User Manual

IMiS/ARChive Storage Server

Version: 7.1.1011

November 2010

Imaging Systems, informacijski sistemi, d.o.o.
Brnčičeva 41g
1000 Ljubljana
Slovenia, Europe

IMAGING SYSTEMS

CONTENTS

FOREWORD

Foreword describes the content and structure of the document User manual for IMiS/ARChive Storage Server and offers helpful advice to users about technical and thematic fields related to the use of this product.

About the User Manual

The user manual explains the installation steps and procedures, as well as post-installation steps and the configuration of the IMiS/ARChive Storage Server archive system – server.

Target Users

Information included in the manual is intended for experienced system administrators with detailed knowledge of the Linux operational system in many of its different versions – distributions. Each administrator authorized for the installation and maintenance of the IMiS/ARChive Storage Server is obligated to know all the necessary procedures.

Conventions

There are different font styles describing important information used in this manual. The fonts are used as demonstrated in the lines below:

Font style:

Style	Used for
`Monospace`	Used for console modes, files, directories, etc.
`Monospace bold`	Used for displaying a user entry
Normal italics	Used for image/table description

Abbreviations

The table below shows abbreviations used in the text and graphics of this document:

Abbreviation	Full description
IMiS/ARC server	IMiS®/ARChive Storage Server server
IMiS/ARC service	IMiS®/ARChive Storage Server application service
IMiS/ARChive server	IMiS®/ARChive Storage Server server

Abbreviation	**Full description**
IMiS/ARChive service	IMiS®/ARChive Storage Server application service
HSM	Hierarchical storage management (hierarchical archiving of documents)
ERP	Enterprise resource planning (Business information systems)
DMS	Document management system
CRM	Customer relationship management
AES	Advanced Encryption Standard
RHEL	Red Hat Enterprise Linux (Linux server platform of the company RedHat)
SLES	SUSE Linux Enterprise Server (Linux server platform of the company Novell)
NAT	Network address translation (the process of hiding private addresses)
HA	High Availability

INTRODUCTION

Presentation

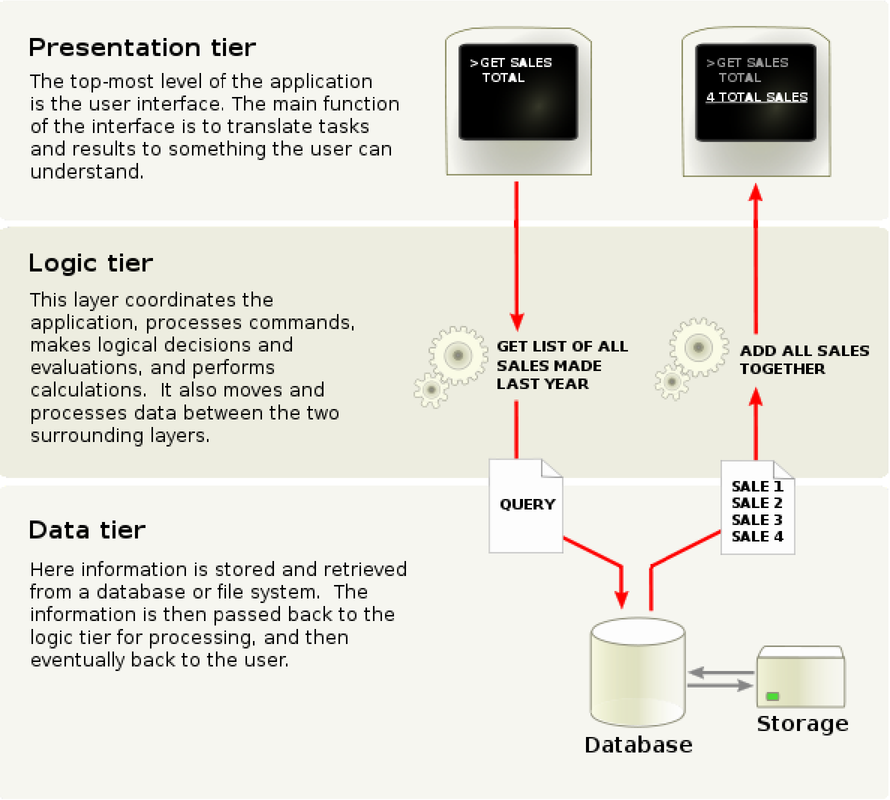
IMiS/ARChive Storage Server is a software product used for storing and managing greater amounts of digital documents over a longer period of time. Digital content can appear in the form of a scanned document, PDF file, audio/video format etc. Objects are saved in a structure of archive profiles, following the principle of hierarchical storage management (HSM). After being archived, each object is given a unique identification number (object identifier or ID), which is then recorded in a logical document of the application solution (ERP, DMS, CRM, …).

In order to access the archived content, one or more IMiS/ARChive Storage Server clients are used. These are adjusted to the specific requirements of the environment, which they are integrated in. Thus there are many different options, such as a classic client product that classifies the product into a Server – Client model, or clients adjusted for server use, which are used by application servers for interaction with the electronic storage etc. IMiS/ARChive Storage Server clients are not the subject of this document and are therefore mentioned only briefly. Additional information regarding the user or technical documentation of these products is available on the Imaging Systems' website (http://www.imis.si) or on request by sending an e-mail to podpora@imis.si or support@imis.si.

Placement

The IMiS/ARChive product is placed in multi-tier architecture, in the so-called data tier or persistent tier; database servers play a similar role in the multi-tier systems since they, from a functional viewpoint, offer safe, audit log-supported and scalable storage of digital content in different databases or other information systems provided by any other provider. The standard architectural model of an imaginary database system includes:

1. on the infrastructural (persistent) data tier there is one or more database servers and IMiS/ARC servers in clusters or replication;
2. on the logic tier there is one or more application servers with application (system), containing all the necessary business logic needed for the access control, safety and document management processes;
3. on the presentation tier there are clients of archive and document systems, such as a browser, applications of different devices (telephone, tablet PC, laptop, desktop computer), which can optionally manage devices for the capture and digitization of physical contents.



Presentation tier

The top-most level of the application is the user interface. The main function of the interface is to translate tasks and results to something the user can understand.

Logic tier

This layer coordinates the application, processes commands, makes logical decisions and evaluations, and performs calculations. It also moves and processes data between the two surrounding layers.

Data tier

Here information is stored and retrieved from a database or file system. The information is then passed back to the logic tier for processing, and then eventually back to the user.

(source: Wikipedia (http://en.wikipedia.org/wiki/Multitier_architecture))

Versioning and Product Labeling

Product versioning is based on the most common and widely accepted sequence-based schemes in the world, consisting of 4 individual numeric identifiers (**MAJOR**, **MINOR**, **RELEASE**, **BUILD**) and the end-point identifier of the target architecture of the processor (**ARCHITECTURE**) (Linux standard). There are a few extra attributes added to the name of the RPM installation file, which are specific to the product and include a unique server identifier (**SERVERID**), the identifier of the included base (**DATABASE**) and the identifier of the installation platform (**PLATFORM**). These attributes are not logged in the RPM database, but are added only to make it easier to separate and place the installation file.

imisarc.MAJOR.MINOR.RELEASE-BUILD.SERVERID.DATABASE.PLATFORM. ARCHITECURE.rpm

example: `imisarc.7.1.1011-530.0001.bdb.el4.i386.rpm`

MAJOR: The MAJOR identifier marks the main/major product version that changes in accordance with the respective arbitrary decision, depending on the scope of the functionalities and changes made. Here the identifier alters extremely rarely and if it does, this signifies a major difference in the product if compared to the previously issued versions with a smaller MAJOR version. The identifier has a set of values from 1-n, is continuous and exclusively increases.

MINOR: This identifier represents a smaller version of the product that changes in accordance with the respective arbitrary decision, depending on the scope of the changes, functionalities or other corrections. The identifier changes often and points to the minor changes and corrections inside the same product generation, represented by a specific MAJOR version. The set of values is from 1-n, the identifier is not continuous and returns to the starting point if the MAJOR version is changed (1).

RELEASE: Contrary to the arbitrary set of values used around the world, this identifier is more specific because it shows the time component identifying the product release, following the "YYMM" scheme. MM stands for the month of release (set of values 01-12), YY shows two numbers representing the current year; an example of such identification is a product released in May 2012, which is labeled in the RELEASE identifier as 1205.

BUILD: The identifier in this place marks a unique sequential number of the product's creation; the number is never repeated. In case of a minor change of the product within one month, this identifier may be replaced, while the rest of them remain the same. The set of values is from 1-n, the identifier is not continuous and exclusively increases.
SERVERID: Each instance of the installed product is given a unique identifier, which is also used for protecting the product and object identifiers. The RPM files are delivered to our clients, are non-transferable and intended strictly for the concrete instance of the product. The set of values is from 0001 – nnnn.

DATABASE: The identifier marks the base with which the product is distributed. The set of values during the period of issuing this version is BDB and RDM.

PLATFORM: This identifier marks the type of the installation platform for which the installation package is intended. The set of values is sles8, el3 and el4, and identifies the target platform; in the case of a discrete platform, a suitable equivalent must be found, in accordance with the environment of the required system libraries. Customers are offered help while making such decisions or they can use compatible system libraries, which enable a product of older platform versions to be used on much more recent ones (for example el3 installation package + compatible libraries used with rhel3 and rhel4 platforms).
The criteria for defining arbitrarily determinable identifiers are part of the internal rules of the company and are subject to the change management process.

New features:

- secure authentication of system users;
- encrypted authentication and (optional) encryption of network traffic between the server and clients;
- audit log of any operation on the archived content (includes the exact time and date of operation, user name, network address and computer name, type of event, reasons for the action and its parameters);
- secure access to the audit log, accessible only to privileged users;
- access to the audit log is possible with a combination of different criteria (user name, address and name of computer, object identifier, date and time of events, …);
- support of the new IPv6 communication network protocol;
- option of restricting the use of certain network addresses in the system (bind-to-address);
- new compression libraries, expanded native support of new client platforms (pure MS.NET 2.0, 3.5 and 4.0, more recent Linux platforms (rhel5, rhel6, sles11 etc.), Windows 7, Windows 8);
- improved and strongly stabilized subsystem for the logging of the events of product processes;
- option of archiving new content types (Office Open XML, Open Document Format, new compressed formats (RAR, 7-ZIP etc.), SAP generic content type, …).

Functionalities:

- secure authentication of system users;
- encrypted authentication and (optional) network traffic between the server and clients;
- storing of digital content (electronic or digitized through scanning);
- access to the archived content in batch or streaming mode;
- maintenance of and access to the basic metadata of the archived content (MIME type, date and time of creation, last access, last change, size etc.);
- option of access to the archived content through a unique external identifier (64 character ASCII string);
- audit log of any operation on the archived content (includes the time and date, user name, network address, computer name, type of event, reasons for the action);
- secure access to the audit log, accessible only to privileged users;
- support of both world-famous network communication systems IPv4 and IPv6;
- highly scalable archive system with basically undetectable time delay during transaction processing in case of large inventories of archived contents (over 10 million objects);
- an included database for storing the HSM configuration and various metadata on the archived inventory;
- optional web interface for product administration (requires a system web server).

TECHNICAL DOCUMENTATION

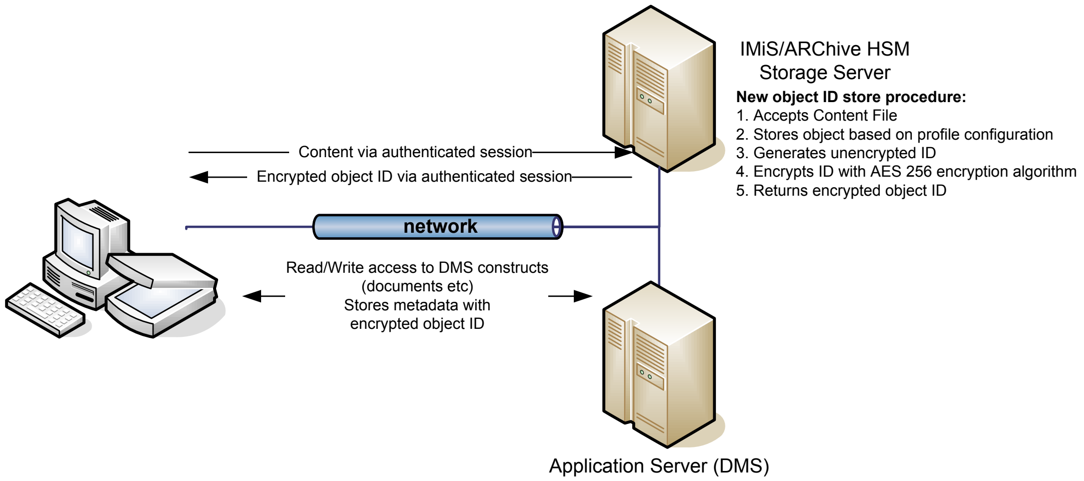
Object Identifier – a Unique Key to the Archived Content

Generation

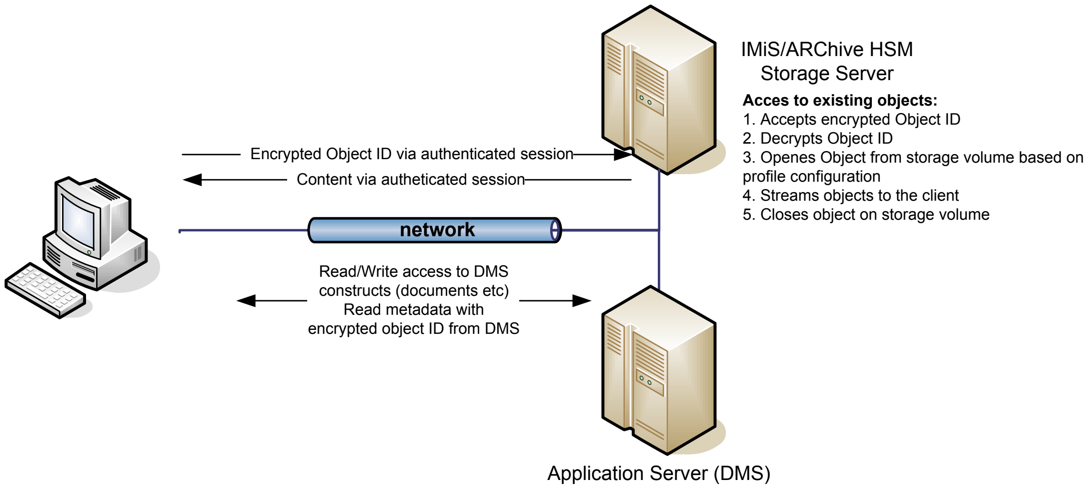
Each instance of the product installed in the execution environment is, after the creation of the binary files and installation package, assigned a unique number, the so-called product identifier, which separates it from all other instances of the product. In the life cycle of this instance, the identifier cannot be changed without simultaneously preventing access to the existing and already archived content. By accepting the license agreement, an individual customer guarantees that the installation package or binary file shall not be distributed to a third party in any form. Similarly, the customer cannot install two instances from the same installation package, since this would disable communication between the two (namely, the product has an integrated mechanism that prevents communication between two instances of the product identified by the same product identifier). In this way the manufacturer, which is also in charge of maintaining the archive systems, and its network of partners guarantees that no two instances of this product found in the world bear the same identifier.

Each archived content or object is assigned a unique 256-bit encrypted identifier upon initial storage**.** Such an identifier is a product of the aforementioned product identifier and a private key, assigned to each instance of the product installed in the execution environment during installation.

In addition to the uniqueness of the product identifier and the private product key, another feature that makes this object identifier so unique is the algorithm used for generating the object identifier. For encrypting and decrypting object identifiers, the product uses the world-wide and world-renowned AES-256 algorithm for block encryption (FIPS 197 standard; http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf). Decrypted object identifiers are used by the server exclusively for internal use and are thus never transmitted via the network protocol outside the setup environment of the product. Since the product outwardly ensures all operations exclusively through the means of encrypted object identifiers, it ensures the protection of the archived content against reproduction or other unauthorized actions (e.g. access).


IMiS/ARChive HSM
Storage Server
New object ID store procedure:
1. Accepts Content File
2. Stores object based on profile configuration
3. Generates unencrypted ID
4. Encrypts ID with AES 256 encryption algorithm
5. Returns encrypted object ID
Content via authenticated session
Encrypted object ID via authenticated session
network
Read/Write access to DMS constructs
(documents etc)
Stores metadata with
encrypted object ID
Application Server (DMS)

Storing the new digital content on the archive server


IMiS/ARChive HSM
Storage Server
Acces to existing objects:
1. Accepts encrypted Object ID
2. Decrypts Object ID
3. Openes Object from storage volume based on
profile configuration
4. Streams objects to the client
5. Closes object on storage volume
Encrypted Object ID via authenticated session
Content via autheticated session
network
Read/Write access to DMS
constructs (documents etc)
Read metadata with
encrypted object ID from DMS
Application Server (DMS)

Access to the existing archived content

Object Identifier Protection

As opposed to other products used for managing digital content, this product is not intended for end-users. It only represents a safe and reliable storage of digital content, accessible to various information systems (DMS/ERP). These do require such functionality, but are unable to provide it due to different (internal/external) factors. This makes it imperative that the application used for storing contents primarily provides a strong and reliable safety barrier that protects it from unauthorized access to the object identifiers, which become part of the metadata of various documents. The burden of visibility and accessibility to the stored object identifiers, which are used as a key to access the archived content, is carried exclusively by the application itself, with its security scheme.

A few other similar implementations are currently known in environments, such as IBM Lotus Notes/Domino (NSF Access Control Lists), IBM WebSphere that uses other

products (e.g. IBM Tivoli Access Manager for e-business), SAP R/3 with its security scheme, Microsoft SharePoint ACLs, Datalab Pantheon and others.
Security schemes and mechanisms of the products mentioned have all proved to be safe and reliable in securing the access to encrypted object identifiers; hence no cases of abuse have been detected so far, despite the considerable amount of archived contents.

Attempt to Reproduce an Identifier, Access to the Archived Content with a Brute Force Attack

The AES-256 is one of the most resistant algorithms when it comes to the so-called brute force attacks. Since identifiers are not based on words taken from dictionaries, attacks with the use of common words (''dictionary attacks'') are pointless. The current implementation of the product can store up to 2^{31} individual objects on one instance. The probability of the reproduction of 1 encrypted object identifier is 1 to 2^{225}. To give a concrete example, an attacker would have to generate and actually carry out 1.71 x 10^{57} attempts to access the archived content in the next 1000 years in order to be successful in at least one attempt.

Documentation Accessibility

For authentication and the communication with its clients, the product uses its own protected (encrypted) protocol. Access to the technical documentation, which might enable a potential attacker to easily understand the complexity of the communication between the server and the client, is limited to a narrow circle of partners, who, as users, are bound by discretion in the use and disclosure of confidential topics, as stated in the license and partnership agreements. This legal impediment restricts access to the documentation which could present a security risk. Likewise, access to the development documentation, which offers the partner network the possibility of communicating with the archive system, is limited to a circle of recognized, loyal, and longstanding partnerships.

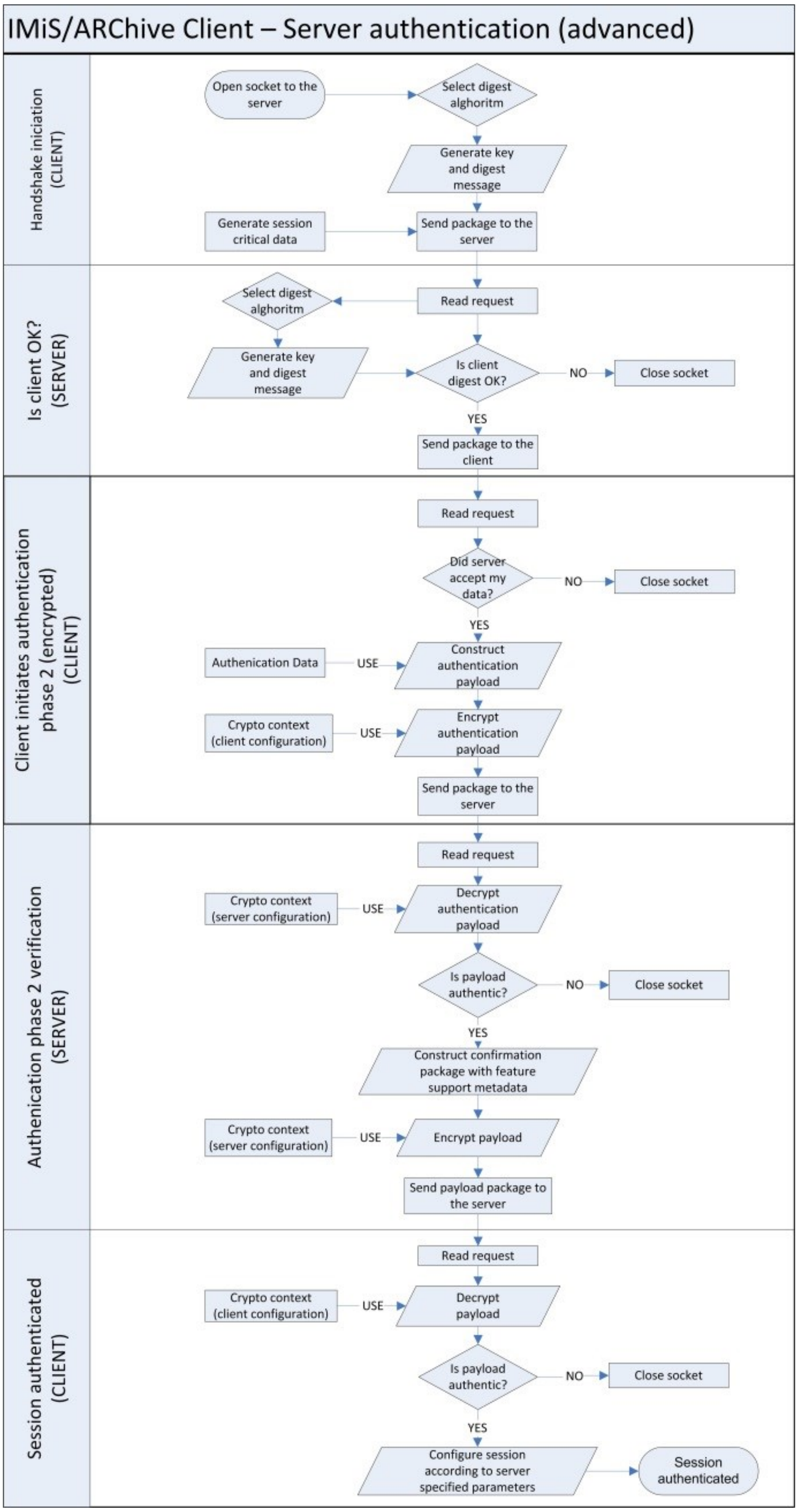
Authentication and Network Traffic

Secure Client Authentication Prevents Unauthorized Access to the Archive

Due to the non-public nature and the specificity of the protocol for communication with the archive system, secure and protected authentication of sessions with the archive system can only be provided by clients issued by our company, Imaging Systems informacijski sistemi, d.o.o.. These are a precondition for accessing the archive content or performing any other operation on it. The time given to the client for completing the establishment of a secure session can be set. It is preset to a very short time in order to narrow the window in which potential attackers could prepare and analyze network packets which they receive or send and eventually carry out their attack.

Authentication is based on the AES variant of the encrypted HMAC authentication (http://en.wikipedia.org/wiki/HMAC) with the use of encrypted one-time hashed longer messages.

According to international standards, the protocol prescribes the currently secure hash algorithms and AES encryption as an additional shield for preventing any unauthorized authentication.


IMiS/ARChive Client – Server authentication (advanced)
Handshake iniciation (CLIENT)
Open socket to the server
Select digest alghoritm
Generate key and digest message
Generate session critical data
Send package to the server
Is client OK? (SERVER)
Read request
Select digest alghoritm
Generate key and digest message
Is client digest OK?
NO
Close socket
YES
Send package to the client
Client initiates authentication phase 2 (encrypted) (CLIENT)
Read request
Did server accept my data?
NO
Close socket
YES
Authenication Data
USE
Construct authentication payload
Crypto context (client configuration)
USE
Encrypt authentication payload
Send package to the server
Authenication phase 2 verification (SERVER)
Read request
Crypto context (server configuration)
USE
Decrypt authentication payload
Is payload authentic?
NO
Close socket
YES
Construct confirmation package with feature support metadata
Crypto context (server configuration)
USE
Encrypt payload
Send payload package to the server
Session authenticated (CLIENT)
Read request
Crypto context (client configuration)
USE
Decrypt payload
Is payload authentic?
NO
Close socket
YES
Configure session according to server specified parameters
Session authenticated

A diagram of secure authentication process and establishing a session with the server

The client also provides its metadata in the authentication message, which serve as a data source for the server when entering events into the audit log (name of computer, internal address of the network interface card establishing the session – due to possible network address translation (NAT), the internal address may be inaccessible to the server etc.).

Network Traffic Protection Reduces Exposure to Eavesdropping

In environments where safety cannot be guaranteed as far as infrastructure is concerned (internet connections or exchange of extremely sensitive information), the product can be set to exchange data with its clients only in encrypted form. For the encryption of traffic between the server and clients, internationally-recognized AES-256 standards of encryption are used (FIPS 197 standard; http://csrc.nist.gov /publications/fips/fips197/fips-197.pdf), with different (adjustable) methods of processing the blocks before/after encryption (''Block cipher modes of operation'', http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation); in the current implementation a pre-shared key is used (http://en.wikipedia.org/wiki/Pre-shared_key), which is known to the client and server alike.
In this manner a safe exchange of information is achieved, without any ''man-in-the-middle'' attacks (http://en.wikipedia.org/wiki/Man-in-the-middle_attack) or eavesdropping on network packets**.** In extremely rare cases, the traffic needs additional protection with SSL v3 or TLS v1 (RFC 2246 - http://tools.ietf.org/html/rfc2246), for which the product has been prepared.

By including replication and a fail-over site, a backup center can be established. This achieves high availability (HA) of the archive system and by dividing systems into separate locations potential natural disasters can be avoided.

Instructions for the Backup Archiving and Restoring of Data

Backup Archiving

Backup of the IMiS/ARC server should be carried out with professional server/client type of tools, such as IBM Tivoli Storage Manager, HP Data Protector, CA ARCserve and others. To make a backup on the IMiS/ARChive server, a file backup agent will suffice. Prior to execution, it is recommendable to make a backup copy of the included base of the IMiS/ARC server with the tool `db_hotbackup` and then export the internal base of the IMiS/ARC server to the backup copy. The whole procedure is explained in the chapter Address Configuration under PRODUCT MANAGEMENT.

For a successful restoring of the data on the IMiS/ARChive, the backup task should save at least the following:

- the base of the IMiS/ARChive server (the default location is in the `/iarc/db` directory);

- volumes of the IMiS/ARChive server with all their contents, recursively (the default location is in the `/iarc/vol` directory);
- the configuration file of the IMiS/ARChive server `iarc.conf` (the default location is in the `/etc` directory);
- the cache of the IMiS/ARChive server for new objects or objects being edited (the default location is in the `/iarc/wcache` directory).

During backup a perfect copy can be obtained if, in addition to the minimum requirements, the backup task also saves:

- directory `/iarc/rcache` with its entire content;
- directory `/iarc/webadmin` with its entire content, recursively;
- directory`/opt/IS/imisarc` with its entire content, recursively;
- `file /etc/init.d/iarcd`;
- directory `/var/log/iarc` with its entire content.

While making the backup copies of the IMiS/ARC server, the possibility of loss or of partial corruption of data on the backup copy or the destruction of the media must also be considered. Good practice includes the making of backup copies and saving duplicates at a remote location. The backup copies and their duplicates should be kept in an appropriately secured fireproof place. The possibility of losing the entire database is minimized also by precisely planning the making and saving of backup copies from a longer period of time.
An example: Backup copies of the IMiS/ARC server are being made daily. The original backup copies are saved in a fireproof cabinet at the location of the server, while the backup duplicates are put in a safe at a remote location. The backup copies made at the end of the week, month or year are kept in a safe for an appropriate period of time, depending on how long the media lasts and the usability of the backed-up content.
The usability of the backup copies should be checked periodically. The data from the backup copy is restored to another location and compared to the original data from the IMiS/ARC server. The plan for making and saving backup copies should be periodically checked at least after a major change, such as changing servers, the media or infrastructure, which directly influences events connected with the IMiS/ARC server. The plan is usually checked by the information system auditor, who also evaluates it.

Data Restore

Restoring the data of the IMiS/ARC server depends on the state of the server and the desired result after restoring the data of the IMiS/ARC server. In case of uncertainty regarding the usability of the data that has remained on the disks or in case there is a chance of restoring the state as it was before the disk failure, we advise you to contact the technical staff of the manufacturer.

The two scenarios described below should be used when the data from the disks cannot be restored to such an extent as is necessary to restart the IMiS/ARC server.

The file system of the server, in which the IMiS/ARC server was located, cannot be returned to a state that would enable the preservation of the data up to a specific point in time in the past.

Solution to the problem: after installing the operating system, a "fresh" installation of the IMiS/ARC server should be carried out from the installation file (see chapter INSTALLATION). This is followed by restoring the IMiS/ARC server's data from the last backup copy and verifying the installation, as described in the chapter INSTALLATION. Additionally check:

- whether all files are in their expected locations;
- the startup of the IMiS/ARC server;
- the accessibility of the objects stored by the IMiS/ARC server.

The file system still contains some data from the IMiS/ARC server up to a specific point in time in the past.

This data is impossible to use, so it needs to be restored from the last backup copy. The operating system, executable programs and the configuration file of the IMiS/ARC server, which is otherwise located in the same disk storage as the operating system, have remained undamaged.

Solution to the problem: after the startup of the server's operating system, one part of the IMiS/ARC server's data has remained on it. The data is then restored from the last backup copy into a temporary directory. The content from the directory in which the volumes and the internal database of the IMiS/ARC server can be found is then deleted (usually the content of the `/iarc` directory) and the entire content from the temporary directory is moved there. Finally, the file ownership is checked and, if necessary, edited to enable normal operation.

SYSTEM REQUIREMENTS

Hardware

Many servers that can be bought on the market nowadays largely meet the requirements of the IMiS/ARC server because the latter needs few resources and can thus function in virtual environments as well. Attention should be given to the appropriate architecture of the server and adjust the latter to one of the supported architectures of the product, in most cases the Intel x86 platforms in 32 and 64-bit versions.

Planning the Server's Processor Power

When selecting the processor power attention should be paid to the estimated server load (number of clients, number of parallel user sessions, average size of the archived content, use of the audit log etc.). With regard to the functional characteristics of the product, the market today offers an adequate amount of processors, either of medium or high capacity, which provide a quality operating environment. Usually the choice of processor power can be aided by the recommended requirements of the operating system itself. For an imaginary system of 500 users with 200 accesses per day on average and with an average size of 100kB of the archived content, 1 processor of Xeon QuadCore technology of medium frequency capacity or 1 processor of the Intel Core i5/i7 family of medium frequency capacity would suffice, even if all the users were simultaneously carrying out transactions in the same time period.

Planning the Server's Memory Capacity

When planning the size of the server's memory, the following should be taken into account:

- requirements of the operating system;
- basic requirements of the IMiS/ARC server, which requires about 128 MB for operation alone;
- the number of concurrent users; each connection will requires about 64 KB;
- the minimum recommended memory size equals the sum of 256MB and the minimum memory size required by the manufacturer of the operating system.

The recommended memory size equals the sum of the memory needs of the services of the operating system itself and 1024MB (1GB) for the operation of the IMiS/ARC product.

Planning the Server's Disk Capacity

When planning the server's disk capacity, the following should be taken into account:

- requirements of the operating system,
- estimated average increase of objects per day,

- estimated increase of objects due to converting an old paper archive into an electronic one,
- average object size,
- the estimated time of server use(e.g. 5 years).

Objects stored in the volumes of the IMiS/ARC server can be of various types and can originate from different computer environments. Objects scanned by the IMiS/Scan with a resolution of 300pixels/inch in black-and-white technique (1-bit color depth), when using the default CCITT G4 T6 compression method, take up on average 45KB per scanned page. With the use of other compression methods, color depths and resolutions, the size generally increases (see table below).

Color depth	**Black/white (1 bit)**	**Gray (8 bit)**	**Full color (24 bit)**
none	605 KB	5 MB	15 MB
CCITT G3	85 KB	x	x
CCITT G4 T6	45 KB	x	x
JBIG	36 KB	x	x
JBIG 2bit	x	84 KB	x
JBIG 3bit	x	165 KB	x
JBIG 4bit	x	420 KB	x
Packed bits	109 KB	5 MB	15 MB
LZW	75 KB	3,2 MB	x
Packed bits 8 bit	x	x	x
Packed bits 24 bit	x	x	x
ZIP	56 KB	3 MB	9 MB
Wang JPEG	x	315 KB	363 KB
Sequential JPEG	x	315 KB	360 KB
Progressive JPEG	x	310 KB	334 KB

Average capacity of scanned images used with different compression methods

When choosing the right compression method, it should be taken into account that the transfer of larger objects via a computer network requires greater bandwidth and can affect the responsiveness of the computer network.
Scanning in gray or full-color is not advisable since the majority of modern scanners intended for document capture uses advanced methods and filters for graphic processing, which provides the optimum quality of the scanned images.

We recommend disk storage with suitable data protection and scalability. Also advisable is the use of contemporary disk controllers, which enable caching of reading and writing. The cache should have an autonomous power supply or be executed by means of ''Flash Memory'' (EEPROM technology), which can store data without electricity, as is required by the static RAM, with which older RAID controllers are equipped. The disks should be joined into a redundant disk array. In interest of efficiency, the RAID5 disk array type with an extra backup disk is recommended. However, not recommended is disk storage that is accessible to the IMiS/ARC server via a local network, e.g.: NAS (network attached storage) or disk storage located on another server and shared by the IMiS/ARC server through protocols like CIFS, NSF etc.

Communication Paths

The IMiS/ARC clients communicate with the IMiS/ARC server through the network port numbered `16807`, unless set otherwise in the `/etc/iarc.conf` configuration file. It is essential to enable communication through this port and set the rules of the firewall or of any other active network device to allow establishment of a client-server connection by the IMiS/ARC client, while the establishment of a server-client connection by the server is not foreseen/necessary.

Connection to Network Devices

We recommend duplicate connections and a connection to the backbone of the local network, with as few agents as possible. Preferably, the server should be connected to the main power switch. The network protocol between the IMiS/ARC client and server is optimized for packets of 32KB in the case of data packets (reading/writing of archived content) and for smaller ones in the case of command packets. An individual network packet never exceeds 32 KB.

Administrator Rights

The rights that the manager of the IMiS/ARC server needs are equal to the ones of the root user – `root`. The rights are usually assigned by the server administrator and should suffice for the installation, upgrade and administration of the IMiS/ARC server. The IMiS/ARC server does not need any privileged rights in order to operate. During installation, the installation script of the IMiS/ARC server creates the `iarc` user account and the `iarc` group, which start all the processes of the IMiS/ARC server. If an attack occurs due to a potential flaw in the server's application code, this disables the taking over of root user rights.

Hardware Operation Control

Upon the purchase of a server, most manufacturers of server hardware enclose a hardware control system (e.g. IBM Tivoli, HP Insight Systems Manager, Dell OpenManage). The use of such a system is quite helpful if any problems arise in the operation of devices or when system monitors need information about the server's operation. It is likewise helpful if the control system enables the reporting of errors in the operation of the systems via a cell phone or electronic mail.

Minimum Requirements

- A server with the Intel Pentium x86 or x86_64 processor 800Mhz or any other compatible processor with x86 architecture (see minimum requirements of the installation platform – operating system)
- 1GB RAM (see minimum requirements of the installation platform – operating system)
- Suitable disk capacity for the anticipated amount of archived contents
- Network access with the TCP/IP protocol (IPv4 or IPv6)
- Any hardware supporting the execution of the Linux operating system with a list of supported distributions in the network mode.

Recommended Requirements

- A server with a multi-core Intel Xeon E5/E7 or Xeon 5xxx/6xxx/7xxx (x86_64) processor 2GHz (or higher),
- 4GB SDRAM (DDR3/DDR4) of high frequency or higher,
- Powerful motherboard with Front Side Bus of higher frequency (1GHz or faster),
- Volumes on RAID5 logical disks/partitions (estimation of the increase of disk space for the next 3-5 years)
- SCSI/SAS controllers with write-back cache capabilities (up to 40% greater efficiency); 128MB cache or higher is recommended with support of battery charging or flash memory in the case of power outages *
- Fast SCSI/SAS disks (10k/15k RPM) with suitable caching *
- Redundant power supply with a set up cooling system
- Redundant network connection of 1Gbps or more with the IPv4 or IPv6 protocol

* The disk subsystem can be replaced by appropriate network SAN volumes, which are, performance-wise, comparable to the recommended local disk capacities.

* The product operates normally in other world-renowned virtualization environments, such as VMware ESX/ESXi, Microsoft Hyper-V, Oracle VM etc., as long as suitable virtual resources are provided, which offer a similar performance environment as that offered by the hardware recommended above.

Software - Operating System

Supported Operating Systems

The IMiS/ARC server works in the x86/x86_64 operating system, in Red Hat and SuSE distributions with the following derivatives:

- RHEL 4.x
- RHEL 5.x
- RHEL 6.x
- CentOS 4.x
- CentOS 5.x
- CentOS 6.x
- SLES 10.x
- SLES 11.x
- OpenSuSE 11.x
- OpenSuSE 12.x

For the installation and operation of the IMiS/ARC server, the operating system must provide the tools and libraries listed below. The tools and libraries of the Linux operating system can be an integral part of different installation packages of the operating system.

<u>List of mandatory system tools:</u>

`bash`	(more at: http://www.linuxmanpages.com/man1/bash.1.php)
`chmod`	(more at: http://www.linuxmanpages.com/man1/chmod.1.php)
`chown`	(more at: http://www.linuxmanpages.com/man1/chown.1.php)
`cp`	(more at: http://www.linuxmanpages.com/man1/cp.1.php)
`echo`	(more at: http://www.linuxmanpages.com/man1/echo.1.php)
`grep`	(more at: http://www.linuxmanpages.com/man1/grep.1.php)
`mv`	(more at: http://www.linuxmanpages.com/man1/mv.1.php)
`ps`	(more at: http://www.linuxmanpages.com/man1/ps.1.php)
`pwd`	(more at: http://www.linuxmanpages.com/man1/pwd.1.php)
`rm`	(more at: http://www.linuxmanpages.com/man1/rm.1.php)
`rmdir`	(more at: http://www.linuxmanpages.com/man1/rmdir.1.php)
`rpm`	(more at: http://www.linuxmanpages.com/man8/rpm.8.php)
`sed`	(more at: http://www.linuxmanpages.com/man1/sed.1.php)
`sh`	(more at: http://www.linuxmanpages.com/man1/sh.1.php)
`su`	(more at: http://www.linuxmanpages.com/man1/su.1.php)
`touch`	(more at: http://www.linuxmanpages.com/man1/touch.1.php)
`ip`	(more at: http://www.linuxmanpages.com/man7/ip.7.php)
`ldconfig`	(more at: http://www.linuxmanpages.com/man1/ps.1.php)
`awk`	(more at: http://www.linuxmanpages.com/man1/awk.1.php)
`find`	(more at: http://www.linuxmanpages.com/man1/find.1.php)
`id`	(more at: http://www.linuxmanpages.com/man1/id.1.php)
`ipcrm`	(more at: http://www.linuxmanpages.com/man8/ipcrm.8.php)
`ipcs`	(more at: http://www.linuxmanpages.com/man8/ipcs.8.php)

`killall`	(more at: http://www.linuxmanpages.com/man1/killall.1.php)
`setsid`	(more at: http://www.linuxmanpages.com/man2/setsid.2.php)
`groupadd`	(more at: http://www.linuxmanpages.com/man8/groupadd.8.php)
`useradd`	(more at: http://www.linuxmanpages.com/man8/useradd.8.php)

http server for the use of the IMiS/ARC Web Admin module

List of mandatory system libraries:

`libc.so.6`

`libm.so.6`

`libpthread.so.0`

`libstdc++.so.5` ali `libstdc++.so.6` (depending on the chosen installation platform)

`rpmlib`

Minimum Requirements

Operating system: Linux OS (RedHat EL/Fedora, SuSE SLES/OpenSuSE, Debian, Ubuntu (all based on any 2.4.x/2.6.x kernel)

Recommended Requirements

Operating system: Linux OS (RedHat EL/Fedora, SuSE SLES/OpenSuSE, Debian, Ubuntu (all based on any 2.4.x/2.6.x kernel)

SETUP

The setup procedure with the aid of console tools is described below.
The setup procedure of the IMiS/ARChive server can be performed by a root user or a user with equivalent rights (`sudo`). The setup procedure of the IMiS/ARChive server is carried out by steps and is the same for all target users that are installing the product.

Setup Procedure

Setup is possible only in an environment that meets at least the minimum setup requirements of one of the supported Linux distributions. The minimum requirements can be upgraded in accordance with the expected needs (see SYSTEM REQUIREMENTS, chapters ''Hardware'' and ''Software – Operating system'').
The setup procedure of the IMiS/ARChive server is simple and is described step by step below.

Step 1
Log into the operating system console as a root user or execute commands with a `root` user equivalent through the `sudo` tool. The disk storage intended for the IMiS/ARChive setup should be ready to use and attached to the `/iarc` directory. The setup is performed by the `rpm` tool, which is a component part of the supported Linux distributions. Setup is possible only in an environment that meets at least the minimum requirements for the setup of one of the supported Linux distributions (see SYSTEM REQUIREMENTS, chapter ''Software – Operating system'').

Step 2
Execute the `rpm` command for installing the installation package:

```
[user1@iarc ~]# sudo rpm -ivh imisarc.7.1.1011-530.0001.bdb.el4.i386.rpm
```

The name of the installation package may differ, depending on the Linux distribution, versions and the identification code of the IMiS/ARChive server.

Step 3
After a successful setup, the following record appears (the record can vary with regard to the Linux distribution used):

```
Preparing    ########################################### [100%]
1:imisarc    ########################################### [100%]
Performing POSTINSTALLATION Actions
POSTINSTALLATION Actions Done
```

Step 4
The installation package creates the following directories and files:

`/iarc/db` directory containing the IMiS/ARChive server databases,

`/iarc/vol` directory containing volumes to which the IMiS/ARChive server stores objects,

`/iarc/wcache` directory used by the IMiS/ARChive server for object caching during creation or editing,

`/iarc/rcache` directory for the caching of objects for which users submit review requests,

`/iarc/webadmin` directory in which the installation package of the IMiS/ARChive administrative module is located,

`/opt/IS/imisarc` includes the executable programs and libraries of the IMiS/ARChive,

`/etc/iarc.conf` configuration file of the IMiS/ARChive server,

`/etc/init.d/iarcd` startup script of the IMiS/ARChive.

Post-Installation Procedures

Post-installation procedures of the IMiS/ARChive server can be performed by a root user or a user with equivalent rights (administrator, qualified staff, …).

Adding Volumes and Profiles

The procedure of adding volumes is described in the chapter on configuration (see PRODUCT MANAGEMENT, chapter ''Configuration'').

Setting the Number of Simultaneously Open Files

Every process in the Linux operating system needs certain rights in order to operate. This is achieved with a process running under a specific user account to which the appropriate rights are assigned.

The assigning of rights and the creation of a user account under the name `iarc` is carried out by the installation itself. What needs to be performed manually is the setting of the number of simultaneously open files for the user account of the IMiS/ARChive server. The recommended number for simultaneously open files is 4096.

This setting is edited in the file `/etc/security/limits.conf` by typing in these two lines:

```
iarc         soft             nofile          4096
iarc         hard             nofile          4096
```

or rights can be set for all users belonging to the `iarc` group, even though this is not explicitly necessary:

```
@iarc        soft             nofile          4096
@iarc        hard             nofile          4096
```

The same effect can be achieved by creating the file `/etc/security/limits.d/iarc.conf` and entering into it the two abovementioned lines, either for a single user or for a group. The decision for one or the other approach should be based on the internal rules regarding the execution of the server's system administration in which the IMiS/ARChive is to be installed, or on the personal preferences of the main system administrator. The `pam_limits` module of the PAM architecture (Pluggable Authentication Modules for Linux, http://en.wikipedia.org/wiki/Linux_PAM) views all setup commands from the directory `/etc/security/limits.d/` as the configuration file `/etc/security/limits.conf`.

Autostart Setup

Upon installation the IMiS/ARChive server is set to autostart. The autostart of the IMiS/ARChive server during the booting of the operating system can be set manually:
for RHEL and CentOS distributions with the command: **`chkconfig iarcd on`**
for SLES and OpenSuSE distributions with the command: **`chkconfig iarcd on`** or **`yast`**
(`yast`: standard configuration tool in the SLES and OpenSuSE distributions).

The autostart setting of the IMiS/ARC server can be checked:
for RHEL and CentOS distributions with the command : **`chkconfig iarcd –list`**
(shows on which levels the service autostarts)
for SLES and OpenSuSE distributions with the command: **`chkconfig iarcd –list`** or **`yast`**.

It is important for the service to start on levels 3 and 5 as confirmed by the record below:

```
[user1@iarc ~]# sudo chkconfig iarcd –list
iarcd           0:off   1:off   2:on    3:on    4:on    5:on    6:off
```

Testing the Installation and Settings

The test of successful installation can be performed in a few steps:

Step 1

In the installation file `/etc/iarc.conf`, in the section `[Log]`, set the parameter `LogLevel` to value 7 and start the IMiS/ARC server service. The following message appears:

```
[user1@iarc ~]# sudo service iarcd start
Starting IMiS/ARChive HSM Storage Server:                     [  OK  ]
```

Step 2

Check the status of all running processes and their threads with the command `pstree -G`. A list appears, a part of which may be the following (the record may vary according to the distribution):

```
[user1@iarc ~]# sudo pstree -G
init─┬─ ...
...
     ├─iarcd─┬─iarcd───7*[{iarcd}]
        └─iavol───{iavol}
```

Such a record appears when in `iarc.conf`, in the section `[Server]`, the parameter `ConnChilds` has a value of 1, while the `ReqThreads` has a value of 7. The record shows the main process (`iarcd`), which manages the linking process (the other `iarcd`), which has 7 threads, and the process `iavol` which has one thread that manages the volumes of the IMiS/ARC server.

Step 3

With the `netstat -tan` command check whether the linking and administrative processes of the IMiS/ARC server at the TCP port, as defined in `iarc.conf,` are expecting any requests.
If the TCP default port is set, the record contains the following:

```
   [user1@iarc ~]# netstat -tan
   Proto Recv-Q Send-Q    Local Address  Foreign Address      State
   ...
   tcp        0      0    *:16807        *:*                  LISTEN
   tcp        0      0    *:16808        *:*                  LISTEN
```

Step 4

The configuration of the storage profiles and the volumes of the IMiS/ARC server is written out with the command `GetStorageInfo`, located in the directory, together with the rest of the executable programs of the IMiS/ARC server. A defined profile named "Documents", which contains two 8 GB volumes, corresponds with the following record:

```
[user1@iarc ~]# sudo /opt/IS/imisarc/GetStorageInfo

Configured IMiS/ARC storage volumes on Mon May 21 23:22:57 CEST 2012:

Name                        Vol.ID   Obj.count   Spc.used  Spc.free  Prof.ID
-----------------------------------------------------------------------------
/iarc/vol/vol00                 0         0        0.0K      8.0G       0
/iarc/vol/vol01                 1         0        0.0K      8.0G       0
-----------------------------------------------------------------------------

Configured IMiS/ARC storage profiles:
```

```
Name              ID     Obj.count   Spc.assig   Spc.used   Spc.free   Grt.M
----------------------------------------------------------------------------
Documents          0         0         16.0G        0.0K      16.0G     0.0K
----------------------------------------------------------------------------
Summary:                     0         16.0G        0.0K      16.0G     0.0K
```

UPGRADE

Upgrades of the IMiS/ARC server can be performed by a root user or a user with equivalent rights (administrator, qualified staff, etc.). It is advisable to perform the following events when upgrading, depending on the version of the upgraded and new IMiS/ARC servers:

- checking the consistency of the IMiS/ARC server's internal database;
- export of the IMiS/ARC server's internal database;
- upgrade of the executable programs;
- library upgrade (optional);
- expansion of the IMiS/ARC server's database scheme;
- import of the IMiS/ARC server's database after the expansion of the scheme;
- managing the rights and ownership on the IMiS/ARC server's files.

Upgrade Procedure

Step 1

Export of the IMiS/ARC server's base and the making of a safety copy, following the procedure described in different chapters of this manual (chapter PRODUCT MANAGEMENT, subchapter "Configuration"), are necessary prior to the upgrade.

Step 2

Upgrade can take a while, depending mostly on the number of objects stored by the IMiS/ARC server. The IMiS/ARC server is upgraded using the command:

```
[user1@iarc ~]#sudo rpm -Uvh imisarc.7.1.1011-530.0001.bdb.el4.i386.rpm
```

If the upgrade procedure performed correctly, the process shows approximately the following record that can vary from distribution to distribution:

```
Shutting down IMiS/ARChive HSM Storage Server: [  OK  ]

Verifying IMiS/ARChive HSM Storage Server Database (BDB edition)
integrity (this may take a while depending on your object store size)...

Database is consistent!

Exporting IMiS/ARChive HSM Storage Server Database (this may take a while
depending on your object store size)...

Database Export succefull! Upgrade can proceed.

Performing POSTINSTALLATION Actions

Importing exported database files (this may take a while depending on
your object store size)...

Done.
```

Step 3

It is advisable to check the successfulness of the transmission of the existing status of the IMiS/ARC's internal database after the upgrade by exporting the database and verifying the entries into the database's text files (see chapter PRODUCT MANAGEMENT, subchapter "Configuration"), and by verifying the file ownership and volume directories and the contents of the file `/etc/iarc.conf`.

Possible Upgrade Complications

Common Complication No. 1

While attempting an upgrade, an error appears:

```
error: can't create transaction lock on /var/lib/rpm/.rpm.lock
(Permissiondenied)
```

Cause: The user performing an upgrade does not have the corresponding rights.
Solution: A root user login is required for an upgrade or the user must use utilities that grant him the rights equivalent to a root user (`sudo`).

Common Complication No. 2

While attempting an upgrade, a warning appears:

```
Changing ownership of volume mountpoint "/iarc/vol/vol00" recursively to
iarc:iarc (this may take a while).

WARNING: Operation failed. You will need to grant access to directories
and objects for user iarc group iarc manually.
```

Cause: While editing the rights, the volume in the location `/iarc/vol/vol00` could not be reached or there is another reason that prevents the root user from changing the ownership of the files and volume directories.
Solution: It is necessary to connect the disk storage in which the missing volumes are located (in this case also `/iarc/vol/vol00`) and manually set the ownership of the directories and files using the command:

```
[user1@iarc ~]#sudo chown <iarc user>:<iarc group><path> -R
```

In this case:

```
[user1@iarc ~]#sudo chown iarc:iarc /iarc/vol/vol00 -R
```

Common Complication No. 3

While attempting an upgrade, an error appears:

```
ERROR: IMiS/ARChive Storage Server BDB Database consistency check
reported an error in one of the database entities. Manually run
'/opt/IS/imisarc/dbtool -A check' from directory /iarc/db to get extended
error information. IMiS/ARChive upgrade can proceed only when database is
```

```
consistent. You need to manually verify and remove any inconsistency of
the database. UPGRADE ABORTED!
```

Cause: The IMiS/ARC server's internal base is not accessible or is corrupt.
Solution: Check the existence of the directory in which the IMiS/ARC server's internal base should be located; see that it is not empty and that the rights to the files of the internal database are granted to the user that is executing the processes of the IMiS/ARC server. Then start the command:

```
[user1@iarc ~]#sudo su – iarc –s /bin/bash –c "cd /opt/IS/imisarc &&
./dbtool –h <path to internal base> -w <path to internal base> -A check
```

In this case:

```
[user1@iarc ~]#sudo su – iarc –s /bin/bash –c "cd /opt/IS/imisarc &&
./dbtool –h /iarc/db -w /iarc/db -A check
```

which will provide more information on the base corruption. If the error exceeds the knowledge of the administrator that is managing the product, there are different ways that can be used and which are defined in the concluded maintenance contract or any other agreement; with advice from the manufacturer, the error can be removed by the manufacturer's maintenance staff.

When attempting to solve problems concerning the IMiS/ARC server upgrade, also read the chapter "TROUBLESHOOTING" and its subchapters.

REMOVAL

Removal procedure of the IMiS/ARC server can be performed by a root user or a user with equivalent rights (administrator, qualified staff, etc.).

Removal Procedure

Step 1

Check the version of the installed IMiS/ARC server in the `rpm` base (records can vary, depending on the distribution used):

```
[user1@iarc ~]#sudo rpm –q imisarc
imisarc-7.1.1011-530.i386
[user1@iarc ~]#
```

Step 2

Stop the IMiS/ARC server service (see chapter PRODUCT MANAGEMENT, subchapter "Start and Stop Procedure"). This action also implicitly executes the action of removal if it detects a working and running service.

Step 3

Uninstallation of the IMis/ARC installation package is performed with the `rpm` command. It is necessary to enter the entire name from the `rpm` base, as shown in Step 1:

```
[user1@iarc ~]#sudo rpm –e imisarc-7.1.1011-530.i386

This uninstall action WILL NOT:
  * remove IMiS/ARChive web admin module (cgi-bin and html files) from
your www server document and cgi-bin root (if installed)
  * remove IMiS/ARChive configuration file (e.g.: /etc/iarc.conf)
  * remove IMiS/ARChive database files
  * remove IMiS/ARChive log files (location set in /etc/iarc.conf)
  * remove IMiS/ARChive pid file (location in /var/run/iarc or overriden
in /etc/iarc.conf)
  * remove IMiS/ARChive stored objects (on all your volume mountpoints)
  * remove IMiS/ARChive process user (iarc) and group (iarc) accounts
from /etc/passwd and /etc/group
  * revert /etc/services to its pre-installation state

Above actions should be performed manually if required!

Uninstall complete.

[user1@iarc ~]#
```

In the event of problems removing the IMiS/ARC server read the chapter "TROUBLESHOOTING".

PRODUCT MANAGEMENT

A root user or a user with equivalent rights (administrator, qualified staff, etc.) can manage the IMiS/ARC server.

Start and Stop Procedure

A startup script is used to start and stop the IMiS/ARC server. In the case of RHEL or CentOS distribution the `iarcd` script is located in the directory `/etc/rc.d/init.d`; in the case of SLES or OpenSuSE distribution it is in the directory `/etc/init.d`.
Use the startup script with the tool `service` in the following way:

```
[user1@iarc ~]# sudo service iarcd <command>
```

Valid values of the option `<command>` of the startup script are:

`start` This command starts the IMiS/ARC server.
If the startup is successful, the script displays:

```
Starting IMiS/ARChive HSM Storage Server: [  OK  ],
```

and if the startup is not successful:

```
Starting IMiS/ARChive HSM Storage Server:  [FAILED].
```

`stop` This command stops the IMiS/ARC server.
If the shutdown is successful, the script displays:

```
Shutting down IMiS/ARChive HSM Storage Server: [  OK  ],
```

and if the shutdown is not successful:

```
Shutting down IMiS/ARChive HSM Storage Server:  [FAILED].
```

`restart` This command performs a restart of the IMiS/ARC server. It is actually a sequence of the commands `start` and `stop` and therefore the records on the console are the same as if both commands were performed in succession.

`status` This command displays the status of the service of the IMiS/ARC server. If it is running, the process identification numbers are displayed as well:

```
Status of IMiS/ARChive HSM Storage Server: iarcd (pid 6222 6216)
is running ...
```

and if the service has been stopped:

```
Status of IMiS/ARChive HSM Storage Server: iarcd is stopped
```

In the event of problems starting the IMiS/ARC server read the chapter “TROUBLESHOOTING” and its subchapters.

Logging the Operation Events (into Logs)

Logging of events is intended for the testing of operation which is performed occasionally or when needed by a server administrator or the IMiS/ARC server administrator. The IMiS/ARC server logs the events according to the set logging levels in the configuration file `/etc/iarc.conf`. The default location of the logs is the directory `/var/log/iarc`. The active log, in which the IMiS/ARC server logs current events, can be found in the location `/var/log/iarc/iarc.log`; older events are saved in archive files of the log and are created when needed, according to the settings with a title scheme `/var/log/iarc/iarc.XX.log` (XX = the sequence of the archive file; the larger the number, the older the event). Logging into logs is performed by the IMiS/ARC server according to the FILO principle ("FILO – first in/last out").

The number of the archive logs and their size can be set in the configuration file `/etc/iarc.conf`, in the section `[Log]`. The time of the information outage from the log can be adjusted by setting the number and size of logs, depending on the quantity of the entries. Good practice suggests settings that enable level 6 information storage for at least three months.

There are 7 levels of logging. Each level means the level of information details that the IMiS/ARC server logs into the log.

Level 0 – Emergency
Records of the so-called null level are errors that prevent further operation of the IMiS/ARC server. They represent a severe error and a probable degradation of the integrity of the IMiS/ARC server's data; when such an error appears, the IMiS/ARC server shuts down immediately and continuation is not possible without intervention from the server administrator. Such errors are usually caused by external devices, e.g. failure of key parts of the server hardware.

Level 1 – Alert
Entries of this level are errors due to which the IMiS/ARC server does not necessarily stop operating. It stops operating if continuation could cause the corruption of the internal base of the IMiS/ARC server or objects. Such errors can be caused by hardware failure, detection of irregular operation of the functions of the operating system, server overload or interference from another program in the IMiS/ARC server's environment or an invalid attempt to configure profiles and volumes.

Level 2 – Critical
Entries of the second level are errors that cause the IMiS/ARC server to stop operating, because continuation could cause the corruption of the internal base of the IMiS/ARC server or objects. Such errors can be caused by detection of irregular operation of the

functions of the operating system, , lack of resources of the operating system or a detected errorin the operation of the IMiS/ARC server.

Level 3 – Error
Entries of the third level are errors that are not critical and do not represent possible data corruption, but that an error in operation was detected by the IMiS/ARC server. Such errors can be caused by the client, use of invalid or inappropriate IMiS/ARC server configuration parameters or by invalid entries into the IMiS/ARC server's base.

Level 4 – Warning
Entries of the fourth level are warnings of the IMiS/ARC server detecting malfunctions that do not interfere substantially with the operation of the IMiS/ARC server and are mostly caused by irregular requests from clients and seldom by invalid entries into the IMiS/ARC server's base or the configuration file.

Level 5 – Notice
Entries of the fifth level are entries concerning important regular (normal) events on the IMiS/ARC server that could interest administrators.

Level 6 – Info
Entries of the sixth level are entries about less important regular (normal) events on the IMiS/ARC server that could interest administrators.

Level 7 – Debug
Entries of the seventh level are uncondensed entries about all the events on the IMiS/ARC server that are used to collect precise data on the operation of the server when causes for the error or warning are not evident.

The IMiS/ARC administrator should pay attention to events from level 4 to 0 because they can detect problems in the operation of the server and in the operation of the IMiS/ARC server, as well as in communication with the clients.

Configuration

Configuration is performed by the root user `root` or a user with equivalent rights using the `sudo` tool with the IMiS/ARC server user account credentials to prevent the corruption of the IMiS/ARC server's internal base.

Expected Tasks

- setting the server parameters in the configuration file `/etc/iarc.conf`
- profile and volume configuration.

The console tools for working with the IMiS/ARC server's internal base are:

`dbtool` This tool enables the IMiS/ARC server administrator to manage the internal database. This tool can only be used once when there are no client requests that would result in changes in the IMiS/ARC server's internal base; it is best used when the IMiS/ARC server is not in operation or is on stand-by.

Syntax:

```
dbtool: -A or any of -CEILMOPSTX must be specified.
usage: dbtool [-a] [-V] [-q(uiet)] [-A]/[-ECILMOPSTX]
       [-h database_dir] [-w working_dir]
[-c compression_txt][-e externid_txt]
[-i lastid_txt] [-l compresslib_txt] [-m volume_txt]
[-o object_txt] [-x auditlog_file] [-p profile_txt]
[-s store_txt] [-t mime_txt]
exp|imp|init|check
```

`db_hotbackup` This tool is used to create a backup copy of the IMiS/ARC server's internal base. This tool can be used during the server's operation.

Syntax:

```
usage: db_hotbackup [-cDuVv]
       [-d data_dir] [-h home] [-l log_dir][-P password]
-b backup_dir
```

`GetStorageInfo` This tool is used to configure profiles, volumes and occupancy data.

Syntax:

```
usage: GetStorageInfo [ path-to-iarc.conf]
```

(together with the path if it is not located in the default location – `/etc`].)

Process of Configuration with Console Tools

Export of the IMiS/ARC server's internal base is performed using the command (records can vary, depending on the server's configuration):

```
[user1@iarc ~]# sudo su – iarc –s /bin/bash –c "cd /opt/IS/imisarc &&
./dbtool –h /iarc/db -w /iarc/db –A exp"
```

```
Exporting iarc.object.db:data (0 records) to object.txt ...  OK.
Exporting iarc.other.db:profile (1 records) to profile.txt ...  OK.
Exporting iarc.other.db:volume (4 records) to volume.txt ...  OK.
Exporting iarc.other.db:compression (1 records) to compression.txt ...  OK.
Exporting iarc.other.db:compresslib (6 records) to compresslib.txt ...  OK.
Exporting iarc.other.db:objtype (1334 records) to objtype.txt ...  OK.
Exporting iarc.other.db:store (1 records) to store.txt ...  OK.
Exporting iarc.externid.db:extid (0 records) to externid.txt ...  OK.
Exporting audit log data (6 records) to auditlog.bin ...  OK.
Exporting iarc.other.db:lastid (3 records) to lastid.txt ...  OK.
Export command completed  with no errors.
```

Note: Numbers (`XX records`) next to each line can change, depending on the number of records.

The result is 9 text files and one binary file. Each of these files contains a part of the IMiS/ARC server's internal base.

Creating a backup copy of the IMiS/ARC server's internal base:

1. create a directory that will contain the backup copy of the IMiS/ARC server's internal base:

   ```
   [user1@iarc ~]# sudo mkdir/iarc/dbbackup
   ```

2. set the ownership of the user account of the IMiS/ARC server to the directory:

   ```
   [user1@iarc ~]# sudo chowniarc:iarc /iarc/dbbackup
   ```

3. create a backup copy of the IMiS/ARC server's internal base (records can vary, depending on the contents of the directory containing the files of the internal base):

   ```
   [user1@iarc ~]# sudo su – iarc –s /bin/bash –c "cd /opt/IS/imisarc &&
   ./db_hotbackup –v –h /iarc/db –b /iarc/dbbackup"
   db_hotbackup: hot backup started at Tue Oct 11 13:45:44 2011
   db_hotbackup: copying /iarc/db/iarc.audituser.db to
   /iarc/dbbackup/iarc.audituser.db
   db_hotbackup: copying /iarc/db/iarc.auditsession.db to
   /iarc/dbbackup/iarc.auditsession.db
   db_hotbackup: copying /iarc/db/iaobjs.bin to /iarc/dbbackup/iaobjs.bin
   db_hotbackup: copying /iarc/db/iarc.auditfmtstr.db to
   /iarc/dbbackup/iarc.auditfmtstr.db
   db_hotbackup: copying /iarc/db/iarc.other.db to
   /iarc/dbbackup/iarc.other.db
   db_hotbackup: copying /iarc/db/iarc.auditaddr.db to
   /iarc/dbbackup/iarc.auditaddr.db
   db_hotbackup: copying /iarc/db/iarc.externid.db to
   /iarc/dbbackup/iarc.externid.db
   db_hotbackup: copying /iarc/db/iarc.auditsessidx.db to
   /iarc/dbbackup/iarc.auditsessidx.db
   db_hotbackup: copying /iarc/db/iarc.auditeventidx.db to
   /iarc/dbbackup/iarc.auditeventidx.db
   db_hotbackup: copying /iarc/db/iarc.auditcompname.db to
   /iarc/dbbackup/iarc.auditcompname.db
   db_hotbackup: copying /iarc/db/iarc.auditevent.db to
   /iarc/dbbackup/iarc.auditevent.db
   db_hotbackup: copying /iarc/db/iarc.object.db to
   /iarc/dbbackup/iarc.object.db
   db_hotbackup: copying /iarc/db/log.0000000001 to
   /iarc/dbbackup/log.0000000001
   db_hotbackup: copying /iarc/db/log.0000000002 to
   /iarc/dbbackup/log.0000000002
   db_hotbackup: copying /iarc/db/log.0000000003 to
   /iarc/dbbackup/log.0000000003
   ```

```
db_hotbackup: copying /iarc/db/log.0000000004 to
/iarc/dbbackup/log.0000000004
db_hotbackup: lowest numbered log file copied: 1
db_hotbackup: /iarc/dbbackup: run catastrophic recovery
db_hotbackup: /iarc/dbbackup: remove unnecessary log files
db_hotbackup: hot backup completed at Tue Oct 11 13:45:53 2011
[user1@iarc ~]#
```

The result of this procedure is a copy of the IMiS/ARC server's internal base in the directory `/iarc/dbbackup`. After a longer period of use of the IMiS/ARC server, it is advisable to add a `–c` switch when performing the command to clean the transaction log back to the last completed transaction.

Checking the consistency of the IMiS/ARC server's internal base:

Log on to the console as a root user or a user with equivalent rights and start the command:

```
[user1@iarc ~]# sudo su – iarc –s /bin/bash –c "cd /opt/IS/imisarc &&
./dbtool –h /iarc/db –w /iarc/db –A check"
```

If the IMiS/ARC server's internal base is consistent, the console displays:

```
check command successfully completed.
```

In the case of errors, the record is different and can vary greatly. The cause for the error must be recognized from the feedback information text; common causes can be recognized from the chapter "TROUBLESHOOTING" and its subchapters.

Adding HSM profiles:

4. create a backup copy of the IMiS/ARC server's internal base (see chapter "Creating a backup copy of the IMiS/ARC server's internal base")
5. stop the operation of the IMiS/ARC server (see PRODUCT MANAGEMENT, subchapter "Start and Stop Procedure")
6. export the IMiS/ARC server's internal base into .txt files (see this chapter, section "Export of the IMiS/ARC server's internal base")
7. edit the `/iarc/db/profile.txt` file and add a new line at the end with a new sequential number (unique identification number) and a definition of a new profile, whose name must not be repeated:

   Example:

   ```
   0,"Documents","",9500,7500,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
   ,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
   ,0,0,0,0,0,0
   1,"IncomingMail","",9500,7500,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
   0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
   0,0,0,0,0,0,0,0
   ```

8. import only the text file of the profile table of the IMiS/ARC server's internal base:

```
[user1@iarc ~]# sudo su – iarc –s /bin/bash –c "cd /opt/IS/imisarc &&
./dbtool –h /iarc/db –w /iarc/db –P imp"
```

9. check the adequacy of the import of the profile table and the consistency of the IMiS/ARC server's internal base by checking the text files after export:

```
[user1@iarc ~]# sudo su – iarc –s /bin/bash –c "cd /opt/IS/imisarc &&
./dbtool –h /iarc/db –w /iarc/db –A check"
check command successfully completed.
[user1@iarc ~]# sudo su – iarc –s /bin/bash –c "cd /opt/IS/imisarc &&
./dbtool –h /iarc/db –w /iarc/db –A exp"
[user1@iarc ~]# sudo less /iarc/db/profile.txt
```

10. If the content of the `/iarc/db/profile.txt` file corresponds to the completed changes prior to import, the IMiS/ARC server can be started (see PRODUCT MANAGEMENT, subchapter "Start and Stop Procedure")

11. In case of problems, refer to the chapter "TROUBLESHOOTING" and its subchapters.

A new profile has thus been added successfully.

Adding HSM volumes:

12. create a backup copy of the IMiS/ARC server's internal base (see chapter "Creating a backup copy of the IMiS/ARC server's internal base")

13. stop the operation of the IMiS/ARC server (see PRODUCT MANAGEMENT, subchapter "Start and Stop Procedure")

14. export the IMiS/ARC server's internal base into .txt files (see this chapter, section "Export of the IMiS/ARC server's internal base")

15. create a new directory on the disk that has enough space left for a new volume and edit the ownership of the directory so that the user performing IMiS/ARC processes has the right to read and write in this directory:

```
[user1@iarc ~]# sudo mkdir /iarc/vol/vol06
[user1@iarc ~]# sudo chmod 750 /iarc/vol/vol06
[user1@iarc ~]# sudo chown iarc:iarc /iarc/vol/vol06
```

16. edit the `/iarc/db/volume.txt` file and add a new line at the end with a new sequential number (unique identification number) and a definition of a new volume, whose name must not be repeated. Field No. 8 should contain the identification number of the profile to which the new volume will belong.
Example:

```
0,"Vol00","","/iarc/vol/vol00",1145585993,8388608,0,0,0,0,0
1,"Vol01","","/iarc/vol/vol01",1145585993,8388608,0,0,0,0,0
2,"Vol02","","/iarc/vol/vol02",1145585993,8388608,0,1,0,0,0
```

```
3,"Vol03","","/iarc/vol/vol03",1145585993,8388608,0,1,0,0,0
4,"Vol04","","/iarc/vol/vol04",1145585993,8388608,0,1,0,0,0
5,"Vol05","","/iarc/vol/vol05",1145585993,8388608,0,0,0,0,0
6,"Vol06","","/iarc/vol/vol06",1145585993,8388608,0,0,0,0,0
```

17. import only the text file of the volume table of the IMiS/ARC server's internal base:

    ```
    [user1@iarc ~]# sudo su – iarc –s /bin/bash –c "cd /opt/IS/imisarc &&
    ./dbtool –h /iarc/db –w /iarc/db –M imp"
    ```

18. check the adequacy of the import of the volume table and the consistency of the IMiS/ARC server's internal base by checking the text files after export:

    ```
    [user1@iarc ~]# sudo su – iarc –s /bin/bash –c "cd /opt/IS/imisarc &&
    ./dbtool –h /iarc/db –w /iarc/db –A check"
    check command successfully completed.
    [user1@iarc ~]# sudo su – iarc –s /bin/bash –c "cd /opt/IS/imisarc &&
    ./dbtool –h /iarc/db –w /iarc/db –A exp"
    [user1@iarc ~]# sudo less /iarc/db/volume.txt
    ```

19. If the content of the file `/iarc/db/volume.txt` corresponds to the completed changes prior to import, the IMiS/ARC server can be started (see PRODUCT MANAGEMENT, subchapter "Start and Stop Procedure")

20. In case of problems, refer to the chapter "TROUBLESHOOTING" and its subchapters.

A new volume has thus been successfully added and assigned to an existing profile.

Administration

Administration tasks can have a significant effect on product operation. A correct system installation and configuration can provide a stable and expected product operation with little or no maintenance interventions; if the configuration is incorrect or incompatible, the system can become compromised and unstable, can operate slowly and its security can become vulnerable. Therefore, interventions into the product administration must be restricted to qualified administrators that are familiar in detail with the manufacturer's instructions and general good practice in the planning and maintenance of information systems. It is advised upon purchase to establish a maintenance contract with the manufacturer, which ensures impeccable and continuous operation of a mission-critical system, which this archive system should represent.

The IMiS/ARC server administrator has access to the administration module and can perform administration tasks as a root (or equivalent) user in the user environment when required.

The IMiS/ARC server administrator can set the parameters in the configuration file depending on the use of the IMiS/ARC server resources and monitor them by periodically checking the server status, log records and requirements of the application environment. In addition to the management of storage profiles and their corresponding volumes, planning server resources, controlling the use of resources and properly adjusting the parameters, the administrator also ensures continuous operation of the IMiS/ARC server over a longer period of time.

It is advisable to create a backup copy of the IMiS/ARC server's internal base and configuration file prior to every intervention in case the restoration of old settings is needed because the adjustment of the settings and/or base was incorrect.

Configuration File iarc.conf

Configuration parameters of the IMiS/ARC server can be set in the file `/etc/iarc.conf`. Default values are used in the following descriptions. Parameters are divided into sections, depending on their purpose and are discussed in detail later on; their following division is made according to the principle:

`Key`: Description (optional set of valid, minimal, maximal, recommended `values`)

Section [Server]

`Path:` Marks the absolute path to the executable files (programs) and libraries of the IMiS/ARC server. The default value is `/opt/IS/imisarc`.

`ConnChilds:` Marks the number of simultaneous linking processes of the IMiS/ARC server. The default and recommended value is `1`; it can be increased if the number of demanded simultaneous sessions with clients exceeds 1024 for every 1024 new sessions. The value does not have an upper limit; however, values over `10` are not sensible performance-wise and can lead to problems.

`ReqThreads:` Marks the number of threads that are executing requests. The default value is `7` and does not have an upper limit. The recommended value is two times the number of threads that the server's processor is capable of executing simultaneously and depends on the number of processor cores.

`StatisticsCycle:` Marks the number of seconds during the task of calculating the statistics, which the IMiS/ARC server maintains regarding operation. The default and recommended value is `180000`. Changing the value downwards may affect the server responsiveness. The lowest value is `1`, the highest `16777216`.

`ClientTimeout:` Marks the time of the client's inactivity in seconds that must pass for the IMiS/ARC server to stop the session. The default value is `3600` seconds. The lowest possible value is `1800` and the highest `86400`.

`AdminPassword:` Marks an encrypted condensed value of the administration password of the IMiS/ARC server through an administrative web interface.

`IdentPassword:` Marks an encrypted condensed value of the password used by the IMiS/ARC server for operation in encryption processes. The value must not be changed after archiving the first object because this value affects the encrypting algorithm for generating the object identifiers.

`Port :` Marks the number of the TCP port at which the linking process of the IMiS/ARC server expects requests from clients. The default value is `16807`.

`Listen:` Marks the network address through which the IMiS/ARC server connects the TCP port at which it expects requests from clients. The values can only be in accordance with the IPv4 or IPv6 title scheme. Examples of valid values:

```
192.168.92.32
fd00:192:168:92::32
192.168.92.32:16807
[fd00:192:168:92::32]:16807
[fd00:192:168:92:2340:efa1:1244:32]
fd00:192:168:92:2340:efa1:1244:32
[fd00:192:168:92:2340:efa1:1244:32]:12345
[::ffff:192.168.92.12]
::ffff:192.168.92.12
[::ffff:192.168.92.12]:65743
localhost
[::]
```

`CXLib:` Marks the relative path to the libraries that contain compression methods for various client platforms within the path that marks the above described `Path` parameter value.

`PartialTimeout:` Marks the time in seconds in which the client must respond to the IMiS/ARC server request. After this time, the server stops the session. The lowest value is `1`, the highest `60` and the recommended `5`.

`PidPath:` Marks the path to the identification file of the IMiS/ARC server's main process. The default value is `/var/run/iarc`.

Section [Database]

`Path:` Marks the absolute path to the IMiS/ARC server's internal base. The default value is `/iarc/db`

Section [Cache]

`ReadPath:` Marks the path to the directory that represents a buffer where the IMiS/ARC server deposits the objects that need to be temporarily deposited for faster object forwarding to the clients. The path rights must be arranged in such a way that the user performing IMiS/ARC processes has the right to read and write files.

`ReadSize:` Marks the smallest size of the buffer. The IMiS/ARC server adapts this limit dynamically, depending on the needs; changing the values is not sensible.

`EditPath:` Marks the path to the directory that represents a buffer where the IMiS/ARC server temporarily deposits objects forwarded by clients. The path rights must be arranged in such a way that the user performing IMiS/ARC processes has the right to read and write files.

`EditSize:` Marks the smallest size of the buffer. The IMiS/ARC server adapts this limit dynamically, depending on the needs; changing the values is not sensible.

Section [Log]

`LogFile:` Marks the basic name of a log file, together with the path to which the IMiS/ARC server logs events. The path and file rights must be arranged in such a way that the user performing IMiS/ARC processes can enter files and create new files if need be.

`MaxSize:` Marks the maximum size of one log file in bytes. The default and recommended value is `1000000`, the lowest `65536` and the highest `2147483648`.

`BackupCount:` Marks the number of archive log files to which the IMiS/ARC server logs events using the first in – last out algorithm. The default value is `1` and the recommended one `9`.

`LogLevel:` The level of events that the IMiS/ARC server logs into the log file (see chapter “Logging of Operation Events (into Logs)”. The lowest value is `1`, the highest `7`, and the recommended `6`.

Section [Admin]

`Timeout:` The time of inactivity in seconds that passes before the IMiS/ARC server closes the session for administrative interventions. The recommended value is `300`.

`WebPath:` The path to the relative root path of the administrative module, seen from the root directory of the local web server that hosts the administrative module of the IMiS/ARC server. The default value is `/iarc/`.

`Port:` Marks the number of the TCP port at which the linking process of the IMiS/ARC server expects requests from clients. The default value is `16808`.

`Listen:` Marks the IP number to which the IMiS/ARC server connects the TCP port at which it expects requests from the administrative module. The values can only be in accordance with the IPv4 or IPv6 title scheme. Examples of valid values:

```
192.168.92.32
fd00:192:168:92::32
192.168.92.32:16807
[fd00:192:168:92::32]:16807
[fd00:192:168:92:2340:efa1:1244:32]
fd00:192:168:92:2340:efa1:1244:32
[fd00:192:168:92:2340:efa1:1244:32]:12345
[::ffff:192.168.92.12]
::ffff:192.168.92.12
[::ffff:192.168.92.12]:65743
localhost
[::]
```

Section [AdminLog]

`LogFile:` Marks the basic name of the log file together with the path to which the IMiS/ARC server logs events connected with the interventions made through the administrative module. The path and file rights must be arranged in such a way that the user performing IMiS/ARC processes can enter files and create new files if need be.

`MaxSize:` Marks the maximum size of one log file in bytes. The default and recommended value is `1000000`, the lowest `65536` and the highest `2147483648`.

`BackupCount:` Marks the number of archive log files to which the IMiS/ARC server logs events using the first in – last out algorithm. The default value is `1` and the recommended one 5.

Section [AuditLog]

`Enabled:` By selecting value `1` the object operations log is enabled; by selecting value `0` the object operations log is disabled. The IMiS/ARC server logs events in an encrypted form to the internal database.

`XXXXX_Events:` (OPTIONAL) Marks a set of operations on objects of the XXXXX profile (profile name, not its identification number) which the IMiS/ARC server logs into the log as events. The valid set of

operations on objects:
`create` (creating an object)
`update` (saving an object)
`delete` (deleting an object)
`openrw` (opening an object to read and change)
`openro`(opening an object to read)
This setting replaces the general settings under the `Events` setting.

`RequiredParams:` The set of required data that the client must deliver when opening a session or an event. If a single required piece of data is missing, the IMiS/ARC server declines the establishment of a session or event. The valid set of required data may contain at least one of the following:
`username` (username of the user that performs the operation)
`computername` (name of the computer from which the operation originates)
`message` (cause/message that the user enters when performing an operation)
The default value is `username, computername`.

`AuthCryptoModes:` Marks the set of potential cryptographic methods that the IMiS/ARC server allows to be used for encryption of the authentication messages and for subsequent communication with the client that wishes to inspect the Audit Log. The identifier represents a combination of an algorithm, key length and a cryptographic method of data packet processing. Valid values are:

```
aes-256-cbc
aes-256-ecb
aes-256-ofb
aes-256-cfb
aes-192-cbc
aes-192-ecb
aes-192-ofb
aes-192-cfb
aes-128-cbc
aes-128-ecb
aes-128-ofb
aes-128-cfb
```

`AuthPreSharedKey:` A cached server key that is used to encrypt the authentication messages and subsequent communication with the client that represents an authorized person for the purpose of access to the Audit Log of the logging of events connected with the sessions and/or objects.

Section [Authentication]

`Methods:` Marks the possible set of methods for the establishment of a session between the client and the IMiS/ARC server. The valid set of values is:

```
basic
advanced
```

Basic (`basic`) represents the older method of establishing a session with the server without forwarding the recorded data on the client; advanced (`advanced`) includes the more complicated (HMAC) method of establishing a session with the server that predicts necessary and unnecessary metadata on the client and (optional) encrypted exchange of network authentication packages.

`CryptoModes:` Marks the set of possible cryptographic methods that the IMiS/ARC server uses for encrypted communication with the client. The identifier represents a combination of an algorithm, key length and a cryptographic method of data packet processing. Valid values are:

```
aes-256-cbc
aes-256-ecb
aes-256-ofb
aes-256-cfb
aes-192-cbc
aes-192-ecb
aes-192-ofb
aes-192-cfb
aes-128-cbc
aes-128-ecb
aes-128-ofb
aes-128-cfb
```

`PreSharedKey:` A cached server key that is used to encrypt the authentication messages and subsequent communication with the client that represents an ordinary, non-privileged client of the IMis/ARC server.

`RequiredParams:` The set of required data that the client must deliver when opening a session or an event. If a single required piece of data is missing, the IMiS/ARC server declines the establishment of a session or event. The valid set of required data may contain at least one of the following:

`username` (username of the user that performs the operation)

`computername` (name of the computer from which the operation originates)

`message` (cause/message that the user enters when performing an operation)

The default setting is empty – it does not contain any itemfrom the set.

Structure of Important Files of the IMiS/ARC Server Internal Base

Profile Table and profile.txt

The line in file `profile.txt` represents an event that marks an individual profile. Example:

```
0,"Documents","",9500,7500,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0
```

Fields are counted from left to right; they are divided by commas and the administrator uses/corrects only the first three fields.

- field No. 1: a unique sequential number of the storage profile and simultaneously a profile identification number that the IMiS/ARC server uses for operations connected with the profile. Possible values are from (including) `0` to `4294967295`;
- field No. 2: a unique profile name. We recommend names as short as possible, yet ones that contain the information that enables the administrator to logically connect the profile to the application, document type etc. which will be saved to this profile. The field must not contain more than 15 characters. Valid characters are letters, numbers and the character "–";
- field No. 3: a description/purpose of the profile. Unlike the first two fields, this one merely provides descriptive information to the IMiS/ARC server administrator. This field can also be empty. The field must not contain more than 63 characters. Valid characters are letters, numbers and the character "–".

Volume Table and volume.txt

The line in file `volume.txt` represents an event that marks an individual volume. Example:

```
0,"Vol00","","/iarc/vol/vol00",1145585993,8388608,0,0,0,0,0
```

Fields are counted from left to right; they are divided by commas.

- field No. 1: a unique sequential number of the storage profile and simultaneously a profile identification number that the IMiS/ARC server uses for operations connected with the volume. Possible values are from (including) `0` to `4294967295`.
- field No. 2: a unique volume name. We recommend names as short as possible. The field must not contain more than 15 characters. Valid characters are letters, numbers and the character "–". It concerns descriptive information for the IMiS/ARC server administrator.

- field No. 3: a description/purpose of the profile. The information is descriptive. This field can also be empty. The field must not contain more than 63 characters. Valid characters are letters, numbers and the character "–".
- field No. 4: contains the name of the directory that represents the logical volume to which the IMiS/ARC will deposit objects belonging to this volume. This field must not contain more than 255 characters. Only characters that are regular characters for labeling directories and files on UNIX/Linux file systems can be used. In any case, avoid using the following characters: "| ; , ! @ # $ ( ) <> \ " ' ` ~ { } [ ] = + & ^ <space><tab>"; if their use is necessary, use the “escaped” sequence of characters.
- field No. 5: the device type that contains the volume. Only one type is currently known – a local disk, because the use of other device types is not sensible in view of the relatively low disk prices. The set of values:
  1145585993: local disk
- field No. 6: volume size in kB that represents the range limit to which the IMiS/ARC server saves objects to this volume. The recommended value is 8GB. Increasing the value above 32GB can, depending on the server capacity, affect the responsiveness of the IMiS/ARC server.
- field No. 7: volume occupancy in kB. This field is managed by the IMiS/ARC server and must not be manually changed because the IMiS/ARC server will correct the value to the actual value after completing the volume inspection that is performed at the startup of the server. An empty volume in this field has the value 0.
- field No. 8: identification number of the storage profile to which the volume belongs.

TROUBLESHOOTING

In the event of problems and errors, it is important that the administrators and users act appropriately.

A potential unprofessional intervention could cause additional deterioration of the state of the IMiS/ARC server and consequently greater difficulties in eliminating the error. Users/Administrators must be acquainted with the correct use of the product and act in accordance with the user documentation. It is recommended that in the event of difficulties they turn to the appropriate expert within the organization (system administrators). System administrators are advised to refer to the documentation in order to determine the location of the error and, if need be, consult with the technical experts of the manufacturer on further action/steps.

How to Avoid Problems

Regular, periodic checks of the operation of the IMiS/ARC server are of crucial importance in detecting potential problems and errors in operation in time. These checks include an inspection of the coordination of the disk system (independent disk or disk array) and the file system. Problems with the disk system can be avoided by choosing reliable hardware and making sure that the used disk storage is connected on the server locally with the proper redundancy. Avoid NAS disk systems or the joint use of disks on other servers or disk storage that can be accessed via a local network.

You should also periodically check the consistency of the internal base of the IMiS/ARC server. This procedure is described in the chapter PRODUCT MANAGEMENT, subchapter "Configuration".

Also of crucial importance is the optional valid maintenance contract with the product's manufacturer, which protects the user from severe errors or outages of the system. Several types of maintenance contracts can be concluded, from primary ones, where the manufacturer takes on all maintenance procedures of the system, to secondary ones, where the manufacturer provides the solution of severe, less common errors, while the user's IT service takes on the elimination of simpler errors and more regular maintenance procedures. Maintenance contracts are part of an agreement between the manufacturer and the buyer; therefore, the details of such are not relevant to this documentation.

Common Problems

Common Problem No. 1

When attempting to view an object stored on the IMiS/ARC server with an IMiS/Scan or IMiS/View client, “Error 61523” appears. Other clients (e.g. IMiS/Storage Connector) report the error:

```
IMiS/ARC Client <IASession.Open> Failed to establish connection to the
cluster node <10.1.1.10, 16807> (Reason: Error <TimedOut> occurred while
opening network connection.).
```

The IMiS/ARC server is accessible over a network; however, the service at the listening port is not accessible (checked with the `telnet` program)

```
[user1@test ~]# ping iarc.acme.com
PING iarc.acme.com (10.1.1.10) 56(84) bytes of data.
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=1 ttl=64 time=0.653 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=2 ttl=64 time=0.190 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=3 ttl=64 time=0.186 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=4 ttl=64 time=0.183 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=5 ttl=64 time=0.164 ms

--- iarc.acme.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 0.164/0.450/1.530/0.540 ms

[user1@test ~]# telnet iarc.acme.com 16807
Trying 10.0.0.10...
.. (longer pause) ...
telnet: connect to address 10.1.1.10: Connection timed out
[user1@test ~]#
```

The IMiS/ARC server is operational, which is checked with a console command on the server on which it is installed:

```
[user1@iarc ~]# sudo service iarcd status
Status of IMiS/ARChive HSM Storage Server: iarcd (pid 23209 23203) is
running...
[user1@iarc ~]#
```

Cause of problem: The firewall on the server or on the network between the client and the server is preventing the clients from communicating with the IMiS/ARC server through the 16807 TCP port or other, if the TCP port is set differently in the `/etc/iarc.conf` file.
Solution to the problem: The firewall must be reconfigured so as to allow communication of the clients with the IMiS/ARC server.

Common Problem No. 2

When attempting to store a new object on the IMiS/ARC server with the IMiS/Scan client, “Error #201” appears. When attempting to store the object from the server, other clients (e.g. IMiS/Storage Connector) receive the following reply:

```
IMiS.IMiSARC.Client.IAClientException: Server reported error while
creating an object (Reason: Invalid or unknown profile used
(IACM_INVPROFID)).
```

The IMiS/ARC server is otherwise accessible over a network; the service at the listening port is responsive (checked with the `telnet` program)

```
[user1@test ~]# ping iarc.acme.com
PING iarc.acme.com (10.1.1.10) 56(84) bytes of data.
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=1 ttl=64 time=0.653 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=2 ttl=64 time=0.190 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=3 ttl=64 time=0.186 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=4 ttl=64 time=0.183 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=5 ttl=64 time=0.164 ms

--- iarc.acme.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 0.164/0.450/1.530/0.540 ms

[user1@test ~]# telnet iarc.acme.com 16807
Trying 10.1.1.10...
Connected to iarc.acme.com.
Escape character is '^]'.
Connection closed by foreign host.
[user1@test ~]#
```

The IMiS/ARC server is operational, which is additionally checked with a console command on the server on which it is installed:

```
 [user1@iarc ~]# sudo service iarcd status
Status of IMiS/ARChive HSM Storage Server: iarcd (pid 23209 23203) is
running...
[user1@iarc ~]#
```

Cause of problem: The client is trying to store the object into a nonexistent storage profile.
Solution to the problem: Check the settings of the default profile for storing on the IMiS/ARC server, which was used in the storage attempt. The procedure for adding a new profile is described in the chapter PRODUCT MANAGEMENT, subchapter "Configuration".

Common Problem No. 3
When attempting to store a new object on the IMiS/ARC server with the IMiS/Scan client, “Error #14” appears. When attempting to store the object from the server, other clients (e.g. IMiS/Storage Connector) receive the following reply:

```
IMiS.IMiSARC.Client.IAClientException: Server reported error while
updating an object (Reason: Profile is out of space (IACM_NOSPACE)).
```

The IMiS/ARC server is otherwise accessible over a network; the service at the listening port is responsive (checked with the `telnet` program)

```
 [user1@test ~]# ping iarc.acme.com
PING iarc.acme.com (10.1.1.10) 56(84) bytes of data.
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=1 ttl=64 time=0.653 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=2 ttl=64 time=0.190 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=3 ttl=64 time=0.186 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=4 ttl=64 time=0.183 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=5 ttl=64 time=0.164 ms

--- iarc.acme.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 0.164/0.450/1.530/0.540 ms

[user1@test ~]# telnet iarc.acme.com 16807
Trying 10.1.1.10...
Connected to iarc.acme.com.
Escape character is '^]'.
Connection closed by foreign host.
[user1@test ~]#
```

The IMiS/ARC server is operational, which is additionally checked with a console command on the server on which it is installed:

```
 [user1@iarc ~]# sudo service iarcd status
Status of IMiS/ARChive HSM Storage Server: iarcd (pid 23209 23203) is
running...
[user1@iarc ~]#
```

Cause of problem: All the volumes in the storage profile that was used when storing the new object have been filled.

Solution to the problem: Add an appropriate number of new volumes to the profile of the IMiS/ARC server which ran out of space. The procedure is explained in the chapter PRODUCT MANAGEMENT, subchapter "Configuration".

Common Problem No. 4

At the startup of the IMiS/ARC server, this record appears on the console:

```
[user1@iarc ~]# sudo service iarcd start

WARNING: Network subsystem not running or (RT)NETLINK interface not
configured in this kernel. If you're sure that your network is UP you can
ignore this message. Continue loading IMiS/ARChive HSM Storage Server...

Starting IMiS/ARChive HSM Storage Server:                    [  OK  ]
[user1@iarc ~]#
```

The IMiS/ARC server is not accessible over a network:

```
[user1@test ~]# ping iarc.acme.com
PING iarc.acme.com (10.1.1.10) 56(84) bytes of data.
... (pause) ...
From 192.168.92.32 icmp_seq=2 Destination Host Unreachable
From 192.168.92.32 icmp_seq=3 Destination Host Unreachable
From 192.168.92.32 icmp_seq=4 Destination Host Unreachable
```

```
... (abort test with CTRL-C) ...
^C
--- iarc.acme.com ping statistics ---
7 packets transmitted, 0 received, +3 errors, 100% packet loss, time
6937ms
[user1@test ~]#
```

Cause of problem: At the startup of the IMiS/ARC server the network subsystem of the operating system did not run.
Solution to the problem: The operation of the network subsystem must be established and the IMiS/ARC server restarted. If the message reappears, it is probably a matter of incompatibility of the IMiS/ARC server with the operating system.

Common Problem No. 5

At the startup of the IMiS/ARC server, this record appears on the console:

```
 [user1@iarc ~]# sudo service iarcd start

WARNING: Network subsystem not running or (RT)NETLINK interface not
configured in this kernel. If you're sure that your network is UP you can
ignore this message. Continue loading IMiS/ARChive HSM Storage Server...

Starting IMiS/ARChive HSM Storage Server:                    [  OK  ]
[user1@iarc ~]#
```

The IMiS/ARC server is not accessible over a network:

```
[user1@test ~]# ping iarc.acme.com
PING iarc.acme.com (10.1.1.10) 56(84) bytes of data.
... (pause) ...
From 192.168.92.32 icmp_seq=2 Destination Host Unreachable
From 192.168.92.32 icmp_seq=3 Destination Host Unreachable
From 192.168.92.32 icmp_seq=4 Destination Host Unreachable
... (abort test with CTRL-C) ...
^C
--- iarc.acme.com ping statistics ---
7 packets transmitted, 0 received, +3 errors, 100% packet loss, time
6937ms
[user1@test ~]#
```

The log contains the following records in sequence:

```
<date and hour of record> [iarcd:<decimal value>:<decimal value>] INFO[6]
Preforking 1 connection handling childs.
<date and hour of record> [iarcd:<decimal value>:<decimal value>] WARN[4]
Cannot bind socket 0 to address [10.1.1.10] on port [16807], error 99:
Cannot assign requested address. Socket will be closed.
<date and hour of record> [iarcd:<decimal value>:<decimal value>] ERR[3]
Server was unable to open any configured listening socket.
<date and hour of record> [iarcd:<decimal value>:<decimal value>]
INFO[6] Child 2922 exited with exit code 0.
<date and hour of record> [iarcd:<decimal value>:<decimal value>]
INFO[6] Fatal error occured. Server is shutting down.
```

Cause of problem: At the startup of the IMiS/ARC server the network subsystem of the operating system does not run or the configuration file contains invalid network settings.
Solution to the problem: The operation of the network subsystem must be checked and the network settings in the configuration file set accordingly `/etc/iarc.conf`.

Common Problem No. 6
At the startup of the IMiS/ARC server, this record appears on the console:

```
[user1@iarc ~]# sudo service iarcd start
Error accessing IMiS/ARChive Database directory (<path to base>). Check
user iarc access to this directory (must be rwx)
[user1@iarc ~]#
```

The IMiS/ARC server is otherwise accessible over a network:

```
[user1@test ~]# ping iarc.acme.com
PING iarc.acme.com (10.1.1.10) 56(84) bytes of data.
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=1 ttl=64 time=0.653 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=2 ttl=64 time=0.190 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=3 ttl=64 time=0.186 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=4 ttl=64 time=0.183 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=5 ttl=64 time=0.164 ms

--- iarc.acme.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 0.164/0.450/1.530/0.540 ms

[user1@test ~]#
```

Cause of problem: The executable program of the IMiS/ARC server cannot access its internal database due to invalid settings in the configuration file `/etc/iarc.conf`, section `[Database]`, key `Path`, and/or incorrectly set access rights and/or ownership of the set directory, or the internal base is not accessible, because the disk on which the internal base of the IMiS/ARC server is located is not connected to the right directory.
Solution to the problem: Check the correctness of the settings of the location of the internal database of the IMiS/ARC server, as defined in the configuration file `/etc/iarc.conf`, section `[Database]`, key `Path`, if one exists. In the event that these settings are not present in the configuration file the default value is `/iarc/db`. Check the rights and ownerships of the directory and of the files within the directory that is listed as the directory containing the files of the internal database. The user that executes the processes of the IMiS/ARC server (default `iarc`) must have the right to read, write and create new files in the directory. For the group to which the user executing the processes of the IMiS/ARC server (default `iarc`) belongs the right to read is sufficient. Should the directory `/iarc` be empty, the most probable cause would be the inaccessibility of the disk which, according to the default settings in the directory

`/iarc/db`, otherwise contains the internal database of the IMiS/ARC server; accessibility of this disk must first be established.

Common Problem No. 7

When attempting to view objects stored on the IMiS/ARC server, after a restart of the entire server, “Error 61523” appears on the IMiS/Scan and IMiS/View clients. Other clients (e.g. IMiS/Storage Connector) report the following error:

```
IMiS/ARC Client <IASession.Open> Failed to establish connection to the
cluster node <10.1.1.10, 16807> (Reason: Error <TimedOut> occurred while
opening network connection.).
```

The IMiS/ARC server is otherwise accessible over a network.

```
[user1@test ~]# ping iarc.acme.com
PING iarc.acme.com (10.1.1.10) 56(84) bytes of data.
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=1 ttl=64 time=0.653 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=2 ttl=64 time=0.190 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=3 ttl=64 time=0.186 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=4 ttl=64 time=0.183 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=5 ttl=64 time=0.164 ms

--- iarc.acme.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 0.164/0.450/1.530/0.540 ms

[user1@test ~]#
```

The IMiS/ARC server is otherwise operational, but the status of the IMiS/ARC server as a service reports the following status:

```
[user1@iarc ~]# sudo service iarcd status
Status of IMiS/ARChive HSM Storage Server: iarcd is stopped
[user1@iarc ~]#
```

Cause of problem: The startup script of the IMiS/ARC server is not activated in the sequence for the startup of server services.
Solution to the problem: Set the autostart of the IMiS/ARC server as a service when the operating system boots:

```
[user1@iarc ~]# sudo chkconfig iarcd on
[user1@iarc ~]#
```

Check the success of the execution of the command:

```
[user1@iarc ~]# sudo chkconfig iarcd --list
iarcd           0:off   1:off   2:on    3:on    4:on    5:on    6:off
[user1@iarc ~]#
```

Then start the IMiS/ARC server with the command:

```
[user1@iarc ~]# sudo service iarcd start
Starting IMiS/ARChive HSM Storage Server:                  [  OK  ]
[user1@iarc ~]#
```

Common Problem No. 8

At the startup of the IMiS/ARC server, this record appears on the console:

```
[user1@iarc ~]# sudo service iarcd start
Starting IMiS/ARChive HSM Storage Server:
WARNING: Maximum number of file handles (ulimit -n) allowed for
user iarc or group iarc is 1024. Set allowable maximum to
at least 4096 by adding following two lines to /etc/security/limits.conf:
iarc            hard            nofile          4096
iarc            soft            nofile          4096
 or
@iarc           hard            nofile          4096
@iarc           soft            nofile          4096
If you still recieve this message after modifying
/etc/security/limits.conf
check if Pluggable Authentication Modules (PAM) include module
pam_limits.so in session service for user iarc and/or group iarc
(see Linux-PAM system administrators guide on how to manage modules)
IMiS/ARChive will continue to run normally with current setting...
                                                           [  OK  ]
[user1@iarc ~]#
```

After startup the service operates normally. In time it becomes inaccessible for new client sessions. The log contains the following records:

```
<date and hour of record> [iarcd:<decimal value>:<decimal value>] CRIT[2]
No child process can accept new connection.
```

Cause of problem: The IMiS/ARC server has reached the highest possible number of open files and cannot accept new connections. The operating system namely detects any connection as an "open file".

Solution to the problem: Check the system settings for the highest possible number of open files for the user `iarc` that is running the IMiS/ARC server (see chapter INSTALLATION, subchapter "Post-Installation Procedures".

Less Common Problems

Rare Problem No. 1

When attempting to view an object stored on the IMiS/ARC server, “Error 11” appears on the IMiS/View or IMiS/Scan client. When attempting to obtain the object from the server, other clients (e.g. IMiS/Storage Connector) receive the following reply:

```
IMiS.IMiSARC.Client.IAClientException: Server reported error while
opening an object (Reason: Error opening or handling IMiS/ARChive object
file (IACM_OPEN)).
```

The IMiS/ARC server is otherwise accessible over a network; the service at the listening port is responsive (checked with the `telnet` program)

```
 [user1@test ~]# ping iarc.acme.com
PING iarc.acme.com (10.1.1.10) 56(84) bytes of data.
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=1 ttl=64 time=0.653 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=2 ttl=64 time=0.190 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=3 ttl=64 time=0.186 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=4 ttl=64 time=0.183 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=5 ttl=64 time=0.164 ms

--- iarc.acme.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 0.164/0.450/1.530/0.540 ms

[user1@test ~]# telnet iarc.acme.com 16807
Trying 10.1.1.10...
Connected to iarc.acme.com.
Escape character is '^]'.
Connection closed by foreign host.
[user1@test ~]#
```

The IMiS/ARC server is operational, which is additionally checked with a console command on the server on which it is installed:

```
 [user1@iarc ~]# sudo service iarcd status
Status of IMiS/ARChive HSM Storage Server: iarcd (pid 23209 23203) is
running...
[user1@iarc ~]#
```

The log of the IMiS/ARC server contains the following record:

```
<date and hour of record> [iarcd:<decimal value>:<decimal value>] WARN[4]
Error opening object.
```

Cause of problem: The client is attempting to open an object which is correctly entered into the internal base of the IMiS/ARC server, but the content of the object is not in its location or is missing.
Solution to the problem: Obtain data on the object identifier from the application that is using the archive system (e.g.: 4c9f36d38b4d6985b1ec111a5a14a7e9db89edd0cb36923010b6624c667ef142), the content of the parameter `IdentPassword` from the configuration file of the IMiS/ARC server `/etc/iarc.conf`, and data on the buyer, and send all of it to the manufacturer. The manufacturer's technical staff will then decrypt the object identifier, which is the basis for information on the further restoring procedures from backup copies or searching through the file system, should it not be located in its original location. This is only possible in the event that someone with server manager rights has moved or deleted it from its original location.

Rare Problem No. 2

When attempting to view an object stored on the IMiS/ARC server, “Error reading IMiS object” appears on the IMiS/Scan or IMiS/View client. When attempting to obtain the object from the server, other clients (e.g. IMiS/Storage Connector) receive the following reply:

```
IMiS.IMiSARC.Client.IAClientException: Server reported error while
opening an object (Reason: IMiS/ARChive database error (IACM_DBERROR)).
```

The IMiS/ARC server is otherwise accessible over a network; the service at the listening port is responsive (checked with the `telnet` program)

```
 [user1@test ~]# ping iarc.acme.com
PING iarc.acme.com (10.1.1.10) 56(84) bytes of data.
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=1 ttl=64 time=0.653 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=2 ttl=64 time=0.190 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=3 ttl=64 time=0.186 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=4 ttl=64 time=0.183 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=5 ttl=64 time=0.164 ms

--- iarc.acme.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 0.164/0.450/1.530/0.540 ms

[user1@test ~]# telnet iarc.acme.com 16807
Trying 10.1.1.10...
Connected to iarc.acme.com.
Escape character is '^]'.
Connection closed by foreign host.
[user1@test ~]#
```

The IMiS/ARC server is operational, which is additionally checked with a console command on the server on which it is installed:

```
[user1@iarc ~]# sudo service iarcd status
Status of IMiS/ARChive HSM Storage Server: iarcd (pid 23209 23203) is
running...
[user1@iarc ~]#
```

The log of the IMiS/ARC server contains the following records in sequence:

```
<date and hour of record> [iarcd:<decimal value>:<decimal value>]

ERR[3] DB record for object with id <decimal value> not found.
<date and hour of record> [iarcd:<decimal value>:<decimal value>]

WARN[4] Error opening object.
```

Cause of problem: The client is attempting to open an object which has not been entered into the internal base of the IMiS/ARC server.
Solution to the problem: Obtain data on the object identifier from the application that is using the archive system (e.g.: 4c9f36d38b4d6985b1ec111a5a14a7e9db89edd0cb36923010b6624c667ef142), the content of the parameter `IdentPassword` from the configuration file of the IMiS/ARC server `/etc/iarc.conf`, the internal database (content of directory `/iarc/db`) in compressed form or its textual form (see chapter on exporting the internal database (PRODUCT MANAGEMENT, subchapter "Configuration"), and data on the buyer, and

send all of it to the manufacturer. The manufacturer's technical staff will then decrypt the object identifier, which is the basis for information on the further procedures of determining the status of the internal database and the cause for the loss of record, which is the basis for performing valid operations on an object in the server's inventory.

List of Service Errors Recorded in the Operations Log

Level 0 – Emergency

EMERG: "Could not connect to database server."
This error means that the IMiS/ARC server has failed to open its internal database, which is listed in `/etc/iarc.conf` or in the default location `/iarc/db`, if it is not listed in the configuration file.

EMERG: "Unknown exception caught."
This error occurs when a severe error takes place in the operation of the IMiS/ARC server, but which is not recorded or foreseen as a potential error. There are different causes for this, ranging from the status of the environment to potential errors in the service's application code.

Level 1 – Alert

ALERT: "Out of memory."
This error means that the IMiS/ARC server has run out of available RAM. In this state it can, nevertheless, continue operation, despite its critical status; in the event of longer exposure to such an environment, the service can stop running.

ALERT: "Error commiting profile (ID: <profile No.>) record."
This error appears when creating a profile. The IMiS/ARC server could not create a profile record in the internal base, because the profile already exists.

ALERT: "Error commiting volume (ID: <volume No.>) record."
This error appears when creating a volume. The IMiS/ARC server could not create a volume record in the internal base, because it already exists.

ALERT: "Thread <thread identifier> error number <error code>. Exiting..."
This error appears when an unrecoverable error occurs in the operation of one of the threads. In this case, the IMiS/ARC server, depending on the severity of the error, aborts the operation of the thread or of the entire executable program, as continuation could jeopardize the consistency of the persistent data.

ALERT: "Maximum number of child processes reached."
This message means that the IMiS/ARC server cannot start a new linking child process and therefore cannot process new requests. In this case, the IMiS/ARC server continues to run until sources are freed up or the number of child processes is increased (set in the `/etc/iarc.conf` file).

ALERT: "Shared memory (hnd = <No.>, ptr = <No.>) error <error code>"
This error message appears if the IMiS/ARC server has detected an error or irregularity in working with part of the shared memory, which is being used for communication between processes. Operation of the IMiS/ARC server shuts down immediately due to the inability to communicate between processes of the IMiS/ARC service family.

Level 2 – Critical

CRIT: "Out of memory. Cannot continue."
This error means that the IMiS/ARC server has run out of available RAM. In this state it can, nevertheless, continue operation, despite its critical status; in the event of longer exposure to such an environment, the service can stop running.

CRIT: "Error is unrecoverable. The process will terminate."
An error has occurred that prevents the process from continuing its operation. This message is usually the result of another error that occurred just before this one and is also recorded in the log.

CRIT: "Unsupported client address structure at <No. of process>."
The IMiS/ARC server has detected an unsupported type of client address in the process <No. of process>. This error means an interruption in communication of the client with the server.

CRIT: "Signal SIGSEGV occurred. Process will shut down ..."
An error has occurred while working with the RAM of the IMiS/ARC server. The IMiS/ARC server immediately stops running. An intervention from the server's administrator is usually required and usually includes restarting the service.

CRIT: "No child process can accept new connection."
The communication child processes cannot accept new requests. This error is usually the result of another error or lack of server resources.

CRIT: "New process couldn't accept new connection."
The IMiS/ARC server has run out of resources. It started a new communication process, but does not have enough resources to accept new requests.

CRIT: "Error <error code> while recording session close to audit log."
CRIT: "Error <error code> while recording session open to audit log."
An error occurred while recording to the audit log; the record was not successfully forwarded and recorded in the internal database. There are different reasons for this. Intervention from the administrator is required.

Level 3 – Error

ERR: "Read returned with error: <error code>."
An error occurred while reading from the socket for client communication. This error is not critical and usually denotes a sudden, irregular interruption of the session by the client.

ERR: "Write returned with error: <error code>."
An error occurred when writing on the socket for client communication. This error is not critical and usually denotes a sudden, irregular interruption of the session by the client.

ERR: "No select file descriptor available."
The highest possible number of open files has been reached, which makes it impossible to use a new i-node, which the IMiS/ARC server requires for handling an object.

ERR: "IDFromIdentShort: Unknown ObjectID version information."
The client has requested an object whose identifier structure is not known to the IMiS/ARC server; the latter cannot decrypt it or it is not recorded in the server's internal database. The IMiS/ARC server denies the client's request.

ERR: "Cannot create object file <code/name of file>."
An error occurred while recording an object to the volume, because a file with the object already exists. Intervention from an expert is required and an answer to the question why a file with the object identifier is already present in this location.

ERR: "Unknown file handling error."
An unexpected error occurred while handling an object. The IMiS/ARC server denies the request.

ERR: "Cannot open object file <name of object file>."
The client has requested an object from the IMiS/ARC server which is entered in the inventory, but the object file does not exist.

ERR: "ObjRemove error <error code>."
The IMiS/ARC server has received a regular request for deleting an object; however, the deletion cannot be performed. Intervention from an expert is required and an answer to the question why the deletion procedure is not possible (usually caused by file system rights and HSM inventory file rights).

ERR: "Cannot open object file <name of object file>."
An error occurred while attempting to read an object; the IMiS/ARC server cannot open the object. Intervention from an expert is required, as this is an object that is otherwise entered in the object inventory; however, the question remains why the procedure is not possible (usually caused by file system rights and HSM inventory file rights).

ERR: "Not enough space available in profile <profile ID>."
The volumes belonging to the profile <profile ID> have run out of space.

ERR: "Invalid profile number."
The client's request used an invalid or nonexistent profile number.

ERR: "Unexpected FIN!"
The client terminated a session unexpectedly or has sent a session termination signal after the IMiS/ARC server had already terminated the session due to inactivity.

ERR: "Error in ConnInfoGetLib request (req->seq). Skipping processing."
The client has sent an invalid request for a communication library to the IMiS/ARC server.

ERR: "Cannot open file <name of library>."
The client has sent a valid request for a communication library to the IMiS/ARC server, but it is not found in its location. This error usually indicates incomplete setup, invalid settings in the configuration file `/etc/iarc.conf` or a problem with the `iarc` user rights.

ERR: "Unknown object handle <code/handle>."
The operating system has relayed an irregular object file handle to the IMiS/ARC server. This error is most likely the result of invalid operation of the operating system or file system.

ERR: "Unknown transmission handle."
The operating system has relayed an irregular i-node transmission handle to the IMiS/ARC server. This error is most likely the result of invalid operation of the operating system.

ERR: "Unknown ConnInfo request: <code> - ignoring!"
The IMiS/ARC server has received an irregular request for data on the client connection. The IMiS/ARC server denies the request.

ERR: "Unknown External ID request size (request size)."
The IMiS/ARC server has received a request for an identification number for a new object for the so-called external system (e.g. SAP/R3). The size of the requested identification number is not regular. The IMiS/ARC server denies the request as invalid.

ERR: "Invalid request size: (request size)."
The IMiS/ARC server has received a request with an irregular size. The IMiS/ARC server denies the request as invalid.

ERR: "Unknown request <request code> received. Closing connection."
The IMiS/ARC server has received an irregular request and closed the open connection. This is most often the result of attempting to establish a connection through a TCP port of the IMiS/ARC server with a protocol unknown to the IMiS/ARC server.

ERR: "Socket <socket code> closed for reading on client side. Connection closed."
The IMiS/ARC server has detected that the socket for communication with the client had been closed and therefore also closed the connection on its side.

ERR: "Socket <socket code> write error <error code>."
The IMiS/ARC server cannot communicate with the client through the socket.

ERR: "Error reading message queue (errno: <error code>)."
During the exchange of data between the processes of the IMiS/ARC service family, an error occurred while reading the data from the interprocess communication queue.

ERR: "Ident(): Initializing crypto engine."
Error initializing the system for object identifier encryption. The error is merely theoretical and a result of the programmer's error; intervention from an expert is required.

ERR: "Ident(): Setting internal key."
Error setting a key for the first level of object identifier encryption. The error is merely theoretical and a result of the programmer's error; intervention from an expert is required.

ERR: "Ident(): Setting external key."
Error setting a key for the second level of object identifier encryption. The error is merely theoretical and a result of the programmer's error; intervention from an expert is required.

ERR: "Ident(): Internal encrypting."
Error on the first level of object identifier encryption. The error is merely theoretical and a result of the programmer's error; intervention from an expert is required.

ERR: "Ident(): External encrypting."
Error on the second level of object identifier encryption. The error is merely theoretical and a result of the programmer's error; intervention from an expert is required.

ERR: "IDFromIdent(): Initializing crypto engine."
Error initializing the system for object identifier decryption. The error is merely theoretical and a result of the programmer's error; intervention from an expert is required.

ERR: "IDFromIdent(): Setting external key."
Error setting a key for the first level of object identifier decryption. The error is merely theoretical and a result of the programmer's error; intervention from an expert is required.

ERR: "IDFromIdent(): Setting internal key."
Error setting a key for the second level of object identifier decryption. The error is merely theoretical and a result of the programmer's error; intervention from an expert is required.

ERR: "IDFromIdent(): External decrypting."
An error has occurred on the first level of object identifier decryption. This error can occur due to an invalid identifier sent by the client.

ERR: "IDFromIdent(): Internal decrypting."
An error has occurred on the second level of object identifier decryption. This error can occur due to an invalid identifier sent by the client.

ERR: "IdentShort(): error <error code> while cyphering internal block."
An error has occurred on the first level of encrypting a short object identifier. This error is merely theoretical and requires an inspection from an expert of the manufacturer.

ERR: "IdentShort(): error <error code> while cyphering external block."
An error has occurred on the second level of encrypting a short object identifier. This error is merely theoretical and requires an inspection from an expert of the manufacturer.

ERR: "IDFromIdentShort: 1st Server id (<server identifier>) does not match."
The client has provided an invalid value for the short form of the object identifier.

ERR: "IDFromIdentShort: Unknown ObjectID version information (<decimal value>)."
The client has provided an invalid value for the short form of the object identifier or the value was created with a newer version of the IMiS/ARC server and the server cannot decrypt it.

ERR: "IDFromIdentShort(): error <error code> while decyphering external block."
An error has occurred on the first level of decrypting the short form of an object identifier. This error can occur due to an invalid short form identifier, sent by the client.

ERR: "IDFromIdentShort(): error <error code> while decyphering internal block."
An error has occurred on the second level of decrypting the short form of an object identifier. This error can occur due to an invalid short form identifier, sent by the client.

ERR: "IDFromIdentShort: Invalid ID data."
Error due to the invalid content of the control data after decrypting the short form of an object identifier. This error occurs due to an invalid short form identifier, sent by the client.

ERR: "Volume client error."
An unidentified error in the operation of the disk media management module has occurred. The cause of the error is usually incorrect operation of the operating system due to the lack of system resources.

ERR: "Invalid audit query size <decimal value>"
The server has received a request for searching the audit log, the size of which is invalid. The cause of the error is incorrect operation of the client; the error is otherwise merely theoretical.

ERR: "Invalid sess_cond.type (<decimal value>)"
The server has received a request for searching the audit log but it contains an invalid value for determining the criterion for session search. The cause of the error is incorrect operation of the client; the error is otherwise merely theoretical.

ERR: "Invalid sess_cond.offset (<decimal value>)"
The server has received a request for searching the audit log but it contains an invalid structure of the criterion for session search. The cause of the error is incorrect operation of the client; the error is otherwise merely theoretical.

ERR: "Invalid ts_cond.offset (<decimal value>)"
The server has received a request for searching the audit log but it contains an invalid structure of the criterion for the time period of events. The cause of the error is incorrect operation of the client; the error is otherwise merely theoretical.

ERR: "Invalid objid_cond.offset (<decimal value>)"
The server has received a request for searching the audit log but it contains an invalid structure of the criterion for determining object identifiers. The cause of the error is incorrect operation of the client; the error is otherwise merely theoretical.

ERR: "AuditQuery::GetNextAddress(), line <decimal value>, error <decimal value>"
The server has received a request for searching the audit log but the criterion for searching the network addresses of clients contains data in invalid form. The cause of the error is incorrect operation of the client; the error is otherwise merely theoretical.

ERR: "ObjectsQueryArray::FindEvents(); Error decrypting object id."
The server has received a request for searching the audit log but it contains an object identifier of invalid value. The cause of the error is incorrect operation of the client; the error is otherwise merely theoretical.

ERR: "msgctl(<system identifier>, IPC_RMID) error <error code>: <description of system error>"
A system error has occurred while setting up a queue for interprocess communication, specifically, in the attempt to remove the existing queue. The cause of the error is usually incorrect operation of the operating system and is described in greater detail with a description under <description of system error>.

ERR: "Cannot acquire database transaction handle."
An error has occurred while starting to work with a database. The cause of the error is usually the lack of system resources.

ERR: "Could not connect to iavol server. Session canceled."
An error has occurred while connecting to the module for working with disk media. The cause of the error is usually the lack of system resources or the inability of the operating system to service the number of client sessions reached.

ERR: "BuildVolTree(): Volume <volume identification> not mounted."
An error has occurred while using a specific volume. The cause for the unusability is one of the errors that were previously recorded in the log.

ERR: "Database server communication error."
An error has occurred while communicating with the module for working with a database. The cause for this is usually a lack of system resources or incorrect operation of the operating system due to various/unknown reasons.

ERR: "Error closing file descriptor."
A system error has occurred while closing a file. This error is usually the result of the programmer's error; however, the cause could also be incorrect operation of the operating system.

ERR: "accept() returned error <error code>."
ERR: "accept() error <error code>: <system error description>."
Error while establishing a new client session. The cause of the error is most likely that too many client sessions are currently established; in the second case, the precise cause is described with <description of system error>.

ERR: "Passed fd <decimal value> is not a listen socket."
Error while waiting for requests to establish new client sessions. The cause of the error is an error in the program and is merely theoretical. Intervention from an expert is required.

ERR: "Error creating thread: 0x<hexadecimal value>."
Error establishing a new processing thread in the program. The cause of the error is usually the lack of system resources.

ERR: "Stats counter error <error code>: "<description of system error>"."
Error while storing statistical data on the number of times objects have been accessed in a given period of time. This error is the result of incorrect operation of the operating system.

ERR: "Profile(<hexadecimal value>): No volumes on level <level number>. Emergency migration skipped."
ERR: "Profile(<hexadecimal value>): No volumes on level <level number>. Scheduled migration skipped."
Error attempting to migrate profile objects to a higher level (<level number>) in the volume hierarchy. This error occurred because the volumes of the profile on this level are not defined and the volumes of a lower level are running out of space.

ERR: "DB error #<error code>; <detailed error description>."
The general error message while working with a database <detailed error description> additionally explains the cause of the error. With such errors it is recommended that you shutdown the IMiS/Arc server as soon as possible and have an expert of the manufacturer perform an intervention/inspection.

ERR: "mkstemp("<file name>") error <error code>."
An error has occurred while creating a temporary file named <file name>. This error is usually the result of lack of disk space, `iarc` user rights or could be the result of incorrect operation of the operating system.

ERR: "unlink("<file name>") error <error code>."
An error has occurred while deleting a file named <file name>. This error could be the result of an error in the program, but it is most likely an error in the `iarc` user access rights or the incorrect operation of the operating system.

ERR: "DB record for object with id <object identifier> not found."
A record for the object with the ID number <object identifier> cannot be found in the database. This error is usually the result of an incorrect shutdown of the IMiS/ARC server and/or the operating system in the past. Intervention from an expert of the manufacturer or your own intervention in the internal database of IMiS/ARC is required.

ERR: "Database cursor not opened."
ERR: "DB Cursor still active."
ERR: "Transaction <hexadecimal value> already active."
ERR: "Transaction <hexadecimal value> still active in clnt_destroy()."
ERR: "Transaction <hexadecimal value> not active."
All of the above-mentioned errors occurred while working with a database. These errors are the result of errors in the program and are merely theoretical. If they occur, intervention from an expert of the manufacturer is required.

<u>Level 4 – Warning</u>

WARN: "File descriptor <decimal value> is too big for select(). Just closing."
A call from the function for closing a user session with an invalid parameter has occurred. The cause of the warning is an error in the program; the error is otherwise merely theoretical and an inspection from an expert of the manufacturer is required.

WARN: "Object header: Illegal server ID."
The object was probably transferred from another server or the object file is damaged. It is also possible that the IMiS/ARC server was upgraded but from a package with another server identifier. All three cases require intervention/inspection and opinion from an expert of the manufacturer.

WARN: "Object header: Illegal head."
The object file is most likely damaged or has been replaced with a file with invalid content without using the IMiS/ARC server. As seen by IMiS/ARC this file is unusable or unreadable.

WARN: "Object header: Object ID mismatch (ObjID: <hexadecimal value>; Header: <hexadecimal value>)."
The object header has an invalid object identifier entered. This could be a damaged object or the error is the result of an error in determining the object identifier. Intervention from an expert of the manufacturer is required. As seen by IMiS/ARC this file is unusable or unreadable.

WARN: "No available volume found in profile <decimal value>."
The storage profile has run out of space. A new volume must be added or the existing profile volumes increased.

WARN: "Seek ofset underflow. Repositioning."
An attempt to access an object in an invalid location has occurred. The cause of the error is the incorrect operation of the client; the error is otherwise merely theoretical.

WARN: "Unsupported Cipher algorithm requested for 128bit key strength (alg_id=<decimal value>)", alg_id)."
WARN: "Invalid Cipher mode requested (id=<decimal value>)", mode_id)."
WARN: "Unsupported Cipher key strength requested (key_strength=<decimal value>)", key_strength)."
WARN: "Unsupported block size identifier (<decimal value>)", bs)."
WARN: "Block size identifier (<decimal value>) doesn't match crypto context.", bs)."
WARN: "Crypto exception occurred (details: <description of details>)", e.what())."
The above-mentioned warnings occur when the client requests an encrypting mode which is not enabled in the server configuration. The cause of the error is incompatible settings of the encryption subsystem of the client or unsuitable server configuration in combination with the configuration of the clients.

WARN: "Unknown exception occurred while setting up crypto context."
An unexpected error has occurred while setting up an environment for encrypted client communication. The error is merely theoretical and requires an inspection from an expert of the manufacturer.

WARN: "Audit Log Query session denied by configuration settings."
The IMiS/ARC server has denied a request for establishing a session for reviewing the audit log, because the client is attempting to establish a session with an unsupported set of encryption parameters.

WARN: "Unsupported key type (type=<value>)."
The key type, which the client is attempting to use for establishing a session for reviewing the audit log, is not supported or allowed. Check the server and client settings and coordinate them.

WARN: "Traffic encryption is not supported."
Due to its settings, the IMiS/ARC server has rejected an attempt to establish an encrypted session with the client. Check the settings for establishing a session.

WARN: "Error creating new object."
An error has occurred while creating a new object, which is why the creation was unsuccessful. A detailed cause of the unsuccessful creation is described in the log's previous records.

WARN: "Profile or content type not found. Skipping creation."
The request from the client for creating a new object contains invalid data on the profile or type of object. The IMiS/ARC server denies the request. The cause of the error is most likely incorrect configuration of the client.

WARN: "Error opening object."
An error has occurred while attempting to open a regular object, which had been requested from the IMiS/ARC server by the client. The object is entered in the internal base of the IMiS/ARC server as a regular object, however, the corresponding file is not in its location.

WARN: "lllegal length of data received (<decimal value>). Ignoring request <decimal value>."
While communicating with the client the IMiS/ARC server received a request of invalid length. The IMiS/ARC server ignores the request and denies it. This error indicates an error in the client's application and is merely theoretical.

WARN: "Error deleting object (<decimal value>)."
An error has occurred while carrying out a request for deleting an object on the IMiS/ARC server. The cause could be incorrectly changed access rights for the object file or that the file is not in its location.

WARN: "Request <hexadecimal value> not expected. Ignored."
The type of request, which the IMiS/ARC server has received from the client, is unexpected in the status of the session as identified by the client session handle or is not regular. The IMiS/ARC server denies the request as invalid. These are usually requests caused by clients, unaware that the server has been restarted, which is why their denial does not cause incorrect operation.

WARN: "Volume "<volume description>" has no profile assigned."
The volume that has been regularly entered in the internal base of the IMiS/ARC server has not been assigned to a profile. The most likely cause is discrepancy in the internal base of the IMiS/ARC server. Intervention from an expert is required (chapter PRODUCT MANAGEMENT, subchapter "Configuration").

WARN: "Cannot create a socket (out of file descriptors?), error <value>: <value>."
The IMiS/ARC server has reached its maximum number of open files. The system setting for the maximum number of open files must be increased for the user under whose privileges the IMiS/ARC server is running (`iarc` default).

WARN: "Configuration parameter '<name of parameter>' has invalid structure and will be ignored."
The configuration parameter in the `/etc/iarc.conf` file has been entered invalidly or does not match the expected set of values. The IMiS/ARC server ignores the setting and applies the default value instead.

WARN: "Error <error code> while getting object id for external id <identifier>."
The database does not contain an object that has previously been connected to an external value identifier <identifier>.

WARN: "Error <error code> while setting external id for object <object identifier>."
An error has occurred while connecting an existing object to an external identifier. This error is merely theoretical; it could also be caused by irregularity in the internal database. An expert of the manufacturer must be informed of the warning.

WARN: "User <username> from <name of computer> did not authenticate with Audit Log Query permissions. Query denied!"
The user has sent a request for searching the audit log, but does not have the right to do so, since the user session has not been properly authenticated. The cause could be invalid client configuration, but could also be a warning of the unauthorized operation of a specific user.

WARN: "semop() ended with error <error code>."
An error has occurred while synchronizing processes. The most likely cause is incorrect operation of the operating system or lack of system resources. Consequently, normal operation of the IMiS/ARC server can be disrupted, yet with no danger to the already stored data. It is recommended that an expert of the manufacturer is informed of the warning and that the operating system, and with it the service itself, be restarted.

WARN: "dup(<decimal value>) error <error code>: <system description of error>."
A system error has occurred while duplicating the system identifier. The most likely cause is incorrect operation of the operating system or lack of system resources and is described in greater detail under <system description of error>. Consequently, normal operation of the IMiS/ARC server can be disrupted, yet with no danger to the already stored data. It is recommended that an expert of the manufacturer is informed of the warning and that the operating system, and with it the service itself, be restarted.

WARN: "Cannot put socket <decimal value> in listen mode, error <error code>: <system description of error>. Skipping to next..."
A system error has occurred while waiting for requests for new client connections. The cause could be a lack of system resources or invalid configuration of the IMiS/ARC server.

WARN: "Cannot accept administrator connection."
An error has occurred while establishing an administrator session. The cause of the warning could be invalid configuration of the IMiS/ARC server or a lack of system resources. An expert of the manufacturer must be informed of the warning.

WARN: "Message queue full. Increase number of serving threads."
The queue for requests has been filled. It is recommended that the number of processing threads in the configuration be increased.

WARN: "Configured service '<name of service>' cannot be resolved to a discreet port number (error: <system description of error>). Falling back to default '<name of service>'..."
WARN: "Default service '<name of service>' cannot be resolved to a discreet port number (error: <system description of error>). Default port will not be configured."
WARN: "Default service '<name of service>' resolves to a unsupported protocol family. Default port will not be configured."
WARN: "Configured service '<name of service>' resolves to a unsupported protocol family. Falling back to default '<name of service>'..."
WARN: "Address '<network address>', service '<name of service>' skipped since it cannot be resolved (error: <system description of error>)."
These warnings indicate an error in initializing the system for network connections. The cause of the error could be invalid configuration of the IMiS/ARC server or incorrect operation of the operating system.

WARN: "Maximum number of listening sockets reached (max = <decimal value>). Additional addresses will not be used!"
These warnings indicate an error in initializing the system for network connections. The cause of the error could be invalid configuration of the IMiS/ARC server or incorrect operation of the operating system.

WARN: "Error loading Common Log (<name of file>)."
WARN: "Error positioning Common Log read offset to <decimal value>."
WARN: "Error loading Admin Log (<name of file>)."
WARN: "Error positioning Admin Log read offset to <decimal value>."
An error has occurred in the administration module while accessing log files. The most likely cause of the error is incorrectly set rights in the file system. Access rights to the log files for the user `iarc` must be checked; in the event of correct settings, it would be reasonable to inform an expert of the manufacturer.

WARN: "Database cursor is active."
WARN: "Transaction <hexadecimal value> active on close. Commiting..."
While closing a client session an irregular status of the resources for working with a database has occurred; the cause is incorrect operation of the program. An expert of the manufacturer must be informed of the warning.