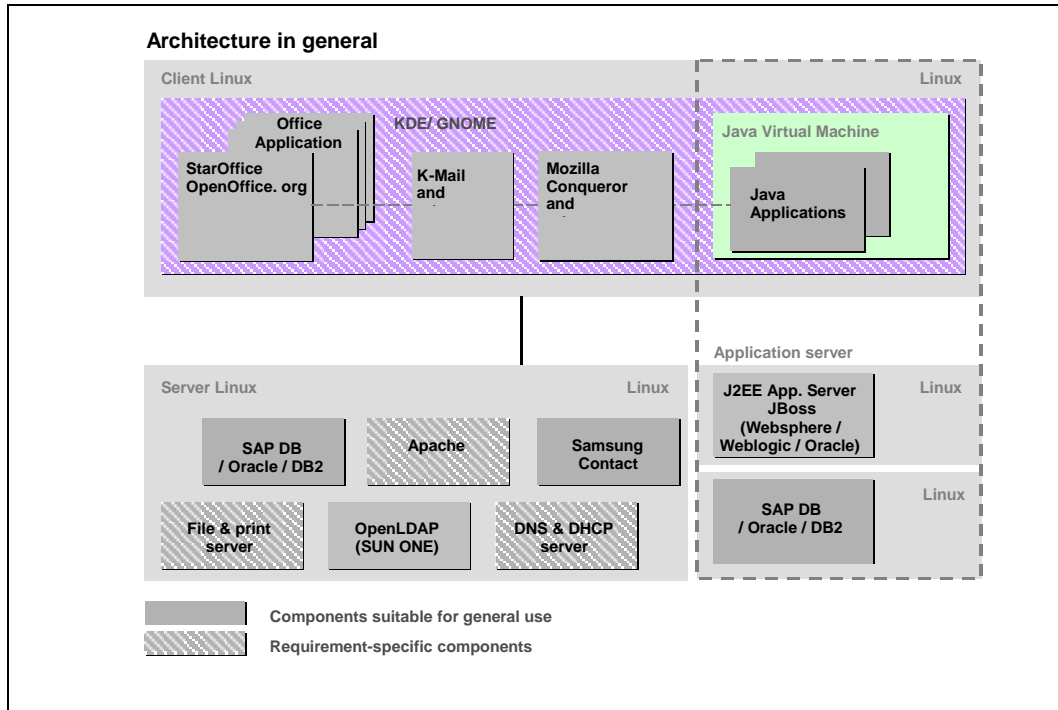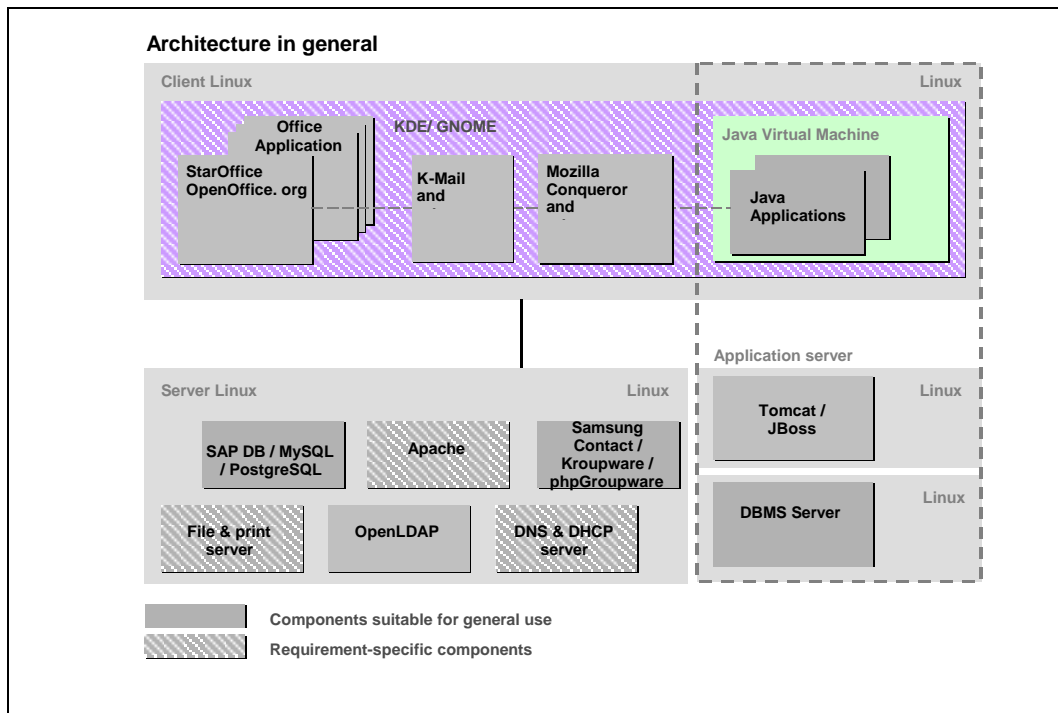

Fig. 78:   IT architecture recommended for a large public agency in the case of complete, "replacing migration"

5.2.2.1   *Database management systems*

The requirements concerning database management system in large, central IT architectures differ, in particular, with a view to increasing stability, performance and security/safety.

Of the pure Open Source database systems, the SAP database is recommended with a view to the requirements of larger administrations. The SAP database is offered by SAP (refer also to chapter 3.13.4) as a certified platform for the R/3 system and its successors, and is used as the core technology in SAP's own products. The functionality includes not just transaction support, but also trigger and stored procedures.

In the event that more far-reaching and/or additional functionalities are needed, the use of commercial standard products for Linux (COLS) is also recommended. Standard products for Linux are today offered by a host of manufacturers. Examples include products from IBM (DB2) and Oracle.

5.2.2.2   Groupware

Samsung Contact (a COLS product) is a Linux-based groupware solution with good scalability for large environments. Thanks to its architecture that comprises several independent components which, in the sense of horizontal scaling, can also be distributed to multiple servers, Samsung Contact is a well-suited product which meets with the special requirements of large environments. Samsung Contact supports not just a single-server installation but also distributed installations at multiple sites and thus offers a scalable solution even for distributed sites.

5.2.2.3   Directory services

Due to their central role for securing the efficiency of system management and IT security, the directory services have a key part to play when it comes to the integration of applications and systems in platforms.

With the increasing importance of authentication services for web applications and due to increased requirements for the user-friendliness of authentication operations, the model of directories (directory services) and meta directories which was already known from the past was supplemented by further components and developed further to an overall system often termed as identity management (refer also to the illustration below).

Directory server	**Identity**
Basic ä Directory servic (LDAP / JNDI)	SS functiona t, Authenticati and authorizati
Meta directory server	**Certificate**
Connecti and of other user	Basic ä Certific servic
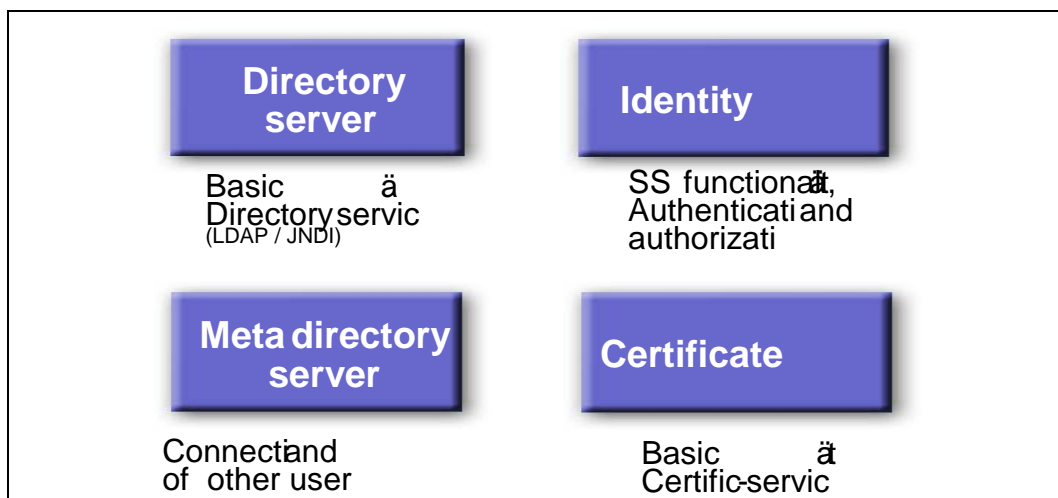
Fig. 79:   Fields of application of directory services using the example of the SunOne platform

Both OSS and COLS products can be generally used to implement directory services. Two major application scenarios are possible in this context as follows:

1. Implementation of basic functions for authentication applications as well as professional management on the basis of the LDAP protocol.

    OpenLDAP as the OSS alternative can usually be considered to be sufficient and economical in this case.

2. Implementation of extended functions for boosting management efficiency, for example, by application-spanning synchronization of user data or authentication.

   One can generally assume in this case that the use of commercial products will lead to advantages compared to own developments in the evaluation of economic efficiency.

5.2.2.4 *System management services*

In view of increased system management requirements, the use of the Tivoli or OpenView system management products should be considered. Besides the commercial solutions mentioned in the foregoing, there are other possibilities to employ management using operating system tools for certain system management tasks (refer to chapter 3.6).

5.2.3 Specialized public agencies with an IT service function

Public agencies which also act as specialized IT service providers within the administration landscape typically operate strongly centralized IT architectures. They often offer their services as computer and data centers and provide IT services for other administrations, for example, as so-called "application service providers" (ASPs). The prevailing central architectures for the implementation of the different special processes (ERP, ...) are often linked to very demanding requirements in terms of performance and scalability of the systems. This is why the hardware systems used are high-quality and partially upmarket hardware systems suitable for automated computer center operation, such as storage area networks (SANs) for data backup and data archiving purposes. These specialist agencies place very high demands on IT security, performance and scalability. The quality standards defined there are usually contractually agreed to with the respective customers and stipulate high system availability and intensive user support. Special system management platforms featuring a high degree of automation are used to ensure effective system management. Furthermore, the computer centers require effective system support in terms of first-level and second-level support, including a comprehensive problem management function.

Fig. 80: IT architecture recommended for a specialized public agency in the case of complete, "replacing migration"

5.2.3.1 Database management system

The recommendations given in section 5.2.2.1 are applicable to the database management systems in this case too. The computer centers additionally require that the systems be certified for certain hardware (SAN) and software as a precondition for their use. Many Linux-based database systems (SAP DB, Oracle, DB2, etc.) are today certified. Furthermore, computer center operators can use certified Linux distributions as the operating system basis for the respective applications.

5.2.3.2 Application server

Application servers are often used for complex application scenarios. Within the special applications, these servers implement complex business processes and rules and, at the same time, access to external systems. The application server must be able to ensure session management for the user. Furthermore, it must offer suitable interfaces with external applications and it must include the required high-availability solutions (cluster, load-balancing, failover). Besides familiar, commercial products (COLS) – such as IBM Websphere, BEA Weblogic, BEA Weblogic, Oracle Application Server and several others – it is also possible to use an Open Source product. The "JBoss" project offers a complete Java application server on an Open Source basis. The application server supports the J2EE specification. It comes with an integrated web server, a JSP and servlet engine, and it supports Enterprise Java Beans, as well as clustering and many other functionalities.

5.2.3.3   *System management services*

In view of partially comparable requirements, the same recommendations are given for specialized public agencies which are also applicable to large and medium public agencies (refer to section).

5.2.4   Small public agencies

Small public agencies usually feature central IT architectures, however, without the character of a computer center, due to their local concentration. Large processes are typically not carried out directly in small public agencies. These services are often outsourced as a lease model and carried out by the computer centers. The quality standards defined within the public agency do not foresee any special requirements in terms of availability and user support (normal working hours). Standard hardware is normally used for backup and archiving purposes. System management platforms are hardly used. The preferred approach is the use of own tools and scripts for handling the agency's tasks. Smaller administrations are characterized by low to medium requirements in terms of IT security, performance and scalability. First-level and second-level support are often combined and usually carried out without support using a problem management tool.

OSS products do not necessarily have to be adapted to the size of a public agency. Scalable products, such as Samsung Contact or SunOne Directory Server, can cover any requirements of smaller public agencies. Any recommendation should, however, consider the fact that large solutions usually require increased installation and configuration efforts and costs.

Concerning the recommendations of the evaluation of economic efficiency in the case of replacing migration for large and medium public agencies, refer to chapters 4.6.1 and 4.8.6.5.

Fig. 81: IT architecture recommended for a small public agency in the case of complete, "replacing migration"

5.2.4.1 Database management systems

A wide range of alternative database systems are on offer in the Open Source area. All the database systems which are discussed in more detail in chapter 3.13.4 are well suited for use within the outlined framework.

Generalized, simple and clear-cut recommendations for SAP DB, My SQL or PostgreSQL cannot be derived from the functional properties. The decision in favor of one database system or another must be made from case to case, always as a function of the planned development and/or runtime environment. However, MySQL constitutes the optimum solution especially with a view to developing database and web applications with PHP means thanks to its deep integration.

5.2.4.2 Groupware

Besides the solution recommended for larger public administrations, the use of the Samsung solution is also conceivable for smaller administrations. Apart from Samsung Contact, the Kroupware solution (refer to 0) can also constitute an adequate basis for smaller to medium organizations in future. The advantage of the Kroupware solution is the deep integration of the GNU/Linux groupware client into the KDE desktop. This means that a solution will be available in future which is subject to GPL and which thus represents an interesting alternative also with a view to the monetary aspect. It should be noted in this context that the "Ägypten" Open Source plug-in, a SPHINX-conforming tool for encrypting and signing e-mails, can be used.

Migration recommendations

Public agencies not interested in offline use of the groupware solution can also use web client access. phpGroupware is also a possible solution in this case.

5.2.4.3 Directory service

The OpenLDAP OSS directory service is recommended for the administration of network-relevant information. The service can, for example, be used for user administration, user authentication, stock-taking of the existing hardware and further infrastructure settings (DNS entries, DHCP configurations, etc.). OpenLDAP offers all the customary and necessary functionalities (refer to chapter 3.7.4) of a full-scale directory service.

5.2.4.4 System management services

The use of the wide range of free on-board tools available under Linux is primarily recommended for smaller administrations. The tools (ssh, cron/at, powerful command line interpreters, utilities and interpreted programming languages) can be used to automate routine jobs to a large extent. Further tools and system administration products are presented in chapter 3.6.

5.3 Completely "continuing migration"

Completely continuing migration means that the Microsoft product line remains in place in all areas. Two starting situations which would justify this form of migration are theoretically conceivable.

However, technical reasons are not the decisive parameters in either of the two situations described below. With only a few exceptions, technical alternatives which can run under Linux exist for each of the requirements discussed. "Continuing migration" is, in the final analysis, motivated by economic reasons.

The first starting situation discussed here was described in chapter 2 of the guide as an NT 4 system environment with Exchange 5.5, MS SQL Server 7, IIS 4 and Office 97 or Office 2000, respectively. It is already characterized by a very high degree of integration. Key parameters for the degree of integration include, for example, the following:

Number of special applications which are available as Windows applications only

Availability of the source codes of such special applications

Integration depth of the individual special applications, especially in the MS Office environment

Extent of use of Microsoft-specific

- development environments

- interfaces

- programming languages

Number of MS Office-specific macros and scriptings (for example, implementation of department-spanning workflows).

The costs and effort needed for replacing migration increase with an increasing degree of integration. A final statement as to which degree of integration justifies continuing migration generally requires a detailed analysis of the components to be migrated in the particular case, as well as a more detailed evaluation of economic efficiency.

In practice, the advancing development of the .NET platform will create a starting situation with such a high degree of integration that will constitute a considerable obstacle to migration. Partial migration at an early stage (refer to chapter5.4) can prevent this development.
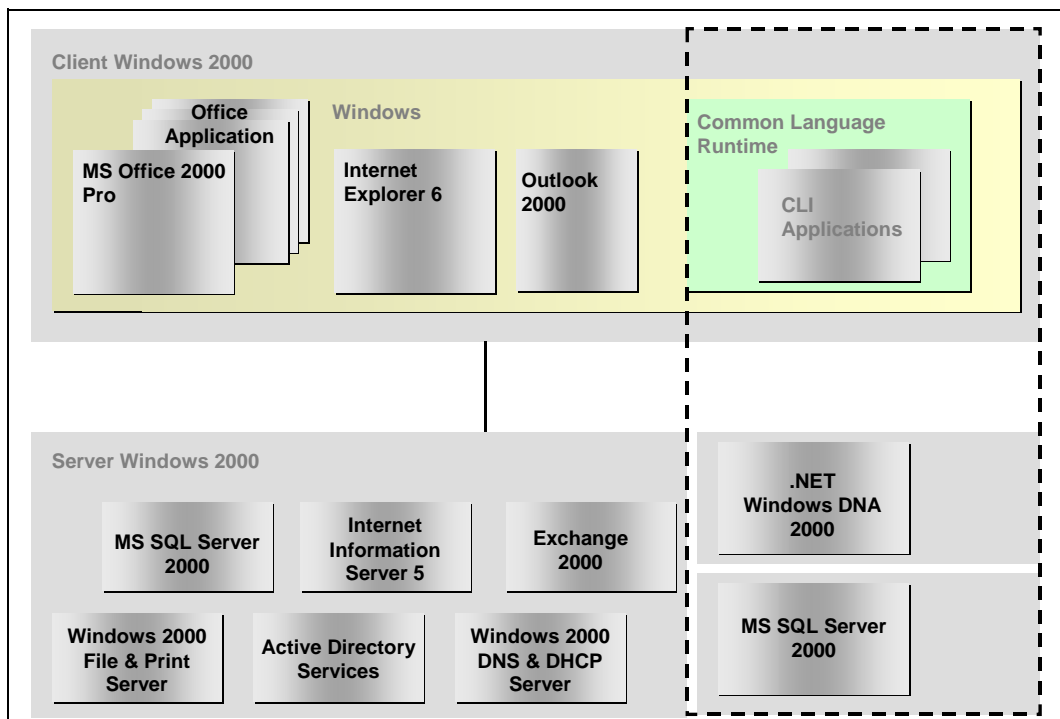
Fig. 82:   Starting situation for continuing migration

The second starting situation considered here describes an IT environment in which complete migration to Windows 2000 and a comprehensive implementation of active directory have already taken place (refer to 82: Starting for continuing migration

). The change was carried out just recently, for example, in the year 2002. With regard to the architecture model underlying the migration recommendations (0), this means that the maximum features of the model are the following:

Workstation computers: Windows 2000 clients with Office 2000

    Web server: Internet Information Server 5

    Database server: MS SQL Server 2000

    Groupware/messaging: Exchange 2000

> Directory service: active directory service
>
> Infrastructure services::
> Windows 2000 Server (Advanced Server)
> (file system, print services and network services)

In the event that individual elements of this architecture are not (yet) in use, adequate solutions can be proposed within the framework of partial migration. Refer to chapter 5.4 for further information and recommendations in this respect.

As far as the above-described starting situation is concerned, the principle of investment protection means that no replacing migration – not even partial migration – can be recommended for components already in use within the next 4 to 5 years.

However, such a starting situation should nevertheless be considered within the scope of the migration recommendations for the following reasons.

> Ways to minimize the above-mentioned degree of integration and hence the dependence on Microsoft products will be described in the following for public agencies in this situation.

> Furthermore, recommendations concerning the future migration paths will also be given to these public agencies as far as this is possible today.

> From a long-term economic perspective, continuing migration is not particularly recommendable, especially against the background of manufacturer-dependence. Continuing migration can make sense especially in cases where the costs of migrating special applications which are based on the Microsoft platform and which would have to be re-programmed in order to be migrated to OS, would be so high that migration to OS is unlikely to be profitable in the long term.

> Concerning the recommendations of the evaluation of economic efficiency in the case of continuing migration, refer to chapters 4.6.2 and4.8.6.6.

5.3.1 Minimizing the degree of integration, protecting degrees of freedom

As already mentioned, continuing migration and the use of Windows 2000, including the active directory, should aim to reduce dependencies on Microsoft products in order to be able to use all options resulting from replacing migration even in the future. The following recommendations should be considered.

Directory service:

> Any use of the active directory should be restricted to an "active directory with reduced functionality" (refer to section 3.7.5).

> The active directory should not be used as an LDAP source for additional applications (such as web applications).

> Personal data of the active directory must be imported from a separate source, such as a MetaDirectory.

If role concepts are planned, software requiring an active directory or having an active directory as its main focus should be avoided.

Desktop

The use of MS Access applications should be avoided. The use of a central database and applications programed, for example, using PHP should be preferred.

The existing VBA applications should be described, analyzed in detail and consolidated if this has not already been carried out during the migration process. New developments in this area should be avoided, wherever possible.

Applications should be selected and application development projects should be initiated with a view to SAGA conformity (refer to chapter 3.8).

Applications from third-party manufacturers requiring MS Office products as the only runtime environment should be avoided, wherever possible. This does not apply to special applications if no alternatives are foreseeable in the medium term.

(Special) applications requiring MS Office products should be gradually migrated.

File system

Reproducibility of the privilege structure must be ensured through the use of scripts (such as Perl). If the graphic user interface is used, detailed and complete documentation of all configurations is mandatory. Since this cannot always be ensured in view of familiar human weaknesses, the script form is the better approach.

Local groups should not be used unless this is absolutely necessary.

Groupware/messaging

Exchange 2000 servers should not be used as central mail routers. OSS products (such as postfix, sendmail) should be used for this purpose in order to secure the option to operate several mail systems parallel.

No applications should be used in public folders of Exchange.

Web applications

Microsoft products should not be used with a view to SAGA conformity and the large number of alternatives (refer to chapter 3.9).

Domain authentication should be avoided through the use of a second authentication instance. An additional password is usually acceptable and can be justified, first and foremost, by security aspects. A variety of OSS products can be used in exceptional situations.

Systems management

The use of products from third-party manufacturers which also support Linux (such as Tivoli) should be preferred.

Network services

OSS solutions should be given preference for the DHCP and DNS network services.

Middleware

Deep integration with SAGA-conforming standards should be chosen for application developments in order to increase reusability.

XML and web service technologies should be used for communication and data exchange with external systems (unless security aspects prevent this; refer to chapters 4 and 5).

5.3.2   Further migration paths

With a view to further migration, migration of the workstation computers to Windows XP will be discussed first. The principle of investment protection is applicable in this case too. In light of this, migration of the workstation computers to Windows XP cannot be recommended already for this reason alone with the stating situation described in the foregoing.

Considering aspects of investment protection, further migration will be conceivable in 4 to 5 years at the earliest. This means that, given migration in 2001, the next change could not take place before 2005. Especially those public agencies that have adopted the above-mentioned recommendations for reducing their dependence on Microsoft products, will then have to check in light of the then prevailing technical and economic conditions whether replacing or continuing migration is to be carried out. The same is also applicable to any other public agencies which are in the same starting position.

5.4   Partial migration

5.4.1   Selective migration

Selective migration means the permanent replacement of a selected Microsoft product by an OSS or COLS solution with all other products being subject to continuing migration. The following section will outline cases of sensible and feasible selective migration.

The most important selective migration concerns the replacement of Exchange 5.5. One reason for this replacement is the fact that, according to the current state of information, Microsoft will discontinue (mainstream)[194] support for Exchange 5.5. The alternative which Microsoft offers within the scope of continuing migration is Exchange 2000. However, continuing migration to Exchange 2000 is not possible for many public agencies because this solution specifies the use of an active directory as a mandatory component. With

---

[194] http://support.microsoft.com/default.aspx?scid=fh;en-us;lifesrvr

Exchange 2000, Microsoft has externalized the previously internal directory service of Exchange 5.5 and developed the active directory on this basis, making it the core of the Windows 2000 world. This means that Exchange 2000 requires Windows 2000 Server or one of its successor products.

Many public agencies are hence profoundly interested in an adequate, alternative groupware/messaging solution which offers a comparable or identical functionality, which does not require an active directory and which permits the continued use of MS Outlook as a client.

Several different alternative solutions are available in this context (refer also to the illustration below). In the case of more demanding compatibility requirements, two solutions are primarily suitable candidates for different requirements, i.e.:

Samsung Contact

Exchange4Linux

Thanks to the good MAPI connection, both solutions enable the continued use of the Outlook client with its most important functions. For a more detailed technical discussion and a comparison of functionalities, please refer to the "Technical descriptions" chapter. A model calculation of the economic efficiency in the case of a migration to Samsung Contact can be found in the "Evaluations of economic efficiency" (refer to chapter 4).
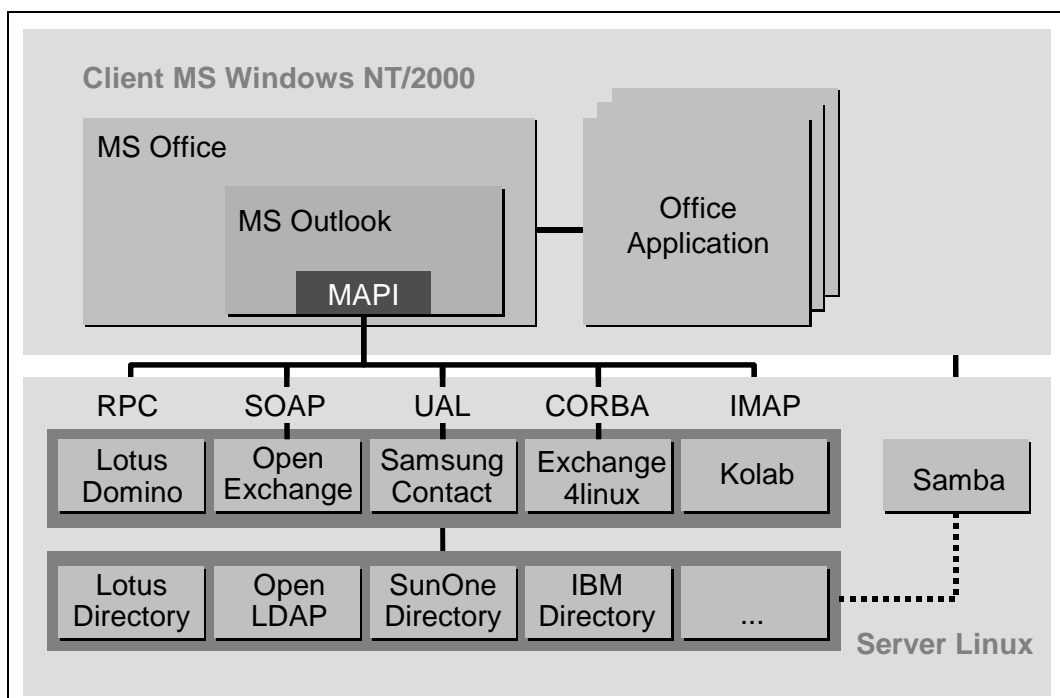
Fig. 83: Different variants for replacing Exchange with partial migration

Samsung Contact, just like Exchange, is no OSS, but constitutes proprietary software which belongs to the COLS category. Migration to Samsung Contact was already discussed in the recommendations concerning complete "replacing

migration" (refer to chapter 0). Samsung Contact is particularly suitable for large and specialized public agencies with special requirements concerning scalability and failure safety.

The lower-priced Exchange4Linux solution can also be recommended for public agencies with up to 500 users. This is primarily an OSS solution. The server component is available as free software. Only the MAPI Connector is a proprietary product which is exclusively available against payment. For more details, please refer to chapter 3.14.4.

Both solutions require Linux as the operating system at the server end. Selective migration offers a number of advantages as follows:

The scope of the migration project is clearly defined and can be well planned.

Necessary adjustments are limited, so that project planning and steering offer crucial advantages.

Operating concepts and experience with a new operating system platform can be developed step by step.

Training is necessary for administrators who are actually involved in the subject. In this way, the newly trained administrators can also serve as multipliers within the IT department.

Another aspect to be mentioned in conjunction with groupware and messaging is that the exclusive migration of the mail functionality is significantly easier in cases where the groupware functionality is not needed. This is, in fact, a tried-and-tested and hence preferred solution.

Another way of selective migration is to replace MS Office by OpenOffice.org or StarOffice. The above-mentioned functional restrictions and especially economic consequences must be considered in this case. An Office migration was already discussed in the chapter on complete "replacing migration" (0).

Concerning the recommendations of the evaluation of economic efficiency in the case of selective migration, refer to chapters 4.6.3.1 and 4.8.6.7.

5.4.2   Partial migration at the server end

The example of wide-spread server migration will be used in the following in order to introduce a sensible and recommendable scenario for partial migration at the server end. The Windows NT environment described in chapter 2.2.1 is assumed as the starting situation.

The recommendations made in conjunction with complete migration (refer also to 0) are, in principle, also applicable to broad migration at the server end. The differences are due to the fact that the client end continues to consist of Windows-based systems.

The recommendations for:

Database system

Web server

Network services

can also be found in section 5.2.

The central requirement for migration at the server end is smooth interaction between the Linux-based server systems and the Windows-based client systems after migration. The probably most important requirement for the migration process itself is the replacement of the file system, print, network and authentication services, including migration of existing file and privilege structures and the import of configuration data.

The evaluation of economic efficiency suggests that around 65% to 80% of the project costs are set off by savings. Personnel costs for changing work account for the balance, i.e. for the costs exceeding the savings. This means that a direct monetary advantage normally does not exist with this form of migration compared to continuing migration. However, soft factors in terms of the criteria for urgency and strategy are likely to be relevant for a project decision.

Concerning the recommendations of the evaluation of economic efficiency in the case of broad migration, refer to chapters 4.6.3.2 and 4.8.6.7.

5.4.2.1   User administration and authentication

A Linux-based Samba server in conjunction with OpenLDAP is recommended as a replacement for a Windows NT 4.0 domain controller. Samba is capable of representing a largely complete Windows domain controller under Linux. Especially the forthcoming Samba version 3.0[195] which was already successfully tested within the scope of the migration project at the German Federal Cartel Office offers almost unrestricted connection of Windows 2000 and Windows XP clients. For more details, please refer to the technical descriptions in chapter 3.

5.4.2.2   File and print services

As already explained, Samba is the sole product for file services to be considered for the smooth integration of the Windows clients. Samba is capable of representing the most important functionalities of a Windows NT-based file server under Linux. The users of Windows clients can also obtain their user profiles and log-on scripts as well as their home or group directories from a Samba server. The XFS and EXT3 file systems are recommended for the physical storage of data on the disk systems of the real server systems. Both file systems (refer to 3.2.3) support POSIX-ACL, journaling functionalities and quotas.

The print services should be implemented via CUPS in conjunction with Samba. CUPS is perfectly integrated into Samba.

---

[195] Not yet released nor fully developed and tested.

5.5   Migration paths

5.5.1   One-step migration

This section outlines the reasons for one-step migration and analyzes the starting situations for which one-step migration is recommended.

One-step migration is the opposite of gentle migration. Both migration paths are headed for complete "replacing migration", i.e. both paths are aimed at the implementation of a purely Linux-based system environment.

One-step migration is characterized not by its speed but by the fact that it takes place in one step within a shorter and, above all, defined period of time. One-step migration has a defined beginning (commencement date) and a defined end (end date). It is concluded by the commencement of full-scale productive operation of a purely Linux-based IT landscape.

One-step migration places high or even very high demands on:

Project organization

Organization of the public agency concerned

Hardware

Finance

Administrators

Users

The requirements for administrator and users, in particular, should not be underrated. This is the more valid the more limited know-how is concerning the new IT landscape on the part of administrators and users. One-step migration, however, also offers the advantage that administrators do not have to handle two different IT orientations over a longer period of time. Within a relatively short period of time (in line with the requirements of the given project), they can fully focus on the new systems.

Another important requirement is that the necessary funds must be available within a relatively short period of time. In the final analysis, the scope and, above all, the complexity and diversity of the applications and systems to be migrated determine when funds must be made available and to what amount. This aspect will be a co-determining factor with regard to the feasibility of one-step migration.

The high requirements for the organization of the public agency focus on the qualification of staff who must continue doing their daily job on the one hand. This means that disruption of operations of the public agency must be minimized. Ongoing IT operations must continue on the other hand. A change in the complete server landscape places particularly high demands on all the parties involved because migration of the individual server services cannot be randomly partitioned and because administrators must guarantee ongoing operations whilst at the same time being trained in the new systems.

These requirements can be addressed by suitable change and rollout concepts. It is also possible to set up a parallel IT landscape, even though this means increased demands on hardware and additional costs.

These demanding requirements inevitably raise the question as to whether one-step migration makes sense at all and/or for whom it makes sense and to whom it can be recommended.

Reasons for one-step migration are the following:

Migration is inevitable, for example, because support for the legacy systems is phased out.

Administrators and users are faced with a far-reaching change, but only once rather than every year anew.

Administrators do not have to handle the complexity of heterogenous worlds over extended periods of time.

Under which conditions and for whom does one-step migration make sense?

A system landscape with a clear-cut configuration and not too many interdependencies is a good precondition for one-step migration in the first place. This means that only a few applications and services are used for task fulfillment. This does not necessarily mean that the administrations and organizations concerned are small or have simple structures. This may, for example, also apply to public agencies and organizations with security functions where most users depend on a few, complex specialized applications which are mostly server-based and which are used to do most of the work. However, it may also apply to small and medium public agencies with a few specialized applications, standard office documentation and the use of Office programs with a small number of complex documents and templates (such as the Commission of Monopolies).

Public agencies where administrators already have the necessary know-how also offer good preconditions for one-step migration. Be it because administrators there use Linux-based systems privately or because individual Linux-based applications and services (such as mail server on Linux) are already officially in use at these agencies. If staff are additionally open to new developments and interested in Linux, this is another ideal precondition for one-step migration.

5.5.2 Gentle migration

This section discusses the reasons for and the ways to gentle migration. But what does gentle migration really mean? Gentle migration is an approach where the target is clear but where the time frame is defined only very generally, with the migration processes taking place component by component on the basis of the architecture model described in the foregoing.

The reasons for gentle migration become clear when we look once again at the requirements and reasons for one-step migration.

Migration recommendations

Public agencies and administrations with tight budgets can distribute the necessary costs to the respective budget situation.

Lacking know-how can be developed gradually, so that costs can be saved. Gentle migration enables individual components to be set aside. The administrators, once trained, subsequently act as multipliers, so that a higher level of know-how is available at the time the next component is to be migrated.

Existing barriers and reservations can be gradually removed.

Complex IT structures can be unraveled piece by piece.

The illustration below show a possible gentle migration process.
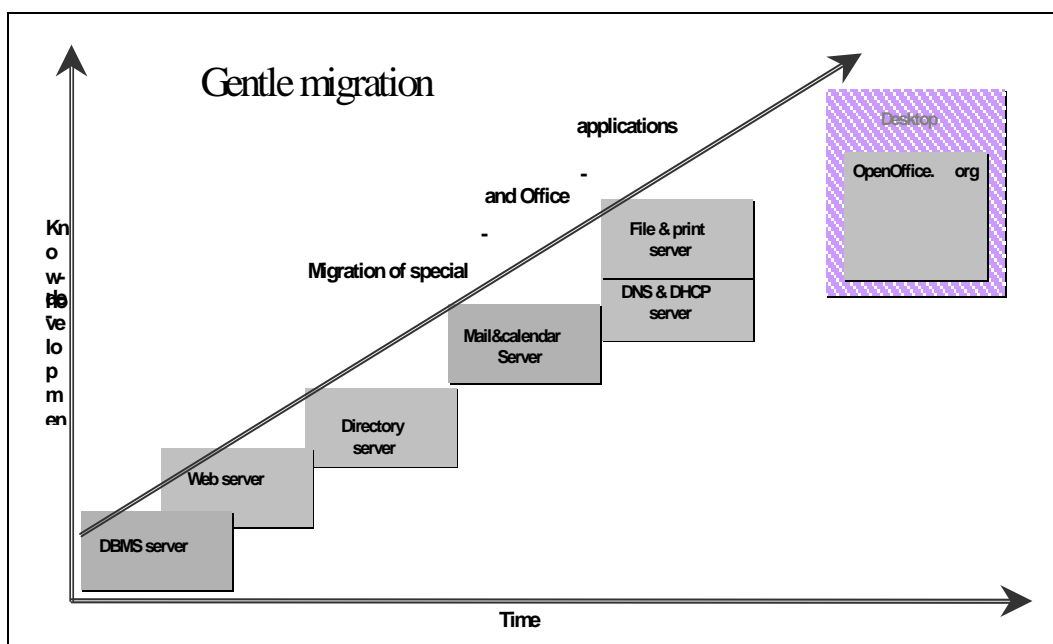
Fig. 84:   Gentle migration

A component which should be easy to single out should be chosen as the first component to be migrated. This is the DBMS server in the example above. The task is not the migration of the database applications but the establishment of a parallel DBMS. Basic DBMS knowledge is assumed to be available, with a DBMS being required during the first migration at the latest, i.e. when the web server is migrated. Although the directory server is initially a stand-alone component, it may already be possible to use it in conjunction with the web server and it may be a precondition for the subsequent groupware migration phase. Migration of the file, network and print services follows. Finally the desktop is migrated after all the specialized and Office applications were migrated in the background parallel to the component migrations.

In the case of gentle migration, it is not possible to randomly exchange and move the components for the individual steps. What belongs together should be left together. Another important aspect is not to overstrain the time schedule and to

fix a realistic deadline. On the other hand, the implementation time must reflect the complexity of updating and upgrading tasks and hence the administrators' job. As administrative requirements in a varied IT landscape are higher than in the case of a homogenous landscape, the entire change process should not include more than 2 to 3 change phases with a generally realistic time horizon even in the case of gentle migration.
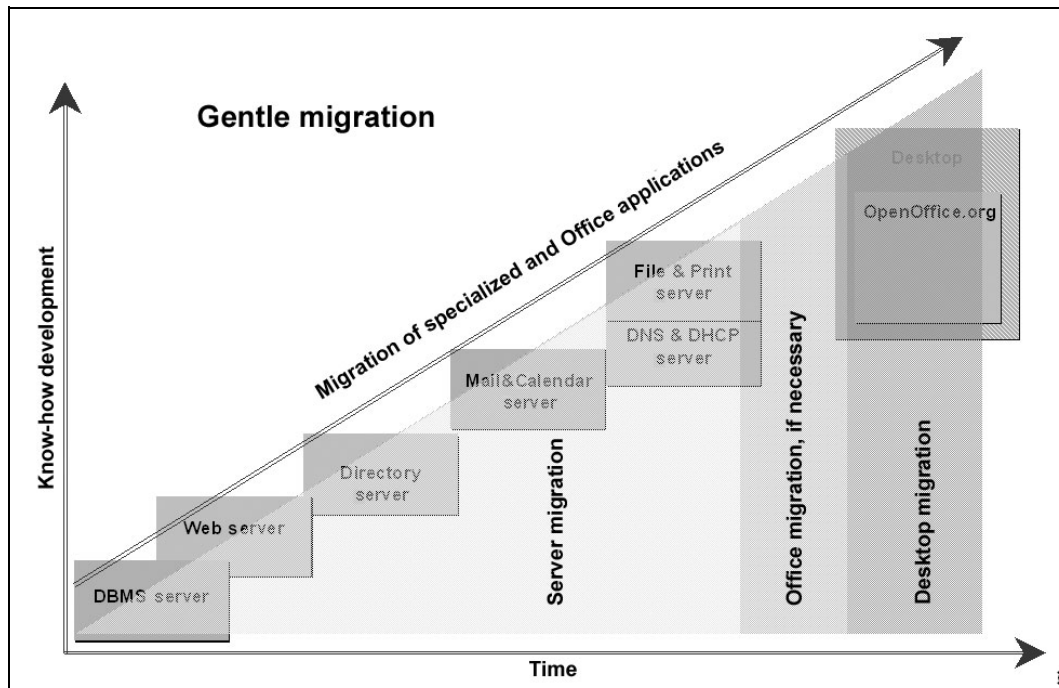
Fig. 85:   Change phases with gentle migration

shows the three migration phases. Migration can then be carried out to a relatively far-reaching extent in a heterogenous environment, especially with the help of Samba, terminal services and the possibility to continue using Outlook as the groupware and messaging client.

At the very end, after all the specialized and Office applications have been migrated parallel to this process, migration of the desktop – i.e. migration at the client end – to Linux can be carried out. On condition that the migration of the specialized and Office applications permit this, one might even consider migrating MS Office to OpenOffice.org or StarOffice on a Windows client in an intermediate step.

5.5.3   Critical success factors

Migration projects are usually complex and involve many aspects. This applies to both complete migration (clients and servers) and to partial (servers only) or selective migration projects. The illustration below shows the multi-phase migration process with its various sub-aspects.

Migration recommendations
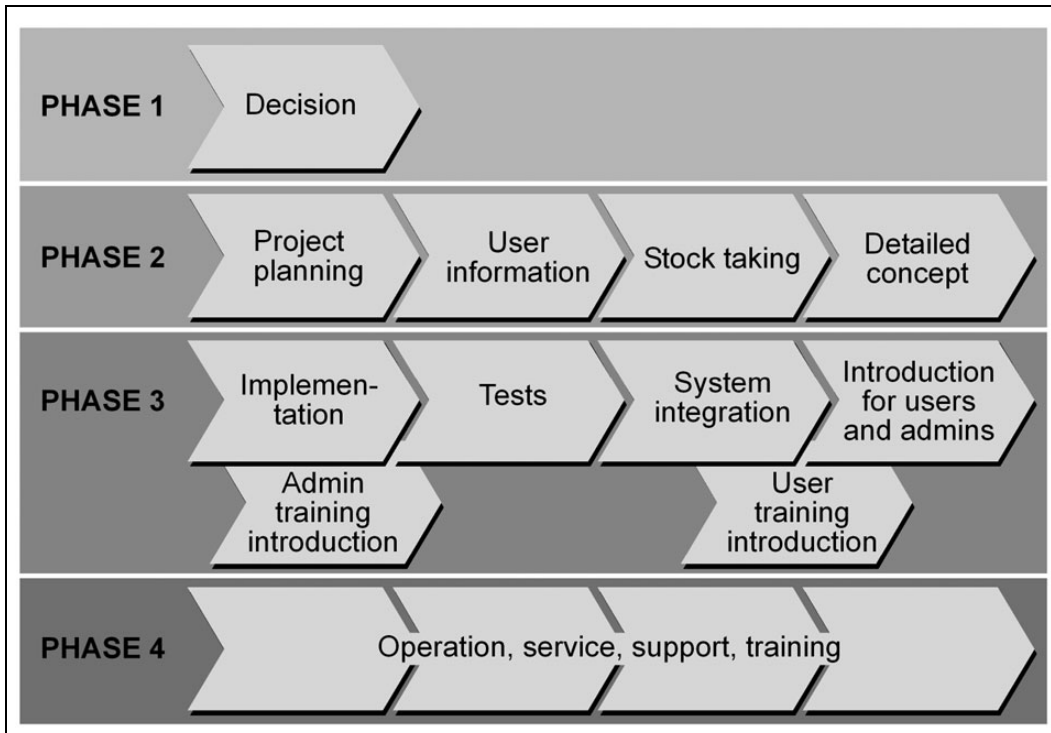
Fig. 86:   Model: gradual migration process

In order to ensure that migration projects as IT projects in general and as innovation projects in particular can be concluded successfully, the factors critical for success must be identified and evaluated well in advance. A migration project is first and foremost a success for all those involved if the desired aims and results are achieved within the planned and agreed time and budget frames.

Furthermore, the contribution of so-called soft factors towards success should not be underestimated. These factors include, for example, staff satisfaction, smooth communication and hence avoidance or reduction of failure, frustration and double work as well as the demand-conforming selection and, of course, acceptance of the new IT landscape by its users.

Irrespective of the size of a public agency and irrespective of the nature of the migration project – i.e. replacing or continuing migration – the parameters which are summarized below contribute, in the authors' opinion, towards the sustainable success of a project.

Identification of clear-cut aims for the migration project

Involvement and positioning of management and decision-making level

Early information and involvement of target groups / staff

Creating a high degree of user acceptance for the target environment

Structured time, project and resource planning, including project controlling

Organizational measures to prepare the migration process, and establish a qualified project team

Detailed stock-taking, including a definition of functional requirements

Optimum project and service selection

Well-timed, sustainable training

Quality management and documentation

A look at the success factors suggests that migration projects do not end with the purchasing and implementation of the required components. Further dependencies and activities must be considered both before, during and after the real migration project.

Migration projects can only be regarded as successful and economically efficient if, besides minimizing operating costs, they also improve work procedures through state-of-the-art, integrative and functionally target-orientated information and communication support and if they lead to a general increase in flexibility and efficiency of and responsiveness to present and future tasks. Further aims, such as manufacturer and/or platform-independence, are central aspects which must satisfy the parameters of an evaluation of economic efficiency.

The following sections will discuss the most important success criteria identified for migration projects in more detail.

5.5.3.1   *Identification of clear-cut aims*

The identification of clear-cut aims is the basis for any project success. Strategic management aims (motivation level) and aims at the server migration level (implementation level) must be distinguished in this context. The underlying reasons for migration must be laid down in a first step, followed by a definition of what migration is expected to yield in another step.

Prior to commencing the project, the aims of the migration project must be explained to those concerned, to the management of the public agency and to the partners to be involved This definition of aims is the basis for any further action, for the project design and for selecting the target software, as well as for selecting the internal and external partners to be involved. Achieving a certain degree of manufacturer and/or platform-independence is hence a rather general aim.

Depending on the particular agency concerned, the following detailed aims can, for example, exist at the server migration level.

Server migration without adaptation and modification of clients (complete import of data, user profiles, file and directory structures, including the existing access privileges)

Complete migration of clients (equivalent replacement of applications and functions, and integration into the legacy computer network of the public agency without affecting the network)

Migration of data and data structures, leaving the database applications in place (with a corresponding selection of free database systems)

Replacement of existing applications on workstation systems with equivalent applications (implementation of an easy-to-use, central system administration; consideration of the IT security components according to Bund Online 2005, such as PKI, authentication via certificate and biometric characteristics)

Creation of an adequate replacement system for user administration and authentication

Smooth conversion of format templates

5.5.3.2 Involvement and positioning of management and decision-making level

The management and decision-making level is the level where key decisions for the migration project are made without being directly and actively involved in the project work. Project management reports to this level. How this level is defined in detail depends on the situation of the particular public agency and on the priority of the project within the public agency.

The role of the management level for project success is often underestimated. It is an empirical fact that people tend to believe that people at management level "know little or nothing about information and communication technology". At the same time, people then also believe that the management of a public agency "only" has a primary interest in having a "functioning and affordable system" in place. However, such a notion is contra-productive. In contrast, the management and decision-making level is responsible for defining agency-specific aims for the migration rather than for the establishment and implementation of the project. The management of a public agency is usually also responsible for amending and revising existing contracts as a result of such a project.

First of all, the migration project has to be launched. For this purpose, managers must define a project mission on the basis of identified deficits and/or concrete project aims (for example, achieving manufacturer and platform-independence) or recognize the need to define a project mission on the basis of requests by subordinate staff.

Communicating the project as a management decision

The management level contributes significantly towards the success of the project by making it clear to all those involved in the project and to staff as a whole that management supports this project initiated by it and that management not only monitors all phases of the project during all of its phases, but also actively supports the project.

Timely and active information for staff

Responsibility for staff communication and motivation is another clearly defined, central management task which begins and which must be carried out even before a migration project actually starts. Leadership takes place via communication, so that leadership and communication styles are inseparably connected, requiring a particularly high degree of social competence. This means that the projects planned must be made transparent to all members of staff and to

all those involved. Both the areas to be changed and the areas to be left unchanged must be identified. (For example, changes to be anticipated and elements to be left unchanged can be precisely described on the basis of the existing operating concept).

Furthermore, different communication channels should be used in order to disseminate information, such as general information meetings, talks with staff, workshops or circulars and announcements, also using the public agency's intranet (avoidance of rumors). Ways and means to respond to questions and suggestions, as well as concerns and fears of staff related to change must be established at an early stage. Personnel representatives and representation bodies must also be involved in the overall process on a timely basis.

Provision of the required funds

The management level must ensure that the funds (non-personnel and personnel) required for the different work packages and for those involved are available when the project commences. Such costs include not just the pure investment and license costs, but also costs for training, external consultants and project support as well as internal personnel costs, for example. Furthermore, adjustment of the required funds may be necessary depending on the progress of the project.

Acceptance of intermediate and final results

A clearly defined division of responsibilities exists between management level, project management and project group members. The decision-makers must make and justify the key decisions at the end of the different project phases on the basis of the documentation prepared by the members of the project group. Changed conditions may require modification of given strategic aims.

5.5.3.3 *Creating a high degree of user acceptance for the target environment*

Migration projects can only make sense and can only be a success at staff level if benefits can be clearly identified and communicated as being sensible and necessary. These benefits are derived from the definition of aims.

The staff concerned should be convinced of the benefits of the migration project in order to support and introduce the project in the individual departments and throughout the entire public agency. At the same time, the limits of open source should be clearly communicated, and the reasons for introducing open source should be explained.

The aim is to ensure a high degree of acceptance and hence motivation and satisfaction among staff. What must be prevented is that unsatisfied staff (people lacking information, motivation or qualification due to a lack of training) jeopardize the overall success of the migration project and communicate failures, if any. In the long term, this could affect the efficiency and performance of the public agency in general. Besides the "compulsory exercise" of ensuring ongoing information even beyond the project term, those responsible should also perform

the "voluntary exercise" of ongoing success monitoring with regard to staff satisfaction in order to be able to take remedial measures, when necessary.

Although the development of concepts and the sustainable implementation of measures is initially a management task, this can only be developed, implemented and, of course, improved on an ongoing basis together with staff. External support, advice and coaching may be a sensible additional means during the initial phase.

5.5.3.4   User and administrator training

As far as training is concerned, administrators must be integrated at an early stage and future users on a time-near basis. A target-group specific training concept must be developed, considering both existing skills, experience and qualifications as well as the future job-specific use of the components. This also concerns user training at the place of work as well as ongoing training, especially for administrators and user support staff in the field of open source software. Furthermore, experience from pilot projects or other migration projects should be actively integrated into the training concept in order to make use of lessons learned. Further concrete measures include the implementation of test and simulation environments, emergency drills, backup and recovery.

This is all the more important if existing skills and experience do not exist or are limited and if ongoing or demand-oriented support is no longer available once the migration project is completed.

5.5.3.5   Organizational measures for preparing the migration process

Establishment of a project group

Typical migration projects are carried out by several people rather than by a single individual. In the interest of successful completion, such projects should have a defined term and clear-cut aims. These are the characteristics of classic project work, with the establishment of a project-oriented organization being recommended.[196]

On this basis, it must be checked whether and to what extent the existing organization structure which is typically process-oriented is still a suitable organization form and adequate for the project. If necessary, the organizational frame of reference must be changed on a temporary basis and the parties involved – apart from the public agency's organization structure – must be given a new organizational framework as members of the project group. Work processes, interfaces, products and resources must be identified and defined in advance with the participation of those involved in the project. The following principles apply to this exercise:

  Project organization is more important than the agency's organizational structure

---

[196] Refer to Federal Ministry of the Interior, "Handbuch für Organisationsuntersuchungen in der Bundesverwaltung" Bonn, 5th edition1988, pp. 23 and following

Clear definition of tasks and responsibilities

Temporary reduction or transfer of routine jobs

Definition of communication and reporting lines

Any plans and measures must be critically evaluated with a view to the extent to which they support the achieving of the project aim from an organizational view. In cases of doubt, priority should be given to those measures which offer a higher support potential.

Project group members

The project manager and the members of the project group are crucial for the success of a project. Even with otherwise favorable conditions, an unsuitable composition of the project team can lead to an unsatisfactory project result, whilst a high-level team can generate acceptable results even under adverse boundary conditions. This is in contrast to the occasional opinion that "nobody should be irreplaceable".

The project manager: The project manager bears the overall responsibility for a project. He coordinates, organizes and communicates the overall project work in order to ensure that the project will be implemented correctly, on schedule and in line with its budget. The project manager is responsible for setting targets and milestones and for monitoring their compliance (including reporting to the steering committee, if applicable).

Depending on the size of the public agency concerned and the nature of the migration project, it may be advisable to appoint further sub-project managers in addition to the project manager.

The project group: The members of the project group develop the project contents and implement the individual phases and stages of the migration process. These are the administrators in the first place, as well as selected users and, if necessary, external specialists (people with experience and practical expertise, advisors).

Involvement of external advisors

Public agencies too are increasingly making use of support by external advisors for projects. Reasons [197] for the use of external expertise include:

Professional, unbiased problem analysis

Time-efficient, target-oriented project management

Ongoing communication on the project with effective progress and result checks

Convincing, well-prepared (meeting) management, presentation and result documentation

---

[197] Federal Ministry of the Interior, "Handbuch für Organisationsuntersuchungen in der Bundesverwaltung", Bonn, 5th edition 1988, pp. 37 and following

Transfer of know-how with regard to the preparation and implementation of complex IT and migration projects.

Definition of the project-specific organization form

The adequate form of organization for the migration project must be set up as a function of the size of both the migration project and the public agency. The project organization in this case represents a parallel organization that does not interfere with the existing organization structure and has a term limited to the term of the project. The establishment of one of the three organization options described below is recommended, depending on the given tasks and aims.

Line project organization: The members of the project team are delegated by existing organization and form a separate organization unit led by a project manager. This leads to increased identification with the project and the members can concentrate fully on the project. At the same time, however, these people are not available to their departments which can lead to different workload levels (overload) for staff. The line organization should be adopted in the case of large and difficult projects.

Staff project organization: The project is managed by a project coordinator who, as a staff unit, has no formal decision-making powers and hence limited responsibility. The project team members remain members of their respective departments and only meet at project meetings. This makes the staff project organization susceptible to disruption and inefficiency.

Advantages of this form of organization are limited organizational requirements (the only new member to be found is the coordinator) and flexible staff workloads (work on the project and in the department). Furthermore, several projects can be underway at the same time. This form of organization is generally suitable for smaller projects only because coordination requirements are otherwise too high.

Matrix project organization: In the case of the matrix project organization, a horizontal command line is introduced in addition to the existing hierarchical structure. As far as the contents of the project are concerned, team members report to the project manager, whilst their line superiors continue to be their superiors in personnel and disciplinary matters. Projects of this kind are complex and require substantial coordination efforts.

The advantages are due to the fact that necessary resources are only used when actually required. In contrast to the staff project organization, the project manager has decision-making powers and is authorized to issue orders.

Disadvantages are due to the fact that the members of the project team "serve two masters". Conflicts with regard to resources or due to conflicting orders can arise, especially if several projects are underway at the same time.

Summary and evaluation of the forms of project organization for migration processes

The table below can serve as an orientation guide when it comes to selecting the appropriate form of project organization. However, adaptation to the particular conditions of the specific public agency is still necessary.

Table 78: Proposed summary of forms of project organization

	Complete migration	Partial migration	Selective migration
Small public agency	Line organization	Staff organization	Staff organization
Medium public agency	Line organization	Matrix organization	Matrix organization
Large public agency	Line organization	Line/matrix organization	Matrix organization

Small public agency: staff of up to 300; medium public agency: staff of up to 1,000; large public agency: staff of 1,000 and above.

5.5.3.6   Involvement of selected user circles

Within the scope of project preparations and depending on the complexity of the migration project, it must be decided at organizational level which user groups are to be actively involved in the migration project and which user groups are to be informed only. This means that users can be actively affected by the change process depending on whether full, partial or selective migration is concerned. If, for example, the servers are replaced within the scope of partial migration, it is usually sufficient to inform users, whilst active involvement on the part of users is not necessary in such a case. Office migration, in contrast, definitely requires active involvement and support from the users concerned.

5.5.3.7   Determining the starting situation

Another crucial success factor is the precise analysis of the starting situation. This is usually quite time-consuming, requiring both manpower and time. Furthermore, the determination of the starting situation is also the basis for identifying the functional requirements for the target systems. Important facts to be considered in this context include, for example, the following:

Databases and data structures

Documents and document formats

Applications and their interfaces

Available functionalities

Availability of data and applications

Shortcomings and problems

...

5.5.3.8 Covering functional requirements

The target software should cover (to the largest extent possible) existing functionalities and requirements. It must meet with objective evaluation standards. A worsening compared to the starting situation is hardly acceptable.

The description of the starting situation is the first step towards identifying functional requirements. Within the framework of an early survey, the concrete demands and requirements applicable to the individual components must be identified from the point of view of both users and administrators. These demands and requirements must then be checked and compiled in a list of requirements or priorities. This approach also includes a critical evaluation as to whether existing functionalities are necessary and reasonable. The criticality of lacking or incomplete functionalities must, in particular, be evaluated and considered within the framework of the selection criteria. Lacking functionalities in the target environment can affect user acceptance, depending on the degree of criticality. This can serve as a basis for comparisons to the available software components, so that the target software suitable for the given demand can then be selected in another step.

The degree of fulfillment of the individual requirements will serve as the yardstick for measuring the success of the overall project.

5.5.3.9 Use of empirical values

The use of empirical values from multiple public agencies with Linux migration projects is another key success factor. This is all the more important because experience in this area is still relatively limited (from a historical perspective). The use of active experience from pilot or other migration projects and integration into planned projects will benefit both administrators and users alike. The establishment of a project database is one measure which can be recommended in this context.

5.5.3.10 Project, time and resource planning

The methods of classic project work are applicable to the migration from Microsoft software to system environments characterized by open source software.

Project plan: Project work starts by drafting a project plan that describes the way to the target and can be understood by third parties. The project plan contains as a minimum the following information: deadline, material and human resources, involvement of external partners, milestones and costs. The project plan is also the basis for effective project management.

The following subjects are worked out within the scope of the project plan:

Who is involved?	Project organization
When must things be done?	Time schedule
How are things to be done?	Project structure

What is to be done?	Jobs
In order to ensure	Costing
the quick and safe	Project strategy
success of the project	Pre-clarified order

The results achieved are documented in the project manual.

Time schedule: The time schedule is used to break down the project in more detail. Such a binding project time schedule ensures that realistic dates and deadlines are set for the individual work packages. The project time schedule depends on the final date specified in the project order. Furthermore, the project time schedule also specifies the beginning, milestones and the completion dates of the individual work packages. The project time schedule also serves as the basis for effective project management and project monitoring.

Cost and resource plan: A cost estimate is carried out in order to reach conclusions as to which inputs (measured in man-days) and resources are likely to be necessary in order to achieve the agreed result. Inputs (depending on the work contents) and time (depending on work intensity) must be differentiated in this context.

The following cost types should be considered when the individual inputs are planned and estimated:

Personnel costs (human resources multiplied by cost rate)

Involvement of the community in migration projects towards open source environments

Resources for establishing and operating test environments

Material costs (consumables, such as printing and paper costs)

Hardware costs (equipment or software to be purchased)

Other costs (travel costs, external services)

Purchasing and license costs

Service, support and training costs

5.5.3.11 Project controlling and management

The project controlling function is an important part of the project organization. Controlling is not limited to pure cost and time monitoring. Especially in the context of IT projects, controlling does not mean retrospective revision but instead preventive intervention as soon as deviations from the planned values are foreseeable in order to ensure that the project aims are adhered to in terms of quality of the final products, completion date and costs of the project work.

5.5.3.12 Documentation and quality assurance of the project

Even during the course of a project and, above all, after its completion, the individual work steps must at all times be understandable for third parties who

were not involved in the migration process. This is a vital precondition for the subsequent maintenance of the system. The following media are available for documentation purposes:

Configuration manuals

User manuals

Training documentation

Inventory lists

Project manual

Logs / status reports

Quality assurance and/or test report

Final documentation

Quality inspection is not limited to checking and evaluating the system design, but must also address issues related to the analysis of potential mistakes and errors as well as the assessment of their consequences during each phase of the project. These error analyses must be documented in the same manner as any other project work.

The establishment of test environments, for example, was found to be one success factor within the scope of quality assurance in pilot projects.

The overall quality assurance area is a separate field of activity in large projects. Depending on the scope of the given project and staff qualifications, the project manager or a project controller can handle this function as part of their other tasks.

The illustration below shows the internal quality control steps.
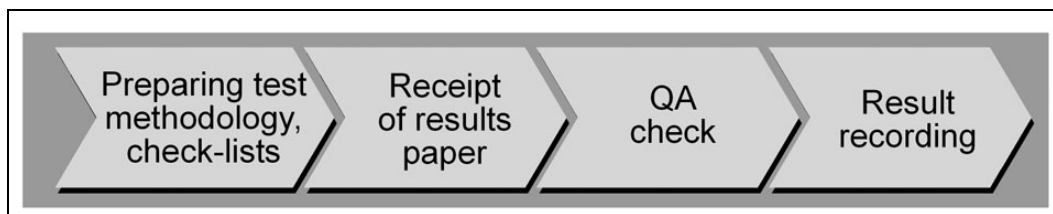
Fig. 87:   Quality control steps

At the end of a project step or project phase, the quality assurance officer prepares the required check-lists and test methods.

Given a positive quality control outcome, the next project step is released. A result which does not meet with the defined quality requirements is returned for rework. The concrete contents to be reworked are specified in detail and are recorded in a test report. Finally, a deadline for re-submission is agreed to and entered in the project plan.

5.5.3.13   *Support during the operating phase*

Another precondition for the sustainable success of a migration project is support for administrators to a reasonable extent. It is, however, not possible at this point to state a generally valid orientation value that describes the extent of this commitment. What does, however, matter is a prompt response as soon as a corresponding requirement is identified. In view of a lack of migration routine, support from external experts is necessary during the phase of familiarization with the new tasks, especially on the part of administrators. This is particularly important if those involved have little or no experience with the new systems (Linux, OSS). The availability of an expert on location would be the best option in any case.

6 Authors*

Frank Gamerdinger, expert for Open Office and StarOffice, contributed towards the technical discussions of the Office migration. <frank.gamerdinger@sun.com>

Peter Ganten has specialized in directory services, migration of Windows NT-based domains to Samba and OpenLDAP under Linux, as well as thin clients and integration of Windows applications on the Linux desktop. He was involved in the corresponding sections of this migration guide. <ganten@univention.de>

Sebastian Hetze contributed towards the sections on databases, file systems, network and system management services in this migration guide. He has specialized in databases and file systems under Linux as well as data interchange formats. <s.hetze@linux-ag.de>

Volker Lendecke is a member of the Samba Core Developer Team. In this field, he made important contributions towards the technical discussions of the following infrastructure services: file system, authentication and print service. <vl@sernet.de>

Michael Meskes has specialized in DBMS and especially in PostgreSQL and contributed towards the technical discussions of these aspects. <Michael.Meskes@credativ.de>

Kurt Pfeifle has specialized in the integration of network-wide print services in heterogenous environments and contributed as an author towards the technical discussions of the print services. <kpfeifle@danka.de>

Dr. Klaus Schmidt is an expert for IT infrastructure and product development. In this capacity, he is, in particular, a specialist for high-availability solutions. He was involved in the corresponding sections of this migration guide.

Sebastian Stöcker has specialized in Microsoft infrastructures and system architectures and wrote important parts of the technical discussions related to the Microsoft components.

Thomas Uhl works on integration of open systems, especially in the open source area. He wrote parts of the technical discussions of groupware and terminal services. <thomas.uhl@to.com>

7   Abbreviations

ACE	Access Control Entries
ACL	Access Control List
AD	Active Directory
ADAM	Active Directory Application Mode
ADC	Active Directory Connector
ADO	ActiveX Data Objects
ADS	Active Directory Service
ADSI	Active Directory Service Interface
AFS	Andrew File System
API	Application Programming Interface
APOP	Authenticated Post Office Protocol
APT	Advanced Package Tool
ASCII	American Standard Code for Information Interchange
ASF	Apache Software Foundation
ASP	Active Server Pages
BB	Bulletin Boards
BDC	Backup Domain Controller
BfD	The Federal Data Protection Commissioner
BHO	Federal Budget Code
BIND	Berkeley Internet Name Domain
BMI	Federal Ministry of the Interior
BSD	Berkeley Software Distribution
BSI	German Federal Office for Information Security
BVA	Bundesverwaltungsamt
CA	Certification Authority
CDO	Collaboration Data Objects
CGI	Common Gateway Interface
CIFS	Common Internet File System
CIM	Common Information Model
CIS	COM Internet Service

Abbreviations

CLR	Common Language Runtime
cn	commonName
CO	Crossover Office
COM	Component Object Models
COM+	Component Object Models
CORBA	Common Objects Request Broker Architecture
COLS	Commercial Linux Software
CPU	Central Processing Unit
CSS	Cascading Style Sheets
CUPS	Common UNIX Printing System
DACL	Discretionary Access Control List
DAV	Distributed Authoring and Versioning
DBMS	Database management system
dc	domainComponent
DCOM	Distributed Component Object Models
DDE	Dynamic Data Exchange
DDNS	Dynamic DNS
DFS	Distributed File System
DHCP	Dynamic Host Configuration Protocol
DLC	Data Link Control
DLL	Dynamic Link Libraries
DMS	Document management system
DNS	Domain Name Server
DNSSEC	Domain Name System Security
DRBD	Distributed Replicated Block Device
DS	Directory Service
DSO	Dynamic Shared Objects
DTD	Document Type Definition
DTS	Data Transformation Services
E2K	Exchange 2000
EFS	Encrypting File System
EJB	Enterprise Java Beans

EMF	Enhanced Meta Format
ESC/P	Epson Printer Language
EXT2	Extendend Filesysten Version 2
EXT3	Extended Filesystem Version 3
FAT	File Allocation Table
FQDN	Full Qualified Domain Name
FRS	File Replication Service
FSG	Free Standard Group
FSMO	Flexible Single Master Operation
FTP	File Transfer Protocol
GC	Global Catalog
GDI	Graphics Device Interface
GNOME	GNU Network Object Model Environment
GNU	GNU's Not UNIX
GPL	General/Gnu Public License
GPOs	Group Policy Objects
GPS	Global Positioning System
GUID	Global Unique Identifier
HACMP	High Availability Cluster Management Protocol
HD	Harddisk
HIS	Host Integration Server
HP	Hewlett-Packard
HSM	Hierarchical Storage Management
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hyper-Text Transfer Protocol Secure
ICA	Independent Computing Architecture
IDE	Integrated Development Enviroment
IEAK	Internet Explorer Administration Kit
IETF	Internet Engineering Task Force
IIOP	Internet Inter-ORB Protocol
IIS	Internet Information Server

Abbreviations

IMAP4	Internet Mail Access Protocol 4
IMAPS	Internet Mail Access Protocol Secure
IPC	Interprocess Communication
IPP	Internet Printing Protocol
Ipsec	Internet Protocol Security Protocol
IPv6	IP Version 6
IPX	Internet Packet Exchange
IRC	Internet Relay Chats
IS	Information Store
ISA	Internet Security and Acceleration
ISAPI	Internet Service Application Programming Interface
ISC	Internet Software Consortium
IT-WiBe	Recommendations on economic efficiency assessments for IT systems at the federal administration
J2EE	Java 2 Enterprise Edition
J2SE	Java 2 Standard Edition
JAXP	Java API for XML
JDBC	Java Database Connection
JFS	Journaled File System
JIT	Just In Time
JMC	Java Message Service
JNDI	Java Naming and Directory Interface
JRE	Java Runtime Environment
JRMI	Java Remote Methode Invocation
JSP	Java Server Pages
JTA	Java Transaction API
JVM	Java Virtual Machine
KBSt	Co-ordinating and Advisory Agency of the Federal Government for Information Technology in the Federal Administration
KDC	Key Distribution Center
KDE	K Desktop Environment
KMS	Key Management Server
LAMP	Linux, Apache, MySQL, PHP

LAN	Local Area Network
LANANA	Linux Assigned Names and Numbers Authority
LDAP	Lightweight Directory Access Protocol
LDIF	LDAP Data Interchange Format
LGPL	Lesser General Public License
Li18nux	Linux Internationalization Initiative
LM	LAN Manager
LMRepl	Directory replication service
LPD	Line Printing Daemon
LPI	Linux Professional Institute
LPR	Line Printing Redirector
LSB	Linux Standard Base
LTSP	Linux Terminal Server Project
LVM	Logical Volume Manager
LVS	Linux Virtual Server
MAC	Media Access Control
MAPI	Messaging Application Programming Interface
MD	Man-day
MDX	Message Digest X
MLP	Message/Multilayer Link Protocol
MMC	Microsoft Management Console
MMQS	Microsoft Message Queue Server
MOM	Microsoft Operation Manager
MPL	Mozilla Public License
MRTG/RRD	Multi Router Traffic Grapher/Round Robin Database
MS	Microsoft
MSMQ	Microsoft Message Queuing
MSPS	Microsoft Proprietary Standards
MTA	Message Transfer Agent
MTBF	mean time between failure
MTS	Microsoft Transaction Server
MTTR	Mean Time To Repair

Abbreviations

NAS	Network Attached Storage
NAT	Network Address Translation
NCSA	National Center for Supercomputing Application
NetBEUI	NetBIOS Extended User Interface
NetBIOS	Network Basic Input and Output System
NetBT	NetBIOS over TCP/IP
NFS	Network File System
NIS	Network Information Service
NNTP	Network News Transport Protocol
NPL	Netscape Public License
NTDS	NT Directory Service
NTFS	NT File System
NTFS4	NT File System 4
NTFS5	New Technology File System 5
NTLM	Windows NT LAN Manager
NTLMv2	Windows NT LAN Manager Version 2
NTP	Network Time Protocol
ODBC	Open Database Connectivity
OLAP	Online Analytical Processing
OLE	Object Linking and Embedding
OMG	Object Management Group
OOo	OpenOffice.org
OOo/SO	Open Office.org/StarOffice
OpenLDAP	Directory service
OSI	Open Systems Interconnection
OSOS	Open Standards mit Open Source
OSS	Open Source Software
OU	Organizational Unit
OWA	Outlook Web Access
PAM	Pluggable Authentication Module
PBS	Portable Batch System
PCL	Printer Control Language

PDA	Personal Digital Assistant
PDC	Primary Domain Controller
PDF	Portable Document Format
Perl	Practical Extraction and Report Language
PHP	PHP Hypertext Pre-processor
PIM	Personal Information Manager
PKI	Public Key Infrastructure
POP3	Post Office Protocol Version 3
POSIX	Portable Operating System Interface for UNIX
PPD	PostScript Printer Descriptions
RAC	Real Application Cluster
RAID	Redundant Array of Inexpensive/Independent Discs
RAM	Random Access Machine/Memory
RAS	Remote Access Service
RAW	Read After Write
RDBMS	Relational Database Management System
RDP	Remote Desktop Protocol
ReiserFS	Reiser File System
RFCs	Request for Comments
RHCE	Red Hat Certified Engineer
RID	Relative Identifier
RISC	Reduced Instruction Set Computer
RPC	Remote Procedure Calls
RPM	Red Hat Packet Management
S/MIME	Secure MIME (Multipurpose Internet Mail Extensions)
SA	System Attendant
SACL	System Access Control List
SAGA	Standards and Architectures for e-government Applications
SAM	Security Accounts Manager
SAN	Storage Area Network
SASL	Simple Authentication and Security Layer
SC	Samsung Contact

Abbreviations

SCM	Security Configuration Manager
SCSI	Small Computer System Interface
SFU	Service for UNIX
SID	Security Identifier
SISL	Sun Industry Source License
SLAs	Service Level Agreements
SMB	Server Message Block
SMS	Short Message Service
SMS	System Management Server
SMTP	Simple Mail Transfer Protocol
SNA	Storage Network Attached
SNMP	Simple Network Management Protocol
SO	StarOffice
SOAP	Simple Object Access Protocol
SPM	Standard TCP/IP Port Monitor
SPX	Sequenced Packet Exchange
SQL	Structured Query Language
SQL-DMO	SQL Distributed Management Objects
SRS	Standard Replication Service
SSH	Secure Shell
SSL	Secure Sockets Layer
SSL/TLS	Secure Sockets Layer / Transport Layer Security
SW	Software
TB	Terabyte
TCL	Tool Command Language
TCO	Total Costs of Ownership
TCP/IP	Transmission Control Protocol / Internet Protocol
TDS	Tabular Data Stream
TGS	Ticket Granting Service
TGT	Ticket Granting Ticket
TTS	Trouble Ticket System
UDDI	Universal Description, Discovery and Integration

UDP	User Datagram Protocol
UHD	User Help Desks
UNC	Uniform Naming Convention
UNO	Universal Network Objects
URL	Uniform Resource Location
USB	Universal Serial Bus
USN	Unique Sequence Number
VBA	Visual Basic for Applications
VBS	Visual Basic Scripting Edition
VBScript	Visual Basic Script
VFS	Virtual File System
VLDB	Very Large Database
VPN	Virtual Private Network
W2K	Windows 2000
W3C	World Wide Web Consortiums
WAP	Wireless Application Protocol
WBEM	Web Based Enterprise Management
WebDAVS	Web Document Authoring And Versioning
WINS	Windows Internet Name Service
WSDL	Web-Services Description Language
WSH	Windows Sripting Host
WWW	World Wide Web
XFS	Extended File System
XSL	Extensible Style Sheet Language
XML	Extensible Markup Language
YaST	Yet another Setup Tool

8 Glossary

ADO
ADO means Active Data Objects and represents a high-level interface (for example, from Visual Basic) for general data access from Microsoft via an OLE DB provider (for example, for SQL Server, ODBC, Oracle, Active Directory Service, etc.). ADO includes objects for the establishment of a connection to a data source, for read, update, write and delete operations.

ACL
An Access Control List is a list with access privileges. These lists serve as the basis for controlling access to the resources of the IT system. The system uses the ACLs in order to decide which access a user has to a resource, such as a directory.

ActiveX
A collective term for a technology introduced by Microsoft which enables (inter)active contents on websites. The browser downloads ActiveX program parts from the server and executes these on the user's PC. ActiveX was developed by Microsoft as an alternative to Java applets.

API
Application Programming Interface (a defined programming interface which can be used for integration and expansion).

ASP
"Active Server Pages"; this being Microsoft's concept for generating dynamic websites (refer also to "JSP") at the server end (using, for example, JavaScript, Visual Basic Script).

C#
An object-oriented programming language developed by Microsoft on the basis of C and C++.

CGI
The Common Gateway Interface is the very first variant of the web server interfaces. Practically every modern web server supports this interface. Applications using CGI can be developed in different programming languages. Besides interpreter languages, such as PERL, it is also possible to use compiled applications which were written in C or C++.

COM
The Component Object Model is a software standard from Microsoft which can enable communication between processes and programs. For this purpose, COM defines an object-oriented interface which a program or a software component uses in order to make services available.

CORBA
CORBA means Common Object Request Broker Architecture and was developed with the aim to enable communication between applications independent of place, platform and implementation. CORBA is an open standard defined by the Object Management Group (OMG).

DCOM
The Distributed Component Object Model is a variant of Microsoft's COM standard. DCOM can be used for the distribution of the services of a software. DCOM uses RPCs (Remote

	Procedure Calls) for implementation in order to call procedures on a remote computer via the exchange of messages.
DDE	Dynamic Data Exchange is a procedure under Windows which enables user programs to exchange data. Data exchange itself is a dynamic process. If a file connected by DDE is changed, the change is automatically transferred to all the files communicating with the file concerned.
DHCP	The Dynamic Host Configuration Protocol creates the basis for the dynamic assignment of IP addresses. The DHCP client dynamically receives an IP address from central DHCP servers. Besides the IP addresses, even further configuration parameters can be sent to the client.
DNS	The Domain Name System is a system with a hierarchical structure for assigning names to computers connected to the Internet/intranet.
DTD	Document Type Definitions formally define the structure of an XML document. They determine the syntax which applies to a particular document type (and hence to a particular data format).
Emulation	The capability of a system or program to simulate the operation of another computer system using hardware or software resources.
Failover	This is a specific hardware or software feature, for example, of a database, server or network, which is configured in such a manner that its services are automatically taken over by a system with a similar or identical function in the case of a temporary system failure.
HTML	Hypertext Markup Language – the open standard and the file format for the presentation of contents on the Internet and in intranets.
HTTP	A standard for electronic interaction during the transmission of web documents to the Internet.
IMAP	The Internet Mail Access Protocol can be used to administer e-mailboxes. In contrast to POP3, IMAP administers the mail on the server. When the mail program starts, only the header data (sender, reference and time of receipt) is loaded by default. The recipient can then select the mails to be downloaded completely. Mail to remain on the server can be filed there in special folders.
IPsec	A standard for network security solutions which is particularly suitable for the implementation of VPNs and for remote access to private networks via dial-up connections.
IPv6	The new version 6 of the Internet protocol (IP) with IP addresses consisting of 128 rather than 32 bits as with IPv4. This may create more addressing options for websites.

Glossary

IPX   A standard for data transmission defined by Novell.

Java   A programming language developed by SUN Microsystems which is especially used in the field of Internet technology. A so-called compiler translates the source texts to a platform-independent intermediate code. This intermediate code can then be executed by a suitable interpreter on any computer. This enables the execution of Java programs on all computer platforms for which a suitable interpreter program exists.

Java Beans   Java Beans are reusable software components implemented in Java.

Java Script   A script language originally defined by Netscape for connecting program code to static HTML pages. The code is typically executed in the user's browser.

JDBC   The Java Database Connectivity offers a mechanism for communication with existing databases. Drivers serve as the interface between the Java program and the database.

JSP   JavaServer Pages are HTML files with embedded Java program code which is once converted to servlets by a JSP engine which are then executed in the web server. The result is then sent in normal HTML format to the client (refer also to ASP).

LAMP   An open source platform for web developers and web applications based on Linux, Apache, MySQL and PHP and/or PERL or Python.

LDAP   The Lightweight Directory Access Protocol (X.509) is a simplified version of the DAP (X.500). LDAP is used to access directory services which can, for example, be used to query user features.

Macro   A combination of individual instructions and/or a sequence of commands and processes which can be recorded and saved. When a macro is called, the processes and actions are automatically executed in the correct order.

MP3   A standard format for compressed audio files which was developed by the Fraunhofer-Institut within the framework of the MPEG and which has become particularly popular on the Internet.

MTA   A software component responsible for the distribution of e-mails between different computer systems. An MTA receives messages both from other MTAs and from MUAs and passes these on to the corresponding recipients.

MUA   The Mail User Agent is the e-mail program which enables users to access, display, read, edit and administer electronic messages.

.NET   A platform for XML-based web services from Microsoft. The platform is designed to connect information, devices and users in a uniform and personalized manner.

NTP   The Network Time Protocol is used to synchronize the time information of different computers via a network. The NTP enables the setting of computer time precise to the millisecond. This is particularly important for processes in which several computers are involved at the same time.

ODBC   A standardized process ensuring access to databases. Application programs, for example, can use ODBC in order to access a diverse range of databases.

OLE   OLE means "Objekt Linking and Embedding" and is a method for the shared use of information. This information can exist in different formats and can have been generated by different applications. Data from a source document is linked to and/or embedded in a target document. When the embedded data is tagged in the target document, the source application is once again opened, so that the data can be edited using the necessary functions in the usual environment. Another term used is "OLE Compound Documents".

OSI   An international standard for exchanging data in networks. OSI consists of seven layers describing the individual communication processes.

PDF   A cross-platform document format from Adobe Systems that enables the generation and presentation of documents which consist of text, images and pictures.

Perl   The Practical Extraction and Report Language is a freely available programming language which is used particularly often for writing CGI scripts. Thanks to a variety of options, especially in conjunction with the processing of strings, Perl programs are often used for administrative routine tasks.

PHP   A server-end script language for generating database-based and dynamic web contents.

POP3   When using the Post Office Protocol in its version 3, the local mail program (client) generally downloads all new mails from the mail server to the local computer after the start. The client is typically configured in such a manner that mail, once downloaded, is deleted on the server.

POSIX   A UNIX-based interface standard according to IEEE which is supported by all UNIX derivatives.

PostScript   A page description language developed by Adobe for controlling printers. Postscript-enabled printers receive their print commands

	from the respective application program in the form of a standardized sequence of instructions which the printer interprets and translates to a print process.
RAS	Microsoft uses this name for the provision of dial-up services within the Microsoft operating system.
RDBMS	The information of a database in a relational database management system is stored in tables which are in a relation to each other. The organization is based on the relational model.
Server	A process, a program or a computer which processes the requests of a client and/or which provides services that can be used by a client.
SQL	The standard query language for relational databases.
SSH	A protocol and the implementation (UNIX/Linux systems) corresponding to this protocol which ensures secure access to the computers connected to a network. The implementation ensures secure data transmission via non-secure connections.
SSL	An encryption technology developed by Netscape and a protocol for secure communication and transmission of documents between web browsers and web servers.
TCP/IP	A set of network protocols which are used within a network in order to offer users various services. TCP (Transmission Control Protocol) and IP (Internet Protocol) are the fundamentals for defining the individual data packets, as well as their sending and service.
UNO	UNO is a component model which ensures interoperability between different programming languages, different object models, different machine architectures and different processes. This can be implemented in a LAN or via the Internet. UNO is developed by the OpenOffice Community in cooperation with the development laboratories of Sun Microsystems. The basic libraries of UNO are independent of OpenOffice and StarOffice and can be used as a framework for other applications. UNO is freely available subject to the LGPL license. Java, C and C++ on Windows, Linux and Solaris are currently supported. (refer also to http://udk.openoffice.org/common-/man/uno.html)
URL	The Uniform Resource Locator identifies a distinguished address in the World Wide Web, such as "http://www.csar-ag.com".
VBA	Visual Basic for Applications
W3C	The World Wide Web Consortium coordinates the development of the WWW and the standardization of HTML, XML and their derivatives.

WebDAV Web-based Distributed Authoring and Versioning is an extension of the Hypertext Transfer Protocol (HTTP) and offers standardized support for the asynchronous, collaborative creation of contents via the Internet and/or intranet.

WINS A Microsoft system for the resolution of names within a network (network names <-> IP addresses).

XML A specification for the definition of languages for formatting documents. XML offers a strict separation of contents and design

XSLT A language recommended by the W3C for creating style templates that convert XML-structures to other XML structures in a rule-based process, for example, to a page description language, such as HTML.

9   Tables

Tables

10   Illustrations

Illustrations

11   Appendix

11.1   Appendix: WiBe (recommendations on economic efficiency assessments for IT systems)

11.1.1   Overview of recommended catalogs of criteria

General catalog of criteria, IT-WiBe21, for migration scenarios by Dr. Peter Röthig Organisations- und Projektberatung, „Empfehlung zur Durchführung von Wirtschaftlichkeitsbetrachtungen in der Bundesverwaltung, insbesondere beim Einsatz der IT", Version 3.0 - 2001, published by KBSt, Federal Ministry of the Interior, KBSt publication series, ISSN 0179-7263, Vol. 52, May 2001

Special catalog of criteria, IT-WiBe21, for IT update and migration projects, by Dr. Peter Röthig Organisations- und Projektberatung and Prof. Dr. Detlef Leipelt, FH des Bundes für öffentliche Verwaltung – Hinweise und Empfehlungen – zur Durchführung von Wirschaftlichkeitsbetrachtungen bei IT-Update- bzw. Umstellungsvorhaben auf Grundlage der IT-WiBe-97, published by KBSt, Federal Ministry of the Interior, KBSt publication series, ISSN 0179-7263, letter 04/2000, November 2000

Special catalog of criteria, IT-WiBe21, for migration objects, compiled as a selection from and amendment to the general catalog of criteria during a workshop of the Federal Ministry of the Interior in cooperation with members of BSI, BVA and C_sar in March 2003

11.1.2   General catalog of criteria, IT-WiBe21, for migration scenarios

All criteria are described on the following catalog pages:

o   Criteria according to WiBe 21 for complete migration scenarios (dark blue color)

o   Criteria which can be omitted for migration objects (orange color)[198]

o   Criteria which are to be adopted for migration projects in addition to those of WiBe 21 (light blue color)

The structure is oriented towards WiBe 21:

1.   1. Development/introduction costs and development benefits

2.   2. Operating costs and operating benefits

3.   3. Urgency criteria

---

[198] Refer to the special catalog of criteria for migration objects

4. 4. Quality/strategy criteria

5. Notes and explanations

11.1.2.1 *Development/introduction costs and development benefits*

Item Column	Note/ recom mendat ion	dg eva et- nt	n- eva bu nt dg et-	Description of criterion
1	x	b	n	Development costs / introduction costs and development benefits
1.1	x	b	n	Development/introduction costs for the new IT method
1.1.1	x	b	n	Planning and introduction/development costs
1.1.1.1	x		n	Personnel costs (own personnel)
1.1.1.2	x	b		Costs of external consultants
1.1.1.3	x	b		Costs of the development environment
1.1.1.4	x	b		Other costs for non-personnel/ancillary items
1.1.1.5	x	b		Travel costs (own personnel)
1.1.2	x	b	n	System costs
1.1.2.1	x	b		Hardware costs
1.1.2.1.1	x	b		Host/server, network operation
1.1.2.1.2	x	b		Workstation computers
1.1.2.2	x	b		Software costs
1.1.2.2.1	x	b		Costs for development and/or acquisition of software
1.1.2.2.2	x	b		Costs for adaptation of software and/or interfaces
1.1.2.2.3	x	b		Costs for evaluation, certification and quality assurance
1.1.2.3	#	b	n	Installation costs
1.1.2.3.1	#	b		Construction/building costs
1.1.2.3.2	#	b		Installation of technical infrastructure
1.1.2.3.3	#	b		Office/room equipment, accessories
1.1.2.3.4	#		n	Personnel costs for system installation
1.1.3	x	b	n	Costs of system introduction
1.1.3.1	x		n	System and integration tests
1.1.3.2	x	b	n	Costs of system installation
1.1.3.3	x	b		Import of data stocks
1.1.3.4	x	b	n	Initial training for users and IT specialists
1.1.3.5	x		n	Familiarization costs for users and IT specialists
1.1.3.6	x	b	n	Other migration costs
1.2	x			Development/introduction benefit due to replacement of the old method
1.2.1	x	b		Once-off cost savings (avoidance of maintenance/ upgrading costs for the old system)
1.2.2	x	b		Once-off revenue (from sale of old system)

Appendix

11.1.2.2 *Operating costs and operating benefits*

Item Column	Note/ recommendation			Description of criterion
2	x	b	n	Operating costs and operating benefits
2.1	x	b	n	Current material costs / cost savings
2.1.1	#	b	n	(Pro-rata) management/communication costs
2.1.1.1	#			Current costs from NEW IT method
2.1.1.2	#			Current benefits from omission of OLD IT method
2.1.2	x	b	n	(Pro-rata) host, server and network costs
2.1.2.1	x	b	n	Current costs from NEW IT method
2.1.2.2	x	b	n	Current benefits from omission of OLD IT method
2.1.3	x	b	n	(Pro-rata) costs for workstation computers
2.1.3.1	x			Current costs from NEW IT method
2.1.3.2	x			Current benefits from omission of OLD IT method
2.1.4	#	b	n	Consumables for hardware
2.1.4.1	#			Current costs from NEW IT method
2.1.4.2	#			Current benefits from omission of OLD IT method
2.1.5	#	b	n	Energy and office space costs
2.1.5.1	#			Current costs from NEW IT method
2.1.5.2	#			Current benefits from omission of OLD IT method
2.2	x	b	n	Current personnel costs / personnel cost savings
2.2.1	x	b	n	Personnel costs from system use
2.2.1.1	x			Current costs from NEW IT method
2.2.1.2	x			Current benefits from omission of OLD IT method
2.2.2	x	b	n	Costs/benefits from service item reclassification
2.2.2.1	x			Current costs from NEW IT method
2.2.2.2	x			Current benefits from omission of OLD IT method
2.2.3	x	b	n	System support and administration
2.2.3.1	x			Current costs from NEW IT method
2.2.3.2	x			Current benefits from omission of OLD IT method
2.2.4	x	b	n	Ongoing training / qualification
2.2.4.1	x			Current costs from NEW IT method
2.2.4.2	x			Current benefits from omission of OLD IT method
2.3	x	b	n	Current costs/savings related to service/system maintenance
2.3.1	#	b		Hardware service/maintenance
2.3.1.1	#			Current costs from NEW IT method
2.3.1.2	#			Current benefits from omission of OLD IT method
2.3.2	x	b		Software service/maintenance
2.3.2.1	x			Current costs from NEW IT method
2.3.2.2	x			Current benefits from omission of OLD IT method
2.3.3	x	b	n	Replacement/upgrading costs
2.3.3.1	x			Current costs from NEW IT method
2.3.3.2	x			Current benefits from omission of OLD IT method
2.4	x	b	n	Other current costs and savings
2.4.1	#	b	n	Data protection / data backup costs
2.4.1.1	#	b	n	Current costs from NEW IT method
2.4.1.2	#	b	n	Current benefits from omission of OLD IT method
2.4.2	x	b	n	Costs of parallel external support
2.4.2.1	x	b	n	Current costs from NEW IT method
2.4.2.2	x	b	n	Current benefits from omission of OLD IT method
2.4.3	#	b	n	Insurance, etc.
2.4.3.1	#	b	n	Current costs from NEW IT method
2.4.3.2	#	b	n	Current benefits from omission of OLD IT method
2.4.4	x	b	n	Other current costs and benefits
2.4.4.1	x			Current costs from NEW IT method
2.4.4.2	x			Current benefits from omission of OLD IT method

Annotation concerning operating costs/benefits:

All items include cost and benefit information of the type shown in 2.1.1 and 2.4.4, for example. This information is not shown here for reasons of limited space.

11.1.2.3 Urgency criteria

Item Column	Note/ recommendation	Budget-relevant evaluation	Non-budget evaluation	Description of criterion
3	x			Urgency criteria
3.1	x			Urgency to replace the old system
3.1.1	x			Continuity of support for the old system
3.1.2	x			Stability of the old system
3.1.2.1	x			Bugs, errors and downtime
3.1.2.2	x			Service problems, personnel bottlenecks
3.1.3	x			Flexibility of the old system
3.1.3.1	x			Limits of expansion/upgrading
3.1.3.2	x			Interoperability, interface problems at present / in future
3.1.3.3	x			User-friendliness
3.2	x			Compliance with administrative rules and laws
3.2.1	x			Compliance with law
3.2.2	x			Ensuring data protection/integrity
3.2.3	x			Correct work processes
3.2.4	x			Compliance with tasks and recommendations

11.1.2.4 Quality/strategy criteria

Item Column	Note/ recommendation	Budget-relevant	Non-budget-relevant	Description of criterion
4	x			Qualitative/strategic criteria
4.1	x			Priority of the IT project
4.1.1	x			Relevance within the general IT concept
4.1.2	x			Integration into the IT landscape of the federal administration in general
4.1.3	x			Follow-up effects for communication partners
4.1.4	x			Pilot project character
4.1.5	x			Manufacturer-independence
4.2	x			Increase in the quality of specialized work
4.2.1	x			Increased job performance
4.2.2	x			Acceleration of work procedures and processes
4.3	x			Information control at the administrative/political level
4.3.1	x			Provision of information for decision-makers and controllers
4.3.2	x			Support of the decision-making /leadership process
4.4	x			Staff-related effects
4.4.1	x			Attractiveness of working conditions
4.4.2	x			Securing/enhancing qualification
4.4.3				Dissemination/availability of training
4.5	x			Effects related to citizen orientation
4.5.1	#			Standardized and uniform administrative action
4.5.2	#			Enhanced clarity and transparency
4.5.3	#			Acceleration of administrative decisions with repercussions on external parties
4.5.4	x			Image improvement
4.6				Dissemination/availability of software
4.6.1				Market penetration
4.6.2				Independent support
4.6.3				Available software certification
4.6.4				Available software admin tools
4.7				IT security
4.7.1				Communication security
4.7.2				Application security
4.7.3				Failure safety
4.7.4				Security management
4.7.5				Investment and planning safety

Appendix

11.1.2.5 Notes and explanations

Notes:

a) In this column, the criteria referred to in the "Hinweisen und Empfehlungen zur Durchführung von Wirtschaftlichkeitsbetrachtungen bei IT-Update- und Umstellungsvorhaben" auf Grundlage der IT-WiBe 97 (Recommendations on economic efficiency assessments for IT systems in conjunction with IT update and migration projects) are marked on the basis of IT-WiBe 97 as follows: X = criterion must be included, # = criterion is omitted.

b) The <u>complete</u> catalog of criteria is applicable to migration scenarios (including, for example, specialized applications)

c) Items in dark blue and light blue are mainly applicable to migration objects!

d) Items in light blue were added to the catalog for migration projects in addition to the general catalog of criteria according to WiBe21.

e) Items in orange can be omitted in the case of migration projects, especially in the case of migration objects or groups of migration objects!

11.1.3 Special catalog of criteria, IT-WiBe21, for migration objects

Item	Description of criterion
1	**Development costs / introduction costs and development benefits / introduction benefits**
1.1	Development/introduction costs for the new IT method
1.1.1	Planning and introduction/development costs
1.1.1.1	Personnel costs (own personnel)
1.1.1.2	Costs of external advisors
1.1.1.3	Costs of the development environment
1.1.2	System costs
1.1.2.1	Hardware costs
1.1.2.1.1	Host/server, network operation
1.1.2.1.2	Workstation computers
1.1.2.2	Software costs
1.1.2.2.1	Costs for the development and acquisition of software

Item	Description of criterion
1.1.2.2.2	Costs for modification of software and/or interfaces
1.1.2.2.3	Costs for evaluation, certification and quality assurance
1.1.2.3	Installation costs
1.1.2.3.4	Personnel costs for system installation
1.1.3	Costs of system introduction
1.1.3.1	System and integration testing
1.1.3.2	Costs of system installation
1.1.3.3	Import of existing data
1.1.3.4	Initial training for users and IT specialists
1.1.3.5	Familiarization costs for users and IT specialists
2	**Operating costs and operating benefits**
2.1	Operating costs / savings of operating costs
2.1.2	(Pro-rata) host, server and network costs
2.1.2.1	Operating costs of NEW IT process
2.1.2.2	Operating benefits from omission of OLD IT process
2.1.3	(Pro-rata) costs for workstation computers
2.1.3.1	Operating costs of NEW IT process
2.2	Operating personnel costs / savings of personnel costs
2.2.2	System management and administration
2.2.2.1	Operating costs of NEW IT process
2.2.2.2	Operating benefits from omission of OLD process
2.2.3	Ongoing training / qualification
2.2.3.1	Operating costs of NEW IT process
2.2.3.2	Operating benefits from omission of OLD process
2.3	Operating costs / savings for maintenance / system service
2.3.1	Hardware maintenance/service
2.3.1.1	Operating costs of NEW IT process
2.3.1.2	Operating benefits from omission of OLD IT process
2.3.2	Software maintenance/update
2.3.2.1	Operating costs of NEW IT process

Item	Description of criterion
2.3.2.2	Operating benefits from omission of OLD IT process
2.3.3	Replacement/supplementing costs
2.3.3.1	Operating costs of NEW IT process
2.3.3.2	Operating benefits from omission of OLD IT process
2.4	Other operating costs and savings
2.4.2	Costs of external advisors working parallel
2.4.2.1	Operating costs of NEW IT process
2.4.2.2	Operating benefits from omission of OLD process
2.4.4	Other operating costs and benefits
2.4.4.1	Operating costs of NEW IT process
2.4.4.2	Operating benefits from omission of OLD process

3	**Urgency criteria**
3.1	Urgency to replace the old system
3.1.1	Support continuity for the legacy system
3.1.2	Stability of the old system
3.1.2.1	Bugs, errors and downtime
3.1.2.2	Service problems, personnel bottlenecks
3.1.3	Flexibility of the old system
3.1.3.1	Limits of expansion / upgrading
3.1.3.2	Interoperability, present/future interface problems
3.1.3.3	User-friendliness
3.2	Compliance with administrative regulations and laws
3.2.1	Compliance with laws
3.2.2	Fulfillment of data protection/security requirements
3.2.3	Correct procedures and work processes
3.2.4	Compliance with requirements and recommendations

4	**Quality/strategy criteria**
4.1	Priority of the IT project

Item	Description of criterion
4.1.1	Relevance within the IT framework concept
4.1.2	Integration into the IT landscape of the federal administration in general
4.1.3	Follow-up effects for communication partners
4.1.4	Pilot project character
4.1.5	Manufacturer independence
4.2	Increase in quality of specialist tasks
4.2.1	Improved job performance
4.2.2	Acceleration of work procedures and processes
4.3	Control of information of the administrative/political level
4.3.1	Provision of information for decision-makers and controllers
4.3.2	Support of decision-making/leadership tasks
4.4	Staff-related effects
4.4.1	Attractiveness of working conditions
4.4.2	Ensuring/expanding qualifications
4.4.3	Dissemination / availability of training
4.5	Effects related to citizen orientation
4.5.4	Image improvement
4.6	Dissemination / availability of software
4.6.1	Market penetration
4.6.2	Independent support
4.6.3	Software certification is available
4.6.4	Administration tools are available for the software
4.7	IT security
4.7.1	Secure communication
4.7.2	Application safety/security
4.7.3	Failure safety
4.7.4	Security management
4.7.5	Investment and planning safety

Appendix

11.1.4 Explanation of additional criteria

The criteria which were newly added to the evaluation of economic efficiency of migration projects besides the original criteria addressed within the scope of the existing WiBe 21 version 3.0 as well as the supplements in the form of the annotations and recommendations from 2000 (see above)[199] . The systematics is oriented towards that the WiBe 21 approach and is referred to in parentheses "()" following the description.

→ **WiBe 21 – chapter 1 – development costs/benefits**

11.1.4.1 Introduction costs/benefits (1.1)

Migration of a complete landscape also includes the specialized applications which become necessary for new developments or re-programming. These activities must be considered as "development costs". Migration of migration objects typically requires no development costs, but costs for introduction. In order to underline these circumstances, the "development cost" criterion is amended by the term "Introduction[200]".

→ **WiBe 21 – chapter 4 – quality/strategy criteria**

11.1.4.2 Dissemination / availability of training (4.4.3)

This criterion addresses the dissemination of training and the availability of the necessary staff. The importance of this criterion must be assessed in qualitative terms.

Dissemination / availability of training

0	2	4	6	8	10
Personnel having the required skills is available on the market. Training is offered on an area-wide basis.	Personnel is available. Training is, however, offered at a few centers only.	Personnel is available. Training is organized mostly on an internal basis.	Personnel is available to a limited extent. Training must be organized internally.	Personnel is hardly available. Training is possible to a limited extent only.	The required training is not available on the market and is not offered either.

11.1.4.3 Dissemination / availability of software (4.6)

Market penetration (4.6.1)

This aspect refers to the market share of the software to be used. Shrinking or obsolete market penetration poses the risk that the software and/or its further development will be discontinued. Furthermore, a good market penetration

---

[199] Refer to "Spezieller Kriterienkatalog IT-WiBe21 für Migrationsobjekte", prepared by a cooperation project of the Federal Ministry of the Interior, BSI, BVA and C_sar.

[200] Refer to the criteria in items 1., 1.1, and 1.1.1

suggests a high degree of acceptance[201] and/or the intensive use of the software which, by converse conclusion, promises the continued existence of the software.

Market penetration

0	2	4	6	8	10
The product is offered on an area-wide basis.	The product is available from selected distributors only.	The product is offered on a regional basis only.	The product is offered on an occasional basis only.	The product is offered on a case-to-case basis only.	The product is not offered (any longer).

Independent support (4.6.2)

This criterion addresses the availability of support by independent companies for the software to be used. Against the background of investment protection, this ensures the continued use of the software even if its manufacturer is no longer capable of ensuring this.

Independent support

0	2	4	6	8	10
Support is offered on an area-wide basis.	Support is available from selected distributors only.	Support is offered on a regional basis only.	Support is offered only seldom.	Support is offered on a case-to-case basis only.	Support is not offered (any longer).

Available software certification (4.6.3)

---

[201] Acceptance is not always the top priority. Business policies occasionally dominate decisions in favor of better or more economical systems.

This criterion addresses the question as to whether the software to be used complies with statutory and/or agency-specific or industry-specific requirements or whether such compliance must be organized by the user organization itself. In the former case, the manufacturer/supplier of the software ensures its certification, so that no further costs are incurred. In the latter case, the user organization must ensure certification in order to cover its business processes. In this case, the user organization itself incurs costs that cannot be calculated on a general basis.

Available software certification

0	2	4	6	8	10
The software is certified, and certification is renewed on a regular basis.	The software is certified, and certification is renewed on an occasional basis.	The software comes with once-off certification.	The software comes with partial certification.	The software comes with rudimentary certification and/or recommend-ations only.	The software is not certified. Certification is not possible either.

Availability of administration tools for the software (4.6.4)

Administration of the software products to be used is sometimes not very user-friendly or even difficult. This criterion refers to tools which perform or support the administration of tables and master data. Suitable, intelligent tools can boost administration efficiency and quality and optimize the use of resources.

Availability of administration tools for the software

0	2	4	6	8	10
Administration tools are available for the software in an adequate form[202]	Administration tools are available to a certain extent.	Administration tools are available to a sporadic extent only.	Administration tools are hardly available.	Administration tools must be created from case to case.	Administration tools are not available and cannot be created from case to case either.

11.1.4.4 IT security (4.7)

The "security" aspect is in part included in the urgency criteria (refer to "downtime" or "data protection and data security"). At this point, this issue in once again pointed out under strategic and quality aspects and the management approach is discussed.

Communication security (4.7.1)

---

[202] Adequate form means that tools are offered by several independent companies.

This criterion addresses the security of internal and, above all, external communications. How is data transmission secured? Are secure protocols used? Are transmission protection, access control mechanisms, etc. in place?

Secure communication

0	2	4	6	8	10
Not endangered.	Hardly en-dangered.	Endangered to a minor extent, still acceptable.	Endangered to an average extent, problematic.	Above-average risk, highly problematic.	Very seriously affected, not acceptable.

Application safety/security (4.7.2)

Can the software be checked with regard to IT security? How susceptible is the software to attack from outside, viruses, etc.? Does the software feature a modular design (separation of system and application programs, option to minimize application programs to the necessary functions)? Are there any access control mechanisms?

Application safety/security

0	2	4	6	8	10
Not endangered.	Hardly en-dangered.	Endangered to a minor extent, still acceptable.	Endangered to an average extent, problematic.	Above-average risk, highly problematic.	Very seriously affected, not acceptable.

Failure safety (4.7.3)

How seriously is operating safety affected by system failures? Are suitable recovery routines in place?

Failure safety

0	2	4	6	8	10
Not endangered.	Hardly en-dangered.	Endangered to a minor extent, still acceptable.	Endangered to an average extent, problematic.	Above-average risk, highly problematic.	Very seriously affected, not acceptable.

Security management (4.7.4)

Appendix

Does security management exist? Does a security concept exist which is known to all those involved? Do a descriptive process for security checks and the related documentation exist?

Security management

0	2	4	6	8	10
Exists	Exists to the largest part	Partially exists	Rudimentary	Sporadic records and documents only	Does not exist

Investment and planning safety (4.7.5)

This criterion covers the aggregate effects of all the security-relevant criteria listed so far, and addresses the question as to whether the investment and any plans based on this will continue to exist in future.

Investment and planning safety

0	2	4	6	8	10
Not endangered.	Hardly endangered.	Endangered to a minor extent, still acceptable.	Endangered to an average extent, problematic.	Above-average risk, highly problematic.	Very seriously affected, not acceptable.