

## Libelle Professional Services: High Availability for SAP NetWeaver™ Environments

Libelle develops and maintains innovative solutions in the area of high availability and disaster recovery – for single databases and server systems up to complete data centers - since 1994. Customers of all branches, from local medium-sized businesses up to global enterprises trust in Libelle technology to strengthen their security and recovery capabilities for their business critical data. Libelle solutions vary from other conservative hardware and software technologies.

More than 80 % of our customers use Libelle high availability and disaster prevention solutions to protect their SAP systems. For this reason you can rely on an extensive knowledge of operation management for SAP systems, infrastructure integration, SAP basis support as well as availability and disaster prevention for SAP environments.

**SAP® Certified**  
Integration with SAP NetWeaver®

### Your Business Continuity Management is upside down with SAP NetWeaver™ 7.0 J2EE!

- Are you currently implementing or operating a solution based on SAP NetWeaver™ and it has to meet requirements for availability of systems and data?
- Do you plan to upgrade to SAP NetWeaver™ 7.0, or do you currently perform this upgrade?
- Are you using the Java/J2EE functionality in your SAP systems and require availability for systems and data?

Then you should read on!

### Why SAP NetWeaver™ 7.0 with J2EE changes your life

To ensure availability of today's SAP systems it is not enough to keep only the database itself and its content available and reliable. Current SAP system architectures consist of a complex conglomerate of components with different dependencies between each other.

Especially using the new SAP NetWeaver™ functionality, which results out of the J2EE stack, complexity of dependencies and components is further increasing. Classical take-over procedures and methods to ensure the vital operation will fail in this case. In particular the upgrade to SAP NetWeaver™ 7.0 and related SAP components will confront you with additional challenges, because SAP implements a part of the new and valuable functionalities exclusively based on the SAP J2EE stack.

Libelle offers with the solution **BusinessShadow®** the capabilities to fulfill these new challenges. **BusinessShadow** consists of components to protect the database (**DBShadow®**), the file systems (**FSShadow®**), and the connectivity (**SwitchApplication**) of your SAP systems.

**BusinessShadow<sup>®</sup>** ensures protection of the following SPOFs (Single Point of Failure) according to the recommendation of SAP and Best Practices:

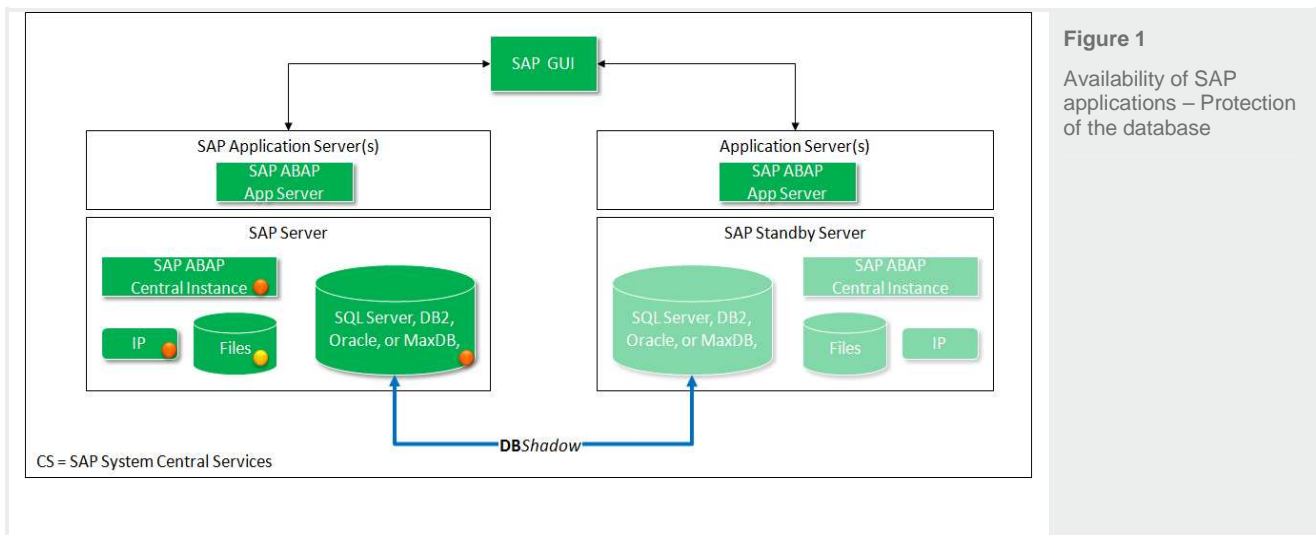
- Time delayed mirroring of the database with **DBShadow<sup>®</sup>**
- Time delayed mirroring of the vital file systems for ABAP and J2EE stack with **FSShadow<sup>®</sup>**, parallel and consistent to the mirroring of the database
- Take-over of the vital IP address and start/stop of the applications with **SwitchApplication** (integrated cluster functionality)

### Technical Background – Classical SAP Architecture

The classical implementation of an SAP system includes the installation of the SAP Database, a SAP Central Instance and operational SAP Application Servers. This concept is based on the SAP ABAP engine storing all data and functionalities in the corresponding database.

If such an SAP environment should be highly available and protected against logical and physical errors, it is necessary to protect the central component – the SAP Database. Such a protection will be done with the **DBShadow** technology.

Figure 1 shows such architecture. All SPOFs are represented with indicating colors, in dependent priority and their impact for the availability of the SAP system. Therefore the red indication marks the central vitality of the SAP system in the case of a take-over.



**Figure 1**  
Availability of SAP applications – Protection of the database

If, as shown in the figure 1, only the database of the SAP environment is mirrored, not all essential SPOFs of the SAP system are protected. Additional SPOFs, like SAP Central Instance with its dependencies to an IP address or host name, and the file system. The file system stores the profiles and parameter, job logs and the executables of the SAP system. It will be accessible for the application servers as an NFS share. So in the architecture of figure 1 these parts are not integrated for the takeover and availability procedures.

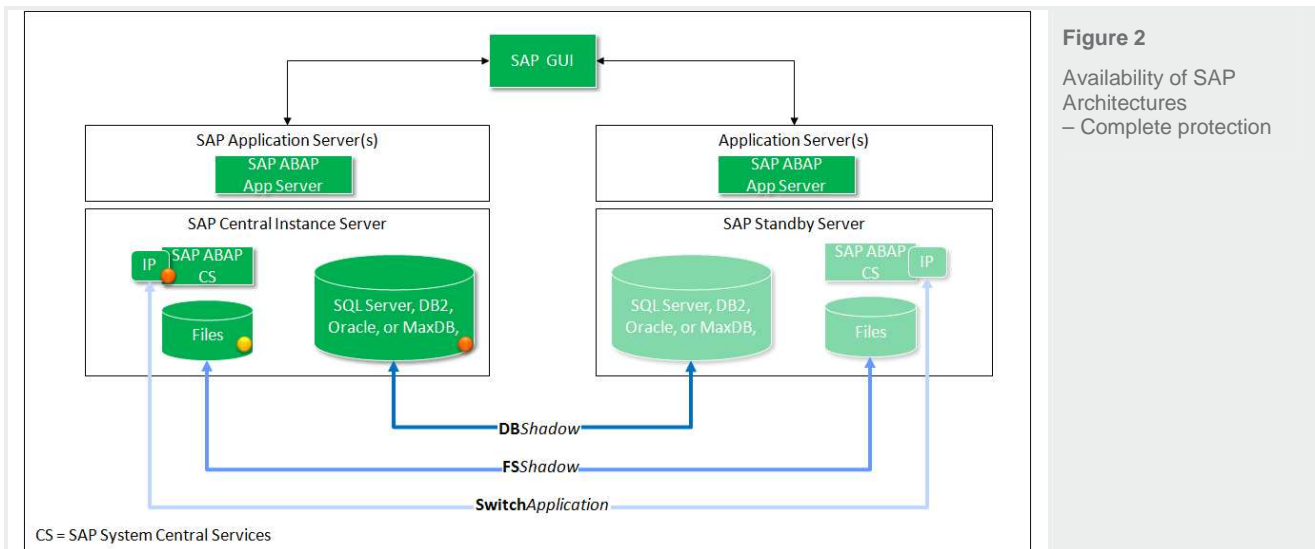
Complete protection of the SAP environment is only given, if the following elements are addressed by take-over scenarios:

- SAP Database
- SAP ABAP Central Services (part of the Central Instance, like ENQ, MSG etc.)
- SAP file systems and appropriate NFS shares
- IP address for SAP ABAP Central Services

Actually the change rate within the “classical” file systems of SAP is not that high. Also start and stop of the SAP Central Instance, including take-over of the IP address and hostname, is not that complex. Therefore in some installations a take-over of the file system, the IP addresses and the start of the SAP Central Instance will be done manually. But this solution is not recommended if there are several systems in a compound or a complex take-over scenario exists.

For this reason the SAP environment should be transferred to the scenario shown in figure 2. It covers components for mirroring the database, and additional components for protecting the file systems and SAP Central Services. Protection of the file system is realized with **FSShadow**® in accordance to the time delayed mirroring of the database. Therefore the database’s time delay will be applied on the file system as well. With this a consistency between database and file system, especially the job logs, is ensured.

The take-over integration with **SwitchApplication** guarantees a stressless management and take-over procedure in case of emergencies, and without for system maintenance purposes. This guarantees availability of the SAP systems.



**Figure 2**  
Availability of SAP Architectures – Complete protection

## Technical background – SAP Architecture with J2EE

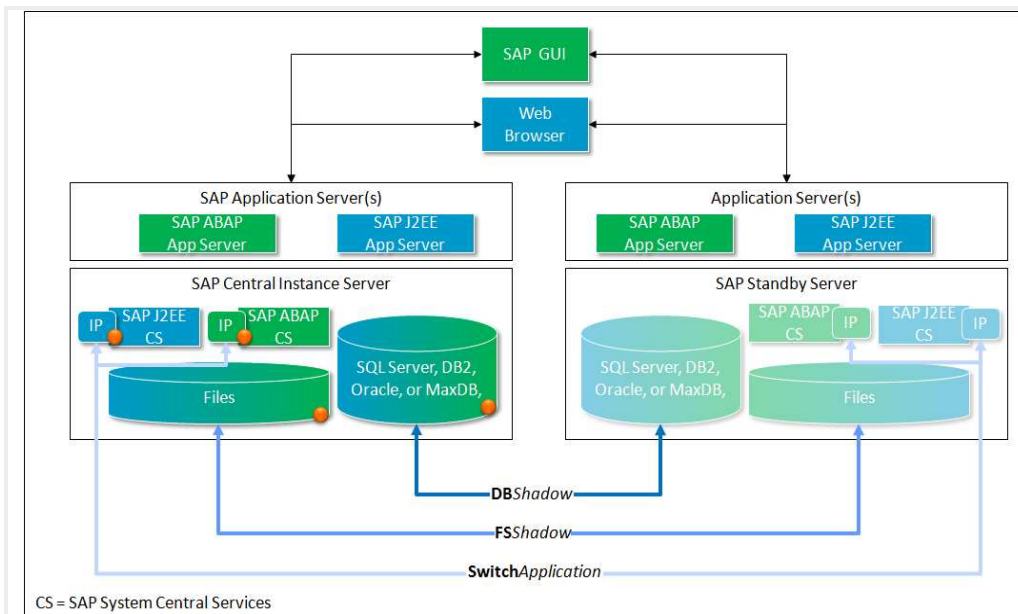
A new challenge means the implementation of an SAP system based on the most current SAP NetWeaver™ product line. The J2EE stack, also called Java stack, does not only add a new stack to the components in the environment. Implementing the J2EE stack, the classical approach to store all relevant application logic and data in the

database is obsolete. Large parts of this relevant data, required to run the SAP systems, now is stored in the file system. The file system now assumes a major role for the vitality of the SAP system environment.

Additionally to those classical architectures' system components mentioned before, it is necessary to integrate the following parts of the J2EE stacks into the procedures and scenarios for high availability and disaster prevention:

- SAP J2EE Central Services (part of the Central Instance, like ENQ, MSG etc.)
- SAP J2EE Filesystem for JAR files and appropriate NFS share
- IP address for SAP J2EE Central Services

To protect the J2EE components, procedures analogue to protect the ABAP stack will be applied.



**Figure 3**  
Availability of an SAP Architecture with J2EE – Complete Protection

Figure 3 shows the architecture of a highly available environment, integrating the ABAP Stack as well as J2EE Stack. The central file system is mirrored by **FShadow** with time funnel on the secondary system, consistently to the database mirroring. Especially the J2EE Stack requires a synchronic status of database and file system, as vital and frequently changing elements are stored in the file system.

Manual copy or copy without time funnel only is the second best solution. In this case of inconsistent SAP Database and Java Stack, a take-over might cause serious complications with start and operation of the emergency system.

An integrated procedure to switch-over resp. take-over IP address and host name is done by **SwitchApplication**, similarly to the ABAP environment.

Additionally to the components mentioned so far, a protection of SAP WebDispatcher (if activated) and SDM (Software Deployment Manager) is necessary. Integration of the WebDispatcher can be realized by **SwitchApplication**, as well. The necessity to protect

SDM fully integrated or just by „Cold Standby“ solutions depends on the change frequency and priority of changes for the operation of the SAP systems.

Furthermore, additional components of the SAP landscape should be integrated into a holistic concept for high availability and disaster protection. In some implementations TREX, SLD (System Landscape Directory), EP (Enterprise Portal) and PI (Process Integration), are of elementary importance, just to mention some examples.

Generally, those methods and procedures described in this document are suited to protect all components of current SAP and Non-SAP Architectures with minor adjustments.

We are pleased to discuss your concrete requirements and support you in the definition of an holistic, integrated and stable solution for the availability and vitality of your SAP systems.

### Trust in Libelle's experience

Libelle's consultants appointed to work in your SAP Architecture are certified SAP Technology Consultants and Architects with long term project experience.

Expect deep knowledge about conception and implementation of SAP NetWeaver™ solutions from each of our consultants.

Also expect deep experience in maintaining and operating SAP Architectures, especially know-how about availability and prevention of disasters.

#### Contact

##### Libelle AG

Gewerbestr. 42  
70565 Stuttgart  
Germany

T +49 711 / 78335-0  
F +49 711 / 78335-148

[consulting@libelle.com](mailto:consulting@libelle.com)

[www.Libelle.com](http://www.Libelle.com)

Libelle does not guarantee that this documentation is error free. The liability for consequential or indirect damages arising out of the delivery or the use of this documentation is not warranted by Libelle within legal limits. All copyrights, especially distribution, reproduction and translation, are reserved. No part of this publication may be reproduced (by photocopy, microfilm or otherwise), processed, reproduced or transmitted by electronic means without prior permission of Libelle.

Libelle, the Libelle Logo, **BusinessShadow**®, **FSShadow**® and **DBShadow**® are trademarks of Libelle AG. All other mentioned products are trademarks of their respective owners.