Our Experience with Introducing Microsoft Office 365 in Kyushu University

Kasahara, Yoshiaki
Kyushu University

Shimayoshi, Takao
Kyushu University

Obana, Masahiro
Kyushu University

Fujimura, Naomi
Kyushu University

出版情報：Proceedings of the 2017 ACM SIGUCCS Annual Conference, pp.109-112, 2017-10-01. Association for Computing Machinery: ACM
バージョン：

Our Experience with Introducing Microsoft Office 365 in Kyushu University

Yoshiaki Kasahara
Kyushu University
744 Motooka Nishi-ku
Fukuoka 819-0395, Japan
kasahara.yoshiaki.820@m.kyushu-u.ac.jp

Takao Shimayoshi
Kyushu University
744 Motooka Nishi-ku
Fukuoka 819-0395, Japan
simayosi@cc.kyushu-u.ac.jp

Masahiro Obana
Kyushu University
744 Motooka Nishi-ku
Fukuoka 819-0395, Japan
obana.masahiro.049@m.kyushu-u.ac.jp

Naomi Fujimura
Kyushu University
744 Motooka Nishi-ku
Fukuoka 819-0395, Japan
fujimura.naomi.274@m.kyushu-u.ac.jp

ABSTRACT

Information Infrastructure Initiative of Kyushu University started serving Office 365 Education for all students and staff members at Kyushu University in November 2016. Since 2007, the university had signed Microsoft EES (Enrollment for Education Solutions) including licenses for the latest Microsoft Windows and Office suite. The EES agreement includes an advantage to provide Office 365 Education to the university members with minimum investments, and there was a demand for Skype for Business which is included in Office 365. To deploy Office 365 for our users, we first needed to configure our on-premises user authentication infrastructure to coordinate with Office 365. During trials, we had a couple of difficulties attributed to some disagreements between Microsoft's and our policy on whether the user identifier, namely the user principal name in Active Directory, was open or private. Additionally, we had to consider which services should be applied to the users, because we have been operating an on-premises email service which is competing with Microsoft Exchange mail service. In this presentation, we share our experiences in Office 365 deployment.

CCS CONCEPTS

• **Social and professional topics → Software selection and adaptation;** • *Security and privacy → Authentication;* • Information systems → Enterprise applications

KEYWORDS

Microsoft Office 365; User Account Management; Public Cloud Service

1 INTRODUCTION

For research, education, and office procedure activities, university staff members and students use productivity software known as “Office suite” every day, for tasks such as writing a document with a word processor, analyzing various data in a spreadsheet, and making a presentation. There are a few alternatives for such software including open-source LibreOffice, but Microsoft’s Office suite dominates the enterprise world because of compatibility and interoperability. When most members in a university needs to purchase and use the same commercial software, it is not cost-effective to purchase the software (licenses) individually because usually there is a “volume discount” available.

To reduce the cost to purchase such software and prevent software piracy, Kyushu University decided to sign a contract with Microsoft called “Campus Agreement” in 2007. The agreement allowed all the staff members to install unlimited number of copies of the latest Microsoft Office suite to PC’s owned by our university, and staff members and students to install one copy per person to their private PC. Information Infrastructure Initiative of Kyushu University handled the actual deployment. The agreement also included upgrade licenses of Windows OS, so we could upgrade our PCs to the latest Windows OS. Later the name of the agreement was changed to

SIGUCCS '17, October 1–4, 2017, Seattle, WA, USA

ACM 978-1-4503-4919-2/17/10…$15.00
https://doi.org/10.1145/3123458.3123491

"Enrollment for Education Solutions (EES)." The agreement was the foundation for our BYOD project for students [1].

In late 2014, we negotiated with Microsoft for our EES contract to include "Student Advantage" and "Teacher Advantage" options which allowed us to use "Office 365 ProPlus" for all the eligible members without additional cost. Office 365 seemed attractive because it allowed each user to install Microsoft Office on up to 5 PCs, 5 phones, and 5 tablets, and "Office 365 Education" (free) also included Skype for Business, OneDrive for Business (up to 1TB of storage), SharePoint Online, and so on. At that time, Office 365 supported synchronizing user credentials with on-premises Active Directory (AD), so it seemed feasible to deploy Office 365 in our university with minimum cost.

In this paper, we describe how we tested and deployed Office 365 in Kyushu University, issues discovered during tests and deployment, current status, and future plans.

2 DESIGN AND IMPLEMENTATION

In this section, we describe our requirements/policies for handling user credentials, how we designed and tested our Office 365 deployment scenario, and the result and current status.

2.1 Identity Management System

In Kyushu University, Information Infrastructure Initiative is operating an identity management system (IDM) for staff members and students [2]. The total number of IDs is about 30,000. The current system was introduced in the end of the 2013 fiscal year. Each user was assigned a unique 10-digit pseudorandom number as a user ID called "SSO-KID." [3] The IDM provides users' personal information including their credentials, names, email addresses, etc. to various information services in Kyushu University through LDAP, AD, Shibboleth Identity Provider (IdP), and CSV files.

SSO-KID was designed in a way to protect users from dictionary and ID generation attacks [3], so there is a policy not to disclose SSO-KID in public (treated somewhat like a social security number in US). The policy prohibits providing a search facility which can disclose SSO-KID directly. Also, there is another policy not to transfer passwords associated with each SSO-KID outside our campus network (even hashed or encrypted). So, we need to build and deploy an Office 365 environment while maintaining these policies.

2.2 First Test

In 2015, we started to test and evaluate Office 365 deployment. First, we designed our test environment as shown in Figure 1. The IDM system can export user information to AD. To synchronize user information with Office 365, we needed an AD Federation Services (ADFS) and DirSync server. Also, to process user authentication requests without providing password information to Office 365, we needed an ADFS Proxy server to receive and redirect requests from Office 365 to our AD Domain Services server. We decided to use "SSO-KID@ms.kyushu-u.ac.jp" as a User Principal Name (UPN) to log on to Office 365 because it seemed natural to use SSO-KID as a part of the login ID. Also, we needed to prepare PowerShell scripts to apply Office 365 licenses to each user (which couldn't be done through AD).

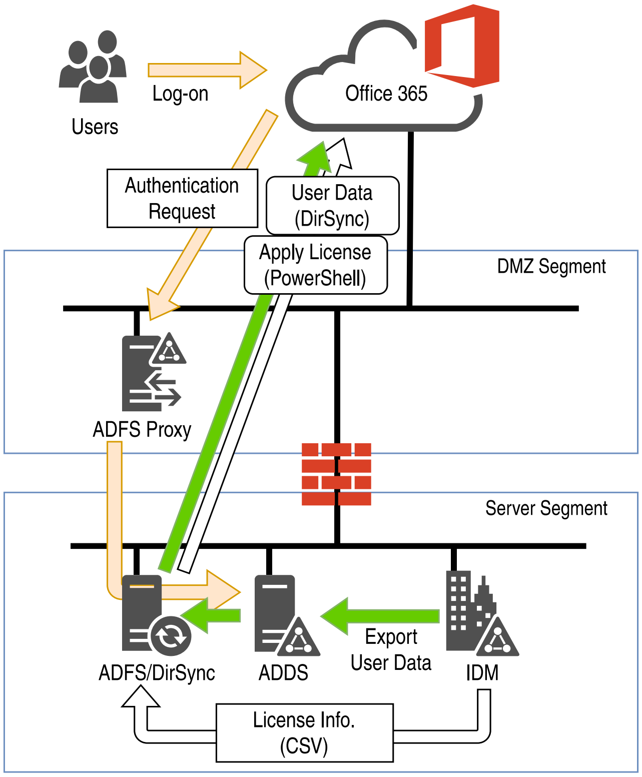

Figure 1: System Overview of the First Test Environment.

After the whole AD environment was built and tested with a small dataset, we synchronized all the members of Kyushu University with Office 365. The synchronization itself was almost successful, but we realized that some functionality of Office 365 violated our ID policy.

First, we found that Lync (now called Skype for Business) allowed users to search other users using a prefix of UPN. That meant that if a user searched "0", all the users whose SSO-KID started from "0" would be listed. Also, the search result showed both email addresses and UPN. Microsoft answered that it was a "feature" and we couldn't control the output of the search result. Microsoft treated UPN as a public information, and this didn't fit well with our policy. Because there were many other services in Office 365 which provided search function, it seemed difficult to control and make sure SSO-KID was not disclosed, and we had to abandon the tested environment and design another.

2.3 Current Implementation

To prevent SSO-KID from being disclosed in Office 365, we needed to use another string as UPN. We didn't have many candidates, and ended up using email addresses of Kyushu University Primary Mail Service [4] and changed the domain part to "ms.kyushu-u.ac.jp." In that case, there was little point to sharing the same password from SSO-KID with this new UPN, so we decided to let Office 365 handle its own password internally.

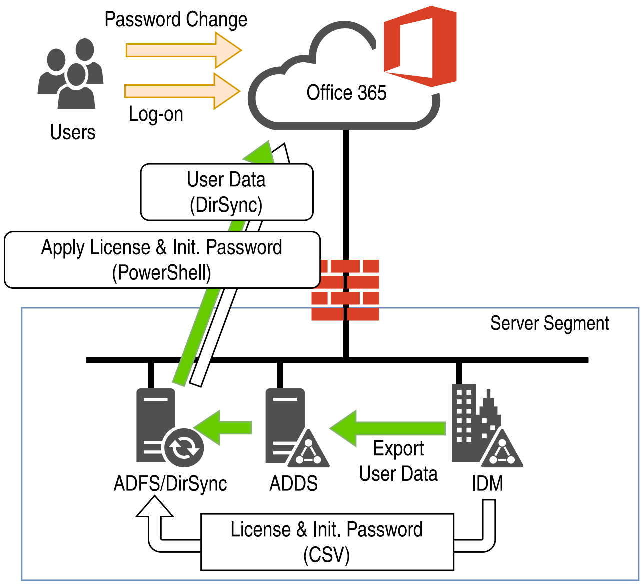

Figure 2: System Overview of the Current Environment.

Still, we needed to ensure that only valid users could sign up with a UPN, so we modified our IDM to generate a random string as an "initial" password for each UPN and exported this to Office 365. A user needed to access our IDM's web UI to retrieve the initial password for Office 365 from their profile page. The first login to Office 365 using this password would start the initial sign-up process including choosing a new password and selecting account recovery options (such as registering a mobile phone number). Figure 2 shows the overview of new environment. There was some strong demand to deploy Office 365 as early as possible, so we decided to go for this design after some tests. We officially announced the availability of Office 365 to the members of Kyushu University in April 2016.

3 REMAINING ISSUES AND FUTURE PLANS

We had been providing Office 365 to our users for more than one year, but we still have several issues which need to be resolved.

3.1 Multi-Factor Authentication

To protect our users' accounts from unauthorized access, we want to encourage users to use multi-factor authentication (MFA) implemented in Office 365. For personal Microsoft accounts, users can enable/disable MFA by themselves, but Office 365 doesn't allow users to do this for some reason. Only an administrator can change users' setting via Admin Center or using PowerShell script.

We modified our IDM to include a switch in a user's profile page to enable/disable MFA. Due to technical difficulty, we had to synchronize the MFA states to Office 365 once a day with a batch process. Later we realized that there were three MFA states: *disabled*, *enabled*, and *enforced*. After an *enabled* user completed the initial MFA registration process, the state would change to *enforced*. The problem was that overwriting the MFA state from *enforced* to *enabled* (by our batch) was not supported by Office 365 and might cause a login problem. We need a bit more complicated procedure to properly update users' MFA states, but it is not yet implemented. Temporarily we disabled the MFA switch in user's profile page.

3.2 Changing UPN

The email address assigned for our Primary Mail Service is based on a user's real name (for staff members) or Student ID (for students). A user's name may change by some life events, and Student IDs always change when the student proceeds from undergraduate to graduate or changes his/her department [5]. The same thing happens for UPNs in Office 365. The mail system automatically processes such an event and notifies users with an email message, but our Office 365 environment doesn't. Currently we process the UPN change manually, but we should decide how to treat the events automatically and implement it. Also, changing the UPN has some ill effects such as broken file sharing URL and online meeting URL. We wanted to use SSO-KID because it was much more stable, so we are still investigating the possibility to use SSO-KID for Office 365 without disclosing it in public.

3.3 Shibboleth/SAML

One such possibility to allow users to log in using SSO-KID is to utilize Shibboleth IdP. Office 365 partially supports Shibboleth IdP. During the initial stage, we discussed the feasibility of using Shibboleth IdP, but Skype for Business didn't support authentication via Shibboleth, so we abandoned the idea.

Recently we were informed that Kyoto University was using Shibboleth with Office 365, but they mainly used email service of Office 365 (Exchange Online). Also, more applications for Office 365 support SAML 2.0. We will continue to collect information about Shibboleth/SAML with Office 365.

3.4 Our mail system versus Exchange Online

Kyushu University is operating an in-house email service called Primary Mail Service [4]. The operation of the current system started at the end of the 2013 fiscal year. Exchange Online bundled with Office 365 offered a 50GB mail box which was much larger than our current email system (8GB). Because we didn't want to discourage users using our email service, we didn't assign Exchange Online license to our Office 365 users in initial deployment.

Later, we realized that Exchange Online was much more tightly integrated with other Office 365 services than we expected. For example, reservation of an online meeting with Skype for Business was much harder and restricted without using Microsoft Outlook with an Exchange account. Notification messages from various Office 365 services were also delivered to the Exchange mail box. As a compromise, we decided to assign Exchange Online license to each user, but forced the Exchange address to forward received messages to Primary Mail Service and disable changing forwarding address by users. Also, we are discussing whether it is feasible to migrate our Primary Mail to Office 365, because we must replace the current system before the end of the 2018 fiscal year.

3.5 Rights Management Services

Recently Kyushu University formulated a rule for document classification. A problem is how to implement a real-world procedure to classify and protect documents based on the classification rule. We are evaluating Microsoft Rights Management Services (RMS) to classify, protect, and track digital documents. Our Office 365 contract doesn't include RMS licenses, and we cannot afford the license fee to cover all the staff members (~9000). Our current plan is to purchase a small number of licenses and assign them to the people who need RMS.

In late 2016, Microsoft introduced "Azure Information Protection", and included some basic functionality in Office 365. Additional licenses are still required to use advanced functionality such as automatic classification and tracking. We don't fully understand the whole picture of Azure Information Protection, and we need to study more.

3.6 OneDrive for Business

For users, OneDrive for Business is also an attractive service because it offers 1TB storage. A major issue is how to handle confidential documents. Currently our security policy prohibits users from exporting confidential information outside our campus network, but it is difficult to use a cloud storage service if we enforce such a rule strictly. RMS might solve the problem if we can enforce a policy to encrypt every document uploaded to OneDrive.

3.7 DirSync to Azure AD Connect

As described in Section 2.2 and 2.3, we used DirSync to synchronize our AD and Office 365. But the official support of DirSync ended on April 13, 2017. Office 365 will stop accepting connection from DirSync on December 31, 2017, so we must upgrade DirSync to Azure AD Connect as soon as possible.

Also, we built the current environment quickly by reusing some parts of the first test environment. Due to this, the system is overly complicated and sometimes unstable. Another concern is that currently we use PowerShell scripts heavily to assign licenses to each user or to change some setting (such as MFA states described in Section 3.1). We need to consult a company with more knowledge about Office 365 and other Microsoft products to improve and stabilize our system.

4 SUMMARY

In this paper, we described the background and motivation to introduce Microsoft Office 365 to the members of Kyushu University, how we designed to coordinate our existing IDM and Office 365, current issues, and some future plans.

Office 365 consists of many services and seems to have a lot of potential to improve our information service, but we don't fully understand the whole picture yet. We will continue to research about Office 365 functionality and encourage our users to use them.

ACKNOWLEDGMENTS

Our thanks to all the users using our IT services, and staff members of the Office 365 task force and the authentication infrastructure working group to develop and maintain these systems in Information Infrastructure Initiative of Kyushu University.

REFERENCES

[1] Fujimura, N. 2013. Bring your own computers project in Kyushu University. In *Proceedings of the SIGUCCS 2013* (Chicago, IL, November 3 – 8, 2013). ACM, New York, NY, 43-50. DOI: http://dx.doi.org/10.1145/2504776.2504789

[2] Ito, E., Kasahara, Y., and Fujimura, N. 2013. Implementation and operation of the Kyushu university authentication system. In *Proceedings of the SIGUCCS 2013* (Chicago, IL, November 3 - 8, 2013). ACM, New York, NY, 137-142. DOI: http://dx.doi.org/10.1145/2504776.2504788.

[3] Nogita, M., Kasahara, Y., Ito. E., and Suzuki, T. 2006. A Study of Identifier Naming Conventions Suitable for User Authentication. *Technical report of IEICE.* ISEC Vol.106, No. 411 (20061206), 67-72.

[4] Kasahara, Y., Ito, E., and Fujimura, N. 2014. Introduction of New Kyushu University Primary Mail Service for Staff Members and Students. In *Proceedings of the SIGUCCS 2014* (Salt Lake City, UT, November 2 - 7, 2014). ACM, New York, NY, 103-106. DOI: http://dx.doi.org/10.1145/2661172.2662965.

[5] Fujimura, N., Togawa, T., Kasahara, Y., and Ito, E. 2012. Introduction and experience with the Primary Mail Service based on their names for students. In *Proceedings of the SIGUCCS 2012* (Memphis, TN, October 17 - 19, 2012). ACM, New York, NY, 11-14. DOI: http://dx.doi.org/10.1145/2382456.2382460.