

Co-operative Service Design for a Cross-University Data Backup Service

Thomas Eifert^{1*} and Nicole Filla¹

¹RWTH Aachen University, IT Center, Seffenter Weg 23, 52074 Aachen, Germany
[eifert|filla]@itc.rwth.aachen.de

Abstract

Every part of a university nowadays is highly dependent on data, be it research, teaching or administration. In the meantime, the diversity of data storing device types increases while the amount of data is growing exponentially in the age of the Internet of Things. Starting from this dependency on data of almost every aspect of a university we are running a cross-university project in the German federal state of North Rhine-Westphalia (NRW) with the aim to build up a cross-university co-operative service for data protection. We derived work packages in order to define the future state-wide service according to the technical, procedural and functional requirements as well as to the expectations and demands of our stakeholders, the latter being confirmed by a survey.

The goal is to fundamentally improve data backup and data availability through the cooperatively provided basic IT service "Datensicherung.nrw" using cross-university processes. This is accompanied by a significant improvement in cyber security and ensuring the digital capacity to act of the participating universities, as well as the creation of synergies in the field of cooperative digitization among the state universities of North Rhine-Westphalia.

1 Introduction

By now, literally all aspects of university work and life depend on IT and, in particular, on data, so the availability and persistence of data and data services is essential. As trivial as this appears, scientific users need to rely on the availability of their data and data stores. As a consequence of this dependency, users expect and need 24/7-availability of services, and, in particular, an assured persistency of once-stored data. This statement holds for universities of all types and sizes. Equally universal is the downside that the growth of data and of the different types of systems makes it very difficult for a university's IT

to cope with these demands. On the other hand, besides “usual” reasons for data loss, we see a growing number of cyber-attacks against universities which aggravates the need for a reliable data protection.

Since these challenges are common to all universities, most of the universities in North-Rhine Westphalia (NRW) started the project “Datensicherung.nrw”^{*} to develop structures for joint, university-spanning services for safe data storage.

Beyond the technical aspect of making copies of data in order to protect these data against loss, the degree of dependency on data makes this an issue of digital sovereignty and empowerment. Consequently, the aim was an on premise approach from the very beginning.

2 Targets

This project aims at providing reliable data backup and the ability for quick recovery to all universities of NRW. While previously there were long-lasting co-operations in exchanging knowledge, we now came to the point the operation was to be concentrated. So, with the guiding theme “few for all” we developed a concept where some of the university data centers in NRW run the service for the others. Consequently, for the vast majority of our project partners, it was a new approach to source a basic IT service from a separate organization. However, the possibility of having a reliable and effective service that addresses the full diversity of systems was very compelling. At the same time, drawing on distributed resources and making synergistic use of the expertise distributed throughout NRW in the university computer centers rounded out the project's profile.

Making a copy of all relevant data is necessary, but by no means sufficient to meet the demands of the various players. Of course, on the service level we have all the typical performance indicators like availability, RTO, RPO, etc. Where the necessary value of these must be derived by the academic or administrative business process. The starting point was to overcome the traditional approach that every university has to do data storage by itself. Hence, we started a project to develop a co-operative, work sharing cross-university service where the technical infrastructure is concentrated at only few service sites and the expertise for certain data storage use cases like applications or specific storage devices is shared among all experts at the universities.

3 Expectations

Building a whole new service architecture poses the need and equally give the chance of re-assuring the demands and expectations of all people and roles involved. In Order to collect these ideas systematically, we conducted a survey between May and July 2020 (Thomas Eifert, 2021). In this survey we asked for the current state e.g. of the ability to backup certain systems or commitments for restore, data volumes etc. and the – most important for building a new service – the desirable future state concerning:

- Functionality: What is needed?
- Service level parameters: What are the commitments that should be agreed upon?
- Roles / self-service: Which of the regular tasks should be assigned to which role?

^{*} <https://datensicherung.dh.nrw/en/>

The aggregated demands for different aspects of functionality mainly went into the forms for an open-ended procurement for a suitable backup software. The service level parameters, as usual, reflect the trade-off between desirable and feasible commitments. Being able to agree here was crucial in order to have reachable demands on the then-future service provider teams. It was equally important for the service receivers to be assured a good service despite the fact that is going to be no longer made by themselves. Here, besides technical aspects like availability of the backup service itself points like service and support time windows are inevitable, too.

Concerning the third question, our survey revealed some differences in the expectations from the various roles (not significantly across universities): The answers from departments and institutes show a clear demand that data backup related everyday tasks like (de-)registering and configuring clients, start an on-demand backup and, in particular, run a partial or full restore should be managed locally. The survey thus gave us a good insight on how such a service should look to its users and which roles should be assigned which task. Additionally, we learned to what degree the view of the universities' central IT departments is coherent with the scientific departments' view and where they diverge.

So, despite of widespread more traditional approaches where all of these tasks are done by the central administration on university level we developed a role model spanning from an end user with his or her laptop to the new service providers' central administrators who are going to serve multiple universities.

4 Concept Phase

Building a whole new service architecture poses the need and equally give the chance of re-designing. "Expectations phase", we derived these key areas that must be agreed upon the following.

Tasks and Roles: To run with such a distributed service we will have the service providers and the experts distributed across several universities. For the co-operative model it is important that customer sites are encouraged to name experts as well. On every customer site we need to have central IT staff to coordinate and act on the service within their respective university and towards the service site. In addition, we have – dependent on a particular university's internal structure – IT staff on the level of faculties or departments, and, finally, the end users within the departments. From this information we derived a role model which enables us to tie every task and every activity to certain roles. In order to realize the role model, we need a software that is able to map these roles within their respective scopes onto local permissions – another highly important requirement for the procurement. Also, we needed a directory service from every university which holds the authentication and role/context information in order to supply this information the self-service portal of the backup software. The organization of this was made in close co-operation with our partner project "Identity Management.nrw"[†]. And, of course, filling these directories has to adhere to each of the universities' local processes.

Support:

Directly connected to these roles, we have specific responsibilities to bring support to every level of people involved. I.e., to help a scientist to recover lost data as well as to help a faculty's IT staff to set up certain policies. In order to scale across universities, support has to happen at the most possible decentralized level with the possibility to escalate to experts within and across universities. To achieve this, we do not touch local processes at all, but have a point where the support at university level can consult the colleagues and experts across universities.

[†] <https://idm.dh.nrw>

Service level:

Many assumptions that work very well on campus fail when acting between universities. In particular the assumption when a service is “good enough”. Therefore, we have to define explicit service levels that cover issues like service availability as well as service response times and commitments on the data persistency.

5 Current state

At this stage, the concept has been completely written down and agreed upon. We are now in the implementation phase, in which the implementation of the uniform software solution used throughout the state is taking place. This meets all the technical and additional requirements of the universities resulting from the cooperative approach.

The measures for implementation will be implemented by the cooperating universities in defined work packages based on a division of labor.

The roll-out of the state-wide service for data backup in NRW by and for universities is planned for summer 2022.

At the EUNIS2022 conference we will be amidst the migration phase and therefore be able to report the then-reached project state.

6 References / Citations

Thomas Eifert, D. D. (10 2021). University’s Core Business - How digitalization, cooperation, and cloud effect IT’s value proposition and metrics. *Proceedings of the European University Information Systems Conference 2021*, S. 41-48. doi:<https://doi.org/10.29007/t9bc>

7 Author biographies



Dr. Thomas Eifert, received his doctoral degree in solid state physics. Since 2013 he holds the role of the CTO at RWTH Aachen Aachen University's IT Center and is thus responsible for the technological strategy of the IT Center. His particular interests are the mutual dependencies of researchers' requirements and appropriate technical solutions, his teaching focuses on scalable IT.



Nicole Filla is working at the RWTH Aachen University's IT Center since 2016. She completed her Bachelor Degree in German and English Studies at the Heinrich-Heine-University in Düsseldorf in 2014. From 2018 to 2019, she was entrusted with quality management and held the position of deputy group leader for marketing and event management. Since 2019, she holds the project management and coordination in the cross-university project “Datensicherung.nrw”