# **Collabora and NextCloud SAML federation pilot**

## Introduction

Documents are at the heart of most projects: people create and share text, spreadsheets, presentations and images. Federated access management has been widely used to control access to published documents, but its use in collaborative creation has usually been limited to wikis and content management systems. Office documents are usually created offline. This pilot explored the use of two new applications that can be used together to provide federated access to both file management and office document creation and collaborative editing.

# Components

## NextCloud

NextCloud is a web-based document management service. Documents can be uploaded and downloaded via a web interface, or synchronised with local files. Files can be shared with other users. NextCloud was recently forked from OwnCloud. They remain very similar, but NextCloud offers new built-in federated access features using SAML in its free version. We used NextCloud's free edition in this pilot, but the commercially supported edition of OwnCloud may be used in a similar way.

0	Files -			م	4	PeteBirkinsha	w@dariah.eu 👻
	All files	*					
()	Recent		Name 🔺			Size	Modified
*	Favourites		OtherDocuments	<		•••• 0 KB	seconds ago
<	Shared with you		another document.odt	<	;	8 KB	15 days ago
« «	Shared with others		Hallo123.odt	<b>&lt;</b> MartinHaase@		••• 15 KB	15 days ago
•	Tags		NewPresentation.odp	<		13 KB	a minute ago
Ľ	External storage		spreadsheet.ods	<		••• 8 KB	15 days ago
			1 folder and 4 files			44 KB	

#### Collabora Online - LibreOffice for the web

Collabora Online is new software that allows the LibreOffice/OpenOffice office suite to run as a shared web application. Most of the desktop LibreOffice's functionality is available to users in a web page, with the added feature of simultaneous collaborative editing - users can work on the same document at the same time.

•	)0	Files	; -																			¢	۹	\$	PeteB	irkinsł	naw@d	ariah.eu	-
•	File	E	Edit	View	Insert	Cells	Help																						8
	B	5	Ċ	<u>+</u> =	Liberation	Sans	•	10 *	B	I	<u>U</u>	<del>C</del>	<u>T</u> .		E	Ē	7	5	\$	%	0,0		.0 <b>0</b>	.00	z↓	×↓			$\sim$
Σ	= [																												
	A	B C		D		E		F		G				н			ΙJ	К	L		М			N		0		Ρ	
1	Ц																												- 1
2																													- 1
3			Bus	iness	Trip I	Bud	lget																						- 1
4																													- 1
5			Genera	I.																									- 1
6																													- 1
7				Compa	ny Name		<comp< td=""><td>any Nar</td><td>ne&gt;</td><td></td><td></td><td></td><td>Leg</td><td>gend</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>- 1</td></comp<>	any Nar	ne>				Leg	gend															- 1
8				Employe	ee Name		<emplo< td=""><td>vee Nar</td><td>ne&gt;</td><td></td><td>Input</td><td>Field</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>- 1</td></emplo<>	vee Nar	ne>		Input	Field																	- 1
9				De	estination		<des< td=""><td>tination</td><td>&gt;</td><td></td><td>Resul</td><td>t Field</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>- 1</td></des<>	tination	>		Resul	t Field																	- 1
10				Trij	p Budget		\$2,	000.00																					- 1
11				Start	: Date (?)		03/	19/2017																					- 1
12				Finish	Date (?)		03/3	26/2017																					- 1
13																													- 1
14																													- 1
15			Overvie	w																									- 1
16						_				_																			- 1
17				Category	/			Total					No	otes															- 1
18			Airfare						\$360.0	00																			- 1
19			Rail Tra	ffic					\$52.0	00																			- 1
20			Car Re	ntal					\$236.0	00																			- 1
21			Gas						\$80.8	37																			
22			Food						\$2154	20																			
23			Miscoll	aneoue					\$250.0	20																			
25			maten	anoods					\$1.837	37																			
26																													
27																													
28		-	Total C	ost of Trip																									
29																													
30			U	Inder Budge	et by			Total					No	otes															
31					\$162.13				\$1,837.8	37																			
32																													
33																													- 1

# Integrating NextCloud and Collabora Online

Collabora Online provides a basic administration user interface, minimal configuration files, and a generic WOPI API (as used by Microsoft Office). It runs as a web application behind an Apache or NGINX reverse-proxy with SSL. Authentication and authorisation are handled via WOPI and resemble Oauth. As such it requires a second application to act as the primary user interface and authentication provider.

NextCloud is a PHP application and performs the role of , user interface, document store and WOPI authentication server. Collabora Online compatibility is now available via a bundled plugin and the only configuration needed is the URL for the Collabora service. When users open a file in NextCloud control is passed to Collabora Online, and the office application interface appears.

•••• Admin -		PeteBirkinshaw@dariah.eu 👻
Server settings	Collabora Online	
Server info	Collabora Online server https://office.looc.aarc.demo.university	
Sharing	URL (and port) of the Collabora Online server that provides the editing functionality as a WOPI client.	
External storages	Apply 2 Use OOXML by default for new files	
Theming		
Encryption		
Workflow		
Collabora Online		

A single Collabora Online service can be used by more than one NextCloud front-end.

# **AAI Integration Options**

NextCloud needs a means of handling its own authentication. Two options are currently available for federated authentication: a built-in SAML SP, and a external SSO option that relies on the web server handling authentication.

#### **Built-In SAML**

NextCloud's SAML implementation is currently rather limited, and only supports one IdP. This means that a proxy IdP would be needed to provide fully federated access to users.

• Admin -		PeteBirkinshaw@dariah.eu
Server settings		
Server info	SSO & SAME authentication	
Sharing	Make sure to configure an administrative user that can access the instance via SSO. Logging-in with your regular Nextcloud account won't be possible anymore.	
Juanug	General	
External storages	um:oid:1.3.6.1.4.1.5923.1.1.1.6	
Theming	<ul> <li>Only allow authentication if an account is existent on some other backend. (e.g. LDAP)</li> <li>Use SAML auth for the Nextcloud desktoo clients (requires user re-authentication)</li> </ul>	
Encryption	Service Provider Data	
Workflow	If your Service Provider should use certificates you can optionally specify them here. Hide Service Provider settings	
Collabora Online	BEGIN CERTIFICATE MIIDXDCCAASgAwiBAgiJAOSGeFEeeiZWMA0GCSqGSib3DQEBBQUAMCoxKDAmBgNV	
SSO & SAML authentication	BECIN DRIVATE KEY	
Usage survey		
Logging	Identity Provider Data	
LOBEINE	Configure your IdP settings here.	
Additional settings	https://idp.de.dariah.eu/idp/shibboleth	
Tips & tricks	https://idp.de.dariah.eu/idp/profile/SAML2/Redirect/SSO	
	Hide optional Identity Provider settings	
	URL Location of the IdP where the SP will send the SLO Request	
	BEGIN CERTIFICATE MIIFpJCCBl6gAwlBAgHGS8yFJEtwDANBgktghkiG99w0BAQsFADBeMQswCQYDVQQG	
	Security settings	
	For increased security we recommend enabling the following settings if supported by your environment. Show security settings	
	Download metadata XML Metadata valie	

More advanced SAML features are planned and development seems to be active.

#### **External authentication**

The second SSO option is to rely on the web server (such as Apache or NGINX) and use basic user information passed as environment variables such as REMOTE\_USER.

• Admin -			PeteBirkinshaw@dariah.eu 👻
Server settings Server info	SSO & SAML authentication		
Sharing	Make sure to configure an administrative user that can access the instance via SSO. Logging in with your regular Nextcloud account won't be possible anymore.		
DAD (AD interration	General		
LUAP / AD Integration	REMOTE_USER		
Theming	<ul> <li>Only allow authentication if an account is existent on some other backend. (e.g. LDAP)</li> </ul>		
Encryption			
Workflow			
SSO & SAML authentication			

This means that the Shibboleth SP software, OpenID Connect or even Kerberos can be used, but integration is weak - only the username is available.

#### Aggregating attributes from LDAP

It is possible to combine federated authentication with LDAP for additional attributes, and to require presence in the LDAP directory for authentication to succeed.

This would hinder usage across a federation (since users would not exist in the LDAP directory) but may help research organisations, as group membership and access control can be handled by a community LDAP server.

OOO Users →								۹. 🗳	PeteBirkinshaw@dariah.eu 👻
+ Add group	Username	Password	Groups -	Create					
Everyone	Username		Full name	Pas	ssword	Email	Groups		Group admin for
Admins	A admin		admin				admin	•	no group 👻
Chili_admins	<b>(</b> )	@dariah.eu	1000			rmstadt.de	jira-developers, dar	iah-de-co 👻	no group 👻
Chili_contributors	<b>A</b>	@dariah.eu			····· #	9ids-mannheim.de 🖋	textgrid-contributo	rs, tf-dari 👻	no group 🔹
DARIAH-DE-Cloudshare-Contr	B	@dariah.eu	100 C			Jb.uni-goettingen.de	jira-developers, dar	iah-de-co 🝷	no group 🔹
DARIAH-Preservation-users	B	ndiid.net					admin	•	no group 👻
ERROR	<b>C</b>	@dariah.eu	-			nglit.tu-darmstadt.de	textgrid-contributo	rs, textgr 👻	no group 👻
LiKuRez19-II	<b>G</b> —	@dariah.eu	-			Juni-wuerzburg.de	jira-developers, dar	iah-de-co 👻	no group 👻
ReDesign-TextGrid	G	@dariah.eu	1000			aw.de	collection-registry-a	admins, c 👻	no group 👻
TextGridDokumentation-adm	0	@dariah.eu	and the second			dirom.de	textgrid-users, Ir_D	ARIAH-Us 🝷	no group 🔹
TextGridDokumentation-cont		9dariah.eu	1000-0000				dariah-de-contribu	tors, dhfv 👻	no group 👻
admins	0	@darlah.eu	-			pmpiwg-berlin.mpg.de	dariah-de-contribu	tors, dari 👻	no group 👻
an dinitala romanietik admine		risk au				Bacdh da	dariah au contribu	torr dari -	00 070UD -

## **Pilot Implementations**

Three different demonstrations were set up, so that different features and integration combinations could be explored.

#### Demonstration 1: Integrated SAML with one IdP

Built-in SAML

https://cloud.looc.aarc.demo.university/nextcloud/index.php/

•••• Admin +		. 4	PeteBirkinshaw@dariah.eu 👻
Server settings			
Server info	SSU & SAME authentication		
Sharing	Make sure to configure an administrative user that can access the instance via SSO. Logging-in with your regular Nextcloud account won't be possible anymore.		
Estample terrore	General		
External storages	um:oid:1.3.6.1.4.1.5923.1.1.1.6		
Theming	<ul> <li>Only allow authentication if an account is existent on some other backend. (e.g. LDAP)</li> <li>Use SAML auth for the Nextcloud desktop clients (requires user re-authentication)</li> </ul>		
Encryption	Service Provider Data		
Workflow	If your Service Provider should use certificates you can optionally specify them here. Hide Service Provider settings		
Collabora Online	BEGIN CERTIFICATE MIIDXDCCAK5gAwiBAgiJAOS6eFEeelZWMA0GCSqGSib3DQEBBQUAMCoxKDAmBgNV		
SSO & SAML authentication	BEGIN PRIVATE KEY		
Usage survey			
Logging	Identity Provider Data		
Additional settings	https://idp.de.dariah.eu/idp/shibboleth		
Productorial accurga	https://ido.de.dariah.eu/ido/orofiie/SAML2/Redirect/SSO		
Tips & tricks	Hide optional Identity Provider settings		
	URL Location of the IdP where the SP will send the SLO Request		
	BEGIN CERTIFICATE MIIFpiCCBlfgAniBAgHcGSbyFExwDANBgkqhsG59x0BAQsFADBeMQswCQYDVQQG		
	Security settings		
	For increased security we recommend enabling the following settings if supported by your environment. Show security settings		
	Download metadata XML. Mountain with		

Configured using NextCloud's built-in SAML to connect to one IdP as if used by a single university or research community using a proxy IdP.

Keys were created using the Shibboleth SP keygen tool and pasted into the configuration form in NextCloud. EPPN was used for NextCloud usernames (identified by URN)

NextCloud generated its own metadata, but the expiry date was only for a few days and so was removed before sharing. Various combinations of encryption and signing can be set.

#### Security settings

For increased security we recommend enabling the following settings if supported by your environment. Hide security settings ...

Signatures and encryption offered

□ Indicates that the nameID of the <samlp:logoutRequest> sent by this SP will be encrypted.

- Indicates whether the <samlp:AuthnRequest> messages sent by this SP will be signed. [Metadata of the SP will offer this info]
- □ Indicates whether the <samlp:logoutRequest> messages sent by this SP will be signed.
- □ Indicates whether the <samlp:logoutResponse> messages sent by this SP will be signed.

Whether the metadata should be signed.

#### Signatures and encryption required

🗌 Indicates a requirement for the <samlp:Response>, <samlp:LogoutRequest> and <samlp:LogoutResponse> elements received by this SP to be signed.

V indicates a requirement for the <saml:Assertion> elements received by this SP to be signed. [Metadata of the SP will offer this info]

- Indicates a requirement for the <saml:Assertion> elements received by this SP to be encrypted.
- □ Indicates a requirement for the NameID element on the SAMLResponse received by this SP to be present.
- □ Indicates a requirement for the NameID received by this SP to be encrypted.

Indicates if the SP will validate all received XMLs.

General

ADFS URL-Encodes SAML data as lowercase, and the toolkit by default uses uppercase. Enable for ADFS compatibility on signature verification.

Download metadata XML

#### Demonstration 2: External authentication (SAML) plus LDAP

#### External SSO

https://cloud.aarc.federated-example.website/nextcloud/index.php/apps/files/

Server	Users	Login Attributes	Groups		Advanced	Expert
When lo	zging in, Ne	xtcloud will find the u	ser based on	the following attributes:		
	LDAP / A	D Username: 🗌				
1	DAP / AD E	mail Address: 🗌				
	Oth	er Attributes: eduP	ersonPrincip	IName +		
	🕁 Edi	t LDAP Query				
		LDAP Filter: (&()	objectclass=0	ariahPerson))(   (eduPersonPrincipalName=%uid)))		
PeteBir	kinshaw@d	ariah. Verify set	ings			
				Configuration OK Back Continue <sup>i</sup> Help		

Configured to use a single IDP, using the external SSO plugin and a conventional Shibboleth SP. NextCloud was configured to search an LDAP directory for records matching the SAML-authenticated user's EduPersonPrincipalName. LDAP was also used to discover which groups a user was a member of. These groups can be used for access control.

Session lifespans for the external authentication service (Shibboleth SP) and Nextcloud's own sessions can become out-of-sync, and require some adjustments to work together consistently.

Internal Username								
By default the internal username w	By default the internal username will be created from the UUID attribute. It makes sure that the username is unique and characters do not need to be converted. The internal username							
the restriction that only these characters are allowed: [ a-zA-Z0-9@- ]. Other characters are replaced with their ASCII correspondence or simply omitted. On collisions a number will t								
added/increased. The internal user	added/increased. The internal username is used to identify a user internally. It is also the default name for the user home folder. It is also a part of remote URLs, for instance for all *DAV							
services. With this setting, the defa	services. With this setting, the default behavior can be overridden. Leave it empty for default behavior. Changes will have effect only on newly mapped (added) LDAP users.							
Internal Username Attribute:	eduPersonPrincipalName							
Override UUID detection								

#### Demonstration 3: Integrated SAML with a federated IdP Proxy

#### Built-in SAML

https://files.looc.aarc.federated-example.website

(Work-in-progress) A similar pilot to the Demonstration 1 but configured to use the Terena Proxy so that it's easier for a wider range of people to log in.

## An Aside: Federated data storage

NextCloud supports "federated sharing", which permits users to share files between different NextCloud services, and browse user directories on other services. Users are given a globally unique scoped identifier that resembles EduPersonPrincipalName. If EPPN is used as the NextCloud username then a user's identifier is scoped twice.

#### Federated Cloud

Your Federated Cloud ID: PeteBirkinshaw@dariah.eu@cloud.aarc.federated-example.website/nextcloud

The External Storage plugin allows remote data storage to be used, including other NextCloud or OwnCloud services, Windows shares and NFS.

#### Caveats

#### Speed

The display of Collabora is generated by sending many tile-like images over the web as individual files, and is rather slow. Over a normal broadband internet connection the display is not quite fast enough to keep up with typing.

Over a much faster connection such as a LAN the speed is greatly improved.

#### The Open Source Collabora Online package has restrictions

The CODE (Collabora Online Developer Edition) Docker container used in these pilots is limited to 10 concurrent users. Collabora offer a commercial edition with no limits.

However, there is an unofficial project to help with installing an alternative open source version of the Collabora Online software without these limitations, and without Docker.

Collabora Online Development	Edition (CODE	:) - Admin console				Settings
Overview	Dash	board				
Analytica	Docur	2 Users online	2 Documents opened			
	PID	Document	Number of views	Memory consumed	Elapsed time	Idle time
	51	Hallo123.odt	1	129.0 MB	1:55 mins	20 s
	17007	another document.odt	1	59.0 MB	27 s	18 s

## Admin accounts must be created before switching to SSO

Admin users (who are able to configure the service) must be created in Nextcloud, using EPPNs, in advance, before SSO is enabled.

#### Cannot easily change SSO methods

NextCloud's SSO plugin offers a choice between the built-in SAML and using external authentication, and it does not seem to be possible to easily switch from one to the other.

#### Application passwords are still required

Users will need to create their own passwords in NextCloud to use for syncing files and other non-web access.

# **Further Information**

- NextCloud admin manual
- Nextcloud SAML documentation
- CODE edition of Collabora
- LibreOffice Online installer project (a community alternative to CODE)
- NextCloud app passwords, for non-web devices