Gathering and Sharing Research Data Without the Cloud

Scott Gage[1]

[1]Team Leader, Research and Data Management Support

University of South Australia, Mawson Lakes, Australia, scott.gage@unisa.edu.au

INTRODUCTION

Data gathering and sharing is crucial to every research project, but especially any that have collaborators across multiple locations.

Sharing data is easy – using web applications like Dropbox, OneDrive, or email but securing data it is a lot more complex. The issue with cloud services is that at any one time you do not know exactly where your data "lives" and who can access it. Some services may have data centres in the US, far from our own institutions. This presents complexities for confidential data sharing and security.

THE PROBLEM

The Information Strategy and Technology Services (ISTS) unit at the University of South Australia (UniSA) provide options for secure storage of data to our researchers. At induction researchers are allocated secure storage housed in our data centres. This enables researchers to store data on servers which are hosted at the University but they could only be accessed by researchers connected to the University's network. As a result, there was also limited sharing options with collaborators outside of the institution.

IMPLEMENTATION OF THE NEW SOLUTION

In 2018 ISTS commenced implementing a new research storage solution powered by NextCloud – a cloud-based file sharing application that could utilise our secure storage while also making sharing easier. The decision was made to use an in-house solution rather than any currently available external solutions due to our strict policies on research data and their dissemination. While others could provide guarantees only by hosting on our own servers could we have complete control and security from the beginning to the end of the process.

Solutions like Cloudstor would get us part of the way to this, but managing our legislative requirements like storing data for up to 7 years becomes much easier if the data is already on our infrastructure. Our infrastructure is also backed up daily, making restoration of lost data relatively simple compared to all other solutions.

Research Data Storage (RDS) provided the benefits of a cloud-based application but with secure storage not just in Australia but in UniSA's own data centres.

The implementation of RDS has been successful, but there have also been some issues. This presentation will outline the implementation plan for the solution and also provide an insight into some of the issues encountered and the solutions that were identified.

- *Promoting the new solution to researchers and encouraging uptake*
- *Training for researchers and external collaborators in how to use the application*
- *Monitoring uptake/usage and measuring success e.g. Infographics – see Figure 1 below*
- *Integration with other corporate applications*
- *Scalability of the solution to meet growing demand*
- *Understanding and meeting expectations… especially cost!*

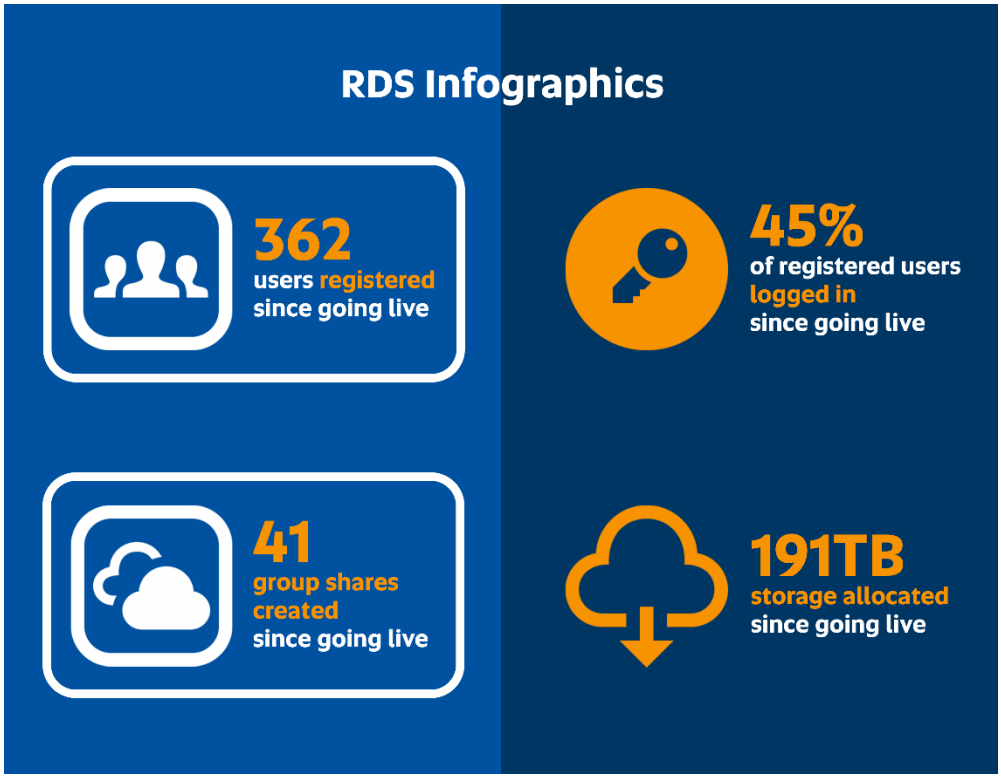

Figure 1: Research Data Storage Usage Since 2018

SECURING DATA "IN THE CLOUD"

Due to the nature of the application, RDS is almost the same as using DropBox to share your files. The two main differences are focussed on security:

- All data is stored on UniSA file storage at our two data centres. No confusion around where in the world your data lives and who has access to those areas. This storage is backed up on a regular basis, allowing UniSA to meet its legislative requirements for data retention and allowing users peace of mind that their data will not be lost.
- No anonymous file uploads. Users can use their UniSA or AAF credentials to access RDS, and external users can use Facebook, Google, LinkedIn or Twitter (once they've been invited by an internal user) to share data as well. There are no files in the system that do not have an author attached.

Virus protection is also a concern when sharing files in any medium. All file uploads to RDS are scanned on upload and regular virus scans are run on the entire storage array.

CONCLUSION

Data storage and security are key issues at the forefront of Research. This presentation will outline how UniSA has implemented a solution that enhances the ability to share data without compromising security. Going forward we hope to see a majority of our research staff and students utilising Research Data Storage from the moment they start with the University.

REFERENCES

UniSA AskResearch Storage: https://i.unisa.edu.au/askresearch/data-management/data-storage/