aws

Guide d’administration

Amazon WorkDocs

Amazon WorkDocs: Guide d’administration

Table of Contents

Remarque : les inscriptions de nouveaux clients et les mises à niveau de compte ne sont plus disponibles pour Amazon. WorkDocs Découvrez les étapes de migration ici : Comment migrer des données depuis WorkDocs.

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.

Qu'est-ce qu'Amazon WorkDocs ?

Amazon WorkDocs est un service de stockage et de partage d'entreprise entièrement géré et sécurisé, doté de contrôles administratifs stricts et de fonctionnalités de feedback qui améliorent la productivité des utilisateurs. Vos fichiers sont stockés dans le cloud en toute sécurité. Les fichiers de vos utilisateurs ne sont visibles que d'eux et de leurs collaborateurs et utilisateurs désignés. Les autres membres de votre organisation n'ont pas accès aux fichiers des autres utilisateurs, sauf si un accès spécifique leur est accordé.

Les utilisateurs peuvent partager leurs fichiers avec d'autres membres de votre organisation à des fins de collaboration ou de vérification. Les applications WorkDocs clientes peuvent être utilisées pour visualiser de nombreux types de fichiers, en fonction du type de support Internet du fichier. WorkDocs prend en charge tous les formats de document et d'image courants, et la prise en charge de types de médias supplémentaires est constamment ajoutée.

Pour plus d'informations, consultez Amazon WorkDocs.

Accès WorkDocs

Les administrateurs utilisent la WorkDocs console pour créer et désactiver WorkDocs des sites. Avec le Panneau de configuration d'administration, ils peuvent gérer les utilisateurs, le stockage et les paramètres de sécurité. Pour plus d'informations, consultez Gestion WorkDocs depuis le panneau de configuration d'administration du site et Inviter et gérer WorkDocs les utilisateurs.

Les utilisateurs non administratifs utilisent les applications clientes pour accéder à leurs fichiers. Ils n'utilisent jamais la WorkDocs console ni le tableau de bord d'administration. WorkDocs propose plusieurs applications client et utilitaires différents :

- Une application web utilisée pour la gestion et la consultation de documents.
- Des applications natives pour appareils mobiles, utilisées pour la consultation des documents.
- WorkDocs Drive, une application qui synchronise un dossier de votre bureau macOS ou Windows avec vos WorkDocs fichiers.

Pour plus d'informations sur la manière dont les utilisateurs peuvent télécharger des WorkDocs clients, modifier leurs fichiers et utiliser des dossiers, consultez les rubriques suivantes du guide de l'WorkDocs utilisateur :

- Commencer avec WorkDocs
- Travailler avec des fichiers
- Travailler avec des dossiers

Tarification

Avec WorkDocs, il n'y a pas de frais initiaux ni d'engagements. Vous ne payez que pour les comptes utilisateurs actifs et pour l'espace de stockage que vous utilisez. Pour plus d'informations, consultez la section Tarification.

Comment démarrer

Pour commencer WorkDocs, voirCréation d'un WorkDocs site.

Migration de données depuis WorkDocs

WorkDocs propose deux méthodes pour migrer des données depuis un WorkDocs site. Cette section fournit une vue d'ensemble de ces méthodes et des liens vers des étapes détaillées pour exécuter, dépanner et optimiser chaque méthode de migration.

Les clients auront deux options pour déconnecter leurs données d'Amazon WorkDocs : la fonctionnalité de téléchargement groupé existante (méthode 1) ou notre nouvel outil de migration de données (méthode 2). Les rubriques suivantes expliquent comment utiliser les deux méthodes.

Rubriques

Méthode 1 : téléchargement de fichiers en masse

Si vous souhaitez contrôler les fichiers que vous migrez, vous pouvez les télécharger manuellement en bloc. Cette méthode vous permet de sélectionner uniquement les fichiers souhaités et de les télécharger sur un autre emplacement, tel que votre disque local. Vous pouvez télécharger des fichiers et des dossiers depuis votre site WorkDocs Web ou depuis WorkDocs Drive.

Rappelez-vous ce qui suit :

- Les utilisateurs de votre site peuvent télécharger des fichiers en suivant les étapes ci-dessous. Si vous préférez, vous pouvez configurer un dossier partagé, demander à vos utilisateurs de déplacer les fichiers vers ce dossier, puis de télécharger le dossier vers un autre emplacement. Vous pouvez également vous en transférer la propriété et effectuer les téléchargements.
- Pour télécharger des documents Microsoft Word contenant des commentaires, consultez la section Téléchargement de documents Word contenant des commentaires dans le Guide de WorkDocs l'utilisateur.
- Vous devez utiliser WorkDocs Drive pour télécharger des fichiers de plus de 5 Go.
- Lorsque vous utilisez WorkDocs Drive pour télécharger des fichiers et des dossiers, vos structures de répertoires, vos noms de fichiers et leur contenu restent intacts. La propriété, les autorisations et les versions des fichiers ne sont pas conservées.

Téléchargement de fichiers depuis le Web

Vous utilisez cette méthode pour télécharger des fichiers lorsque :

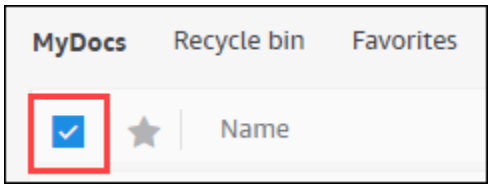
- Vous souhaitez uniquement télécharger certains fichiers à partir d'un site.
- Vous souhaitez télécharger des documents Word contenant des commentaires et conserver ces commentaires dans leurs documents respectifs. L'outil de migration télécharge tous les commentaires, mais il les écrit dans un fichier XML distinct. Les utilisateurs du site peuvent alors avoir du mal à associer des commentaires à leurs documents Word.

Pour télécharger des fichiers depuis le Web

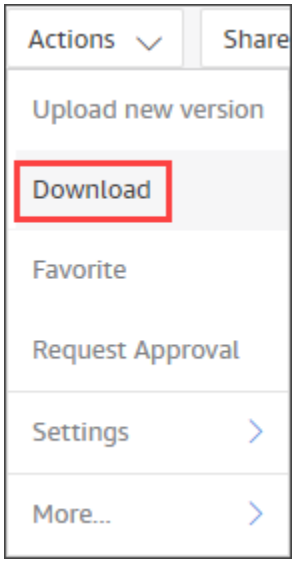
1. Connectez-vous à WorkDocs.
2. Le cas échéant, ouvrez le dossier contenant les fichiers que vous souhaitez télécharger.
3. Cochez la case à côté des fichiers que vous souhaitez télécharger.

   —OU—

   Cochez la case en haut de la liste pour sélectionner tous les fichiers du dossier.



4. Ouvrez le menu Actions et choisissez Télécharger. .



Sur un PC, les fichiers téléchargés apparaissent par défaut dans le nom du dossier Downloads/ WorkDocsDownloads/. Sur un Macintosh, les fichiers atterrissent par défaut dans le nom du disque dur /Users/ user name/. WorkDocsDownloads

Téléchargement de dossiers depuis le Web

> **Note**
>
> Lorsque vous téléchargez des dossiers, vous téléchargez également tous les fichiers qu'ils contiennent. Si vous souhaitez uniquement télécharger certains fichiers d'un dossier, déplacez les fichiers indésirables vers un autre emplacement ou vers la corbeille, puis téléchargez le dossier.

Pour télécharger des dossiers depuis le Web

1. Connectez-vous à WorkDocs
2. Cochez la case à côté de chacun des dossiers que vous souhaitez télécharger.

   —OU—

   Ouvrez les dossiers et cochez les cases à côté des sous-dossiers que vous souhaitez télécharger.
3. Ouvrez le menu Actions et choisissez Télécharger. .

   Sur un PC, les dossiers téléchargés apparaissent par défaut dans le nom du dossier Downloads/ WorkDocsDownloads/. Sur un Macintosh, les fichiers atterrissent par défaut dans le nom du disque dur /Users/ user name/. WorkDocsDownloads

Utilisation WorkDocs de Drive pour télécharger des fichiers et des dossiers

> **Note**
>
> Vous devez installer WorkDocs Drive pour effectuer les étapes suivantes. Pour plus d'informations, consultez la section Installation de WorkDocs Drive dans le guide de l'utilisateur de WorkDocs Drive.

Pour télécharger des fichiers et des dossiers depuis WorkDocs Drive

1. Lancez l'explorateur de fichiers ou le Finder et ouvrez votre lecteur W :.
2. Sélectionnez les dossiers ou les fichiers que vous souhaitez télécharger.
3. Appuyez longuement (avec le bouton droit de la souris) sur les éléments sélectionnés et choisissez Copier, puis collez les éléments copiés dans leur nouvel emplacement.

   —OU—

   Faites glisser les éléments sélectionnés vers leur nouvel emplacement.
4. Supprimez les fichiers d'origine de WorkDocs Drive.

Méthode 2 : utiliser l'outil de migration

Vous utilisez l'outil de WorkDocs migration lorsque vous souhaitez migrer toutes les données d'un WorkDocs site.

L'outil de migration déplace les données d'un site vers un bucket Amazon Simple Storage Service. L'outil crée un fichier ZIP compressé pour chaque utilisateur. Le fichier compressé inclut tous les fichiers et dossiers, les versions, les autorisations, les commentaires et les annotations de chacun des utilisateurs finaux de votre WorkDocs site.

Rubriques

Prérequis

Vous devez disposer des éléments suivants pour utiliser l'outil de migration.

- Un compartiment Amazon S3. Pour plus d'informations sur la création d'un compartiment Amazon S3, consultez la section Création d'un compartiment dans le guide de l'utilisateur Amazon S3.

Votre bucket doit utiliser le même compte IAM et résider dans la même région que votre WorkDocs site. Vous devez également bloquer l'accès public au bucket. Pour plus d'informations à ce sujet, consultez la section Blocage de l'accès public à votre espace de stockage Amazon S3 dans le guide de l'utilisateur Amazon S3.

Pour WorkDocs autoriser le téléchargement de vos fichiers, configurez la politique de compartiment comme indiqué dans l'exemple suivant. La politique utilise les clés de `aws:SourceArn` condition `aws:SourceAccount` et pour réduire la portée de la politique, ce qui constitue une bonne pratique en matière de sécurité.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowWorkDocsFileUpload",
            "Effect": "Allow",
            "Principal": {
                "Service": "workdocs.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::BUCKET-NAME/*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "AWS-ACCOUNT-ID"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:workdocs:REGION:AWS-ACCOUNT-
ID:organization/WORKDOCS-DIRECTORY-ID"
                }
            }
        }
    ]
}
```

> **Note**
>
> - *WORKDOCS-DIRECTORY-ID*est l'identifiant de l'organisation de votre WorkDocs site. Cela se trouve dans le tableau « Mes sites » de la WorkDocs console AWS
> - Pour plus d'informations sur la configuration d'une politique de compartiment, consultez Ajouter une politique de compartiment à l'aide de la console Amazon S3

- Une stratégie IAM. Pour démarrer une migration sur la WorkDocs console, le principal appelant IAM doit avoir la politique suivante attachée à son ensemble d'autorisations :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowStartWorkDocsMigration",
            "Effect": "Allow",
            "Action": [
                "workdocs:StartInstanceExport"
            ],
            "Resource": [
                "arn:aws:workdocs:REGION:AWS-ACCOUNT-ID:organization/WORKDOCS-
DIRECTORY-ID"
            ]
        },
        {
            "Sid": "AllowDescribeWorkDocsMigrations",
            "Effect": "Allow",
            "Action": [
                "workdocs:DescribeInstanceExports",
                "workdocs:DescribeInstances"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "AllowS3Validations",
            "Effect": "Allow",
            "Action": [
                "s3:HeadBucket",
                "s3:ListBucket",
                "s3:GetBucketPublicAccessBlock",
                "kms:ListAliases"
            ],
            "Resource": [
                "arn:aws:s3:::BUCKET-NAME"
            ]
        },
        {
            "Sid": "AllowS3ListMyBuckets",
```

```
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

- Vous pouvez éventuellement utiliser une AWS KMS clé pour chiffrer les données inactives de votre compartiment. Si vous ne fournissez pas de clé, le paramètre de chiffrement standard du bucket s'applique. Pour plus d'informations, consultez la section Création de clés dans le Guide du développeur du service de gestion des AWS clés.

  Pour utiliser une AWS KMS clé, ajoutez les instructions suivantes à la politique IAM. Vous devez utiliser une clé active du type SYMMETRIC_DEFAULT.

```
{
    "Sid": "AllowKMSMigration",
     "Effect": "Allow",
     "Action": [
         "kms:CreateGrant",
         "kms:DescribeKey"
     ],
     "Resource": [

         "arn:aws:kms:REGION:AWS-ACCOUNT-ID:key/KEY-RESOURCE-ID"
     ]
}
```

Limites

L'outil de migration présente les limites suivantes :

- L'outil écrit toutes les autorisations, commentaires et annotations des utilisateurs dans des fichiers CSV séparés. Vous devez mapper ces données aux fichiers correspondants manuellement.
- Vous ne pouvez migrer que les sites actifs.
- L'outil est limité à une migration réussie par site pour chaque période de 24 heures.

- Vous ne pouvez pas exécuter des migrations simultanées d'un même site, mais vous pouvez exécuter des migrations simultanées pour différents sites.
- Chaque fichier zip sera d'au plus 50 Go. Les utilisateurs disposant de plus de 50 Go de données WorkDocs pourront exporter plusieurs fichiers zip vers Amazon S3.
- L'outil n'exporte pas les fichiers de plus de 50 Go. L'outil répertorie tous les fichiers de plus de 50 Go dans un fichier CSV portant le même préfixe que les fichiers ZIP. Par exemple, / workdocs///skippedFiles.csv***site-alias***. ***created-timestamp-UTC*** Vous pouvez télécharger les fichiers listés par programme ou manuellement. Pour plus d'informations sur le téléchargement par programmationhttps://docs.aws.amazon.com/workdocs/latest/developerguide/download-documents.html, reportez-vous au Guide du WorkDocs développeur. Pour plus d'informations sur le téléchargement manuel des fichiers, reportez-vous aux étapes de la méthode 1, plus haut dans cette rubrique.
- Le fichier zip de chaque utilisateur contiendra uniquement les and/or dossiers de fichiers qu'il possède. Tous les and/or dossiers de fichiers partagés avec l'utilisateur figureront dans le fichier zip de l'utilisateur propriétaire des and/or dossiers de fichiers.
- Si un dossier est vide (ne contient aucun fichier/dossier imbriqué) WorkDocs, il ne sera pas exporté.
- Il n'est pas garanti que les données (fichiers, dossiers, versions, commentaires, annotations) créées après le lancement de la tâche de migration seront incluses dans les données exportées dans S3.
- Vous pouvez migrer plusieurs sites vers un compartiment Amazon S3. Il n'est pas nécessaire de créer un bucket par site. Cependant, vous devez vous assurer que vos politiques IAM et de bucket autorisent plusieurs sites.
- La migration augmente les coûts liés à Amazon S3, en fonction de la quantité de données que vous migrez vers le compartiment. Pour plus d'informations, consultez la page de tarification d'Amazon S3.

Exécution de l'outil de migration

Les étapes suivantes expliquent comment exécuter l'outil de WorkDocs migration.

Pour migrer un site

1. Ouvrez la WorkDocs console à l'adresse https://console.aws.amazon.com/zocalo/.

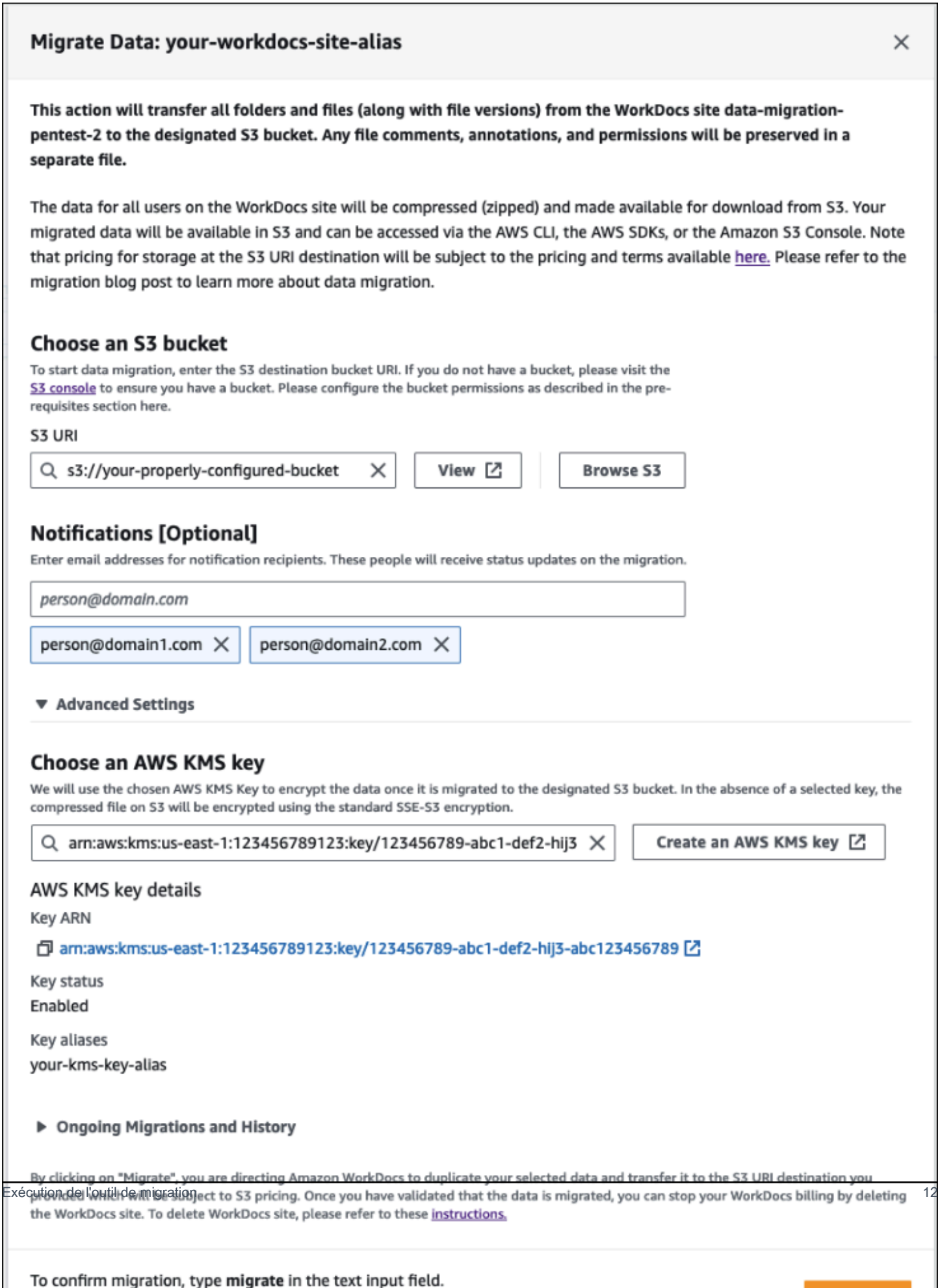
2. Dans le volet de navigation, choisissez Mes sites, puis sélectionnez le bouton radio à côté du site que vous souhaitez migrer.
3. Ouvrez la liste des actions et choisissez Migrer les données.
4. Sur la page du nom du site Migrate Data, entrez l'URI de votre compartiment Amazon S3.

   —OU—

   Choisissez Browse S3 et procédez comme suit :

   a. Au besoin, recherchez le compartiment.
   b. Sélectionnez le bouton radio à côté du nom du bucket, puis sélectionnez Choisir.
5. (Facultatif) Sous Notifications, entrez un maximum de cinq adresses e-mail. L'outil envoie des e-mails sur l'état de la migration à chaque destinataire.
6. (Facultatif) Dans Paramètres avancés, sélectionnez une clé KMS pour chiffrer vos données stockées.
7. Entrez **`migrate`** dans la zone de texte pour confirmer la migration, puis choisissez Démarrer la migration.

   Un indicateur apparaît et indique l'état de la migration. Les délais de migration varient en fonction de la quantité de données d'un site.


Migrate Data: your-workdocs-site-alias
This action will transfer all folders and files (along with file versions) from the WorkDocs site data-migration-pentest-2 to the designated S3 bucket. Any file comments, annotations, and permissions will be preserved in a separate file.
The data for all users on the WorkDocs site will be compressed (zipped) and made available for download from S3. Your migrated data will be available in S3 and can be accessed via the AWS CLI, the AWS SDKs, or the Amazon S3 Console. Note that pricing for storage at the S3 URI destination will be subject to the pricing and terms available here. Please refer to the migration blog post to learn more about data migration.
Choose an S3 bucket
To start data migration, enter the S3 destination bucket URI. If you do not have a bucket, please visit the S3 console to ensure you have a bucket. Please configure the bucket permissions as described in the pre-requisites section here.
S3 URI
s3://your-properly-configured-bucket
View
Browse S3
Notifications [Optional]
Enter email addresses for notification recipients. These people will receive status updates on the migration.
person@domain.com
person@domain1.com
person@domain2.com
Advanced Settings
Choose an AWS KMS key
We will use the chosen AWS KMS Key to encrypt the data once it is migrated to the designated S3 bucket. In the absence of a selected key, the compressed file on S3 will be encrypted using the standard SSE-S3 encryption.
arn:aws:kms:us-east-1:123456789123:key/123456789-abc1-def2-hij3
Create an AWS KMS key
AWS KMS key details
Key ARN
arn:aws:kms:us-east-1:123456789123:key/123456789-abc1-def2-hij3-abc123456789
Key status
Enabled
Key aliases
your-kms-key-alias
Ongoing Migrations and History
By clicking on "Migrate", you are directing Amazon WorkDocs to duplicate your selected data and transfer it to the S3 URI destination you provided which will be subject to S3 pricing. Once you have validated that the data is migrated, you can stop your WorkDocs billing by deleting the WorkDocs site. To delete WorkDocs site, please refer to these instructions.
To confirm migration, type migrate in the text input field.

Lorsque la migration est terminée :

- L'outil envoie des e-mails de « réussite » aux adresses saisies lors de la configuration, le cas échéant.
- Votre compartiment Amazon S3 contiendra un dossier /workdocs/ ***site-alias***//***created-timestamp-UTC***. Ce dossier contient un dossier zippé pour chaque utilisateur possédant des données sur le site. Chaque dossier zippé contient les dossiers et les fichiers de l'utilisateur, y compris les fichiers CSV de mappage des autorisations et des commentaires.
- Si un utilisateur supprime tous ses fichiers avant la migration, aucun dossier compressé n'apparaît pour cet utilisateur.
- Versions — Les documents comportant plusieurs versions ont un identifiant d'horodatage de création _ version _. L'horodatage utilise des millisecondes d'époque. Par exemple, un document nommé « TestFile .txt » avec 2 versions apparaît comme suit :

```
        TestFile.txt (version 2 - latest version)
        TestFile_version_1707437230000.txt
```

- Autorisations — L'exemple suivant montre le contenu d'un fichier CSV d'autorisations typique.

```
PathToFile,PrincipalName,PrincipalType,Role
/mydocs/Projects,user1@domain.com,USER,VIEWER
/mydocs/Personal,user2@domain.com,USER,VIEWER
/mydocs/Documentation/Onboarding_Guide.xml,user2@domain.com,USER,CONTRIBUTOR
/mydocs/Documentation/Onboarding_Guide.xml,user1@domain.com,USER,CONTRIBUTOR
/mydocs/Projects/Initiative,user2@domain.com,USER,CONTRIBUTOR
/mydocs/Notes,user2@domain.com,USER,COOWNER
/mydocs/Notes,user1@domain.com,USER,COOWNER
/mydocs/Projects/Initiative/Structures.xml,user3@domain.com,USER,COOWNER
```

- Commentaires — L'exemple suivant montre le contenu d'un fichier CSV de commentaires classique.

```
PathToFile,PrincipalName,PostedTimestamp,Text
/mydocs/Documentation/
Onboarding_Guide.xml,user1@domain.com,2023-12-28T20:57:40.781Z,TEST ANNOTATION 1
/mydocs/Documentation/
Onboarding_Guide.xml,user2@domain.com,2023-12-28T22:18:09.812Z,TEST ANNOTATION 2
```

```
/mydocs/Documentation/
Onboarding_Guide.xml,user3@domain.com,2023-12-28T22:20:04.099Z,TEST ANNOTATION 3
/mydocs/Documentation/
Onboarding_Guide.xml,user1@domain.com,2023-12-28T20:56:27.390Z,TEST COMMENT 1
/mydocs/Documentation/
Onboarding_Guide.xml,user2@domain.com,2023-12-28T22:17:10.348Z,TEST COMMENT 2
/mydocs/Documentation/
Onboarding_Guide.xml,user3@domain.com,2023-12-28T22:19:42.821Z,TEST COMMENT 3
/mydocs/Projects/Agora/
Threat_Model.xml,user1@domain.com,2023-12-28T22:21:09.930Z,TEST ANNOTATION 4
/mydocs/Projects/Agora/
Threat_Model.xml,user1@domain.com,2023-12-28T20:57:04.931Z,TEST COMMENT 4
```

- Fichiers ignorés — L'exemple suivant montre le contenu d'un fichier CSV typique de fichiers ignorés. Nous avons raccourci l'identifiant et ignoré les valeurs de motif pour une meilleure lisibilité.

```
FileOwner,PathToFile,DocumentId,VersionId,SkippedReason
user1@domain.com,/mydocs/LargeFile1.mp4,45e433b5469...,170899345...,The file is too
 large. Please notify the document owner...
user2@domain.com,/mydocs/LargeFile2.pdf,e87f725898c1...,170899696...,The file is too
 large. Please notify the document owner...
```

Téléchargement de données migrées depuis Amazon S3

Comme la migration augmente les coûts liés à Amazon S3, vous pouvez télécharger les données migrées depuis Amazon S3 vers une autre solution de stockage. Cette rubrique explique comment télécharger vos données migrées et propose des suggestions pour le téléchargement de données vers une solution de stockage.

> **Note**
>
> Les étapes suivantes expliquent comment télécharger un fichier ou un dossier à la fois. Pour plus d'informations sur les autres méthodes de téléchargement de fichiers, consultez la section Téléchargement d'objets dans le guide de l'utilisateur Amazon S3.

Pour télécharger des données

1. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Sélectionnez le compartiment cible et accédez à l'alias du site.

3. Cochez la case à côté du dossier zippé.

   —OU—

   Ouvrez le dossier compressé et cochez la case à côté du fichier ou du dossier pour un utilisateur individuel.
4. Choisissez Téléchargement.

Suggestions de solutions de stockage

Pour les sites de grande taille, nous recommandons de configurer une EC2 instance à l'aide d'une Amazon Machine Image compatible basée sur Linux pour télécharger par programmation vos données depuis Amazon S3, les décompresser, puis les télécharger sur votre fournisseur de stockage ou sur votre disque local.

Résolution des problèmes de migration

Suivez les étapes ci-dessous pour vous assurer que vous avez correctement configuré votre environnement :

- Si une migration échoue, un message d'erreur apparaît dans l'onglet Historique des migrations de la WorkDocs console. Passez en revue le message d'erreur.
- Vérifiez les paramètres de votre compartiment Amazon S3.
- Réexécutez la migration.

Si le problème persiste, contactez AWS Support. Incluez l'URL du WorkDocs site et l'ID du job de migration, situés dans le tableau de l'historique des migrations.

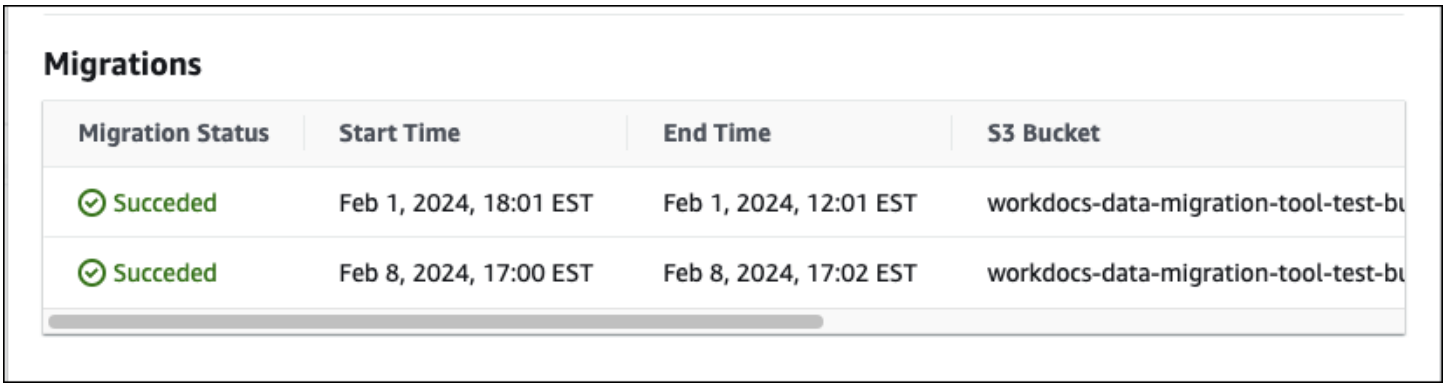
Consulter l'historique de vos migrations

Les étapes suivantes expliquent comment consulter l'historique de vos migrations.

Pour consulter votre historique

1. Ouvrez la WorkDocs console à l'adresse https://console.aws.amazon.com/zocalo/.
2. Sélectionnez le bouton radio situé à côté du WorkDocs site souhaité.
3. Ouvrez la liste des actions et choisissez Migrer les données.
4. Sur la page du nom du site Migrate Data, sélectionnez Migrations en cours et historique.

L'historique des migrations apparaît sous Migrations. L'image suivante montre un historique typique.



Conditions préalables pour Amazon WorkDocs

Pour configurer de nouveaux WorkDocs sites ou gérer des sites existants, vous devez effectuer les tâches suivantes.

Inscrivez-vous pour un Compte AWS

Si vous n'en avez pas Compte AWS, procédez comme suit pour en créer un.

Pour vous inscrire à un Compte AWS

1. Ouvrez l'https://portal.aws.amazon.com/billing/inscription.
2. Suivez les instructions en ligne.

   Une partie de la procédure d'inscription consiste à recevoir un appel téléphonique ou un message texte et à saisir un code de vérification sur le clavier du téléphone.

   Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l'utilisateur racine a accès à l'ensemble des Services AWS et des ressources de ce compte. La meilleure pratique de sécurité consiste à attribuer un accès administratif à un utilisateur, et à utiliser uniquement l'utilisateur racine pour effectuer les tâches nécessitant un accès utilisateur racine.

AWS vous envoie un e-mail de confirmation une fois le processus d'inscription terminé. À tout moment, vous pouvez consulter l'activité actuelle de votre compte et gérer votre compte en accédant à https://aws.amazon.com/et en choisissant Mon compte.

Création d'un utilisateur doté d'un accès administratif

Après vous être inscrit à un Compte AWS, sécurisez Utilisateur racine d'un compte AWS AWS IAM Identity Center, activez et créez un utilisateur administratif afin de ne pas utiliser l'utilisateur root pour les tâches quotidiennes.

Sécurisez votre Utilisateur racine d'un compte AWS

1. Connectez-vous en AWS Management Consoletant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.

Pour obtenir de l'aide pour vous connecter en utilisant l'utilisateur racine, consultez Connexion en tant qu'utilisateur racine dans le Guide de l'utilisateur Connexion à AWS .

2. Activez l'authentification multifactorielle (MFA) pour votre utilisateur racine.

   Pour obtenir des instructions, voir Activer un périphérique MFA virtuel pour votre utilisateur Compte AWS root (console) dans le guide de l'utilisateur IAM.

Création d'un utilisateur doté d'un accès administratif

1. Activez IAM Identity Center.

   Pour obtenir des instructions, consultez Activation d' AWS IAM Identity Center dans le Guide de l'utilisateur AWS IAM Identity Center .

2. Dans IAM Identity Center, octroyez un accès administratif à un utilisateur.

   Pour un didacticiel sur l'utilisation du Répertoire IAM Identity Center comme source d'identité, voir Configurer l'accès utilisateur par défaut Répertoire IAM Identity Center dans le Guide de AWS IAM Identity Center l'utilisateur.

Connexion en tant qu'utilisateur doté d'un accès administratif

- Pour vous connecter avec votre utilisateur IAM Identity Center, utilisez l'URL de connexion qui a été envoyée à votre adresse e-mail lorsque vous avez créé l'utilisateur IAM Identity Center.

  Pour obtenir de l'aide pour vous connecter en utilisant un utilisateur d'IAM Identity Center, consultez la section Connexion au portail AWS d'accès dans le guide de l'Connexion à AWS utilisateur.

Attribution d'un accès à d'autres utilisateurs

1. Dans IAM Identity Center, créez un ensemble d'autorisations qui respecte la bonne pratique consistant à appliquer les autorisations de moindre privilège.

   Pour obtenir des instructions, consultez Création d'un ensemble d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .

2. Attribuez des utilisateurs à un groupe, puis attribuez un accès par authentification unique au groupe.

Pour obtenir des instructions, consultez Ajout de groupes dans le Guide de l'utilisateur AWS IAM Identity Center .

Sécurité sur Amazon WorkDocs

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cette notion par les termes sécurité du cloud et sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de conformitéAWS. Pour en savoir plus sur les programmes de conformité applicables à Amazon WorkDocs, consultez la section AWS Services concernés par programme de conformité.
- Sécurité dans le cloud : le AWS service que vous utilisez détermine votre responsabilité. Vous êtes également responsable d'autres facteurs, y compris la sensibilité de vos données, les exigences de votre entreprise, et la législation et la réglementation applicables. Les rubriques de cette section vous aident à comprendre comment appliquer le modèle de responsabilité partagée lors de son utilisation WorkDocs.

> **Note**
>
> Les utilisateurs d'une WorkDocs organisation peuvent collaborer avec des utilisateurs extérieurs à cette organisation en envoyant un lien ou une invitation vers un fichier. Toutefois, cela ne s'applique qu'aux sites qui utilisent un connecteur Active Directory. Consultez les paramètres des liens partagés de votre site et sélectionnez l'option qui répond le mieux aux exigences de votre entreprise.

Les rubriques suivantes expliquent comment procéder à la configuration WorkDocs pour atteindre vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos WorkDocs ressources.

Rubriques

- Gestion des identités et des accès pour Amazon WorkDocs

- Journalisation et surveillance sur Amazon WorkDocs
- Validation de conformité pour Amazon WorkDocs
- Résilience chez Amazon WorkDocs
- Sécurité de l'infrastructure sur Amazon WorkDocs

Gestion des identités et des accès pour Amazon WorkDocs

AWS Identity and Access Management (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser WorkDocs les ressources. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez. WorkDocs

Utilisateur du service : si vous utilisez le WorkDocs service pour effectuer votre travail, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Au fur et à mesure que vous utilisez de nouvelles WorkDocs fonctionnalités pour effectuer votre travail, vous aurez peut-être besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne pouvez pas accéder à une fonctionnalité dans WorkDocs, consultez Résolution des problèmes liés à WorkDocs l'identité et à l'accès à Amazon.

Administrateur du service — Si vous êtes responsable des WorkDocs ressources de votre entreprise, vous avez probablement un accès complet à WorkDocs. C'est à vous de déterminer les WorkDocs

fonctionnalités et les ressources auxquelles les utilisateurs de votre service doivent accéder. Vous devez ensuite soumettre les demandes à votre administrateur IAM pour modifier les autorisations des utilisateurs de votre service. Consultez les informations sur cette page pour comprendre les concepts de base d'IAM. Pour en savoir plus sur la manière dont votre entreprise peut utiliser IAM avec WorkDocs, voirComment Amazon WorkDocs travaille avec IAM.

Administrateur IAM – Si vous êtes un administrateur IAM, vous souhaiterez peut-être en savoir plus sur la façon d'écrire des politiques pour gérer l'accès à WorkDocs. Pour consulter des exemples de politiques WorkDocs basées sur l'identité que vous pouvez utiliser dans IAM, consultez. Exemples de politiques WorkDocs basées sur l'identité d'Amazon

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié (connecté à AWS) en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en AWS tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAM Identity Center), l'authentification unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez avec une identité fédérée, votre administrateur aura précédemment configuré une fédération d'identités avec des rôles IAM. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez la section Comment vous connecter à votre compte Compte AWS dans le guide de Connexion à AWS l'utilisateur.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer des demandes vous-même, consultez AWS Signature Version 4 pour les demandes d'API dans le Guide de l'utilisateur IAM.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser

l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour plus d'informations, consultez Authentification multifactorielle dans le Guide de l'utilisateur AWS IAM Identity Center et Authentification multifactorielle AWS dans IAM dans le Guide de l'utilisateur IAM.

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des utilisateurs IAM ayant des informations d'identification à long terme telles que des mots de passe et des clés d'accès. Toutefois, si certains cas d'utilisation spécifiques nécessitent des informations d'identification à long terme avec les utilisateurs IAM, nous vous recommandons d'effectuer une rotation des clés d'accès. Pour plus d'informations, consultez Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification dans le Guide de l'utilisateur IAM.

Un groupe IAM est une identité qui concerne un ensemble d'utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez nommer un groupe IAMAdminset lui donner les autorisations nécessaires pour administrer les ressources IAM.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour plus d'informations, consultez Cas d'utilisation pour les utilisateurs IAM dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité au sein de vous Compte AWS dotée d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Pour assumer temporairement un rôle IAM dans le AWS Management Console, vous pouvez passer d'un rôle d'utilisateur à un rôle IAM (console). Vous pouvez assumer un rôle en appelant une opération d' AWS API AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez Méthodes pour endosser un rôle dans le Guide de l'utilisateur IAM.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Accès utilisateur fédéré : pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour obtenir des informations sur les rôles pour la fédération, consultez Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les jeux d'autorisations, consultez Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .
- Autorisations d'utilisateur IAM temporaires : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.
- Accès intercompte : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains Services AWS cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour en savoir plus sur la différence entre les rôles et les politiques basées sur les ressources pour l'accès intercompte, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.
- Accès multiservices — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.
  - Sessions d'accès direct (FAS) : lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez Transmission des sessions d'accès.
  - Rôle de service : il s'agit d'un rôle IAM attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer un rôle de service à partir d'IAM.

Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.

- Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS fichier et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une EC2 instance et qui envoient des demandes AWS CLI d' AWS API. Cela est préférable au stockage des clés d'accès dans l' EC2 instance. Pour attribuer un AWS rôle à une EC2 instance et le rendre disponible pour toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes exécutés sur l' EC2 instance d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utiliser un rôle IAM pour accorder des autorisations aux applications exécutées sur des EC2 instances Amazon dans le guide de l'utilisateur IAM.

Gestion des accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations sur la structure et le contenu des documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Les politiques IAM définissent les autorisations d'une action, quelle que soit la méthode que vous utilisez pour exécuter l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle à partir de AWS Management Console AWS CLI, de ou de l' AWS API.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Définition d'autorisations IAM personnalisées avec des politiques gérées par le client dans le Guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les politiques AWS gérées et les politiques gérées par le client. Pour découvrir comment choisir entre une politique gérée et une politique en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

Politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Listes de contrôle d'accès (ACL)

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLs sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3 et AWS WAF Amazon VPC sont des exemples de services compatibles. ACLs Pour en savoir plus ACLs, consultez la présentation de la liste de contrôle d'accès (ACL) dans le guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- Limite d'autorisations : une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le nombre maximal d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM (utilisateur ou rôle IAM). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.
- Politiques de contrôle des services (SCPs) : SCPs politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans AWS Organizations. AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer des politiques de contrôle des services (SCPs) à l'un ou à l'ensemble de vos comptes. Le SCP limite les autorisations pour les entités figurant dans les comptes des membres, y compris chacune Utilisateur racine d'un compte AWS d'entre elles. Pour plus d'informations sur les Organizations SCPs, voir Politiques de contrôle des services dans le Guide de AWS Organizations l'utilisateur.
- Politiques de contrôle des ressources (RCPs) : RCPs politiques JSON que vous pouvez utiliser pour définir le maximum d'autorisations disponibles pour les ressources de vos comptes sans mettre à jour les politiques IAM associées à chaque ressource que vous possédez. Le RCP limite les autorisations pour les ressources des comptes membres et peut avoir un impact sur les

autorisations effectives pour les identités, y compris Utilisateur racine d'un compte AWS, qu'elles appartiennent ou non à votre organisation. Pour plus d'informations sur les Organizations RCPs, y compris une liste de ces Services AWS supports RCPs, consultez la section Resource control policies (RCPs) dans le guide de AWS Organizations l'utilisateur.

- Politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez Politiques de session dans le Guide de l'utilisateur IAM.

> **Note**
>
> WorkDocs ne prend pas en charge les politiques de contrôle des services pour Slack Organizations.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de l'utilisateur IAM.

Comment Amazon WorkDocs travaille avec IAM

Avant d'utiliser IAM pour gérer l'accès à WorkDocs, vous devez connaître les fonctionnalités IAM disponibles. WorkDocs Pour obtenir une vue d'ensemble de la façon dont WorkDocs les autres AWS services fonctionnent avec IAM, consultez la section AWS Services compatibles avec IAM dans le Guide de l'utilisateur d'IAM.

Rubriques

- WorkDocsPolitiques basées sur l'identité
- WorkDocsPolitiques basées sur les ressources
- Autorisation basée sur les balises WorkDocs

- WorkDocs Rôles IAM

WorkDocsPolitiques basées sur l'identité

Avec les politiques basées sur l'identité IAM, vous pouvez spécifier des actions autorisées ou refusées. WorkDocs soutient des actions spécifiques. Pour en savoir plus sur les éléments que vous utilisez dans une politique JSON, veuillez consulter Références des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

Actions

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Les actions de stratégie portent généralement le même nom que l'opération AWS d'API associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une politique afin d'accorder l'autorisation d'exécuter les opérations associées.

Les actions de politique en WorkDocs cours utilisent le préfixe suivant avant l'action :`workdocs:`. Par exemple, pour autoriser quelqu'un à exécuter l'opération WorkDocs `DescribeUsers` d'API, vous devez inclure l'`workdocs:DescribeUsers`action dans sa politique. Les déclarations de politique doivent inclure un élément `Action` ou `NotAction`. WorkDocs définit son propre ensemble d'actions qui décrivent les tâches que vous pouvez effectuer avec ce service.

Pour spécifier plusieurs actions dans une seule déclaration, séparez-les par des virgules comme suit :

```
"Action": [
      "workdocs:DescribeUsers",
      "workdocs:CreateUser"
```

Vous pouvez aussi spécifier plusieurs actions à l'aide de caractères génériques (*). Par exemple, pour spécifier toutes les actions qui commencent par le mot `Describe`, incluez l'action suivante :

```
"Action": "workdocs:Describe*"
```

> **Note**
>
> Pour garantir la rétrocompatibilité, incluez l'`zocalo`action. Par exemple :
>
> ```
> "Action": [
> "zocalo:*",
> "workdocs:*"
> ],
> ```

Pour consulter la liste des WorkDocs actions, reportez-vous à la section Actions définies par WorkDocs dans le guide de l'utilisateur IAM.

Ressources

WorkDocs ne prend pas en charge la spécification de ressources ARNs dans une politique.

Clés de condition

WorkDocs ne fournit aucune clé de condition spécifique au service, mais il prend en charge l'utilisation de certaines clés de condition globales. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

Exemples

Pour consulter des exemples de politiques WorkDocs basées sur l'identité, consultez. Exemples de politiques WorkDocs basées sur l'identité d'Amazon

WorkDocsPolitiques basées sur les ressources

WorkDocs ne prend pas en charge les politiques basées sur les ressources.

Autorisation basée sur les balises WorkDocs

WorkDocs ne prend pas en charge le balisage des ressources ni le contrôle de l'accès en fonction des balises.

WorkDocs Rôles IAM

Un rôle IAM est une entité de votre AWS compte qui dispose d'autorisations spécifiques.

Utilisation d'informations d'identification temporaires avec WorkDocs

Nous vous recommandons vivement d'utiliser des informations d'identification temporaires pour vous connecter à la fédération, assumer un rôle IAM ou assumer un rôle multicompte. Vous obtenez des informations d'identification de sécurité temporaires en appelant des opérations d' AWS STS API telles que AssumeRoleou GetFederationToken.

WorkDocs prend en charge l'utilisation d'informations d'identification temporaires.

Rôles liés à un service

Les rôles liés aux AWS services permettent aux services d'accéder aux ressources d'autres services pour effectuer une action en votre nom. Les rôles liés à un service s'affichent dans votre compte IAM et sont la propriété du service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

WorkDocs ne prend pas en charge les rôles liés à un service.

Rôles de service

Cette fonction permet à un service d'endosser une fonction du service en votre nom. Ce rôle autorise le service à accéder à des ressources d'autres services pour effectuer une action en votre nom. Les rôles de service s'affichent dans votre compte IAM et sont la propriété du compte. Cela signifie qu'un administrateur IAM peut modifier les autorisations associées à ce rôle. Toutefois, une telle action peut perturber le bon fonctionnement du service.

WorkDocs ne prend pas en charge les rôles de service.

Exemples de politiques WorkDocs basées sur l'identité d'Amazon

> **Note**
>
> Pour plus de sécurité, créez des utilisateurs fédérés plutôt que des utilisateurs IAM dans la mesure du possible.

Par défaut, les utilisateurs et les rôles IAM ne sont pas autorisés à créer ou modifier les ressources WorkDocs . Ils ne peuvent pas non plus effectuer de tâches à l'aide de l' AWS API AWS Management

Console AWS CLI, ou. Un administrateur IAM doit créer des politiques IAM autorisant les utilisateurs et les rôles à exécuter des opérations d'API spécifiques sur les ressources spécifiées dont ils ont besoin. Il doit ensuite attacher ces politiques aux utilisateurs ou aux groupes IAM ayant besoin de ces autorisations.

> **Note**
>
> Pour garantir la rétrocompatibilité, incluez `zocalo` cette action dans vos politiques. Par exemple :
>
> ```
> {
>     "Version": "2012-10-17",
>     "Statement": [
>         {
>             "Sid": "VisualEditor0",
>             "Effect": "Deny",
>             "Action": [
>             "zocalo:*",
>             "workdocs:*"
>             ],
>             "Resource": "*"
>         }
>     ]
> }
> ```

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, veuillez consulter Création de politiques dans l'onglet JSON dans le Guide de l'utilisateur IAM.

Rubriques

- Bonnes pratiques en matière de politiques
- Utilisation de la console WorkDocs
- Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations
- Autoriser les utilisateurs à accéder aux ressources en lecture seule WorkDocs
- Autres exemples de WorkDocs politiques basées sur l'identité

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer WorkDocs des ressources dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.
- Accordez les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation d'IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utilisez des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez l'Analyseur d'accès IAM pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : l'Analyseur d'accès IAM valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez Validation de politiques avec IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue.

Compte AWS Pour exiger la MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Sécurisation de l'accès aux API avec MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Utilisation de la console WorkDocs

Pour accéder à la WorkDocs console Amazon, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et de consulter les détails des WorkDocs ressources de votre AWS compte. Si vous créez une politique basée sur l'identité qui est plus restrictive que les autorisations minimales requises, la console ne fonctionnera pas comme prévu pour les utilisateurs ou les entités de rôle IAM.

Pour garantir que ces entités peuvent utiliser la WorkDocs console, associez également les politiques AWS gérées suivantes aux entités. Pour plus d'informations sur l'attachement de politiques, consultez la section Ajouter des autorisations à un utilisateur dans le guide de l'utilisateur IAM.

- AmazonWorkDocsFullAccess
- AWSDirectoryServiceFullAccess
- AmazonEC2FullAccess

Ces politiques accordent à l'utilisateur un accès complet aux WorkDocs ressources, aux opérations du AWS Directory Service et aux EC2 opérations Amazon dont Amazon WorkDocs a besoin pour fonctionner correctement.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API que vous tentez d'effectuer.

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM d'afficher les politiques en ligne et gérées attachées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide de l'API AWS CLI or AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Autoriser les utilisateurs à accéder aux ressources en lecture seule WorkDocs

La AmazonWorkDocsReadOnlyAccesspolitique AWS gérée suivante accorde à un utilisateur IAM un accès en lecture seule aux ressources. WorkDocs La politique permet à l'utilisateur d'accéder à toutes les WorkDocs `Describe` opérations. L'accès aux deux EC2 opérations Amazon est nécessaire pour WorkDocs obtenir une liste de vos sous-réseaux VPCs et de vos sous-réseaux. L'accès à l' Directory Service `DescribeDirectories`opération est nécessaire pour obtenir des informations sur vos Directory Service annuaires.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "workdocs:Describe*",
                "ds:DescribeDirectories",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets"
            ],
            "Resource": "*"
        }
    ]
}
```

Autres exemples de WorkDocs politiques basées sur l'identité

Les administrateurs IAM peuvent créer des politiques supplémentaires pour autoriser un rôle ou un utilisateur IAM à accéder à l' WorkDocs API. Pour plus d'informations, consultez Authentification et contrôle d'accès pour les applications administratives dans le Manuel du développeur WorkDocs .

Résolution des problèmes liés à WorkDocs l'identité et à l'accès à Amazon

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec WorkDocs IAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action dans WorkDocs
- Je ne suis pas autorisé à effectuer iam : PassRole
- Je souhaite autoriser des personnes extérieures à mon AWS compte à accéder à mes WorkDocs ressources

Je ne suis pas autorisé à effectuer une action dans WorkDocs

S'il vous AWS Management Console indique que vous n'êtes pas autorisé à effectuer une action, vous devez contacter votre administrateur pour obtenir de l'aide. Votre administrateur est la personne qui vous a fourni votre nom d'utilisateur et votre mot de passe.

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez une erreur selon laquelle vous n'êtes pas autorisé à exécuter `iam:PassRole` l'action, vos stratégies doivent être mises à jour afin de vous permettre de transmettre un rôle à WorkDocs.

Certains vous Services AWS permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour exécuter une action dans WorkDocs. Toutefois, l'action nécessite que le service ait des autorisations accordées par une fonction de service. Mary ne dispose pas des autorisations nécessaires pour transférer le rôle au service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite autoriser des personnes extérieures à mon AWS compte à accéder à mes WorkDocs ressources

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACLs), vous pouvez utiliser ces politiques pour autoriser les utilisateurs à accéder à vos ressources.

Pour plus d'informations, consultez les éléments suivants :

- Pour savoir si ces fonctionnalités sont prises WorkDocs en charge, consultezComment Amazon WorkDocs travaille avec IAM.
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.

- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.
- Pour en savoir plus sur la différence entre l'utilisation des rôles et des politiques basées sur les ressources pour l'accès intercompte, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Journalisation et surveillance sur Amazon WorkDocs

Les administrateurs WorkDocs du site Amazon peuvent consulter et exporter le flux d'activité d'un site entier. Ils peuvent également être utilisés AWS CloudTrail pour capturer des événements depuis la WorkDocs console.

Rubriques

- Exportation du flux d'activité à l'échelle du site
- Utilisation AWS CloudTrail pour enregistrer les appels WorkDocs d'API Amazon

Exportation du flux d'activité à l'échelle du site

Les administrateurs peuvent afficher et exporter le flux d'activités de l'ensemble du site. Pour utiliser cette fonctionnalité, vous devez d'abord installer WorkDocs Companion. Pour installer WorkDocs Companion, consultez la section Applications et intégrations pour WorkDocs.

Pour afficher et exporter le flux d'activités de l'ensemble du site

1. Dans l'application Web, sélectionnez Activité.
2. Choisissez Filtrer, puis déplacez le curseur d'activité à l'échelle du site pour activer le filtre.
3. Sélectionnez les filtres Activity Type (Type d'activité) et choisissez Date Modified (Date modifiée) si nécessaire, puis choisissez Apply (Appliquer).
4. Lorsque les résultats du flux d'activités filtré s'affichent, recherchez par fichier, dossier ou nom d'utilisateur pour affiner vos résultats. Vous pouvez également ajouter ou supprimer des filtres si nécessaire.

5. Choisissez Export (Exporter) pour exporter le flux d'activités vers les fichiers `.csv` et `.json` de votre bureau. Le système exporte les fichiers vers l'un des emplacements suivants :

   - Windows : WorkDocsDownloadsdossier dans le dossier Téléchargements de votre PC
   - macOS : `/users/`**`username`**`/WorkDocsDownloads/folder`

   Le fichier exporté reflète tous les filtres que vous appliquez.

   > **Note**
   >
   > Les utilisateurs qui ne sont pas des administrateurs peuvent afficher et exporter le flux d'activités de leur seul contenu. Pour plus d'informations, consultez la section Affichage du flux d'activité dans le guide de WorkDocs l'utilisateur Amazon.

Utilisation AWS CloudTrail pour enregistrer les appels WorkDocs d'API Amazon

Vous pouvez utiliser AWS CloudTrail ; pour enregistrer les appels WorkDocs d'API Amazon. CloudTrail fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans WorkDocs. CloudTrail capture tous les appels d'API WorkDocs sous forme d'événements, y compris les appels depuis la WorkDocs console et les appels de code vers le WorkDocs APIs.

Si vous créez un suivi, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris les événements pour WorkDocs. Si vous ne créez pas de trace, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements.

Les informations collectées par CloudTrail incluent les demandes, les adresses IP à partir desquelles les demandes ont été effectuées, les utilisateurs qui ont fait les demandes et les dates des demandes.

Pour plus d'informations CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

WorkDocs informations dans CloudTrail

CloudTrail est activé sur votre AWS compte lorsque vous le créez. Lorsqu'une activité se produit dans WorkDocs, cette activité est enregistrée dans un CloudTrail événement avec d'autres

événements de AWS service dans l'historique des événements. Vous pouvez consulter, rechercher et télécharger les événements récents dans votre AWS compte. Pour plus d'informations, consultez la section Affichage des événements avec l'historique des CloudTrail événements.

Pour un enregistrement continu des événements de votre AWS compte, y compris des événements pour WorkDocs, créez un parcours. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un journal d'activité dans la console, il s'applique à toutes les régions. Le journal enregistre les événements de toutes les régions de la AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez :

- Présentation de la création d'un journal d'activité
- CloudTrail services et intégrations pris en charge
- Configuration des notifications Amazon SNS pour CloudTrail
- Réception de fichiers CloudTrail journaux de plusieurs régions et réception de fichiers CloudTrail journaux de plusieurs comptes

Toutes les WorkDocs actions sont enregistrées CloudTrail et documentées dans le Amazon WorkDocs API Reference. Par exemple, les appels aux `UpdateDocument` sections`CreateFolder`, `DeactivateUser` et génèrent des entrées dans les fichiers CloudTrail journaux.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été effectuée avec des informations d'identification d'utilisateur root ou IAM.
- Si la demande a été effectuée avec des informations d'identification de sécurité temporaires pour un rôle ou un utilisateur fédéré.
- Si la demande a été faite par un autre AWS service.

Pour de plus amples informations, veuillez consulter l'élément userIdentity CloudTrail .

Comprendre les entrées du fichier WorkDocs journal

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux

contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

WorkDocs génère différents types d' CloudTrail entrées, celles du plan de contrôle et celles du plan de données. La différence importante entre les deux est que l'identité de l'utilisateur pour les entrées du plan de contrôle est un utilisateur IAM. L'identité de l'utilisateur pour les entrées du plan de données est l'utilisateur du WorkDocs répertoire.

> **Note**
>
> Pour plus de sécurité, créez des utilisateurs fédérés plutôt que des utilisateurs IAM dans la mesure du possible.

Les informations sensibles, telles que les mots de passe, les jetons d'authentification, les commentaires sur les fichiers et le contenu des fichiers, sont consignées dans les entrées de journal. Ils apparaissent sous la forme HIDDEN_DUE_TO_SECURITY_REASONS dans les journaux. CloudTrail Ils apparaissent sous la forme HIDDEN_DUE_TO_SECURITY_REASONS dans les journaux. CloudTrail

L'exemple suivant montre deux entrées de CloudTrail journal pour WorkDocs : le premier enregistrement concerne une action du plan de contrôle et le second une action du plan de données.

```
{
  Records : [
    {
      "eventVersion" : "1.01",
      "userIdentity" :
      {
        "type" : "IAMUser",
        "principalId" : "user_id",
        "arn" : "user_arn",
        "accountId" : "account_id",
        "accessKeyId" : "access_key_id",
        "userName" : "user_name"
      },
      "eventTime" : "event_time",
      "eventSource" : "workdocs.amazonaws.com",
```

```
      "eventName" : "RemoveUserFromGroup",
      "awsRegion" : "region",
      "sourceIPAddress" : "ip_address",
      "userAgent" : "user_agent",
      "requestParameters" :
      {
        "directoryId" : "directory_id",
        "userSid" : "user_sid",
        "group" : "group"
      },
      "responseElements" : null,
      "requestID" : "request_id",
      "eventID" : "event_id"
    },
    {
      "eventVersion" : "1.01",
      "userIdentity" :
      {
        "type" : "Unknown",
        "principalId" : "user_id",
        "accountId" : "account_id",
        "userName" : "user_name"
      },
      "eventTime" : "event_time",
      "eventSource" : "workdocs.amazonaws.com",
      "awsRegion" : "region",
      "sourceIPAddress" : "ip_address",
      "userAgent" : "user_agent",
      "requestParameters" :
      {
        "AuthenticationToken" : "**-redacted-**"
      },
      "responseElements" : null,
      "requestID" : "request_id",
      "eventID" : "event_id"
    }
  ]
}
```

Validation de conformité pour Amazon WorkDocs

Pour savoir si un programme Services AWS de conformité Service AWS s'inscrit dans le champ d'application de programmes de conformité spécifiques, consultez Services AWS la section de

conformité et sélectionnez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de AWS conformité Programmes AWS de .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir Téléchargement de rapports dans AWS Artifact .

Votre responsabilité en matière de conformité lors de l'utilisation Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Conformité et gouvernance de la sécurité : ces guides de mise en œuvre de solutions traitent des considérations architecturales et fournissent les étapes à suivre afin de déployer des fonctionnalités de sécurité et de conformité.
- Référence des services éligibles HIPAA : liste les services éligibles HIPAA. Tous ne Services AWS sont pas éligibles à la loi HIPAA.
- AWS Ressources de https://aws.amazon.com/compliance/resources/ de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- AWS Guides de conformité destinés aux clients — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière de sécurisation Services AWS et décrivent les directives relatives aux contrôles de sécurité dans de nombreux cadres (notamment le National Institute of Standards and Technology (NIST), le Payment Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).
- Évaluation des ressources à l'aide des règles du guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub CSPM— Cela Service AWS fournit une vue complète de votre état de sécurité interne AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez Référence des contrôles Security Hub.
- Amazon GuardDuty — Cela Service AWS détecte les menaces potentielles qui pèsent sur vos charges de travail Comptes AWS, vos conteneurs et vos données en surveillant votre environnement pour détecter toute activité suspecte et malveillante. GuardDuty peut vous aider à répondre à diverses exigences de conformité, telles que la norme PCI DSS, en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.

- AWS Audit Manager— Cela vous Service AWS permet d'auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Résilience chez Amazon WorkDocs

L'infrastructure AWS mondiale est construite autour des AWS régions et des zones de disponibilité. AWS Les régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées par un réseau à faible latence, à haut débit et hautement redondant. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone de disponibilité à l'autre sans interruption. Les zones de disponibilité sont plus hautement disponibles, tolérantes aux pannes et évolutives que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur AWS les régions et les zones de disponibilité, consultez la section Infrastructure AWS mondiale.

Sécurité de l'infrastructure sur Amazon WorkDocs

En tant que service géré, Amazon WorkDocs est protégé par les procédures de sécurité du réseau AWS mondial. Pour plus d'informations, consultez la section Sécurité de l'infrastructure dans AWS Identity and Access Management dans le guide de l'utilisateur IAM et les meilleures pratiques en matière de sécurité, d'identité et de conformité dans le centre AWS d'architecture.

Vous utilisez des appels d'API AWS publiés pour accéder WorkDocs via le réseau. Les clients doivent prendre en charge le protocole TLS (Transport Layer Security) 1.2, et nous recommandons d'utiliser le protocole TLS 1.3. Les clients doivent également prendre en charge les suites de chiffrement parfaitement confidentielles, telles que Ephemeral Diffie-Hellman ou Elliptic Curve Ephemeral Diffie-Hellman. La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Commencer avec WorkDocs

WorkDocs utilise un répertoire pour stocker et gérer les informations d'organisation relatives à vos utilisateurs et à leurs documents. À son tour, vous attachez un répertoire à un site lorsque vous approvisionnez ce site. Lorsque vous le faites, une WorkDocs fonctionnalité appelée Activation automatique ajoute les utilisateurs du répertoire au site en tant qu'utilisateurs gérés, ce qui signifie qu'ils n'ont pas besoin d'informations d'identification distinctes pour se connecter à votre site et qu'ils peuvent partager des fichiers et collaborer sur ceux-ci. Chaque utilisateur dispose de 1 To de stockage, sauf s'il en achète davantage.

Vous n'avez plus besoin d'ajouter et d'activer des utilisateurs manuellement, mais vous pouvez toujours le faire. Vous pouvez également modifier les rôles et les autorisations des utilisateurs chaque fois que vous en avez besoin. Pour plus d'informations à ce sujetInviter et gérer WorkDocs les utilisateurs, reportez-vous à la section suivante de ce guide.

Si vous devez créer des répertoires, vous pouvez :

- Créer un annuaire Simple AD.
- Créez un répertoire AD Connector pour vous connecter à votre annuaire local.
- Activez WorkDocs cette option pour travailler avec un AWS répertoire existant.
- J'ai WorkDocs créé un répertoire pour vous.

Vous pouvez également créer une relation de confiance entre votre annuaire AD et un AWS Managed Microsoft AD annuaire.

> **Note**
>
> Si vous adhérez à un programme de conformité tel que PCI, FedRAMP ou DoD, vous devez créer AWS Managed Microsoft AD un annuaire pour répondre aux exigences de conformité. Les étapes décrites dans cette section expliquent comment utiliser un annuaire Microsoft AD existant. Pour plus d'informations sur la création d'un annuaire Microsoft AD, consultez AWS Managed Microsoft AD dans le Guide d'administration du AWS Directory Service.

Table des matières

- Activation de l'authentification unique
- Activation de l'authentification multi-facteurs
- Promotion d'un utilisateur en tant qu'administrateur

Création d'un WorkDocs site

Les étapes décrites dans les sections suivantes expliquent comment configurer un nouveau WorkDocs site.

Tâches

- Avant de commencer
- Création d'un WorkDocs site

Avant de commencer

Vous devez disposer des éléments suivants avant de créer un WorkDocs site.

- Un AWS compte pour créer et administrer WorkDocs des sites. Toutefois, les utilisateurs n'ont pas besoin d'un AWS compte pour se connecter et utiliser WorkDocs. Pour de plus amples informations, veuillez consulter Conditions préalables pour Amazon WorkDocs.
- Si vous envisagez d'utiliser Simple AD, vous devez remplir les conditions requises définies dans la section Prérequis de Simple AD du Guide d'AWS Directory Service administration.
- Un AWS Managed Microsoft AD annuaire si vous appartenez à un programme de conformité tel que PCI, FedRAMP ou DoD. Les étapes décrites dans cette section expliquent comment utiliser un annuaire Microsoft AD existant. Pour plus d'informations sur la création d'un annuaire Microsoft AD, consultez AWS Managed Microsoft AD dans le Guide d'administration du AWS Directory Service.
- Informations de profil pour l'administrateur, y compris le prénom et le nom de famille, ainsi qu'une adresse e-mail.

Création d'un WorkDocs site

Suivez ces étapes pour créer un WorkDocs site en quelques minutes.

Pour créer le WorkDocs site

1. Ouvrez la WorkDocs console à l'adresse https://console.aws.amazon.com/zocalo/.

2. Sur la page d'accueil de la console, sous Créer un WorkDocs site, choisissez Commencer maintenant.

   —OU—

   Dans le volet de navigation, choisissez Mes sites, puis sur la page Gérer vos WorkDocs sites, choisissez Créer un WorkDocs site.

   Ce qui se passe ensuite dépend de la présence ou non d'un répertoire.

   - Si vous avez un répertoire, la page Sélectionner un répertoire apparaît et vous permet de choisir un répertoire existant ou d'en créer un.
   - Si vous n'avez pas d'annuaire, la page Configurer un type d'annuaire apparaît et vous permet de créer un annuaire Simple AD ou AD Connector

   Les étapes suivantes expliquent comment effectuer les deux tâches.

   Pour utiliser un répertoire existant

   1. Ouvrez la liste des répertoires disponibles et choisissez le répertoire que vous souhaitez utiliser.
   2. Choisissez Enable directory.

   Pour créer un annuaire

   1. Répétez les étapes 1 et 2 ci-dessus.

      À ce stade, la procédure à suivre varie selon que vous souhaitez utiliser Simple AD ou créer un AD Connector.

      Pour utiliser Simple AD

      a. Choisissez Simple AD, puis Next.

         La page Créer un site Simple AD s'affiche.

      b. Sous Point d'accès, dans le champ URL du site, entrez l'URL du site.

c. Sous Définir un WorkDocs administrateur, entrez l'adresse e-mail, le prénom et le nom de famille de l'administrateur.

d. Si nécessaire, complétez les options sous Détails du répertoire et Configuration du VPC.

e. Choisissez Créer un site Simple AD.

Pour créer un répertoire AD Connector

a. Choisissez AD Connector, puis Next.

La page du site Create AD Connector s'affiche.

b. Remplissez tous les champs sous Détails du répertoire.

c. Sous Point d'accès, dans le champ URL du site, entrez l'URL de votre site.

d. Si vous le souhaitez, complétez les champs facultatifs sous Configuration VPC.

e. Choisissez Create AD Connector site.

WorkDocs effectue les opérations suivantes :

- Si vous avez choisi Configurer un VPC en mon nom à l'étape 4 ci-dessus, WorkDocs créez un VPC pour vous. Un répertoire du VPC stocke les informations relatives à l'utilisateur et au WorkDocs site.
- Si vous avez utilisé Simple AD, WorkDocs crée un utilisateur de répertoire et définit cet utilisateur en tant qu' WorkDocsadministrateur. Si vous avez créé un annuaire AD Connector, WorkDocs définit l'utilisateur de l'annuaire existant que vous avez indiqué en tant qu' WorkDocs administrateur.
- Si vous avez utilisé un répertoire existant, vous WorkDocs invite à saisir le nom d'utilisateur de l' WorkDocs administrateur. L'utilisateur doit être membre de l'annuaire.

> **Note**
>
> WorkDocs n'informe pas les utilisateurs du nouveau site. Vous devez leur communiquer l'URL et leur faire savoir qu'ils n'ont pas besoin d'un identifiant distinct pour utiliser le site.

Activation de l'authentification unique

AWS Directory Service permet aux utilisateurs d'accéder à Amazon à WorkDocs partir d'un ordinateur connecté au même répertoire que celui dans lequel ils WorkDocs sont enregistrés, sans avoir à saisir leurs informations d'identification séparément. WorkDocs les administrateurs peuvent activer l'authentification unique à l'aide de la Directory Service console. Pour plus d'informations, consultez la section Authentification unique dans le Guide AWS Directory Service d'administration.

Une fois que l' WorkDocs administrateur a activé l'authentification unique, les utilisateurs du WorkDocs site peuvent également avoir besoin de modifier les paramètres de leur navigateur Web pour autoriser l'authentification unique. Pour plus d'informations, consultez les sections Authentification unique pour IE et Chrome et Authentification unique pour Firefox dans le Guide d'AWS Directory Service administration.

Activation de l'authentification multi-facteurs

Vous utilisez la console des services d' AWS annuaire à l'adresse https://console.aws.amazon.com/directoryservicev2/pour activer l'authentification multifactorielle pour votre annuaire AD Connector. Pour activer l'authentification MFA, vous devez posséder une solution MFA qui est un serveur Remote authentication dial-in user service (RADIUS), ou disposer d'un plugin sur un serveur RADIUS déjà installé dans votre infrastructure sur site. Votre solution d'authentification MFA doit utiliser des codes secrets uniques que les utilisateurs obtiennent à partir d'un périphérique physique ou d'un logiciel exécuté sur un périphérique, par exemple un téléphone portable.

RADIUS est un client/server protocole standard qui assure l'authentification, l'autorisation et la gestion de la comptabilité afin de permettre aux utilisateurs de se connecter aux services réseau. AWS Managed Microsoft AD inclut un client RADIUS qui se connecte au serveur RADIUS sur lequel vous avez implémenté votre solution MFA. Votre serveur RADIUS valide le nom d'utilisateur et le code secret unique. Si votre serveur RADIUS valide correctement l'utilisateur, AWS Managed Microsoft AD authentifie ensuite l'utilisateur auprès d'AD. Une fois l'authentification AD réussie, les utilisateurs peuvent alors accéder à l'application AWS. La communication entre le client Microsoft AD RADIUS géré par AWS et votre serveur RADIUS nécessite que vous configuriez des groupes de sécurité AWS qui permettent la communication via le port 1812.

Pour plus d'informations, consultez Activer l'authentification multifactorielle pour AWS Managed Microsoft AD dans le Guide d'administration du AWS Directory Service.

> **Note**
>
> L'authentification multifactorielle n'est pas disponible pour les annuaires Simple AD.

Promotion d'un utilisateur en tant qu'administrateur

Vous utilisez la WorkDocs console pour promouvoir un utilisateur au rang d'administrateur. Procédez comme suit :

Pour promouvoir un utilisateur en administrateur

1. Ouvrez la WorkDocs console à l'adresse https://console.aws.amazon.com/zocalo/.
2. Dans le volet de navigation, sélectionnez Mes sites.

   La page Gérer vos WorkDocs sites s'affiche.
3. Sélectionnez le bouton situé à côté du site souhaité, choisissez Actions, puis choisissez Définir un administrateur.

   La boîte de dialogue Définir WorkDocs l'administrateur s'affiche.
4. Dans le champ Nom d'utilisateur, entrez le nom d'utilisateur de la personne que vous souhaitez promouvoir, puis choisissez Définir un administrateur.

Vous pouvez également utiliser le panneau de configuration de l'administrateur du WorkDocs site pour rétrograder un administrateur. Pour de plus amples informations, veuillez consulter Modification d'utilisateurs.

Gestion WorkDocs depuis la AWS console

Vous utilisez les outils suivants pour gérer vos WorkDocs sites :

- La AWS console de https://console.aws.amazon.com/zocalo/.
- Le panneau de configuration d'administration du site, accessible aux administrateurs de tous les WorkDocs sites.

Chacun de ces outils propose un ensemble d'actions différent, et les rubriques de cette section expliquent les actions proposées par la AWS console. Pour plus d'informations sur le panneau de configuration de l'administration du site, consultezGestion WorkDocs depuis le panneau de configuration d'administration du site.

Configuration des administrateurs du site

Si vous êtes administrateur, vous pouvez autoriser les utilisateurs à accéder au panneau de configuration du site et aux actions qu'il propose.

Pour définir un administrateur

1. Ouvrez la WorkDocs console à l'adresse https://console.aws.amazon.com/zocalo/.
2. Dans le volet de navigation, sélectionnez Mes sites.

   La page Gérer vos WorkDocs sites apparaît et affiche la liste de vos sites.
3. Cliquez sur le bouton situé à côté du site pour lequel vous souhaitez définir un administrateur.
4. Ouvrez la liste des actions et choisissez Définir un administrateur.

   La boîte de dialogue Définir WorkDocs l'administrateur s'affiche.
5. Dans le champ Nom d'utilisateur, entrez le nom du nouvel administrateur, puis choisissez Définir l'administrateur.

Renvoyer des e-mails d'invitation

Vous pouvez renvoyer un e-mail d'invitation à tout moment.

Pour renvoyer l'e-mail d'invitation

1. Ouvrez la WorkDocs console à l'adresse https://console.aws.amazon.com/zocalo/.
2. Dans le volet de navigation, sélectionnez Mes sites.

   La page Gérer vos WorkDocs sites apparaît et affiche la liste de vos sites.
3. Cliquez sur le bouton situé à côté du site pour lequel vous souhaitez renvoyer l'e-mail.
4. Ouvrez la liste des actions et choisissez Renvoyer l'e-mail d'invitation.

   Un message de réussite apparaît dans une bannière verte en haut de la page.

Gestion de l'authentification multifactorielle

Vous pouvez activer l'authentification multifactorielle après avoir créé un WorkDocs site. Pour de plus amples informations sur l'authentification, veuillez consulter Activation de l'authentification multi-facteurs.

Configuration du site URLs

> **Note**
>
> Si vous avez suivi le processus de création du site enCommencer avec WorkDocs, vous avez saisi une URL de site. Par conséquent, la commande WorkDocs Définir l'URL du site n'est pas disponible, car vous ne pouvez définir une URL qu'une seule fois. Vous ne devez suivre ces étapes que si vous déployez Amazon WorkSpaces et que vous l'intégrez à WorkDocs. Le processus WorkSpaces d'intégration d'Amazon vous oblige à saisir un numéro de série au lieu d'une URL de site. Vous devez donc saisir une URL une fois l'intégration terminée. Pour plus d'informations sur l'intégration d'Amazon WorkSpaces et WorkDocs consultez la section Intégrer avec WorkDocs dans le guide de WorkSpaces l'utilisateur Amazon.

Pour définir l'URL d'un site

1. Ouvrez la WorkDocs console à l'adresse https://console.aws.amazon.com/zocalo/.
2. Dans le volet de navigation, sélectionnez Mes sites.

   La page Gérer vos WorkDocs sites apparaît et affiche la liste de vos sites.

3. Sélectionnez le site que vous avez intégré à Amazon WorkSpaces. L'URL contient l'ID de répertoire de votre WorkSpaces instance Amazon, tel que https://{directory_id}.awsapps.com.
4. Cliquez sur le bouton situé à côté de cette URL, ouvrez la liste des actions, puis choisissez Définir l'URL du site.

   La boîte de dialogue Définir l'URL du site apparaît.
5. Dans le champ URL du site, entrez l'URL du site, puis choisissez Définir l'URL du site.
6. Sur la page Gérer vos WorkDocs sites, choisissez Actualiser pour voir la nouvelle URL.

Gestion des notifications

> **Note**
>
> Pour plus de sécurité, créez des utilisateurs fédérés plutôt que des utilisateurs IAM dans la mesure du possible.

Les notifications permettent aux utilisateurs ou aux rôles IAM d'appeler l'CreateNotificationSubscriptionAPI, que vous pouvez utiliser pour définir votre propre point de terminaison pour le traitement des messages SNS envoyés. WorkDocs Pour plus d'informations sur les notifications, consultez la section Configuration des notifications pour un utilisateur ou un rôle IAM dans le Guide du WorkDocs développeur.

Vous pouvez créer et supprimer des notifications. Les étapes suivantes expliquent comment effectuer les deux tâches.

> **Note**
>
> Pour créer une notification, vous devez disposer de votre IAM ou de votre ARN de rôle. Pour trouver votre ARN IAM, procédez comme suit :
>
> 1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
> 2. Dans la barre de navigation, sélectionnez Utilisateurs.
> 3. Sélectionnez votre nom d'utilisateur.
> 4. Sous Résumé, copiez votre ARN.

Pour créer une notification

1. Ouvrez la WorkDocs console à l'adresse https://console.aws.amazon.com/zocalo/.
2. Dans le volet de navigation, sélectionnez Mes sites.

   La page Gérer vos WorkDocs sites apparaît et affiche la liste de vos sites.
3. Cliquez sur le bouton situé à côté du site souhaité.
4. Ouvrez la liste des actions et choisissez Gérer les notifications.

   La page Gérer les notifications s'affiche.
5. Choisissez Create notification (Créer une notification).
6. Dans la boîte de dialogue Nouvelle notification, entrez votre IAM ou l'ARN de votre rôle, puis choisissez Créer des notifications.

Pour supprimer une notification

1. Ouvrez la WorkDocs console à l'adresse https://console.aws.amazon.com/zocalo/.
2. Dans le volet de navigation, sélectionnez Mes sites.

   La page Gérer vos WorkDocs sites apparaît et affiche la liste de vos sites.
3. Cliquez sur le bouton situé à côté du site qui contient la notification que vous souhaitez supprimer.
4. Ouvrez la liste des actions et choisissez Gérer les notifications.
5. Sur la page Gérer les notifications, cliquez sur le bouton situé à côté de la notification que vous souhaitez supprimer, puis sélectionnez Supprimer les notifications.

Suppression d'un site

Vous utilisez la WorkDocs console pour supprimer un site.

> **Warning**
>
> Vous perdez tous les fichiers lorsque vous supprimez un site. Ne supprimez un site que si vous êtes absolument certain que ces informations ne sont plus nécessaires.

Pour supprimer un site

1. Ouvrez la WorkDocs console à l'adresse https://console.aws.amazon.com/zocalo/.
2. Dans la barre de navigation, sélectionnez Mes sites.

   La page Gérer vos WorkDocs sites s'affiche.
3. Cliquez sur le bouton situé à côté du site que vous souhaitez supprimer, puis sélectionnez Supprimer.

   La boîte de dialogue Supprimer l'URL du site apparaît.
4. Vous pouvez également sélectionner Supprimer également l'annuaire des utilisateurs.

   > **Important**
   >
   > Si vous ne fournissez pas votre propre répertoire pour WorkDocs, nous en créons un pour vous. Lorsque vous supprimez le WorkDocs site, le répertoire que nous créons vous est facturé, sauf si vous le supprimez ou que vous l'utilisez pour une autre application AWS. Pour plus d'informations sur la tarification, reportez-vous à la section Tarification d'AWS Directory Service.
5. Dans le champ URL du site, entrez l'URL du site, puis choisissez Supprimer.

   Le site est immédiatement supprimé et n'est plus disponible.

Gestion WorkDocs depuis le panneau de configuration d'administration du site

Vous utilisez les outils suivants pour gérer vos WorkDocs sites :

- Le panneau de configuration d'administration du site, accessible aux administrateurs de tous les WorkDocs sites, et décrit dans les rubriques suivantes.
- La AWS console de https://console.aws.amazon.com/zocalo/.

Chacun de ces outils propose un ensemble d'actions différent. Les rubriques de cette section expliquent les actions proposées par le panneau de configuration de l'administrateur du site. Pour plus d'informations sur les tâches disponibles dans la console, consultezGestion WorkDocs depuis la AWS console.

Paramètres de langue préférée

Vous pouvez spécifier la langue des notifications par e-mail.

Pour modifier les paramètres de langue

1. Sous My account (Mon compte), choisissez Open admin control panel (Ouvrir le panneau de configuration d'administration).
2. Pour Preferred Language Settings (Paramètres de langue favoris), choisissez votre langue préférée.

Hancom Online Editing et Office Online

Activez ou désactivez les paramètres Hancom Online Editing et Office Online depuis Admin control panel (Panneau de configuration de l'administrateur). Pour de plus amples informations, veuillez consulter Activation de l'édition collaborative.

Stockage

Spécifiez le volume de stockage reçu par les nouveaux utilisateurs.

Pour modifier les paramètres de stockage

1. Sous My account (Mon compte), choisissez Open admin control panel (Ouvrir le panneau de configuration d'administration).
2. Pour Storage (Stockage), choisissez Change (Modifier).
3. Dans la boîte de dialogue Storage Limit (Limite de stockage), choisissez d'accorder un stockage limité ou illimité aux nouveaux utilisateurs.
4. Choisissez Save Changes (Enregistrer les modifications).

La modification du paramètre de stockage affecte uniquement les utilisateurs qui sont ajoutés après la modification. Il ne modifie pas le volume de stockage alloué aux utilisateurs existants. Pour modifier la limite de stockage pour un utilisateur existant, consultez Modification d'utilisateurs.

Liste des autorisations IP

WorkDocs les administrateurs du site peuvent ajouter des paramètres de liste d'adresses IP autorisées pour restreindre l'accès au site à une plage d'adresses IP autorisée. Vous pouvez ajouter jusqu'à 500 paramètres de liste d'adresses IP autorisées par site.

> **Note**
>
> La liste d'adresses IP autorisées ne fonctionne actuellement que pour IPv4 les adresses. La liste de refus d'adresses IP n'est actuellement pas prise en charge.

Pour ajouter une plage d'adresses à la IP Allow List (Liste d'adresses IP autorisées)

1. Sous My account (Mon compte), choisissez Open admin control panel (Ouvrir le panneau de configuration d'administration).
2. Pour IP Allow List (Liste d'adresses IP autorisées), choisissez Change (Modifier).
3. Pour Enter CIDR value, entrez le bloc Classless Inter-Domain Routing (CIDR) pour les plages d'adresses IP, puis choisissez Ajouter.
   - Pour n'autoriser l'accès que depuis une seule adresse IP, spécifiez `/32` comme préfixe CIDR.
4. Choisissez Save Changes (Enregistrer les modifications).

5. Les utilisateurs qui se connectent à votre site à partir des adresses IP de IP Allow List (Liste d'adresses IP autorisées) se voient autoriser l'accès. Les utilisateurs qui tentent de se connecter à votre site à partir d'adresses IP non autorisées reçoivent une réponse indiquant que l'accès ne leur est pas autorisé.

> **Warning**
>
> Si vous entrez une valeur de CIDR qui vous empêche d'utiliser votre adresse IP actuelle pour accéder au site, un message d'avertissement s'affiche. Si vous choisissez de continuer avec la valeur de CIDR actuelle, votre accès au site sera bloqué avec votre adresse IP actuelle. Cette action ne peut être annulée qu'en contactant AWS Support.

Sécurité — ActiveDirectory Sites simples

Cette rubrique décrit les différents paramètres de sécurité pour les ActiveDirectory sites simples. Si vous gérez des sites qui utilisent le ActiveDirectory connecteur, reportez-vous à la section suivante.

Pour utiliser les paramètres de sécurité

1. Choisissez l'icône de profil dans le coin supérieur droit du WorkDocs client.

2. Sous Admin, choisissez Ouvrir le panneau de configuration d'administration.
3. Faites défiler la page jusqu'à Sécurité, puis sélectionnez Modifier.

   La boîte de dialogue Paramètres de stratégie apparaît. Le tableau suivant répertorie les paramètres de sécurité pour les ActiveDirectory sites simples.

Réglage	Description
Sous Choisissez votre paramètre pour les liens partageables, sélectionnez l'une des options suivantes :	
N'autorisez pas les liens partageables à l'échelle du site ou publics	Désactive le partage de liens pour tous les utilisateurs.

Réglage	Description
Autorisez les utilisateurs à créer des liens partageables à l'échelle du site, mais ne les autorisez pas à créer des liens partageables publics	Limite le partage de liens aux seuls membres du site. Les utilisateurs gérés peuvent créer ce type de lien.
Autorisez les utilisateurs à créer des liens partageables à l'échelle du site, mais seuls les utilisateurs expérimentés peuvent créer des liens partageables publics	Les utilisateurs gérés peuvent créer des liens à l'échelle du site, mais seuls les utilisate urs expérimentés peuvent créer des liens publics. Les liens publics permettent à n'importe qui d'accéder à Internet.
Tous les utilisateurs gérés peuvent créer des liens partageables publics et à l'échelle du site	Les utilisateurs gérés peuvent créer des liens publics.

Sous Activation automatique, cochez ou décochez la case.

Permettez à tous les utilisateurs de votre répertoire d'être automatiquement activés lors de leur première connexion à votre WorkDocs site.	Active automatiquement les utilisateurs lorsqu'ils se connectent pour la première fois à votre site.

Sous Qui devrait être autorisé à inviter de nouveaux utilisateurs WorkDocs sur votre site, sélectionnez l'une des options suivantes :

Seuls les administrateurs peuvent inviter de nouveaux utilisateurs.	Seuls les administrateurs peuvent inviter de nouveaux utilisateurs.
Les utilisateurs peuvent inviter de nouveaux utilisateurs où qu'ils soient en partageant des fichiers ou des dossiers avec eux.	Permet aux utilisateurs d'inviter de nouveaux utilisateurs en partageant des fichiers ou des dossiers avec ces utilisateurs.
Les utilisateurs peuvent inviter de nouveaux utilisateurs issus de quelques domaines spécifiques en partageant des fichiers ou des dossiers avec eux.	Les utilisateurs peuvent inviter de nouvelles personnes des domaines spécifiés en partageant des fichiers ou des dossiers avec elles.

Réglage	Description
Sous Configurer le rôle pour les nouveaux utilisateurs, cochez ou décochez la case.	
Les nouveaux utilisateurs de votre répertoire seront des utilisateurs gérés (ce sont des utilisateurs invités par défaut)	Convertit automatiquement les nouveaux utilisateurs de votre répertoire en utilisateurs gérés.

4. Lorsque vous avez terminé, choisissez Enregistrer les modifications.

Sécurité — sites ActiveDirectory de connexion

Cette rubrique décrit les différents paramètres de sécurité pour les sites de ActiveDirectory connecteurs. Si vous gérez des sites qui utilisent Simple ActiveDirectory, consultez la section précédente.

Pour utiliser les paramètres de sécurité

1. Choisissez l'icône de profil dans le coin supérieur droit du WorkDocs client.

2. Sous Admin, choisissez Ouvrir le panneau de configuration d'administration.
3. Faites défiler la page jusqu'à Sécurité, puis sélectionnez Modifier.

   La boîte de dialogue Paramètres de stratégie apparaît. Le tableau suivant répertorie et décrit les paramètres de sécurité pour les sites de ActiveDirectory connecteurs.

Réglage	Description
Sous Choisissez votre paramètre pour les liens partageables, sélectionnez l'une des options suivantes :	
N'autorisez pas les liens partageables à l'échelle du site ou publics	Lorsque cette option est sélectionnée, le partage de liens est désactivé pour tous les utilisateurs.

Réglage	Description
Autorisez les utilisateurs à créer des liens partageables à l'échelle du site, mais ne les autorisez pas à créer des liens partageables publics	Limite le partage de liens aux seuls membres du site. Les utilisateurs gérés peuvent créer ce type de lien.
Autorisez les utilisateurs à créer des liens partageables à l'échelle du site, mais seuls les utilisateurs expérimentés peuvent créer des liens partageables publics	Les utilisateurs gérés peuvent créer des liens à l'échelle du site, mais seuls les utilisate urs expérimentés peuvent créer des liens publics. Les liens publics permettent à n'importe qui d'accéder à Internet.
Tous les utilisateurs gérés peuvent créer des liens partageables publics et à l'échelle du site	Les utilisateurs gérés peuvent créer des liens publics.

Sous Activation automatique, cochez ou décochez la case.

Permettez à tous les utilisateurs de votre répertoire d'être automatiquement activés lors de leur première connexion à votre WorkDocs site.	Active automatiquement les utilisateurs lorsqu'ils se connectent pour la première fois à votre site.

Sous Qui devrait être autorisé à activer les utilisateurs de l'annuaire WorkDocs sur votre site ? , sélectionnez l'une des options suivantes :

Seuls les administrateurs peuvent activer de nouveaux utilisateurs depuis votre annuaire.	Permet uniquement aux administrateurs d'activer de nouveaux utilisateurs de l'annuair e.
Les utilisateurs peuvent activer de nouveaux utilisateurs depuis votre répertoire en partageant des fichiers ou des dossiers avec eux.	Permet aux utilisateurs d'activer les utilisate urs de l'annuaire en partageant des fichiers ou des dossiers avec les utilisateurs de l'annuaire.

Réglage	Description
Les utilisateurs peuvent activer de nouveaux utilisateurs à partir de quelques domaines spécifiques en partageant des fichiers ou des dossiers avec eux.	Les utilisateurs ne peuvent partager que des fichiers ou des dossiers provenant d'utilisateurs appartenant à des domaines spécifiques. Lorsque vous choisissez cette option, vous devez saisir les domaines.

Sous Qui devrait être autorisé à inviter de nouveaux utilisateurs WorkDocs sur votre site ? , sélectionnez l'une des options suivantes :

Partager avec des utilisateurs externes **Note** Les options ci-dessous n'apparaissent qu'une fois que vous avez sélectionné ce paramètre.	Permet aux administrateurs et aux utilisateurs d'inviter de nouveaux utilisateurs externes WorkDocs sur votre site.
Seuls les administrateurs peuvent inviter de nouveaux utilisateurs externes	Seuls les administrateurs peuvent inviter des utilisateurs externes.
Tous les utilisateurs gérés peuvent inviter de nouveaux utilisateurs	Permet aux utilisateurs gérés d'inviter des utilisateurs externes.
Seuls les utilisateurs expérimentés peuvent inviter de nouveaux utilisateurs externes.	Permet uniquement aux utilisateurs expérimentés d'inviter de nouveaux utilisateurs externes.

Sous Configurer le rôle pour les nouveaux utilisateurs, sélectionnez l'une ou les deux options.

Les nouveaux utilisateurs de votre répertoire seront des utilisateurs gérés (ce sont des utilisateurs invités par défaut)	Convertit automatiquement les nouveaux utilisateurs de votre répertoire en utilisateurs gérés.
Les nouveaux utilisateurs externes seront des utilisateurs gérés (ils sont des utilisateurs invités par défaut)	Convertit automatiquement les nouveaux utilisateurs externes en utilisateurs gérés.

4. Lorsque vous avez terminé, choisissez Enregistrer les modifications.

Conservation dans la corbeille de récupération

Lorsqu'un utilisateur supprime un fichier, il le WorkDocs stocke dans sa corbeille pendant 30 jours. WorkDocs Déplace ensuite les fichiers dans une corbeille de récupération temporaire pendant 60 jours, puis les supprime définitivement. Seuls les administrateurs peuvent voir le bac de restauration temporaire. En modifiant la politique de conservation des données à l'échelle du site, les administrateurs du site peuvent modifier la période de conservation des bacs de récupération à un minimum de zéro jour et un maximum de 365 jours.

Pour modifier la période de conservation de la corbeille de récupération

1. Sous My account (Mon compte), choisissez Open admin control panel (Ouvrir le panneau de configuration d'administration).
2. En regard de Recovery bin retention (Conservation de la corbeille de récupération), choisissez Change (Modifier).
3. Entrez le nombre de jours pendant lesquels les fichiers doivent être conservés dans la corbeille de récupération, puis choisissez Enregistrer.

> **Note**
>
> La période de conservation par défaut est de 60 jours. Vous pouvez utiliser une période de 0 à 365 jours.

Les administrateurs peuvent restaurer les fichiers utilisateur à partir de la corbeille de récupération avant de WorkDocs les supprimer définitivement.

Pour restaurer le fichier d'un utilisateur

1. Sous My account (Mon compte), choisissez Open admin control panel (Ouvrir le panneau de configuration d'administration).
2. Sous Manage Users (Gérer les utilisateurs), choisissez l'icône de dossier de l'utilisateur.
3. Sous Corbeille de récupération, sélectionnez le ou les fichiers à restaurer, puis choisissez l'icône Récupérer.

4. Pour Restore file (Restaurer un fichier), choisissez l'emplacement où restaurer le fichier, puis choisissez Restore (Restaurer).

Gestion des paramètres utilisateur

Vous pouvez gérer les paramètres des utilisateurs, y compris modifier les rôles utilisateur, et inviter, activer ou désactiver les utilisateurs. Pour de plus amples informations, veuillez consulter Inviter et gérer WorkDocs les utilisateurs.

Déploiement de WorkDocs Drive sur plusieurs ordinateurs

Si vous possédez un parc de machines rattaché à un domaine, vous pouvez utiliser Group Policy Objects (GPO) ou System Center Configuration Manager (SCCM) pour installer le client Drive. WorkDocs Vous pouvez télécharger le client depuis https://amazonworkdocs.com/en/les clients.

Au fur et à mesure, n'oubliez pas que WorkDocs Drive nécessite un accès HTTPS sur le port 443 pour toutes les adresses IP AWS. Vous devez également vérifier que vos systèmes cibles répondent aux exigences d'installation de WorkDocs Drive. Pour plus d'informations, consultez la section Installation de WorkDocs Drive dans le guide de WorkDocs l'utilisateur Amazon.

> **Note**
>
> Lorsque vous utilisez GPO ou SCCM, il est recommandé d'installer le client WorkDocs Drive une fois que les utilisateurs se sont connectés.

Le programme d'installation MSI pour WorkDocs Drive prend en charge les paramètres d'installation facultatifs suivants :

- **`SITEID`**— Pré-remplit les informations du WorkDocs site pour les utilisateurs lors de l'inscription. Par exemple, `SITEID=`*`site-name`*.
- **`DefaultDriveLetter`**— Pré-remplit la lettre du lecteur à utiliser pour le montage WorkDocs du lecteur. Par exemple, `DefaultDriveLetter=`*`W`*. N'oubliez pas que chaque utilisateur doit avoir une lettre de lecteur différente. Les utilisateurs peuvent également modifier le nom du lecteur, mais pas la lettre du lecteur, après avoir démarré WorkDocs Drive pour la première fois.

L'exemple suivant déploie WorkDocs Drive sans interface utilisateur ni redémarrage. Notez qu'il utilise le nom par défaut du fichier MSI :

```
msiexec /i "AWSWorkDocsDriveClient.msi" SITEID=your_workdocs_site_ID
DefaultDriveLetter=your_drive_letter REBOOT=REALLYSUPPRESS /norestart /qn
```

Inviter et gérer WorkDocs les utilisateurs

Par défaut, lorsque vous attachez un annuaire lors de la création du site, la fonctionnalité d'activation automatique WorkDocs ajoute tous les utilisateurs de ce répertoire au nouveau site en tant qu'utilisateurs gérés.

Dans WorkDocs, les utilisateurs gérés n'ont pas besoin de se connecter avec des informations d'identification distinctes. Ils peuvent partager des fichiers et collaborer sur ceux-ci, et ils disposent automatiquement de 1 To de stockage. Toutefois, vous pouvez désactiver l'activation automatique lorsque vous souhaitez uniquement ajouter certains utilisateurs dans un annuaire. Les étapes décrites dans les sections suivantes expliquent comment procéder.

En outre, vous pouvez inviter, activer ou désactiver des utilisateurs, et modifier les rôles et les paramètres des utilisateurs. Vous pouvez également promouvoir un utilisateur en tant qu'administrateur. Pour plus d'informations sur la promotion des utilisateurs, consultezPromotion d'un utilisateur en tant qu'administrateur.

Vous effectuez ces tâches dans le panneau de configuration d'administration du client WorkDocs Web, et les étapes décrites dans les sections suivantes expliquent comment procéder. Mais, si vous êtes nouveau dans ce WorkDocs domaine, prenez quelques minutes pour découvrir les différents rôles des utilisateurs avant de vous lancer dans les tâches administratives.

Table des matières

Présentation des rôles utilisateur

WorkDocs définit les rôles utilisateur suivants. Vous pouvez modifier les rôles des utilisateurs en modifiant leur profil utilisateur. Pour de plus amples informations, veuillez consulter Modification d'utilisateurs.

- Admin (Administrateur) : utilisateur payé disposant d'autorisations administratives pour la totalité du site, notamment pour la gestion des utilisateurs et la configuration des paramètres du site. Pour en savoir plus sur la promotion d'un utilisateur en tant qu'administrateur, consultez Promotion d'un utilisateur en tant qu'administrateur.
- Utilisateur expérimenté : utilisateur payant qui dispose d'un ensemble d'autorisations spéciales de la part de l'administrateur. Pour plus d'informations sur la façon de définir des autorisations pour un utilisateur expérimenté, reportez-vous Sécurité — ActiveDirectory Sites simples aux sections etSécurité — sites ActiveDirectory de connexion.
- Utilisateur : utilisateur payant qui peut enregistrer des fichiers et collaborer avec d'autres utilisateurs WorkDocs sur un site.
- Guest user (Utilisateur invité) : Un utilisateur non payé qui peut uniquement afficher des fichiers. Vous pouvez mettre à niveau les utilisateurs invités vers les rôles d'utilisateur, d'utilisateur avancé ou d'administrateur.

> **Note**
>
> Lorsque vous modifiez le rôle d'un utilisateur invité, vous effectuez une action ponctuelle que vous ne pouvez pas annuler.

WorkDocs définit également ces types d'utilisateurs supplémentaires.

Utilisateur WS

Un utilisateur auquel est assigné un WorkSpaces WorkSpace.

- Accès à toutes les WorkDocs fonctionnalités
- Stockage par défaut de 50 Go (possibilité de payer pour bénéficier d'1 To)
- Aucun frais mensuel

Utilisateur WS mis à niveau

Un utilisateur auquel un espace de stockage a été attribué WorkSpaces WorkSpace et mis à niveau.

- Accès à toutes les WorkDocs fonctionnalités
- Stockage par défaut de 1 To (stockage supplémentaire disponible sur une pay-as-you-go base donnée)
- Frais mensuels

WorkDocs utilisateur

Un WorkDocs utilisateur actif sans assignation WorkSpaces WorkSpace.

- Accès à toutes les WorkDocs fonctionnalités
- Stockage par défaut de 1 To (stockage supplémentaire disponible sur une pay-as-you-go base donnée)
- Frais mensuels

Démarrage du panneau de configuration d'administration

Vous utilisez le panneau de contrôle administratif du client WorkDocs Web pour activer ou désactiver l'activation automatique et pour modifier les rôles et les paramètres des utilisateurs.

Pour ouvrir le panneau de configuration d'administration

1. Choisissez l'icône de profil dans le coin supérieur droit du WorkDocs client.

2. Sous Administrateur, choisissez Ouvrir le panneau de configuration d'administration.

> **Note**
>
> Certaines options du panneau de configuration diffèrent entre les annuaires cloud et les annuaires connectés.

Désactiver l'activation automatique

Vous désactivez l'activation automatique lorsque vous ne souhaitez pas ajouter tous les utilisateurs d'un annuaire à un nouveau site et lorsque vous souhaitez définir des autorisations et des rôles différents pour les utilisateurs que vous invitez sur un nouveau site. Lorsque vous désactivez l'activation automatique, vous pouvez également décider qui est autorisé à inviter de nouveaux utilisateurs sur le site : utilisateurs actuels, utilisateurs expérimentés ou administrateurs. Ces étapes expliquent comment effectuer les deux tâches.

Pour désactiver l'activation automatique

1. Choisissez l'icône de profil dans le coin supérieur droit du WorkDocs client.

2. Sous Administrateur, choisissez Ouvrir le panneau de configuration d'administration.
3. Faites défiler l'écran jusqu'à Sécurité et choisissez Modifier.

   La boîte de dialogue Paramètres de stratégie apparaît.
4. Sous Activation automatique, décochez la case à côté de Autoriser l'activation automatique de tous les utilisateurs de votre répertoire lors de leur première connexion à votre WorkDocs site.

   Les options changent sous Qui devrait être autorisé à activer les utilisateurs de l'annuaire WorkDocs sur votre site. Vous pouvez autoriser les utilisateurs actuels à inviter de nouveaux utilisateurs, ou vous pouvez donner cette possibilité à des utilisateurs expérimentés ou à d'autres administrateurs.
5. Sélectionnez une option, puis cliquez sur Enregistrer les modifications.

Répétez les étapes 1 à 4 pour réactiver l'activation automatique.

Gestion du partage de liens

Cette rubrique explique comment gérer le partage de liens. WorkDocs les utilisateurs peuvent partager leurs fichiers et dossiers en partageant des liens vers ceux-ci. Ils peuvent partager des liens vers des fichiers à l'intérieur et à l'extérieur de votre organisation, mais ils ne peuvent partager des liens vers des dossiers qu'en interne. En tant qu'administrateur, vous déterminez qui peut partager des liens.

Pour activer le partage de liens

1. Choisissez l'icône de profil dans le coin supérieur droit du WorkDocs client.

2. Sous Administrateur, choisissez Ouvrir le panneau de configuration d'administration.
3. Faites défiler l'écran jusqu'à Sécurité et choisissez Modifier.

   La boîte de dialogue Paramètres de stratégie apparaît.
4. Sous Choisissez votre paramètre pour les liens partageables, sélectionnez une option :

   - Ne pas autoriser les liens partageables à l'échelle du site ou publics : désactive le partage de liens pour tous les utilisateurs.
   - Autorisez les utilisateurs à créer des liens partageables à l'échelle du site, mais ne les autorisez pas à créer des liens partageables publics — Limite le partage de liens aux seuls membres du site. Les utilisateurs gérés peuvent créer ce type de lien.
   - Autorisez les utilisateurs à créer des liens partageables à l'échelle du site, mais seuls les utilisateurs expérimentés peuvent créer des liens partageables publics. Les utilisateurs gérés peuvent créer des liens à l'échelle du site, mais seuls les utilisateurs expérimentés peuvent créer des liens publics. Les liens publics permettent à quiconque d'accéder à Internet.
   - Tous les utilisateurs gérés peuvent créer des liens partagés publics et à l'échelle du site. Les utilisateurs gérés peuvent créer des liens publics.
5. Choisissez Save Changes (Enregistrer les modifications).

Contrôle des invitations des utilisateurs avec activation automatique activée

Lorsque vous activez l'activation automatique (et n'oubliez pas qu'elle est activée par défaut), vous pouvez donner aux utilisateurs la possibilité d'inviter d'autres utilisateurs. Vous pouvez accorder l'autorisation à l'une des entités suivantes :

- Tous les utilisateurs
- Utilisateurs expérimentés
- Administrateurs.

Vous pouvez également désactiver complètement les autorisations. Ces étapes expliquent comment procéder.

Pour définir les autorisations d'invitation

1. Choisissez l'icône de profil dans le coin supérieur droit du WorkDocs client.

2. Sous Administrateur, choisissez Ouvrir le panneau de configuration d'administration.
3. Faites défiler l'écran jusqu'à Sécurité et choisissez Modifier.

   La boîte de dialogue Paramètres de stratégie apparaît.
4. Sous Qui devrait être autorisé à activer les utilisateurs de l'annuaire WorkDocs sur votre site, cochez la case Partager avec des utilisateurs externes, sélectionnez l'une des options situées sous la case à cocher, puis cliquez sur Enregistrer les modifications.

   —OU—

   Décochez la case si vous ne souhaitez pas que quiconque invite de nouveaux utilisateurs, puis choisissez Enregistrer les modifications.

Invitation de nouveaux utilisateurs

Vous pouvez inviter de nouveaux utilisateurs à rejoindre un annuaire. Vous pouvez également autoriser les utilisateurs existants à inviter de nouveaux utilisateurs. Pour plus d'informations, consultez Sécurité — ActiveDirectory Sites simples et Sécurité — sites ActiveDirectory de connexion dans ce guide.

Pour inviter de nouveaux utilisateurs

1. Choisissez l'icône de profil dans le coin supérieur droit du WorkDocs client.

2. Sous Administrateur, choisissez Ouvrir le panneau de configuration d'administration.
3. Sous Manage Users (Gérer les utilisateurs), choisissez Invite Users (Inviter des utilisateurs).

4. Dans la boîte de dialogue Inviter des utilisateurs, pour Qui aimeriez-vous inviter ? , entrez l'adresse e-mail de l'invité, puis choisissez Envoyer. Répétez cette étape pour chaque invitation.

WorkDocs envoie un e-mail d'invitation à chaque destinataire. L'e-mail contient un lien et des instructions sur la façon de créer un WorkDocs compte. Le lien d'invitation expire après 30 jours.

Modification d'utilisateurs

Vous pouvez modifier les informations et les paramètres utilisateur.

Pour modifier des utilisateurs

1. Choisissez l'icône de profil dans le coin supérieur droit du WorkDocs client.

2. Sous Administrateur, choisissez Ouvrir le panneau de configuration d'administration.
3. Sous Gérer les utilisateurs, choisissez l'icône en forme de crayon (✎) en regard du nom de l'utilisateur.
4. Dans la boîte de dialogue Edit User (Modifier l'utilisateur), vous pouvez modifier les options suivantes :

   First Name (Prénom) (annuaire dans le cloud uniquement)

   Le prénom de l'utilisateur.

   Last Name (Nom) (annuaire dans le cloud uniquement)

   Le nom de l'utilisateur.

   Statut

   Spécifie si l'utilisateur est actif ou inactif. Pour de plus amples informations, veuillez consulter Désactivation d'utilisateurs.

Rôle

Spécifie si une personne est un utilisateur ou un administrateur. Vous pouvez également mettre à niveau ou rétrograder les utilisateurs WorkSpaces WorkSpace auxquels un Pour de plus amples informations, veuillez consulter Présentation des rôles utilisateur.

Stockage

Spécifie la limite de stockage pour un utilisateur existant.

5. Choisissez Save Changes (Enregistrer les modifications).

Désactivation d'utilisateurs

Vous désactivez l'accès d'un utilisateur en modifiant son statut en Inactif.

Pour faire passer le statut d'un utilisateur à Inactive (Inactif).

1. Choisissez l'icône de profil dans le coin supérieur droit du WorkDocs client.

2. Sous Admin, choisissez Ouvrir le panneau de configuration d'administration.
3. Sous Gérer les utilisateurs, choisissez l'icône en forme de crayon (✎) en regard du nom de l'utilisateur.
4. Choisissez Inactive (Inactif), puis Save Changes (Enregistrer les modifications).

L'utilisateur inactivé ne peut pas accéder à votre WorkDocs site.

> **Note**
>
> Le fait qu'un utilisateur passe au statut inactif ne supprime pas ses fichiers, ses dossiers ou ses commentaires de votre WorkDocs site. Vous pouvez toutefois transférer les fichiers et dossiers d'un utilisateur inactif vers un utilisateur actif. Pour de plus amples informations, veuillez consulter Transfert de la propriété d'un document.

Supprimer des utilisateurs en attente

Vous pouvez supprimer les utilisateurs Simple AD, AWS Managed Microsoft et AD Connector dont le statut est En attente. Pour supprimer l'un de ces utilisateurs, cliquez sur l'icône de corbeille ( ) à côté du nom de l'utilisateur.

Votre WorkDocs site doit toujours avoir au moins un utilisateur actif qui n'est pas un utilisateur invité. Si vous devez supprimer tous les utilisateurs, supprimez l'intégralité du site.

Nous vous recommandons de ne pas supprimer d'utilisateurs enregistrés. Vous devez plutôt faire passer un utilisateur du statut Actif à Inactif pour l'empêcher d'accéder à votre WorkDocs site.

Transfert de la propriété d'un document

Vous pouvez transférer les fichiers et les dossiers d'un utilisateur inactif à un utilisateur actif. Pour plus d'informations sur la désactivation d'un utilisateur, consultezDésactivation d'utilisateurs.

> **Warning**
>
> Vous ne pouvez pas annuler cette action.

Pour transférer la propriété d'un document

1. Choisissez l'icône de profil dans le coin supérieur droit du WorkDocs client.

2. Sous Admin, choisissez Ouvrir le panneau de configuration d'administration.
3. Sous Gérer les utilisateurs, recherchez l'utilisateur inactif.
4. Choisissez l'icône en forme de crayon ( ) en regard du nom de l'utilisateur inactif.
5. Sélectionnez Transférer la propriété du document et saisissez l'adresse e-mail du nouveau propriétaire.
6. Choisissez Save Changes (Enregistrer les modifications).

Téléchargement de listes d'utilisateurs

Pour télécharger une liste d'utilisateurs depuis le panneau de configuration d'administration, vous devez installer WorkDocs Companion. Pour installer WorkDocs Companion, consultez la section Applications et intégrations pour WorkDocs.

Pour télécharger une liste d'utilisateurs

1. Choisissez l'icône de profil dans le coin supérieur droit du WorkDocs client.

2. Sous Admin, choisissez Ouvrir le panneau de configuration d'administration.
3. Sous Gérer les utilisateurs, choisissez Télécharger l'utilisateur.
4. Pour Download user (Télécharger un utilisateur), choisissez l'une des options suivantes pour exporter une liste d'utilisateurs en tant que fichier `.json` sur votre bureau :

   - Tous les utilisateurs
   - Utilisateur invité
   - Utilisateur WS
   - Utilisateur
   - Utilisateur avancé
   - Administrateur
5. WorkDocs enregistre le fichier dans l'un des emplacements suivants :

   - Windows – `Downloads/WorkDocsDownloads`
   - macOS : *`hard drive`*`/users/`*`username`*`/WorkDocsDownloads/folder`

   > **Note**
   >
   > Les téléchargements peuvent prendre un certain temps. De plus, les fichiers téléchargés n'atterrissent pas dans votre `/~users` dossier.

Pour plus d'informations sur les rôles d'utilisateur, consultez Présentation des rôles utilisateur.

Partage et collaboration

Vos utilisateurs peuvent partager du contenu en envoyant un lien ou une invitation. Les utilisateurs peuvent également collaborer avec des utilisateurs externes si vous activez le partage externe.

WorkDocs contrôle l'accès aux dossiers et aux fichiers grâce à l'utilisation d'autorisations. Le système applique les autorisations en fonction du rôle de l'utilisateur.

Table des matières

Partage de liens

Les utilisateurs peuvent choisir Partager un lien pour copier et partager rapidement des hyperliens vers WorkDocs du contenu avec des collègues et des utilisateurs externes à l'intérieur et à l'extérieur de leur organisation. Lorsque les utilisateurs partagent un lien, ils peuvent le configurer pour autoriser l'une des options d'accès suivantes :

- Tous les membres du WorkDocs site peuvent rechercher, consulter et commenter le fichier.
- Toute personne disposant du lien, même les personnes qui ne sont pas membres du WorkDocs site, peut consulter le fichier. Cette option de lien limite les autorisations d'affichage uniquement.

Les destinataires avec les autorisations d'affichage peuvent uniquement afficher un fichier. Les autorisations de commentaires permettent aux utilisateurs de commenter et d'effectuer des opérations de mise à jour ou de suppression, comme le chargement d'un nouveau fichier ou la suppression d'un fichier existant.

Par défaut, tous les utilisateurs gérés peuvent créer des liens publics. Pour changer cette valeur, modifiez vos paramètres Security (Sécurité) dans votre panneau de configuration d'administration. Pour de plus amples informations, veuillez consulter Gestion WorkDocs depuis le panneau de configuration d'administration du site.

Partage par invitation

Lorsque vous activez le partage par invitation, les utilisateurs de votre site peuvent partager des fichiers ou des dossiers avec des utilisateurs individuels et avec des groupes en envoyant des e-mails d'invitation. Les invitations contiennent des liens vers le contenu partagé, et les invités peuvent ouvrir les fichiers ou dossiers partagés. Les invités peuvent également partager ces fichiers ou dossiers avec d'autres membres du site et avec des utilisateurs externes.

Vous pouvez définir des niveaux d'autorisation pour chaque utilisateur invité. Vous pouvez également créer des dossiers d'équipe à partager sur invitation avec les groupes de répertoires que vous créez.

> **Note**
>
> Les invitations de partage n'incluent pas les membres des groupes imbriqués. Pour inclure ces membres, vous devez les ajouter à la liste Partager sur invitation.

Pour de plus amples informations, veuillez consulter Gestion WorkDocs depuis le panneau de configuration d'administration du site.

Partage externe

Le partage externe permet aux utilisateurs gérés d'un WorkDocs site de partager des fichiers et des dossiers et de collaborer avec des utilisateurs externes sans encourir de frais supplémentaires. Les utilisateurs du site peuvent partager des fichiers et des dossiers avec des utilisateurs externes sans que les destinataires soient des utilisateurs payants du WorkDocs site. Lorsque vous activez le partage externe, les utilisateurs peuvent saisir l'adresse e-mail de l'utilisateur externe avec lequel ils souhaitent partager et définir les autorisations de partage de visionnage appropriées. Lorsque des utilisateurs externes sont ajoutés, les autorisations sont limitées aux utilisateurs uniquement et aucune autre autorisation n'est disponible. Les utilisateurs externes reçoivent une notification par e-mail avec un lien vers le fichier ou dossier partagé. En choisissant le lien, les utilisateurs externes sont redirigés vers le site, où ils saisissent leurs informations d'identification pour se connecter WorkDocs. Ils peuvent voir le fichier ou le dossier partagé dans la vue Partagé avec moi.

Les propriétaires du fichier peuvent modifier les autorisations de partage et supprimer l'accès d'un utilisateur externe à un fichier ou un dossier à tout moment. Le partage externe pour le site doit être activé par l'administrateur du site pour que des utilisateurs gérés puissent partager un contenu avec

des utilisateurs externes. Pour que des utilisateurs invités (Guest users) deviennent des participants ou des copropriétaires, ils doivent être mis à niveau au niveau User (utilisateur) par l'administrateur du site. Pour de plus amples informations, veuillez consulter Présentation des rôles utilisateur.

Par défaut, le partage externe est activé et tous les utilisateurs peuvent inviter des utilisateurs externes. Pour changer cette valeur, modifiez vos paramètres Security (Sécurité) dans votre panneau de configuration d'administration. Pour de plus amples informations, veuillez consulter Gestion WorkDocs depuis le panneau de configuration d'administration du site.

Autorisations

WorkDocs utilise des autorisations pour contrôler l'accès aux dossiers et aux fichiers. Les autorisations sont appliquées en fonction des rôles des utilisateurs.

Table des matières

Rôles utilisateurs

Les rôles des utilisateurs contrôlent les autorisations relatives aux dossiers et aux fichiers. Vous pouvez appliquer les rôles utilisateur suivants au niveau du dossier :

- Propriétaire du dossier : propriétaire d'un dossier ou d'un fichier.
- Copropriétaire du dossier : utilisateur ou groupe désigné par le propriétaire comme copropriétaire d'un dossier ou d'un fichier.
- Contributeur au dossier : personne disposant d'un accès illimité à un dossier.
- Visionneuse de dossiers : personne disposant d'un accès limité (autorisations en lecture seule) à un dossier.

Vous pouvez appliquer les rôles utilisateur suivants au niveau de chaque fichier :

- Propriétaire : propriétaire d'un fichier.

- Copropriétaire : utilisateur ou groupe désigné par le propriétaire comme copropriétaire du fichier.
- Contributeur* — Personne autorisée à donner des commentaires sur le fichier.
- Visionneuse : personne disposant d'un accès limité (autorisations de lecture seule et d'accès aux activités d'affichage) au fichier.
- Lecteur anonyme : utilisateur non enregistré extérieur à l'organisation qui peut consulter un fichier partagé à l'aide d'un lien de consultation externe. Sauf indication contraire, un lecteur anonyme dispose des mêmes autorisations de lecture seule qu'un spectateur. Les utilisateurs anonymes ne peuvent pas voir l'activité des fichiers.

* Les contributeurs ne peuvent pas renommer les versions de fichiers existantes. Ils peuvent toutefois télécharger une nouvelle version d'un fichier portant un nom différent.

Autorisations pour les dossiers partagés

Les autorisations suivantes s'appliquent aux rôles utilisateur pour les dossiers partagés :

> **Note**
>
> Les autorisations appliquées à un dossier s'appliquent également aux sous-dossiers et aux fichiers de ce dossier.

- Afficher : affiche le contenu d'un dossier partagé.
- Afficher les sous-dossiers : affiche un sous-dossier.
- Afficher les partages : affiche les autres utilisateurs avec lesquels un dossier est partagé.
- Télécharger le dossier — Téléchargez un dossier.
- Ajouter un sous-dossier — Ajoutez un sous-dossier.
- Partager : partagez le dossier de premier niveau avec d'autres utilisateurs.
- Révoquer le partage : révoque le partage du dossier de premier niveau.
- Supprimer le sous-dossier — Supprime un sous-dossier.
- Supprimer le dossier de premier niveau : supprimez le dossier partagé de niveau supérieur.

	Vue	Afficher les sous-dossiers	Afficher les partages	Dossier de téléchargement	Ajouter un sous-dossier	Partager	Révoquer le partage	Supprimer le sous-dossier	Supprimer le dossier de premier niveau
Propriétaire du dossier	✓	✓	✓	✓	✓	✓	✓	✓	✓
Copropriétaire du dossier	✓	✓	✓	✓	✓	✓	✓	✓	✓
Contributeur au dossier	✓	✓	✓	✓	✓				
Visionneuse de dossiers	✓	✓	✓	✓					

Autorisations pour les fichiers dans des dossiers partagés

Les autorisations suivantes s'appliquent aux rôles utilisateur pour les fichiers d'un dossier partagé :

- Annoter : ajoutez des commentaires à un fichier.
- Supprimer — Supprime un fichier dans un dossier partagé.
- Renommer — Renommez les fichiers.
- Téléverser — Importez les nouvelles versions d'un fichier.
- Télécharger — Téléchargez un fichier. Il s'agit de l'autorisation par défaut. Vous pouvez utiliser les propriétés des fichiers pour autoriser ou refuser le téléchargement de fichiers partagés.
- Empêcher le téléchargement : empêche le téléchargement d'un fichier.

> **Note**
>
> - Lorsque vous sélectionnez cette option, les utilisateurs autorisés à afficher peuvent toujours télécharger des fichiers. Pour éviter cela, ouvrez le dossier partagé et désactivez le paramètre Autoriser les téléchargements pour chacun des fichiers que vous ne souhaitez pas que ces utilisateurs téléchargent.
> - Lorsque le propriétaire ou le copropriétaire d'un MP4 fichier interdit le téléchargement de ce fichier, les contributeurs et les utilisateurs ne peuvent pas le lire dans le client WorkDocs Web Amazon.

- Partager — Partagez un fichier avec d'autres utilisateurs.
- Révoquer le partage : révoque le partage d'un fichier.
- Afficher : permet d'afficher un fichier dans un dossier partagé.
- Afficher les partages : affiche les autres utilisateurs avec lesquels un fichier est partagé.
- Afficher les annotations : consultez les commentaires des autres utilisateurs.
- Afficher l'activité : affiche l'historique des activités d'un fichier.
- Afficher les versions : affiche les versions précédentes d'un fichier.
- Supprimer des versions : supprimez une ou plusieurs versions d'un fichier.
- Restaurer les versions : permet de récupérer une ou plusieurs versions supprimées d'un fichier.
- Afficher tous les commentaires privés — Le propriétaire/copropriétaire peut voir tous les commentaires privés d'un document, même s'il ne s'agit pas de réponses à leur commentaire.

	Annoter	Supprimer	Renommer	Charger	Télécharger	Empêcher le téléchargement	Partager	Révoquer le partage	Vue	Afficher les partages	Afficher les annotations	Afficher l'activité	Afficher les versions	Supprimer des versions	Restaurer des versions	Afficher tous les commentaires privés**
Propriétaire du fichier	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

	Annoter	Supprimer	Renommer	Charger	Télécharger	Empêcher le téléchargement	Partager	Révoquer le partage	Vue	Afficher les partages	Afficher les annotations	Afficher l'activité	Afficher les versions	Supprimer des versions	Restaurer des versions	Afficher tous les commentaires privés**
Propriétaire du dossier	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Copropriétaire du dossier	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Contributeur au dossier*	✓			✓	✓				✓	✓	✓	✓	✓			
Visiteur de dossier					✓				✓	✓		✓				
Visiteur anonyme									✓	✓						

* Dans ce cas, le propriétaire du fichier est la personne qui a chargé la version originale d'un fichier dans un dossier partagé. Les autorisations associées à ce rôle s'appliquent uniquement au fichier détenu, et non à tous les fichiers du dossier partagé.

** Les propriétaires et copropriétaires peuvent voir tous les commentaires privés. Les participants peuvent uniquement afficher les commentaires privés qui sont des réponses à leurs propres commentaires.

*** Les contributeurs ne peuvent pas renommer les versions de fichiers existantes. Ils peuvent toutefois télécharger une nouvelle version d'un fichier portant un nom différent.

Autorisations pour les fichiers ne figurant pas dans des dossiers partagés

Les autorisations suivantes s'appliquent aux rôles utilisateur pour les fichiers qui ne résident pas dans un dossier partagé :

- Annoter : ajoutez des commentaires à un fichier.
- Supprimer — Supprime un fichier.
- Renommer — Renommez les fichiers.
- Téléverser — Importez les nouvelles versions d'un fichier.
- Télécharger — Téléchargez un fichier. Il s'agit de l'autorisation par défaut. Vous pouvez utiliser les propriétés des fichiers pour autoriser ou refuser le téléchargement de fichiers partagés.
- Empêcher le téléchargement : empêche le téléchargement d'un fichier.

> **Note**
>
> Lorsque le propriétaire ou le copropriétaire d'un MP4 fichier interdit le téléchargement de ce fichier, les contributeurs et les utilisateurs ne peuvent pas le lire dans le client WorkDocs Web Amazon.

- Partager — Partagez un fichier avec d'autres utilisateurs.
- Révoquer le partage : révoque le partage d'un fichier.
- Afficher — Afficher un fichier.
- Afficher les partages : affiche les autres utilisateurs avec lesquels un fichier est partagé.
- Afficher les annotations : consultez les commentaires des autres utilisateurs.
- Afficher l'activité : affiche l'historique des activités d'un fichier.
- Afficher les versions : affiche les versions précédentes d'un fichier.
- Supprimer des versions : supprimez une ou plusieurs versions d'un fichier.

- Restaurer les versions : permet de récupérer une ou plusieurs versions supprimées d'un fichier.

	Annoter	Supprimer	Renommer	Charger	Télécharger	Empêcher le téléchargement	Partager	Révoquer le partage	Vue	Afficher les partages	Afficher les annotations	Afficher l'activité	Afficher les versions	Supprimer des versions	Restaurer des versions
Propriétaire*	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Copropriétaire*	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Contributeur**	✓			✓	✓				✓	✓	✓	✓	✓		
Lecteur					✓				✓	✓		✓			
Visiteur anonyme									✓	✓					

* Les propriétaires et copropriétaires du fichier peuvent voir tous les commentaires privés. Les participants peuvent uniquement afficher les commentaires privés qui sont des réponses à leurs propres commentaires.

** Les contributeurs ne peuvent pas renommer les versions de fichiers existantes. Ils peuvent toutefois télécharger une nouvelle version d'un fichier portant un nom différent.

Activation de l'édition collaborative

Vous utilisez la section Paramètres d'édition en ligne de votre panneau de configuration d'administration pour activer les options d'édition collaborative.

Table des matières

Activation de Hancom ThinkFree

Vous pouvez activer Hancom ThinkFree pour votre WorkDocs site afin que les utilisateurs puissent créer et modifier des fichiers Microsoft Office de manière collaborative à partir de l'application WorkDocs Web. Pour plus d'informations, consultez Modifier avec Hancom. ThinkFree

Hancom ThinkFree est disponible sans frais supplémentaires pour les WorkDocs utilisateurs. Aucune licence ou installation logicielle supplémentaire n'est nécessaire.

Pour activer Hancom ThinkFree

Activez l' ThinkFree édition Hancom depuis le panneau de configuration d'administration.

1. Sous My account (Mon compte), choisissez Open admin control panel (Ouvrir le panneau de configuration d'administration).
2. Pour Hancom Online Editing, choisissez Change (Modifier).
3. Sélectionnez Enable Hancom Online Editing Feature (Activer la fonctionnalité Hancom Online Editing), vérifiez les conditions d'utilisation, puis choisissez Save (Enregistrer).

Pour désactiver Hancom ThinkFree

Désactivez l' ThinkFree édition Hancom depuis le panneau de configuration d'administration.

1. Sous My account (Mon compte), choisissez Open admin control panel (Ouvrir le panneau de configuration d'administration).
2. Pour Hancom Online Editing, choisissez Change (Modifier).
3. Décochez la case Enable Hancom Online Editing Feature (Activer la fonctionnalité Hancom Online Editing), puis choisissez Save (Enregistrer).

Activation d'Ouvrir avec Office Online

Activez Open with Office Online pour votre WorkDocs site, afin que les utilisateurs puissent modifier des fichiers Microsoft Office de manière collaborative à partir de l'application WorkDocs Web.

Open with Office Online est disponible sans frais supplémentaires pour WorkDocs les utilisateurs qui possèdent également un compte Microsoft Office 365 Work ou School avec une licence leur permettant de modifier dans Office Online. Pour plus d'informations, consultez Ouvrir avec Office Online.

Pour activer Ouvrir avec Office Online

Activez Ouvrir avec Office Online depuis Admin control panel (Panneau de configuration d'administration).

1. Sous My account (Mon compte), choisissez Open admin control panel (Ouvrir le panneau de configuration d'administration).
2. Pour Office Online, choisissez Change (Modifier).
3. Sélectionnez Enable Office Online (Activer Office Online), puis choisissez Save (Enregistrer).

Pour désactiver Ouvrir avec Office Online

Désactivez Ouvrir avec Office Online depuis Admin control panel (Panneau de configuration d'administration).

1. Sous My account (Mon compte), choisissez Open admin control panel (Ouvrir le panneau de configuration d'administration).
2. Pour Office Online, choisissez Change (Modifier).
3. Décochez la case Enable Office Online (Activer Office Online), puis choisissez Save (Enregistrer).

Migration de fichiers vers WorkDocs

WorkDocs les administrateurs peuvent utiliser le service de WorkDocs migration pour effectuer une migration à grande échelle de plusieurs fichiers et dossiers vers leur WorkDocs site. Le service de WorkDocs migration fonctionne avec Amazon Simple Storage Service (Amazon S3). Cela vous permet de migrer les partages de fichiers départementaux et les partages de fichiers sur le disque principal ou les partages de fichiers utilisateur vers WorkDocs.

Au cours de ce processus, WorkDocs fournit une politique AWS Identity and Access Management (IAM) pour vous. Utilisez cette politique pour créer un nouveau rôle IAM qui accorde l'accès au service de WorkDocs migration pour effectuer les opérations suivantes :

- Lisez et listez le compartiment Amazon S3 que vous désignez.
- Lisez et écrivez WorkDocs sur le site que vous désignez.

Exécutez les tâches suivantes pour migrer vos fichiers et dossiers vers WorkDocs. Avant de commencer, vérifiez que vous disposez des autorisations suivantes :

- Autorisations d'administrateur pour votre WorkDocs site
- Autorisations pour créer un rôle IAM

Si votre WorkDocs site est configuré dans le même répertoire que votre WorkSpaces flotte, vous devez respecter les exigences suivantes :

- N'utilisez pas Admin pour le nom d'utilisateur de votre WorkDocs compte. Admin est un rôle d'utilisateur réservé dans WorkDocs.
- Le type d'utilisateur de votre WorkDocs administrateur doit être Upgraded WS User. Pour plus d'informations, consultez Présentation des rôles utilisateur et Modification d'utilisateurs.

> **Note**
>
> La structure des répertoires, les noms de fichiers et le contenu des fichiers sont préservés lors de la migration vers. WorkDocs La propriété des fichiers et les autorisations ne sont pas préservées.

Tâches

Étape 1 : Préparation du contenu pour la migration

Pour préparer votre contenu en vue de la migration

1. Sur votre WorkDocs site, sous Mes documents, créez un dossier vers lequel vous souhaitez migrer vos fichiers et dossiers.
2. Assurez-vous des points suivants :
   - Le dossier source ne contient pas plus de 100 000 fichiers et sous-dossiers. Les migrations échouent si vous dépassez cette limite.
   - Aucun fichier individuel ne dépasse 5 To.
   - Chaque nom de fichier contient 255 caractères ou moins. WorkDocs Drive affiche uniquement les fichiers dont le chemin de répertoire complet est inférieur ou égal à 260 caractères.

> **Warning**
>
> Les tentatives de migration de fichiers ou de dossiers avec des noms contenant les caractères suivants peuvent entraîner des erreurs et mettre fin au processus de migration. Si cela se produit, choisissez Download report (Télécharger le rapport) pour télécharger un journal qui répertorie les erreurs, les fichiers n'ayant pas pu être migrés et les fichiers migrés avec succès.

- Espaces de fin — Par exemple : un espace supplémentaire à la fin du nom d'un fichier.
- Périodes au début ou à la fin : par exemple : `.file.file.ppt`, `.`, `..`, ou `file.`
- Tildes au début ou à la fin — Par exemple : `file.doc~~file.doc`, ou `~$file.doc`
- Noms de fichiers se terminant par `.tmp` — Par exemple : `file.tmp`

- Les noms de fichiers correspondent exactement à ces termes qui distinguent les majuscules des minuscules : `Microsoft User DataOutlook files`,`Thumbs.db`, ou `Thumbnails`
- Noms de fichiers contenant l'un des caractères suivants : `*` (astérisque), `/` (barre oblique avant), `\` (barre oblique arrière), `:` (deux-points), (inférieur à), < (supérieur à), > (point d'interrogation), `?` (barre verticale/tube), `|` (guillemets doubles) ou `"` `\202E` (code de caractère 202E).

Étape 2 : Chargement de fichiers sur Amazon S3

Pour charger des fichiers sur Amazon S3

1. Créez un nouveau compartiment Amazon Simple Storage Service (Amazon S3) dans AWS votre compte dans lequel vous souhaitez télécharger vos fichiers et dossiers. Le compartiment Amazon S3 doit se trouver dans le même AWS compte et dans la même AWS région que votre WorkDocs site. Pour plus d'informations, consultez Getting started with Amazon Simple Storage Service dans le guide de l'utilisateur d'Amazon Simple Storage Service.
2. Téléchargez vos fichiers dans le compartiment Amazon S3 que vous avez créé à l'étape précédente. Nous vous recommandons AWS DataSync de l'utiliser pour charger vos fichiers et dossiers dans le compartiment Amazon S3. DataSync fournit des fonctionnalités supplémentaires de suivi, de création de rapports et de synchronisation. Pour plus d'informations, consultez les sections AWS DataSync Fonctionnement et Utilisation des politiques basées sur l'identité (politiques IAM) DataSync dans le Guide de l'AWS DataSync utilisateur.

Étape 3 : Planification d'une migration

Après avoir effectué les étapes 1 et 2, utilisez le service de WorkDocs migration pour planifier la migration. Le service de migration peut prendre jusqu'à une semaine pour traiter votre demande de migration et vous envoyer un e-mail indiquant que vous pouvez commencer votre migration. Si vous lancez la migration avant de recevoir l'e-mail, la console de gestion affiche un message vous demandant d'attendre.

Lorsque vous planifiez la migration, le paramètre de stockage de votre compte WorkDocs utilisateur passe automatiquement à Illimité.

> **Note**
>
> La migration de fichiers qui dépassent votre limite WorkDocs de stockage peut entraîner des coûts supplémentaires. Pour plus d'informations, consultez Tarification d'WorkDocs .

Le service de WorkDocs migration fournit une politique AWS Identity and Access Management (IAM) que vous pouvez utiliser pour la migration. Avec cette politique, vous créez un nouveau rôle IAM qui accorde au service de WorkDocs migration l'accès au compartiment Amazon S3 et au WorkDocs site que vous désignez. Vous vous abonnez également aux notifications par e-mail d'Amazon SNS pour recevoir des mises à jour lorsque votre demande de migration est planifiée, ainsi que lorsqu'elle commence et se termine.

Pour planifier une migration

1. Dans la WorkDocs console, choisissez Apps, Migrations.
   - Si c'est la première fois que vous accédez au service de WorkDocs migration, vous êtes invité à vous abonner aux notifications par e-mail Amazon SNS. Abonnez-vous, confirmez dans l'e-mail que vous recevez, puis choisissez Continue (Continuer).
2. Choisissez Create Migration (Créer une migration.
3. Pour Source Type (Type de source), choisissez Amazon S3.
4. Choisissez Suivant.
5. Pour Source de données et validation, sous Exemple de politique, copiez la stratégie IAM fournie.
6. Utilisez la stratégie IAM que vous avez copiée à l'étape précédente pour créer une nouvelle stratégie et un nouveau rôle IAM, comme suit :
   a. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
   b. Choisissez Stratégies, Créer une stratégie.
   c. Choisissez JSON et collez la politique IAM que vous avez copiée précédemment dans votre presse-papiers.
   d. Choisissez Examiner une politique. Entrez un nom de stratégie et une description.
   e. Choisissez Create Policy (Créer une politique).
   f. Choisissez Roles (Rôles), Create role (Créer un rôle).
   g. Choisissez Autre compte AWS. Pour ID de compte, entrez l'une des valeurs suivantes :

- Pour la région USA Est (Virginie du Nord), entrez `899282061130`
- Pour la région USA Ouest (Oregon), entrez `814301586344`
- Pour la région Asie-Pacifique (Singapour), entrez `900469912330`
- Pour la région Asie-Pacifique (Sydney), entrez `031131923584`
- Pour la région Asie-Pacifique (Tokyo), entrez `178752524102`
- Pour la région Europe (Irlande), entrez `191921258524`

h. Sélectionnez la nouvelle stratégie que vous avez créée précédemment, puis choisissez Suivant : Vérification. Si vous ne voyez pas cette nouvelle stratégie, sélectionnez l'icône d'actualisation.

i. Saisissez un nom de rôle et une description. Choisissez Créer un rôle.

j. Sur la page Rôles, sous Nom du rôle, sélectionnez le rôle que vous venez de créer.

k. Sur la page Résumé, définissez la durée maximale de CLI/API session sur 12 heures.

l. Copiez l'ARN de rôle dans votre presse-papiers pour l'utiliser à l'étape suivante.

7. Retournez au service de WorkDocs migration. Pour Source de données et validation, sous ARN du rôle, collez l'ARN du rôle à partir du rôle IAM que vous avez copié à l'étape précédente.
8. Pour Bucket, sélectionnez le compartiment Amazon S3 à partir duquel migrer les fichiers.
9. Choisissez Suivant.
10. Pour Sélectionner un WorkDocs dossier de destination, sélectionnez le dossier de destination WorkDocs vers lequel migrer les fichiers.
11. Choisissez Suivant.
12. Sous Review (Vérification), dans Title (Titre), entrez un nom pour la migration.
13. Sélectionnez la date et l'heure de la migration.
14. Sélectionnez Send (Envoyer).

Étape 4 : Suivi d'une migration

Vous pouvez suivre votre migration depuis la page d'accueil du service de WorkDocs migration. Pour accéder à la page d'accueil depuis le WorkDocs site, sélectionnez Applications, Migrations. Choisissez votre migration pour afficher ses détails et suivre sa progression. Vous pouvez également choisir Cancel Migration (Annuler la migration) si vous devez l'annuler, ou Update (Mettre à jour) pour mettre à jour à chronologie pour la migration. Une fois qu'une migration est terminée, vous pouvez

choisir Download report (Télécharger le rapport) pour télécharger un journal répertoriant les fichiers migrés avec succès, les échecs et les erreurs.

Les états de migration suivants fournissent le statut de votre migration:

Planifié

La migration est planifiée mais pas démarrée. Vous pouvez annuler des migrations ou mettre à jour des heures de démarrage de migration jusqu'à cinq minutes avant l'heure de démarrage planifiée.

Migrating

La migration est en cours.

Réussite

La migration est terminée.

Partial Success (Succès partiel)

La migration est partiellement terminée. Pour plus de détails, affichez le récapitulatif de migration et téléchargez le rapport fourni.

Échec

La migration a échoué. Pour plus de détails, affichez le récapitulatif de migration et téléchargez le rapport fourni.

Annulé

La migration est annulée.

Étape 5 : Nettoyage des ressources

Lorsque votre migration est terminée, supprimez la politique de migration et le rôle que vous avez créés à partir de la console IAM.

Pour supprimer la politique et le rôle IAM

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Choisissez Stratégies.
3. Recherchez et choisissez la stratégie que vous avez créée.

4. Pour Policy actions (Actions de stratégie), choisissez Delete (Supprimer).
5. Sélectionnez Delete (Supprimer).
6. Sélectionnez Roles (Rôles).
7. Recherchez et choisissez le rôle que vous avez créé.
8. Choisissez Delete role (Supprimer le rôle), Delete (Supprimer).

Lorsqu'une migration planifiée démarre, le paramètre de stockage de votre compte WorkDocs utilisateur passe automatiquement à Illimité. Après la migration, vous pouvez utiliser le panneau de configuration d'administration pour modifier ce paramètre. Pour de plus amples informations, veuillez consulter Modification d'utilisateurs.

Résolution des problèmes rencontrés avec WorkDocs

Les informations suivantes peuvent vous aider à résoudre les problèmes liés à WorkDocs.

Problèmes

Impossible de configurer mon WorkDocs site dans une AWS région spécifique

Si vous configurez un nouveau WorkDocs site, sélectionnez la région AWS lors de la configuration. Pour en savoir plus, consultez le didacticiel en rapport avec votre cas d'utilisation spécifique sous Commencer avec WorkDocs.

Je souhaite configurer mon WorkDocs site dans un Amazon VPC existant

Lorsque vous configurez votre nouveau WorkDocs site, créez un répertoire à l'aide du cloud privé virtuel (VPC) existant. WorkDocs utilise ce répertoire pour authentifier les utilisateurs.

Les utilisateurs doivent réinitialiser leur mot de passe

Les utilisateurs peuvent réinitialiser leur mot de passe en choisissant Forgot password? (Mot de passe oublié ?) sur leur écran de connexion.

Un utilisateur a partagé par erreur un document sensible

Pour révoquer l'accès au document, choisissez Share by invite (Partager par invitation) en regard du document, puis supprimez les utilisateurs qui ne doivent plus avoir accès. Si le document a été partagé au moyen d'un lien, choisissez Share a link (Partager un lien), puis désactivez ce lien.

L'utilisateur a quitté l'organisation et n'a pas transféré la propriété du document

Transférez la propriété d'un document à un autre utilisateur dans le panneau de configuration d'administration. Pour de plus amples informations, veuillez consulter Transfert de la propriété d'un document.

Nécessité de déployer WorkDocs Drive ou WorkDocs Companion sur plusieurs utilisateurs

Pour effectuer un déploiement à l'intention de plusieurs utilisateurs au sein d'une entreprise, utilisez une stratégie de groupe. Pour de plus amples informations, veuillez consulter Gestion des identités et des accès pour Amazon WorkDocs. Pour obtenir des informations spécifiques sur le déploiement de WorkDocs Drive auprès de plusieurs utilisateurs, consultezDéploiement de WorkDocs Drive sur plusieurs ordinateurs.

La modification en ligne est inopérante

Vérifiez que WorkDocs Companion est installé sur votre ordinateur. Pour installer WorkDocs Companion, consultez la section Applications et intégrations pour WorkDocs.

Gestion WorkDocs pour Amazon Business

Si vous êtes administrateur d' WorkDocs Amazon Business, vous pouvez gérer les utilisateurs en vous connectant à https://workdocs.aws/ à l'aide de vos informations d'identification Amazon Business.

Pour inviter un nouvel utilisateur WorkDocs à rejoindre Amazon Business

1. Connectez-vous avec vos informations d'identification Amazon Business à l'adresse https://workdocs.aws/.
2. Sur la WorkDocs page d'accueil d'Amazon Business, ouvrez le volet de navigation sur la gauche.
3. Choisissez Admin Settings (Paramètres d'administration).
4. Choisissez Add people (Ajouter des personnes).
5. Pour Recipients (Destinataires), entrez les adresses e-mail ou les noms d'utilisateur des utilisateurs à inviter.
6. (Facultatif) Personnalisez le message d'invitation.
7. Sélectionnez Exécuté.

Pour rechercher un utilisateur sur WorkDocs Amazon Business

1. Connectez-vous avec vos informations d'identification Amazon Business à l'adresse https://workdocs.aws/.
2. Sur la WorkDocs page d'accueil d'Amazon Business, ouvrez le volet de navigation sur la gauche.
3. Choisissez Admin Settings (Paramètres d'administration).
4. Pour Search users (Rechercher des utilisateurs), entrez le prénom de l'utilisateur et appuyez sur **`Enter`**.

Pour sélectionner des rôles d' WorkDocs utilisateur sur Amazon Business

1. Connectez-vous avec vos informations d'identification Amazon Business à l'adresse https://workdocs.aws/.
2. Sur la WorkDocs page d'accueil d'Amazon Business, ouvrez le volet de navigation sur la gauche.
3. Choisissez Admin Settings (Paramètres d'administration).
4. Sous People (Personnes), en regard de l'utilisateur, sélectionnez le rôle à attribuer à l'utilisateur.

Pour supprimer un WorkDocs utilisateur sur Amazon Business

1. Connectez-vous avec vos informations d'identification Amazon Business à l'adresse https://workdocs.aws/.
2. Sur la WorkDocs page d'accueil d'Amazon Business, ouvrez le volet de navigation sur la gauche.
3. Choisissez Admin Settings (Paramètres d'administration).
4. Sous People (Personnes), choisissez l'ellipse (...) en regard de l'utilisateur.
5. Sélectionnez Delete (Supprimer).
6. Si vous y êtes invité, entrez un nouvel utilisateur vers lequel transférer les fichiers de l'utilisateur, puis choisissez Delete (Supprimer).

Adresse IP et domaines à ajouter à votre liste d'autorisations

Si vous implémentez le filtrage IP sur les appareils qui y accèdent WorkDocs, ajoutez les adresses IP et les domaines suivants à votre liste d'autorisations. Cela permet WorkDocs à WorkDocs Drive de se connecter au WorkDocs service.

- zocalo.ap-northeast-1.amazonaws.com
- zocalo.ap-southeast-2.amazonaws.com
- zocalo.eu-west-1.amazonaws.com
- zocalo.eu-central-1.amazonaws.com
- zocalo.us-east-1.amazonaws.com
- zocalo. us-gov-west-1. amazonaws.com
- zocalo.us-west-2.amazonaws.com
- awsapps.com
- amazonaws.com
- cloudfront.net
- aws.amazon.com
- amazonworkdocs.com
- console.aws.amazon.com
- cognito-identity.us-east-1.amazonaws.com
- firehose.us-east-1.amazonaws.com

Si vous souhaitez utiliser des plages d'adresses IP, consultez la section Plages d'adresses AWS IP dans la référence AWS générale.

Historique du document

Le tableau suivant décrit les modifications importantes apportées au guide d' WorkDocs administration Amazon à compter de février 2018. Pour recevoir les notifications des mises à jour de cette documentation, abonnez-vous à un flux RSS.

Modification	Description	Date
Nouvelles autorisations du propriétaire du fichier	Les administrateurs peuvent désormais fournir les autorisations de suppression de version et de restauration de version. Les autorisations font partie de la publication de l'DeleteDocumentVersionAPI.	29 juillet 2022
WorkDocs Sauvegarde	Suppression de la documentation WorkDocs Backup du guide d' WorkDocs administration Amazon car le composant n'est plus pris en charge.	24 juin 2021
Gestion WorkDocs pour Amazon Business	WorkDocs for Amazon Business prend en charge la gestion des utilisateurs par les administrateurs. Pour plus d'informations, consultez Managing WorkDocs for Amazon Business dans le guide d' WorkDocs administration Amazon.	26 mars 2020
Migration de fichiers vers Amazon WorkDocs	WorkDocs les administrateurs peuvent utiliser le service de WorkDocs migration pour effectuer une migration à	8 août 2019

	grande échelle de plusieurs fichiers et dossiers vers leur WorkDocs site. Pour plus d'informations, consultez la section Migration de fichiers vers WorkDocs le guide d' WorkDocs administration Amazon.	
Paramètres de la liste d'adresses IP autorisées	Les paramètres de la liste d'adresses IP autorisées sont disponibles pour filtrer l'accès à votre WorkDocs site par plage d'adresses IP. Pour plus d'informations, consultez la section Paramètres des listes d'adresses IP autorisées dans le Guide WorkDocs d'adminis tration Amazon.	22 octobre 2018
Hancom ThinkFree	Hancom ThinkFree est disponible. Les utilisateurs peuvent créer et modifier des fichiers Microsoft Office de manière collaborative à partir de l'application WorkDocs Web. Pour plus d'informations, consultez la section Enabling Hancom ThinkFree dans le guide d' WorkDocs administr ation Amazon.	21 juin 2018

Ouvrir avec Office Online	Ouvrir avec Office Online est disponible. Les utilisateurs peuvent modifier des fichiers Microsoft Office de manière collaborative à partir de l'application WorkDocs Web. Pour plus d'informations, consultez la section Activation d'Open with Office Online dans le guide d' WorkDocs administration Amazon.	6 juin 2018
Dépannage	Ajout d'une rubrique de dépannage. Pour plus d'informations, consultez la section Résolution WorkDocs des problèmes dans le Guide WorkDocs d'administration Amazon.	23 mai 2018
Modifier la période de conservation du bac de récupération	La période de conservation de la corbeille de récupération peut être modifiée. Pour plus d'informations, consultez la section Paramètres de rétention du bac de récupération dans le guide WorkDocs d'administration Amazon.	27 février 2018