Backlog Courrier - Fonctionnalité #24657

TMA - ANALYSE - Edition de documents via le protocole WebDAV

17/04/2023 19:36 - Nathanaël TRAVIER

Statut:	R&D - Terminé	**Début:**	20/03/2023
Priorité:	1-Majeur	**Echéance:**	04/07/2023
Assigné à:	Jean-Laurent DUZANT		
Catégorie:			
Version cible:	21.03 TMA8		
Version applicable MC:	21.03 TMA	**Tags Courrier:**	

Description

Les solutions existantes d'édition de documents ont été écartées par le client pour des raisons techniques et/ou fonctionnelles (via JAVA - pb de sécurité ; via Sharepoint - pb de confidentialité ; via OnlyOffice - expérience utilisateur différente de windows).

La piste de l'édition de document sous Office en mobilisant le protocole Webdav a été soulevée. Ce protocole servirait les mêmes besoins que les appels java précédemment utilisés. L'étude de la mise en place de cette fonctionnalité pourrait-elle être lancée ?

Avant d'engager les développements, il importera de valider avec le client le flux Webdav et l'architecture de la solution pour éviter un développement inutile.

A. Compréhension

En tant qu'administrateur, je souhaite paramétrer l'édition bureautique au moyen du protocole Webdav

B. Proposition

Analyser la complexité et le risque.
Autres solutions ? WOPI ?

Valider avec l'environnement client. (spécificités)
MacOS / Windows

POC minimum
Attendu : description des flux

C. Impacts

D. Evaluation

US ANALYSE : EFFORT : 8

Historique

#2 - 17/04/2023 19:37 - Nathanaël TRAVIER

Emmanuel, tu pourrais nous donner une estimation de quand un tel dév pourrait être imaginé ? Même si c'est lointain, qu'on puisse avoir une idée de l'horizon, car une solution de contournement (OnlyOffice) va être probablement mise en place.

#3 - 17/04/2023 19:37 - Nathanaël TRAVIER

- Privée changé de Oui à Non

#4 - 18/04/2023 09:28 - Emmanuel DILLARD

- Sujet changé de [DGAC] Edition de documents via WebDAV à TMA - ANALYSE - Edition de documents via WebDAV

- Echéance mis à 24/04/2023

- Statut changé de A traiter à R&D - A étudier

- Version cible changé de 2301 à 21.03 TMA7

#7 - 24/04/2023 12:15 - Emmanuel DILLARD

- Sujet changé de TMA - ANALYSE - Edition de documents via WebDAV à TMA - ANALYSE - Edition de documents via le protocole WebDAV

- Description mis à jour

- Statut changé de R&D - A étudier à En attente financement

- Assigné à changé de Emmanuel DILLARD à Nathanaël TRAVIER

#9 - 24/04/2023 17:07 - Nathanaël TRAVIER

- Assigné à changé de Nathanaël TRAVIER à Emmanuel DILLARD

#11 - 24/04/2023 17:15 - Emmanuel DILLARD

- Echéance 24/04/2023 supprimé

- Statut changé de En attente financement à R&D - A planifier

#12 - 27/04/2023 11:52 - Emmanuel DILLARD

- Version cible changé de 21.03 TMA7 à 21.03 TMA8

#14 - 24/05/2023 10:33 - Emmanuel DILLARD

- Priorité changé de 1-Majeur à 0-Bloquant

- Version applicable MC mis à 21.03 TMA

#16 - 24/05/2023 10:35 - Emmanuel DILLARD

- Description mis à jour

#18 - 06/06/2023 14:57 - Emmanuel DILLARD

- Echéance mis à 20/06/2023

- Statut changé de R&D - A planifier à R&D - En cours

#19 - 06/06/2023 15:14 - Emmanuel DILLARD

- Assigné à Emmanuel DILLARD supprimé

#20 - 08/06/2023 09:56 - Jean-Laurent DUZANT

- Assigné à mis à Jean-Laurent DUZANT

#21 - 20/06/2023 09:49 - Jean-Laurent DUZANT

Point WebDAV - DGAC pour 21/06/2023 16:00 - 17:00

#22 - 20/06/2023 10:38 - Emmanuel DILLARD

- Echéance 20/06/2023 supprimé

- Priorité changé de 0-Bloquant à 1-Majeur

#23 - 20/06/2023 11:46 - Emmanuel DILLARD

- Echéance mis à 04/07/2023

#24 - 23/06/2023 10:36 - Jean-Laurent DUZANT

Après avoir fait quelques recherches et fait quelques preuves de concept, il y a plusieurs sujets où l'utilisation de Webdav avec Maarch Courrier ne correspond pas.

Authentification

WebDAV peut être utilisé sans authentification, mais il n'est pas recommandé pour des raisons de sécurité.
Par défaut, WebDAV ne nécessite pas d'authentification, ce qui signifie que toute personne ayant accès a WebDAV peut lire, écrire et modifier des fichiers et des dossiers.
Le manque d'authentification pose un risque de sécurité important, en particulier lorsque WebDAV est exposé à Internet.

Sans authentification, quiconque découvre le serveur WebDAV peut potentiellement accéder à des données sensibles, télécharger des fichiers malveillants ou modifier des fichiers existants.
Cela peut entraîner un accès non autorisé, des violations de données ou d'autres incidents de sécurité.

WebDAV prend en charge plusieurs mécanismes d'authentification pour sécuriser l'accès aux ressources, il suffit de configurer le virtual host de Webdav
Voici quelques méthodes d'authentification couramment utilisées dans WebDAV :

1. Authentification de base : l'authentification de base est la forme d'authentification la plus simple dans WebDAV. Il s'agit d'envoyer le nom d'utilisateur et le mot de passe en clair à chaque demande. Bien que facile à mettre en œuvre, il n'est pas considéré comme sécurisé car les informations d'identification sont transmises sans cryptage.
2. Authentification Digest : L'authentification Digest est une amélioration par rapport à l'authentification de base car elle envoie une version hachée du mot de passe au lieu du mot de passe réel. Il offre un niveau de sécurité en évitant la transmission de mots de passe en clair. Le serveur génère une valeur nonce, que le client utilise pour créer une réponse hachée.
3. OAuth : OAuth est une norme ouverte d'authentification et d'autorisation. Il permet aux utilisateurs d'accorder à des applications tierces l'accès à leurs ressources sans partager leurs mots de passe. OAuth est couramment utilisé pour l'authentification avec les API et les services Web, y compris WebDAV.
4. Authentification basée sur les jetons : L'authentification basée sur les jetons implique l'émission d'un jeton à un client lors d'une authentification réussie. Le client inclut ensuite ce jeton dans les demandes ultérieures pour s'authentifier. Les jetons peuvent avoir un délai d'expiration et peuvent être utilisés pour plusieurs demandes jusqu'à leur expiration.
5. Authentification par certificat client SSL/TLS : L'authentification par certificat client SSL/TLS implique l'utilisation de certificats client pour authentifier lauthentificationes utilisateurs. Le serveur vérifie le certificat du client pendant le processus de prise de contact SSL/TLS, fournissant une méthode d'authentification sécurisée et fiable.

Dans le périmetre du POC, nous avons utilisé la méthode Base et Digest pour s'authentifier de puis Maarch Courrier.

WebDAV nécessite une référence à sa base de données (en fonction du type d'authentification) pour gérer les processus d'authentification.
Il est possible que le compte utilisé pour WebDAV et le compte utilisé pour Maarch Courrier soient différents.
Dans mes tests, j'ai utilisé le compte Maarch Courrier pour créer le compte WebDAV d'un utilisateur.
Dans ce scénario, Maarch Courrier devrait exécuter des commandes Linux, mais il sera bloqué lors de la saisie des mots de passe car cela doit être fait manuellement.
Par conséquent, si un administrateur réseau crée de nouveaux comptes pour les utilisateurs de Maarch Courrier, il serait peu performant de vérifier et de synchroniser les comptes WebDAV et Maarch Courrier en exécutant un script toutes les minutes.

Il est important de comprendre que Maarch Courrier et WebDAV sont des systèmes distincts avec leurs propres exigences d'authentification.
Cela peut entraîner des limitations lors de la gestion des comptes utilisateur et de l'authentification entre les deux systèmes.
Des solutions alternatives peuvent être nécessaires pour synchroniser les comptes et assurer une expérience utilisateur fluide.

Accès du fichier ou répertoire

WebDAV utilise les autorisations des utilisateurs pour contrôler l'accès aux fichiers et répertoires.

Il exploite le système d'autorisations sous-jacent du système de fichiers pour déterminer les actions que les utilisateurs peuvent effectuer sur des fichiers et des répertoires spécifiques.

L'implémentation spécifique peut varier en fonction du serveur WebDAV et du système d'exploitation sur lequel il s'exécute.
Voici une explication générale de la façon dont WebDAV utilise les autorisations des utilisateurs :

1. Autorisations du système de fichiers : WebDAV hérite des autorisations du système de fichiers sous-jacent. Chaque fichier et répertoire possède un ensemble d'autorisations qui définissent qui peut effectuer des actions spécifiques dessus.
   Les niveaux d'autorisation courants sont :

- Lecture : Permet à un utilisateur de visualiser le contenu d'un fichier ou d'un répertoire.
- Écriture : Permet à un utilisateur de modifier le contenu d'un fichier ou d'un répertoire, y compris la création, la modification et la suppression.
- Exécution : Relatif aux fichiers exécutables, permet à l'utilisateur d'exécuter le fichier ou de le lancer.
- Suppression : Autorise l'utilisateur à supprimer un fichier ou un répertoire.
- Liste : Permet à l'utilisateur de voir la liste des fichiers et répertoires dans un répertoire spécifique.

1. Authentification de l'utilisateur : Les utilisateurs doivent s'authentifier auprès du serveur WebDAV en utilisant des identifiants valides (nom d'utilisateur et mot de passe) ou d'autres mécanismes d'authentification. Ce processus d'authentification vérifie l'identité de l'utilisateur.
2. Mappage des autorisations des utilisateurs : Une fois authentifié, le serveur WebDAV fait correspondre l'utilisateur authentifié au compte utilisateur correspondant sur le système d'exploitation. Le serveur vérifie ensuite les autorisations de l'utilisateur sur le fichier ou le répertoire demandé.

3. Contrôle d'accès : Le serveur WebDAV applique des règles de contrôle d'accès en fonction des autorisations mappées de l'utilisateur et de l'action demandée (par exemple, lecture, écriture, suppression). Si l'utilisateur dispose des autorisations nécessaires, l'action est autorisée ; sinon, elle est refusée.
4. Propagation des autorisations : Lorsque des fichiers ou des répertoires sont créés dans un serveur WebDAV, ils héritent par défaut des autorisations du répertoire parent. Cette propagation garantit que les autorisations appropriées sont maintenues dans toute la hiérarchie des fichiers. Il est important de noter que les détails des autorisations des utilisateurs dans WebDAV peuvent varier en fonction de l'implémentation et de la configuration du serveur. Certains serveurs peuvent proposer des fonctionnalités supplémentaires pour un contrôle d'accès plus précis, comme la définition de groupes d'utilisateurs, la configuration d'autorisations spécifiques pour chaque utilisateur ou groupe, et la mise en place de règles de contrôle d'accès basées sur des attributs tels que les types de fichiers ou les métadonnées.

Sans authentification utilisateur, WebDAV peut utiliser les permissions d'utilisateur pour contrôler l'accès aux fichiers et aux répertoires.
Il prend en charge les permissions standard du système de fichiers telles que la lecture, l'écriture et l'exécution, qui peuvent être appliquées aux fichiers et aux répertoires individuels.

Lorsqu'un serveur WebDAV est configuré, il peut définir des règles de contrôle d'accès qui déterminent quels utilisateurs ou groupes ont la permission d'effectuer des opérations spécifiques sur les fichiers et les répertoires.
Ces permissions peuvent être définies à différents niveaux, tels que le niveau du serveur, le niveau du répertoire ou le niveau du fichier individuel.

Le serveur WebDAV maintient une liste d'utilisateurs ou de groupes et de leurs permissions correspondantes.
Lorsqu'un utilisateur tente d'accéder à un fichier ou à un répertoire, le serveur vérifie les permissions associées à cet utilisateur ou à ce groupe et détermine si l'opération demandée est autorisée.

Par exemple, un serveur peut définir qu'un certain utilisateur a des permissions de lecture et d'écriture sur un répertoire particulier, ce qui lui permet de visualiser et de modifier les fichiers à l'intérieur de ce répertoire.
Un autre utilisateur pourrait n'avoir que des permissions de lecture, limitant ainsi son accès à la visualisation des fichiers mais pas à leur modification.
Ces permissions peuvent être personnalisées et gérées en fonction des exigences spécifiques du serveur WebDAV.

Il est important de noter que, bien que WebDAV puisse contrôler l'accès aux fichiers et aux répertoires en fonction des permissions d'utilisateur, il est toujours recommandé d'utiliser l'authentification utilisateur chaque fois que possible pour garantir que les utilisateurs corrects accèdent au serveur et pour fournir une couche de sécurité supplémentaire.
L'authentification utilisateur contribue à prévenir l'accès non autorisé et garantit que les permissions sont appliquées aux utilisateurs ou groupes appropriés.

sans authentification, l'accès aux fichiers et répertoires via WebDAV est restreint.
Même si les autorisations du système de fichiers sont définies pour permettre certaines actions sur les fichiers et répertoires, un utilisateur doit toujours s'authentifier auprès du serveur WebDAV pour accéder à ces ressources.

Les autorisations du système de fichiers définissent uniquement les permissions accordées aux utilisateurs qui ont été authentifiés et qui ont fourni les informations d'identification appropriées.

L'authentification est une étape cruciale pour garantir que seules les personnes autorisées peuvent accéder aux fichiers et répertoires via WebDAV.
Cela permet de contrôler précisément les actions qu'un utilisateur peut effectuer sur les ressources, en fonction de son identité et de ses autorisations spécifiques.

Edition d'un document

Il n'est malheureusement pas possible d'éditer un document en temps réel en utilisant le protocole WebDAV.
WebDAV offre des fonctionnalités telles que l'accès, le téléchargement et le partage de fichiers, mais il ne permet pas d'effectuer des modifications en temps réel.

Pour modifier un document, vous devez suivre une procédure spécifique.
Tout d'abord, vous devez télécharger une copie du document sur votre ordinateur.
Ensuite, vous pouvez apporter les modifications nécessaires à cette copie locale en utilisant un logiciel d'édition approprié.
Une fois les modifications terminées, vous devez téléverser la nouvelle version du document vers le serveur en utilisant WebDAV.

Cette approche est nécessaire en raison des limitations du protocole WebDAV qui ne prend pas en charge la synchronisation en temps réel des modifications.
Afin de préserver l'intégrité des données et d'éviter les conflits, il est important de travailler sur une copie locale du document et de téléverser les modifications une fois que vous avez terminé.

Dans Maarch Courrier, vous pouvez accéder à un document via WebDAV et profiter de plusieurs fonctionnalités telles que l'affichage, le téléchargement local sur votre ordinateur, la mise à jour et la suppression directement depuis votre navigateur.
Cependant, il est important de noter que Maarch Courrier ne prend pas en charge l'édition directe des documents situés sur votre ordinateur. Cette limitation est mise en place pour des raisons de sécurité.
Maarch Courrier fonctionne à travers un navigateur Internet, et les navigateurs modernes ont mis en place des mesures de sécurité strictes pour protéger les utilisateurs contre les risques potentiels, tels que l'accès non autorisé à leurs fichiers personnels.
Permettre l'édition directe des documents sur l'ordinateur de l'utilisateur depuis le navigateur pourrait compromettre la sécurité de vos fichiers.

En conclusion, WebDAV peut être utilisé sans authentification, mais cela n'est pas recommandé en raison des risques de sécurité associés.
Il est préférable de configurer WebDAV avec des mécanismes d'authentification appropriés pour contrôler l'accès aux ressources.

Les autorisations du système de fichiers sont utilisées par WebDAV pour déterminer les actions qu'un utilisateur peut effectuer sur les fichiers et répertoires.
Cependant, ces autorisations ne sont appliquées qu'aux utilisateurs qui se sont authentifiés avec succès.

En ce qui concerne l'édition des documents, le protocole WebDAV lui-même ne prend pas en charge l'édition en temps réel.
Pour modifier un document, vous devez télécharger une copie sur votre ordinateur, apporter les modifications nécessaires localement, puis téléverser la nouvelle version sur le serveur via WebDAV.

Il est important de noter que Maarch Courrier ne prend pas en charge l'édition directe des documents situés sur votre ordinateur depuis le navigateur pour des raisons de sécurité.
Les mesures de sécurité des navigateurs modernes empêchent l'accès non autorisé aux fichiers personnels des utilisateurs.

#25 - 23/06/2023 11:25 - Jean-Laurent DUZANT

- Fichier unlock-file-in-webdav.png ajouté

- Fichier lock-file-in-webdav.png ajouté

- Fichier unlock-file-in-webdav.png ajouté

- Fichier lock-file-in-webdav.png ajouté

- Fichier unlock-file-in-webdav.png ajouté

#26 - 23/06/2023 11:26 - Jean-Laurent DUZANT

- Fichier unlock-file-in-webdav.png supprimé

#27 - 23/06/2023 11:26 - Jean-Laurent DUZANT

- Fichier lock-file-in-webdav.png supprimé

#28 - 23/06/2023 11:26 - Jean-Laurent DUZANT

- Fichier unlock-file-in-webdav.png supprimé

#29 - 23/06/2023 11:26 - Jean-Laurent DUZANT

- Fichier lock-file-in-webdav.png supprimé

#30 - 23/06/2023 11:26 - Jean-Laurent DUZANT

- Fichier unlock-file-in-webdav.png supprimé

#31 - 23/06/2023 11:27 - Jean-Laurent DUZANT

- Fichier lock-file-in-webdav.png ajouté

- Fichier unlock-file-in-webdav.png ajouté

#32 - 23/06/2023 11:28 - Jean-Laurent DUZANT

- Fichier get-folder-info.png ajouté

#33 - 23/06/2023 11:29 - Jean-Laurent DUZANT

- Statut changé de R&D - En cours à R&D - En test

#36 - 28/06/2023 13:00 - Jean-Laurent DUZANT

- Statut changé de R&D - En test à R&D - Terminé

Fichiers

lock-file-in-webdav.png	20,5 ko	23/06/2023	Jean-Laurent DUZANT
unlock-file-in-webdav.png	16,4 ko	23/06/2023	Jean-Laurent DUZANT
get-folder-info.png	33,6 ko	23/06/2023	Jean-Laurent DUZANT