On-premises Content Collaboration Platforms の更改

太田 憲治

東北大学電気通信研究所 やわらかい情報システムセンター

kenji.ota@riec.tohoku.ac.jp

Renewal of On-premises Content Collaboration Platforms

Kenji Ota

Flexible Information System Center, RIEC, TohokuUniv.

概要

東北大学電気通信研究所では,2016 年 4 月より OpenSouceSoftware である OwnCloud を用いた On-premises Content Collaboration Platforms によるサービス提供を行っている. 2019 年 7 月に,G Suite for Education（Google 社）の契約により Google Drive が利用可能になったことから廃止を検討するが,柔軟に対応できるユーザ管理とインハウスネットワークを超えたファイルシェア,プライベートクラウドに対する根強い要望があり,2019 年 8 月に Own Cloud の更改が決定した.更改に向けた取り組みを,検討 phase,構築 phase,運用 phase に分けて紹介する.

1 はじめに

東北大学電気通信研究所では,利用者からのファイルバックアップ,メールに添付できない大容量ファイルのシェア,WebDAV によるファイル管理などの要望を受けて,2016 年に Content Collaboration Platforms の検討を行った. 費用のかからない無料のシステムを検討するが,通信速度やセキュリティ,容量などの不安要素があり,Open Souce Software である OwnCloud を用いて構築を行った. 2019 年 7 月に東北大学が Google 社と G Suite for Education の契約を結び Google Drive の利用が可能になったことから,OwnCloud のサービス提供を廃止することを検討したが,ユーザ管理の問題とオンプレミス型に対する根強い要望があり,サービスの継続を行うことを決定した.OwnCloud は,導入から 3 年が経ち安定期に入っているが,セキュリティ面の問題もあり OwnCloud のリプレイスを検討し始めた.

2 OwnCloud とは

OwnCloud は , Open Souce Software の On-premises Content Collaboration Platforms である.DropBox や GoogleDrive と同様に,パソコンやタブレット等のデータをサーバ内に保存することができる. Network Attached Storag(NAS)とも比較されるが,インハウスネットワーク以外の人や学外からでも Web ブラウザを利用してファイルやフォルダの共有をすることができ,様々な専用アプリを利用して,カレンダー機能やメールクライアント機能,LDAP サーバとの連携機能が標準で備わっている違いがある.

Owncloud の最大の特徴は,Open Souce Software の為,様々な機能を無償で利用できることにある.

3 OwnCloud 更改の検討 phase

3.1 現状の問題点

OwnCloud には,Community Edition, Standard Edition, Enterprise Edition の 3 つの Edition が用意されているが,無償提供されているのは Community Edition と Standard Edition の二つの Editon に限られている.監査ログ,ファイルのアクセス制限,SAML/Shibboleth 連携機能等を利用したい場合は,有償ライセンスである Enterprise Edition が必要になる為, 管理者にとって確認したいログ機能やアクセスを制限する機能が不足しておりセキュリティ面で問題があった.利用者側としても,スマートデバイス用アプリが ITunes Store や Google Play などから提供されているが,有償で購入する必要がる.[1]

3.2 新しいソフトウェアの検討

OwnCloud を導入してから 3 年が経ち,利用頻度の高い利用者からの操作や機能に関する問い合わせは少なく,不満の声も無いことから,できる限り操作性や機能性を変えずに,ログ機能やアクセス制限機能を備えているソフトウェアを検討した.

検討段階で,2016 年 6 月に OwnCloud プロジェクトの創設者である Frank Karlitschek らが,操作性や機能性を継承した「NextCloud プロジェクト」を立ち上げていることを知った [2].長期運用する上で持続的なソフトウェアであるか確認すると,初期バージョンを 2016 年 6 月にリリース[3]して以降,半年に一回定期的にアップデートされている. [4].

さらに,機能面では,ファイルストレージ機能,ファイル・フォルダ共有機能など現行の OwnCloud と同様の機能が備われているのに加え,監査ログ,ファイルのアクセス制限,SAML/Shibboleth 連携機能等[5]も備わっていた.現状の問題点を改善することができ,操作性が変わらない唯一のソフトウェアであると考え NextCloud を採用することに決めた.

4 NextCloud の構築 phase

ソフトウェアやデータベースにて障害が発生した際に,切り分けや復旧作業をやりやすくする構成と,セキュリティ,パフォーマンスに配慮したシステム構築を目指した.構築には,NextCloud の Admin manual[6]を参考に構築を行った.

4.1 システムの構成

VMware 社の vSphere 上にプロキシサーバ,アプリケーションサーバ,データベースサーバを分けて構築を行った.

3つに分けた理由としては,現在の OwnCloud サーバも Proxy サーバ配下に設置してあることから,その形を継承した.また,アプリケーションサーバとデータベースサーバに関しては,運用中の OwnCloud にて,CPU やメモリの負荷が高い状況に陥り「アプリケーションの問題か」「データベースの問題か」が最終的に判断付かないまま運用途中で構成変更した経緯があり,論理的に分割をし,パフォーマンス問題等が発生した場合の視認性を高める為に構成を分けた.

ハードウェア/ソフトウェアの構成については,プロキシサーバ,アプリケーションサーバ,データベースサーバ,使用機器の順に記載する.

<プロキシサーバ>

・ハードウェア
- CPU:2vCPU
- メモリ:2048MB
- HDD60GB

・ソフトウェア
- CentOS：7.6.1810 (Core)
- Apach: Apache/2.4.6-89 (CentOS)

<アプリケーションサーバ>

・ハードウェア
- CPU:4vCPU
- メモリ:12288MB
- HDD:30TB

・ソフトウェア
- NextCloud: 16.0.3
- PHP: 7.2.10
- Apache: 2.4.6-89 (CentOS)
- Radis: 3.2.12
- Fail2Ban: 0.9.7-1.el7

<データベースサーバ>

・ハードウェア
- CPU: 4vCPU
- メモリ: 8192MB
- HDD:300GB

・ソフトウェア
- MariaDB: 10.3.17-1
- phpMyAdmin: 4.9.0.1

<使用機器>

サーバ

Cisco UCS B300 M3 (vSphere)

ストレージ

Synology RackStation RS3617xs+

ネットワーク

HPE FlexFabric 5700 Switch(10Gb 接続)

※サーバ・ストレージ間は,10Gb で通信されている.

4.2 セキュリティ対策

当センターで構築している,多くのサーバ OS は,CentOS を利用しており,使い慣れていることから CentOS7 を基本 OS とした.

昨今,学外からのサイバー攻撃が高まっており,不正アクセス攻撃対策として,自動遮断ツール Fail2ban を採用した.

Fail2ban は,NextCloud 側の監査ログに記録されるログイン失敗に関する情報を用いて,ログイン失敗回数と失敗期間を設定し,攻撃してきた IP アドレスをしてする期間ブロックするソフトウェアである.

設定としては,監査ログの内容をフィルタするファイルを /etc/fail2ban/filter.d/ に,[nextcloud.conf]として作成した.作成例は,次の通りである.

failregex={"reqId":".*","level":2,"time":".*","remoteAddr":".*","user":"--","app":"core","method":"POST","url":"¥/nextcloud¥/index.php¥/login","message":"Login failed: '.*' (Remote IP: '.*')","userAgent":"*.","version":".*"}

次に Ban する動作の内容を決める為,/etc/fail2ban/へ[jail.local]を次の通りに作成した.

[nextcloud]
enabled = true
filter = nextcloud
port = http,https
bantime = 315360000 <x 秒間止る(10 年)>
findtime = 600 <失敗期間(10 分)>
maxretry = 5 <連続失敗回数(5 回)>
logpath = /home/data/nextcloud.log

ホワイトリストの設定も可能になっており,学内からのアクセスや特定の IP アドレスをホワイトリストとして別途登録することができる.

この仕組みは,電気通信研究所内の SSH ポートをファイアウォールで許可しているすべてのサーバに対して導入している.

4.3 パフォーマンス対策

特に,NextCloud を高速化する上で,PHP のキャッシュ設定は重要である.Apache Bench を用いて,PHP キャッシュの設定をする前と後の一秒間当たりのリクエスト処理数（図１）と一リクエスト当たりの処理時間（図 2）を比較してみた.

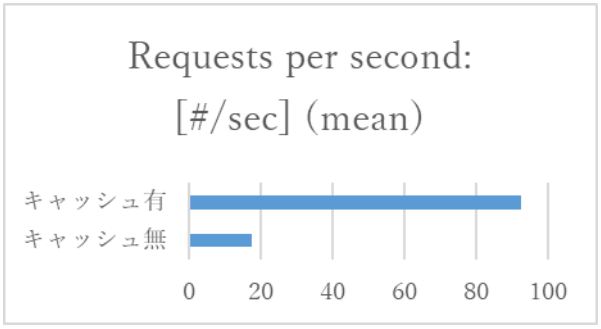

図-1 一秒間のリクエスト処理

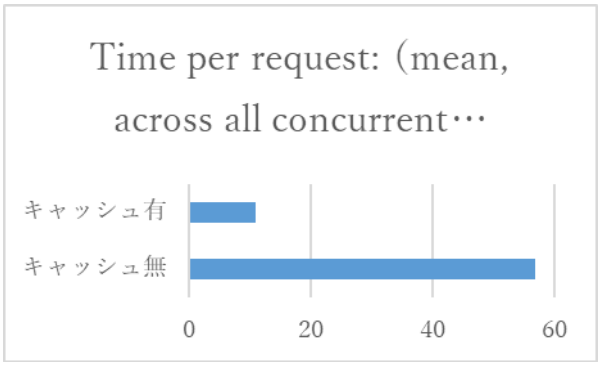

図-2 一秒間の処理時間

Nextcloud では,Alternative PHP Cache User Cache (APCu)が,ローカルキャッシュとして動作する為,2 回目以降のアクセスに対して高いパフォーマンスを発揮する.[7] さらに,Remote Dictionary Server (Redis)を用いて操作中にファイルが破損しないようにファイルをロックする働きをインメモリ処理する為,高速に処理を行うことができる.[8]

4.3 カスタマイズ

現行の OwnCloud では,独自性を出すために,ログイン画面やログイン後の個人ページなどの背景色・ロゴなどのカスタマイズを行っている.以前は,themes ディレクトリ内を変更し,config ファイルも一部変更するなどの手前がかかっていたが,NextCloud 側では[Therming]機能が実装されたことにより,画像データのアップロードや色の

変更が Web 管理画面よりでき作業が軽減された.

NextCloud の Top 画面では,デフォルトでパスワードリセットに関する Link が表示されるようになっていた.ログイン画面よりパスワードの変更をさせないように設定する為,Link の削除を config.php 内の ['lost_password_link' => 'disabled',]行を追加し,表示されないように設定を行った[9].

独自性を出すために,デフォルトの Top 画面 (図 3)をカスタマイズした Top 画面(図 4)へカスタマズする際,現行の OwnCloud システムよりも作業が軽減された.

図 3 変更前のデフォルトの Top 画面

図 5 変更後のカスタマイズの Top 画面

5 運用 phase

5.1 利用目的

Google Drive を利用可能になったことから,個人のバックアップやファイル共有は,基本的に Google Drive を利用してもらい,研究室のファイルサーバとしての役割や事務と教員の共有データ保管場所などが主な利用と考えている.

5.2 利用方法

利用したい人や研究室・部署よりメールにて申請してもらいアカウントを発行する方法とする.原則として,センターが管理するユーザアカウントに限定してサービスを提供する.

ログインする際に,2 要素認証を検討したが,ユーザの使い勝手を優先する為,導入を見送った.

5.3 ユーザ管理

柔軟なユーザアカウントの配布ができるよう研究所内の LDAP サーバとの連携を行わず,ローカルユーザーをセンター側で作成・削除するやり方を取る.

5.4 使用量の制限

現在の OwnCloud システムでは,構成員全員が利用してもらえるように 50GB と限られた領域しか提供出来なかったが,NextCloud システムでは,利用者の数は限られると判断し 1TB と容量を大幅に増加させる.

5.2 保守運用

セキュリティ対策として,定期的なアップデートを行う.アップデート作業が属人化しないようにアップデートマニュアルを作成し全員に共有する.

5 今後の課題とまとめ

5.1 今後の課題

2 要素認証を取り入れない代わりに,新規ログインした際に,メールでログインした IP を知らせる機能を付加したいと考えているが,NextCloud 専用アプリは提供しされていない為,ソースコードを編集して仕組みを作らなければいけない.

5.2 まとめ

On-premises Content Collaboration Platforms の更改に向けた取り組みを紹介した.近年クラウドサービスの飛躍的な進化により Google Drive や Drop Box などが誰でも簡易的に利用できるようになっている.本学でも,オンプレミスよりもクラウドの利用が多くなってきているのが現状であるが,利用が増すと同時にアカウントの問題や柔軟なカスタマイズ性などが問題視されることも出てきている.

オンプレミス版クラウドシステムの提供を考えている担当者に,この情報が届いてもらえれば幸いである.

参考文献

[1] 株式会社スタイルズ Enterprise ライセンス（有償ライセンス）について https://owncloud.jp/solutions/enterprise

[2] nextcloud.org Core ownCloud Contributors Fork ownCloud Into Nextcloud https://nextcloud.com/press/pr20160602/

[3] nextcloud.org Nextcloud 9 Released Ahead of Promised Date and Fully Committed to Open Source https://nextcloud.com/press/pr20160614/

[4] nextcloud.org Nextcloud Server Changelog https://nextcloud.com/changelog/.

[5] nextcloud.org Architecture Overview https://nextcloud.com/whitepapers/

[6] nextcloud.org Administration Manual https://docs.nextcloud.com/server/16/admin_manual/

[7] The PHP Group APC User Cache https://www.php.net/manual/ja/book.apcu.php

[8] nextcloud.org Transactional file locking https://docs.nextcloud.com/server/16/admin_manual/configuration_files/files_locking_transactional.html

[9] nextcloud.org Remove the possibility to reset password for users https://help.nextcloud.com/t/remove-the-possibility-to-reset-password-for-users/27570