aws

Guide d’administration

# Amazon WorkDocs

# Amazon WorkDocs: Guide d’administration

# Table of Contents


..... vi
Qu'est-ce qu'Amazon WorkDocs ? ..... 1
Accès à Amazon WorkDocs ..... 1
Tarification ..... 2
Comment démarrer ..... 2
Prérequis ..... 3
S'inscrire à un Compte AWS ..... 3
Création d'un utilisateur administratif ..... 3
Sécurité ..... 5
Gestion des identités et des accès ..... 6
Public ciblé ..... 6
Authentification par des identités ..... 7
Gestion des accès à l'aide de politiques ..... 10
Comment Amazon WorkDocs travaille avec IAM ..... 13
Exemples de politiques basées sur l'identité ..... 16
Résolution des problèmes ..... 21
Journalisation et surveillance ..... 23
Exportation du flux d'activité à l'échelle du site ..... 23
CloudTrail journalisation ..... 24
Validation de conformité ..... 27
Résilience ..... 29
Sécurité de l'infrastructure ..... 29
Premiers pas ..... 30
Création d'un WorkDocs site Amazon ..... 31
Avant de commencer ..... 31
Création d'un WorkDocs site Amazon ..... 31
Activation de l'authentification unique ..... 34
Activation de l'authentification multi-facteurs ..... 34
Promotion d'un utilisateur en tant qu'administrateur ..... 35
Gérer Amazon WorkDocs depuis la AWS console ..... 36
Configuration des administrateurs du site ..... 36
Renvoyer des e-mails d'invitation ..... 36
Gestion de l'authentification multifactorielle ..... 37
Configuration des URL du site ..... 37

Gestion des notifications ... 38
Suppression d'un site ... 39
Gérer Amazon WorkDocs depuis le panneau de configuration d'administration du site ... 41
Déploiement d'Amazon WorkDocs Drive sur plusieurs ordinateurs ... 50
Invitation et gestion des utilisateurs ... 51
Rôles utilisateur ... 52
Démarrage du panneau de configuration d'administration ... 53
Désactivation de l'activation automatique ... 54
Gestion du partage de liens ... 54
Contrôle des invitations utilisateur avec l'activation automatique activée ... 55
Invitation de nouveaux utilisateurs ... 56
Modification d'utilisateurs ... 57
Désactivation d'utilisateurs ... 58
Suppression des utilisateurs en attente ... 59
Transfert de la propriété d'un document ... 59
Téléchargement de listes d'utilisateurs ... 60
Partage et collaboration ... 62
Partage de liens ... 62
Partage par invitation ... 63
Partage externe ... 63
Autorisations ... 64
Rôles utilisateurs ... 64
Autorisations pour les dossiers partagés ... 65
Autorisations pour les fichiers contenus dans des dossiers partagés ... 66
Autorisations pour les fichiers ne figurant pas dans des dossiers partagés ... 69
Activation de l'édition collaborative ... 70
Activation de Hancom ThinkFree ... 70
Activation d'Ouvrir avec Office Online ... 71
Migration de fichiers ... 73
Étape 1 : Préparation du contenu pour la migration ... 74
Étape 2 : Chargement de fichiers sur Amazon S3 ... 75
Étape 3 : Planification d'une migration ... 75
Étape 4 : Suivi d'une migration ... 77
Étape 5 : Nettoyage des ressources ... 78
Résolution des problèmes ... 80
Impossible de configurer mon Amazon WorkDocs site dans unAWSRégion ... 80

Je veux configurer mon Amazon WorkDocs site dans un Amazon VPC existant ..... 80
Les utilisateurs doivent réinitialiser leur mot de passe ..... 80
Un utilisateur a partagé par erreur un document sensible ..... 81
L'utilisateur a quitté l'organisation et n'a pas transféré la propriété du document ..... 81
Nécessité de déployer Amazon WorkDocs Drive ou Amazon WorkDocs Accessoire pour plusieurs utilisateurs ..... 81
La modification en ligne est inopérante ..... 41
Gestion d'Amazon WorkDocs pour Amazon Business ..... 82
Adresse IP et domaines à ajouter à votre liste d'autorisation ..... 84
Historique du document ..... 85
Glossaire AWS ..... 88

Vous devez être un administrateur WorkDocs système Amazon pour suivre les étapes de ce guide. Si vous avez besoin d'aide pour utiliser Amazon WorkDocs, consultez Getting started with Amazon WorkDocs dans le guide de WorkDocs l'utilisateur Amazon.

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 Amazon peuvent être utilisées pour visualiser de nombreux types de fichiers, en fonction du type de support Internet du fichier. Amazon WorkDocs prend en charge tous les formats de documents et d'images courants, et la prise en charge de types de supports supplémentaires est constamment ajoutée.

Pour plus d'informations, consultez Amazon WorkDocs.

## Accès à Amazon WorkDocs

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

Les utilisateurs non administratifs utilisent les applications clientes pour accéder à leurs fichiers. Ils n'utilisent jamais la WorkDocs console Amazon ni le tableau de bord d'administration. Amazon 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.
- Amazon WorkDocs Drive, une application qui synchronise un dossier sur votre bureau macOS ou Windows avec vos WorkDocs fichiers Amazon.

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

- Commencer à utiliser Amazon WorkDocs
- Travailler avec des fichiers
- Travailler avec des dossiers

## Tarification

Avec Amazon WorkDocs, il n'y a aucun frais initial ni aucun engagement. 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 à utiliser Amazon WorkDocs, consultezCréation d'un WorkDocs site Amazon.

# Conditions préalables pour Amazon WorkDocs

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

## S'inscrire à un Compte AWS

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

Pour s'inscrire à un Compte AWS

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

   Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

   Lorsque vous souscrivez à un Compte AWS, un Utilisateur racine d'un compte AWS est créé. Par défaut, seul l'utilisateur root 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 administratif, et à uniquement utiliser l'utilisateur root pour effectuer tâches nécessitant un accès utilisateur root.

AWS vous envoie un e-mail de confirmation lorsque le processus d'inscription est terminé. Vous pouvez afficher l'activité en cours de votre compte et gérer votre compte à tout moment en accédant à https://aws.amazon.com/ et en cliquant sur Mon compte.

## Création d'un utilisateur administratif

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

Sécurisation de votre Utilisateur racine d'un compte AWS

1. Connectez-vous à la AWS Management Console en tant que propriétaire du compte en sélectionnant Root user (utilisateur root) et en saisissant l'adresse e-mail de Compte AWS. Sur la page suivante, saisissez votre mot de passe.

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

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

   Pour obtenir des instructions, consultez Activation d'un dispositif MFA virtuel pour l'utilisateur root de votre Compte AWS (console) dans le Guide de l'utilisateur IAM.

### Création d'un utilisateur administratif

1. Activez IAM Identity Center.

   Pour obtenir des instructions, consultez Configuration 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 administratif.

   Pour profiter d'un didacticiel sur l'utilisation du Répertoire IAM Identity Center comme source d'identité, consultez Configuration de l'accès utilisateur avec le répertoire Répertoire IAM Identity Center par défaut dans le Guide de l'utilisateur AWS IAM Identity Center.

### Connexion en tant qu'utilisateur 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 à l'aide d'un utilisateur IAM Identity Center, consultez Connexion au portail d'accès AWS dans le Guide de l'utilisateur Connexion à AWS.

# Sécurité sur Amazon WorkDocs

Chez AWS, la sécurité dans le cloud est notre priorité numéro 1. En tant que client AWS, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des organisations les plus pointilleuses en termes de sécurité.

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

- Sécurité du cloud : AWS est responsable de la protection de l'infrastructure qui exécute des services AWS dans le cloud AWS. AWS vous fournit également les 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 conformité AWS. Pour en savoir plus sur les programmes de conformité applicables à Amazon WorkDocs, consultez la section AWSServices 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 l'utilisation d'Amazon 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 configurer Amazon pour WorkDocs 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 Amazon.

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

Rubriques


- Public ciblé
- Authentification par des identités
- Gestion des accès à l'aide de politiques
- Comment Amazon WorkDocs travaille avec IAM
- Exemples de politiques WorkDocs basées sur l'identité d'Amazon
- Résolution des problèmes d' WorkDocs identité et d'accès à Amazon


## Public ciblé

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

Utilisateur du service — Si vous utilisez le WorkDocs service Amazon 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 plus en plus de WorkDocs fonctionnalités Amazon 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 parvenez pas à accéder à une fonctionnalité d'Amazon WorkDocs, consultezRésolution des problèmes d' WorkDocs identité et d'accès à Amazon.

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

de déterminer à quelles WorkDocs fonctionnalités et ressources Amazon les utilisateurs de vos services 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 Amazon WorkDocs, consultezComment Amazon WorkDocs travaille avec IAM.

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

## Authentification par des identités

L'authentification correspond au processus par lequel vous vous connectez à AWS avec vos informations d'identification. Vous devez vous authentifier (être connecté à AWS) en tant qu'Utilisateur racine d'un compte AWS, en tant qu'utilisateur IAM ou en endossant un rôle IAM.

Vous pouvez vous connecter à AWS en tant qu'identité fédérée à l'aide des informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAM Identity Center), l'authentification de connexion 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 en utilisant la fédération, vous endossez indirectement un rôle.

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

Si vous accédez à AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes en utilisant vos informations d'identification. Si vous n'utilisez pas les outils AWS, vous devez signer les requêtes vous-même. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer des demandes vous-même, consultez Signature des demandes d'API AWS 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, AWS vous recommande d'utiliser

l'authentification multifactorielle (MFA) pour améliorer la sécurité de votre compte. Pour en savoir plus, veuillez consulter Authentification multifactorielle dans le Guide de l'utilisateur AWS IAM Identity Center et Utilisation de l'authentification multifactorielle (MFA) dans l'interface AWS dans le Guide de l'utilisateur IAM.

## Utilisateurs et groupes IAM

Un utilisateur IAM est une identité dans votre Compte AWS qui dispose d'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 tels que les 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 de faire pivoter les 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 avoir un groupe nommé IAMAdmins et accorder à ce groupe les autorisations d'administrer des 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 en savoir plus, consultez Quand créer un utilisateur IAM (au lieu d'un rôle) dans le Guide de l'utilisateur IAM.

## Rôles IAM

Un rôle IAM est une entité au sein de votre Compte AWS qui dispose d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Vous pouvez temporairement endosser un rôle IAM dans la AWS Management Console en changeant de rôle. Vous pouvez obtenir un rôle en appelant une opération d'API AWS CLI ou AWS à l'aide d'une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez Utilisation de rôles IAM 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, certains Services AWS vous permettent d'attacher une politique directement à une ressource (au lieu d'utiliser un rôle en tant que proxy). Pour en savoir plus sur la différence entre les rôles et les politiques basées sur les ressources pour l'accès intercompte, consultez Différence entre les rôles IAM et les politiques basées sur les ressources dans le Guide de l'utilisateur IAM.
- Accès interservices : certains Services AWS utilisent des fonctions 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, une fonction du service ou un rôle lié au service.
  - Forward access sessions (FAS) – Lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions dans AWS, vous êtes considéré comme un principal. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui déclenche une autre action dans un autre service. FAS utilise les autorisations du principal appelant Service AWS, combinées à la demande Service AWS pour effectuer des demandes aux services en aval. Les demandes de FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres 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 la politique relative à la transmission de demandes FAS, consultez Sessions de transmission d'accès.
  - Fonction du 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 une fonction du 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 au service – Un rôle lié au service est un type de fonction du 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 s'affichent dans votre Compte AWS et sont détenus par le service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

- Applications s'exécutant sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer des informations d'identification temporaires pour les applications s'exécutant sur une instance EC2 et effectuant des demandes d'API AWS CLI ou AWS. Cette solution est préférable au stockage des clés d'accès au sein de l'instance EC2. Pour attribuer un rôle AWS à une instance EC2 et le rendre disponible à toutes les applications associées, vous pouvez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes qui s'exécutent sur l'instance EC2 d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utilisation d'un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des instances Amazon EC2 dans le Guide de l'utilisateur IAM.

Pour savoir dans quel cas utiliser des rôles ou des utilisateurs IAM, consultez Quand créer un rôle IAM (au lieu d'un utilisateur) dans le Guide de l'utilisateur IAM.

## Gestion des accès à l'aide de politiques

Vous contrôlez les accès dans AWS en créant des politiques et en les attachant à des identités AWS ou à des ressources. Une politique est un objet dans AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit les autorisations de ces dernières. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur racine ou séance de rôle) envoie une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées dans AWS en tant que documents JSON. Pour plus d'informations sur la structure et le contenu des documents de politique JSON, consultez Présentation des politiques JSON dans le Guide de l'utilisateur IAM.

Les administrateurs peuvent utiliser les politiques JSON AWS 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 avec cette politique peut obtenir des informations utilisateur à partir de la AWS Management Console, de la AWS CLI ou de l'API AWS.

### 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 Création de politiques IAM 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 attacher à plusieurs utilisateurs, groupes et rôles dans votre Compte AWS. Les politiques gérées incluent les politiques gérées par AWS 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. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment Amazon S3. 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 des Services AWS.

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

## Listes de contrôle d'accès (ACL)

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

Amazon S3, AWS WAF et Amazon VPC sont des exemples de services prenant en charge les ACL. Pour en savoir plus sur les listes de contrôle d'accès, consultez Présentation des listes 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 courantes. 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 fonction 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 qui en résultent 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 remplace 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 (SCP) - les SCP sont des politiques JSON qui spécifient le nombre maximal d'autorisations pour une organisation ou une unité d'organisation (OU) dans AWS Organizations. AWS Organizations est un service qui vous permet de regrouper et de gérer de façon centralisée plusieurs Comptes AWS détenus par votre entreprise. Si vous activez toutes les fonctions d'une organisation, vous pouvez appliquer les politiques de contrôle des services (SCP) à l'un ou à l'ensemble de vos comptes. La SCP limite les autorisations pour les entités dans les comptes membres, y compris dans chaque Utilisateur racine d'un compte AWS. Pour plus d'informations sur les organisations et les SCP, consultez Fonctionnement des SCP dans le Guide de l'utilisateur AWS Organizations.
- 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 la séance obtenue 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 remplace l'autorisation. Pour plus d'informations, consultez Politiques de séance dans le Guide de l'utilisateur IAM.

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

### Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations obtenues sont plus compliquées à comprendre. Pour découvrir la façon dont AWS détermine s'il convient d'autoriser une demande en présence de plusieurs types de politiques, veuillez consulter Logique d'évaluation de politiques dans le Guide de l'utilisateur IAM.

## Comment Amazon WorkDocs travaille avec IAM

Avant d'utiliser IAM pour gérer l'accès à Amazon WorkDocs, vous devez comprendre quelles fonctionnalités IAM peuvent être utilisées avec Amazon. WorkDocs Pour obtenir une vue d'ensemble de la manière dont Amazon WorkDocs et les autres AWS services fonctionnent avec IAM, consultez la section AWSServices compatibles avec IAM dans le Guide de l'utilisateur d'IAM.

Rubriques

- Politiques basées sur WorkDocs l'identité d'Amazon
- Politiques basées sur WorkDocs les ressources d'Amazon
- Autorisation basée sur les WorkDocs tags Amazon
- Rôles Amazon WorkDocs IAM

### Politiques basées sur WorkDocs l'identité d'Amazon

Vous pouvez préciser les actions autorisées ou refusées grâce aux stratégies basées sur les identités IAM. Amazon 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 JSON AWS 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 politique possèdent généralement le même nom que l'opération d'API AWS 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 stratégie afin d'accorder l'autorisation d'exécuter les opérations associées.

Les actions politiques sur Amazon WorkDocs utilisent le préfixe suivant avant l'action :`workdocs:`. Par exemple, pour autoriser quelqu'un à exécuter l'opération d' WorkDocs `DescribeUsers`API Amazon, vous devez inclure l'`workdocs:DescribeUsers`action dans sa politique. Les déclarations de politique doivent inclure un élément `Action` ou `NotAction`. Amazon WorkDocs définit son propre ensemble d'actions décrivant 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 Amazon, consultez la section Actions définies par Amazon WorkDocs dans le guide de l'utilisateur IAM.

Ressources

Amazon WorkDocs ne prend pas en charge la spécification des ARN des ressources dans une politique.

Clés de condition

Amazon WorkDocs ne fournit aucune clé de condition spécifique à un service, mais prend en charge l'utilisation de certaines clés de condition globales. Pour afficher toutes les clés de condition globales AWS, consultez Clés de contexte de condition globale AWS dans le Guide de l'utilisateur IAM.

Exemples

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

## Politiques basées sur WorkDocs les ressources d'Amazon

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

## Autorisation basée sur les WorkDocs tags Amazon

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

## Rôles Amazon WorkDocs IAM

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

Utilisation d'informations d'identification temporaires avec Amazon 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 STSAPI telles que AssumeRoleou GetFederationToken.

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

Rôles liés à un service

Les rôles liés à un service permettent aux services AWS d'accéder à des ressources dans 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.

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

Fonctions du 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 fonctions du 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.

Amazon 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 à modifier des WorkDocs ressources Amazon. Ils ne peuvent pas non plus exécuter des tâches à l'aide de AWS Management Console, AWS CLI ou de l'API AWS. 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 WorkDocs console Amazon
- Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations
- Autoriser les utilisateurs à accéder en lecture seule aux ressources Amazon WorkDocs
- Autres exemples de politiques WorkDocs basées sur l'identité d'Amazon

## Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer WorkDocs des ressources Amazon 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 :

- Démarrer avec AWS gérées et évoluez vers les autorisations de moindre privilège - Pour commencer à accorder des autorisations à vos utilisateurs et charges de travail, utilisez les politiques gérées AWS qui accordent des autorisations dans de nombreux cas d'utilisation courants. Elles sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client AWS qui sont spécifiques à vos cas d'utilisation. Pour de plus amples informations, consultez AWS Politiques gérées ou AWS Politiques gérées pour les activités professionnelles dans le Guide de l'utilisateur IAM.
- Accorder 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.
- Utiliser 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 via un Service AWS spécifique, comme AWS CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez IAM Access Analyzer pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles - IAM Access Analyzer 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 politique IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Authentification multifactorielle (MFA) nécessaire : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root dans votre Compte AWS, activez l'authentification multifactorielle pour une sécurité renforcée. Pour exiger le MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Configuration de l'accès aux API protégé par 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 WorkDocs console Amazon

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 Amazon 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 Amazon, 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
- Amazon EC2 FullAccess

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

Vous n'avez pas besoin d'accorder les autorisations minimales de console pour les utilisateurs qui effectuent des appels uniquement à AWS CLI ou à l'API AWS. 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 nécessaires pour réaliser cette action sur la console ou par programmation à l'aide de l'AWS CLI ou de l'API 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 en lecture seule aux ressources Amazon WorkDocs

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

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

```
                "ec2:DescribeSubnets"
            ],
            "Resource": "*"
        }
    ]
}
```

### Autres exemples de politiques WorkDocs basées sur l'identité d'Amazon

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

## Résolution des problèmes d' WorkDocs identité et d'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 Amazon WorkDocs et IAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action sur Amazon 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 Amazon

### Je ne suis pas autorisé à effectuer une action sur Amazon WorkDocs

Si la AWS Management Console indique que vous n'êtes pas autorisé à exécuter 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 un message d'erreur indiquant que vous n'êtes pas autorisé à effectuer l'`iam:PassRole`action, vos politiques doivent être mises à jour pour vous permettre de transmettre un rôle à Amazon WorkDocs.

Certains Services AWS vous permettent de transmettre un rôle existant à ce service, au lieu de créer une nouvelle fonction du service ou 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 effectuer une action sur Amazon WorkDocs. Toutefois, l'action nécessite que le service ait des autorisations accordées par une fonction du 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 encore besoin d'aide, contactez votre administrateur AWS. Votre administrateur vous a fourni vos informations de connexion.

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

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 (ACL), vous pouvez utiliser ces politiques pour donner l'accès à vos ressources.

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si Amazon WorkDocs prend en charge ces fonctionnalités, consultezComment Amazon WorkDocs travaille avec IAM.
- Pour savoir comment octroyer l'accès à vos ressources à des Comptes AWS dont vous êtes propriétaire, consultez la section Fournir l'accès à un utilisateur IAM dans un autre Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.
- Pour savoir comment octroyer l'accès à vos ressources à des tiers Comptes AWS, consultez Fournir l'accès aux Comptes AWS appartenant à 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 découvrir quelle est la différence entre l'utilisation des rôles et l'utilisation des politiques basées sur les ressources pour l'accès entre comptes, consultez Différence entre les rôles IAM et les politiques basées sur les ressources 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 Amazon.

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 Amazon WorkDocs Companion. Pour installer Amazon WorkDocs Companion, consultez la section Applications et intégrations pour Amazon 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 sur Amazon WorkDocs. CloudTrail capture tous les appels d'API pour Amazon WorkDocs sous forme d'événements, y compris les appels depuis la WorkDocs console Amazon et les appels de code vers les WorkDocs API Amazon.

Si vous créez un suivi, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris des événements pour Amazon 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 Amazon dans CloudTrail

CloudTrail est activé sur votre AWS compte lorsque vous le créez. Lorsqu'une activité a lieu sur Amazon WorkDocs, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Vous pouvez afficher, rechercher et télécharger les événements récents dans votre compte AWS. 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 Amazon 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 d'activité consigne les événements de toutes les régions dans la partition AWS et livre les fichiers journaux dans le compartiment Amazon S3 de votre choix. 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. section withinPour 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 Amazon 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 effectuée par un autre service AWS.

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

## Comprendre les entrées des fichiers WorkDocs journaux Amazon

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.

Amazon 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 de l' WorkDocs annuaire Amazon.

> **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 Amazon WorkDocs : le premier enregistrement concerne une action sur le plan de contrôle et le second concerne une action sur le 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 Service AWS fait partie du champ d'application de programmes de conformité spécifiques, consultez Services AWS dans le champ d'application par programme de conformité

et choisissez le programme de conformité qui vous intéresse. Pour obtenir des renseignements généraux, consultez Programmes de conformité AWS.

Vous pouvez télécharger les rapports d'audit externes avec AWS Artifact. Pour plus d'informations, consultez Téléchargement des rapports dans AWS Artifact.

Votre responsabilité de conformité lors de l'utilisation de Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise, ainsi que par la législation et la réglementation applicables. AWS fournit les ressources suivantes pour faciliter le respect de la conformité :

- Guides Quick Start de la sécurité et de la conformité : ces guides de déploiement traitent de considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de référence dans AWS centrés sur la sécurité et la conformité.
- Architecture pour la sécurité et la conformité HIPAA sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent utiliser AWS pour créer des applications éligibles à la loi HIPAA.

  > **Note**
  >
  > Tous les Services AWS ne sont pas éligibles à HIPAA. Pour plus d'informations, consultez HIPAA Eligible Services Reference.

- Ressources de conformité AWS : cet ensemble de manuels et de guides peut s'appliquer à votre secteur d'activité et à votre emplacement.
- AWSGuides 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 de règles dans le Guide du développeur AWS Config : le service AWS Config évalue dans quelle mesure vos configurations de ressources sont conformes aux pratiques internes, aux directives sectorielles et aux réglementations.
- AWS Security Hub : ce Service AWS fournit une vue complète de votre état de sécurité dans 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.

- AWS Audit Manager : ce service Service AWS vous aide à auditer en continu votre utilisation d'AWS pour simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

## Résilience chez Amazon WorkDocs

L'infrastructure mondiale AWS s'articule autours de régions et de zones de disponibilité AWS. AWS Les régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées, reliées par un réseau à latence faible, 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 les régions et les zones de disponibilité AWS, consultez AWS Infrastructure 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 à Amazon 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 à utiliser Amazon WorkDocs

Amazon WorkDocs utilise un annuaire 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 Amazon 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 à tout moment. Pour plus d'informations à ce sujetInviter et gérer WorkDocs les utilisateurs Amazon, 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.
- Permettez WorkDocs à Amazon de travailler avec un AWS annuaire existant.
- Demandez à Amazon de WorkDocs créer un annuaire pour vous.

Vous pouvez également créer une relation d'approbation entre votre annuaire AD et un annuaire AWS Managed Microsoft AD.

> **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

- Création d'un WorkDocs site Amazon

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

# Création d'un WorkDocs site Amazon

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

Tâches

- Avant de commencer
- Création d'un WorkDocs site Amazon

## Avant de commencer

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

- Un AWS compte pour créer et administrer WorkDocs des sites Amazon. Toutefois, les utilisateurs n'ont pas besoin de AWS compte pour se connecter à Amazon et l'utiliser WorkDocs. Pour plus d'informations, consultez 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 Serviceadministration.
- 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 Amazon

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

Pour créer le WorkDocs site Amazon

1. Ouvrez la WorkDocs console Amazon 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 apparaît.

      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.

Amazon WorkDocs effectue les opérations suivantes :

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

> **Note**
>
> Amazon 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 Servicepermet aux utilisateurs d'accéder à Amazon à WorkDocs partir d'un ordinateur connecté au même répertoire auprès duquel Amazon WorkDocs est enregistré, sans avoir à saisir les informations d'identification séparément. WorkDocs Les administrateurs Amazon peuvent activer l'authentification unique à l'aide de la AWS 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 Amazon a activé l'authentification unique, les utilisateurs du WorkDocs site Amazon devront peut-être également 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 Serviceadministration.

# Activation de l'authentification multi-facteurs

Vous utilisez la console des services d'AWSannuaire 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 protocole client/serveur 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 Amazon pour promouvoir un utilisateur au rang d'administrateur. Procédez comme suit :

Pour promouvoir un utilisateur en administrateur

1. Ouvrez la WorkDocs console Amazon 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.
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 d'administration WorkDocs du site Amazon pour rétrograder un administrateur. Pour plus d'informations, consultez Modification d'utilisateurs.

# Gérer Amazon WorkDocs depuis la AWS console

Vous utilisez ces outils pour gérer vos WorkDocs sites Amazon :

- La AWS console à l'adresse https://console.aws.amazon.com/zocalo/.
- Le panneau de configuration d'administration du site, disponible pour les administrateurs de tous les WorkDocs sites Amazon.

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, consultezGérer Amazon 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 Amazon 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 Amazon 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 Amazon. Pour de plus amples informations sur l'authentification, veuillez consulter Activation de l'authentification multi-facteurs.

## Configuration des URL du site

> **Note**
>
> Si vous avez suivi le processus de création du site enCommencer à utiliser Amazon WorkDocs, vous avez saisi une URL de site. Par conséquent, Amazon WorkDocs rend la commande Set site URL non 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 Amazon 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 d'Amazon, WorkDocs consultez Intégrer avec WorkDocs dans le guide de WorkSpaces l'utilisateur Amazon.

Pour définir l'URL d'un site

1. Ouvrez la WorkDocs console Amazon 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 manuel Amazon WorkDocs Developer Guide.

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 Amazon 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 Amazon 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 Amazon 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 Amazon 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 Amazon WorkDocs, nous en créons un pour vous. Lorsque vous supprimez le WorkDocs site Amazon, 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.

# Gérer Amazon WorkDocs depuis le panneau de configuration d'administration du site

Vous utilisez ces outils pour gérer vos WorkDocs sites Amazon :

- Le panneau de configuration d'administration du site, disponible pour les administrateurs sur tous les WorkDocs sites Amazon, et décrit dans les rubriques suivantes.
- La AWS console à l'adresse 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, consultezGérer Amazon 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

Les administrateurs WorkDocs du site Amazon 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 IP Allow List (Liste d'adresses IP autorisées) ne fonctionne actuellement que pour les adresses IPv4. 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 utilisateurs 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'annuaire. |
| 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 utilisateurs 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<br><br>**Note**<br>Les options ci-dessous n'apparaissent qu'une fois que vous avez sélectionné ce paramètre. | Enables administrators and users to invite new external users to your Amazon WorkDocs 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, Amazon le WorkDocs stocke dans la corbeille de l'utilisateur pendant 30 jours. Amazon WorkDocs déplace ensuite les fichiers vers 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 depuis la corbeille de récupération avant qu'Amazon ne les WorkDocs supprime 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 Amazon.

# Déploiement d'Amazon WorkDocs Drive sur plusieurs ordinateurs

Si vous disposez d'un parc de machines jointes à un domaine, vous pouvez utiliser des objets de stratégie de groupe (GPO) ou System Center Configuration Manager (SCCM) pour installer le client Amazon WorkDocs Drive. Vous pouvez télécharger le client depuishttps://amazonworkdocs.com/en/clients.

Au fur et à mesure, n'oubliez pas qu'Amazon 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 d'Amazon WorkDocs Drive. Pour de plus amples informations, veuillez consulterInstallation d'Amazon WorkDocs Drivedans leGuide de l'utilisateur Amazon WorkDocs.

> **Note**
>
> La meilleure pratique lors de l'utilisation de GPO ou de SCCM, installez le client Amazon WorkDocs Drive une fois que les utilisateurs se connectent.

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

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

L'exemple suivant montre comment déployer Amazon 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=votre_drive_lettre_REBOOT=REALLYSUPPRESS /norestart /qn
```

# Inviter et gérer WorkDocs les utilisateurs Amazon

Par défaut, lorsque vous joignez un annuaire lors de la création d'un site, la fonctionnalité d'activation automatique d'Amazon 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 des fichiers, et ils disposent automatiquement de 1 To de stockage. Toutefois, vous pouvez désactiver l'activation automatique lorsque vous souhaitez uniquement ajouter certains utilisateurs à 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 de plus amples 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 Amazon. Les étapes décrites dans les sections suivantes expliquent comment procéder. Toutefois, si vous êtes un nouvel utilisateur d'Amazon WorkDocs, prenez quelques minutes pour découvrir les différents rôles utilisateur avant de vous lancer dans les tâches administratives.

Table des matières


- Présentation des rôles utilisateur
- Démarrage du panneau de configuration d'administration
- Désactivation de l'activation automatique
- Gestion du partage de liens
- Contrôle des invitations utilisateur avec l'activation automatique activée
- Invitation de nouveaux utilisateurs
- Modification d'utilisateurs
- Désactivation d'utilisateurs
- Transfert de la propriété d'un document
- Téléchargement de listes d'utilisateurs

# Présentation des rôles utilisateur

Amazon WorkDocs définit les rôles utilisateur suivants. Vous pouvez modifier les rôles des utilisateurs en modifiant leur profil utilisateur. Pour plus d'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 définition des autorisations pour un utilisateur expérimenté, consultezSécurité — ActiveDirectory Sites simples etSécurité — sites ActiveDirectory de connexion.
- Utilisateur : utilisateur payant qui peut enregistrer des fichiers et collaborer avec d'autres utilisateurs sur un WorkDocs site Amazon.
- Guest user (Utilisateur invité) : Un utilisateur non payé qui peut uniquement afficher des fichiers. Vous pouvez faire passer les utilisateurs invités aux rôles d'utilisateur, d'utilisateur avancé ou d'administrateur.

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

Amazon définit WorkDocs également ces types d'utilisateurs supplémentaires.

Utilisateur WS

Utilisateur auquel un utilisateur est assigné WorkSpaces WorkSpace.

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

Utilisateur WS mis à niveau

Utilisateur disposant d'un espace de stockage attribué WorkSpaces WorkSpace et mis à niveau.

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

WorkDocs Utilisateur Amazon

Un WorkDocs utilisateur Amazon actif qui n'est pas assigné WorkSpaces WorkSpace.

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

# Démarrage du panneau de configuration d'administration

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

Pour ouvrir le panneau de configuration de l'administrateur

1. Choisissez l'icône en forme d'icône en forme d'icône en forme d'icône en forme d'icône dans le coin supérieur droit du WorkDocs client.

2. Sous Administrateur, choisissez Ouvrir le panneau de configuration de l'administrateur.

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

# Désactivation de 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 peut inviter de nouveaux utilisateurs sur le site : utilisateurs actuels, utilisateurs expérimentés ou administrateurs. Ces étapes expliquent comment réaliser ces deux tâches.

Pour désactiver l'activation automatique

1. Choisissez l'icône en forme d'icône en forme d'icône en forme d'icône en forme d'icône dans le coin supérieur droit du WorkDocs client.

   

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

   La boîte de dialogue Paramètres de Stratégie s'affiche.
4. Sous Activation automatique, décochez la case Autoriser l'activation automatique de tous les utilisateurs de votre annuaire lors de leur première connexion à votre WorkDocs site.

   Les options changent sous Qui doit 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 choisissez 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 d'Amazon 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 en forme d'icône en forme d'icône en forme d'icône en forme d'icône dans le coin supérieur droit du WorkDocs client.

   

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

   La boîte de dialogue Paramètres de Stratégie s'affiche.
4. Sous Choisissez vos paramètres pour les liens partageables, sélectionnez une option :

   - N'autorisez pas 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 l'accès à toute personne sur Internet.
   - Tous les utilisateurs gérés peuvent créer des liens partageables à l'échelle du site et publics. Les utilisateurs gérés peuvent créer des liens publics.
5. Choisissez Save Changes (Enregistrer les modifications).

# Contrôle des invitations utilisateur avec l'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'en inviter d'autres. Vous pouvez accorder l'autorisation à l'un des suivants :

- Tous les utilisateurs
- Usagers expérimentés
- Administrateurs.

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

Pour définir les autorisations d'invitation

1. Choisissez l'icône en forme d'icône en forme d'icône en forme d'icône en forme d'icône dans le coin supérieur droit du WorkDocs client.

   

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

   La boîte de dialogue Paramètres de Stratégie s'affiche.
4. Sous Qui doit 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 choisissez 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 de plus amples informations, veuillez consulterSécurité — ActiveDirectory Sites simples et,Sécurité — sites ActiveDirectory de connexion dans ce guide.

Pour inviter de nouveaux utilisateurs

1. Choisissez l'icône en forme d'icône en forme d'icône en forme d'icône en forme d'icône dans le coin supérieur droit du WorkDocs client.

2. Sous Administrateur, choisissez Ouvrir le panneau de configuration de l'administrateur.
3. Sous Manage Users (Gérer les utilisateurs), choisissez Invite Users (Inviter des utilisateurs).
4. Dans la boîte de dialogue Inviter des utilisateurs, pour Qui souhaitez-vous inviter ? , entrez l'adresse e-mail de l'invité, puis choisissez Envoyer. Répétez cette étape pour chaque invitation.

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

# Modification d'utilisateurs

Vous pouvez modifier les informations et les paramètres de l'utilisateur.

Pour modifier des utilisateurs

1. Choisissez l'icône en forme d'icône en forme d'icône en forme d'icône en forme d'icône dans le coin supérieur droit du WorkDocs client.

2. Sous Administrateur, choisissez Ouvrir le panneau de configuration de l'administrateur.
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.

État

Spécifie si l'utilisateur est actif ou inactif. Pour plus d'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 auxquels un WorkSpaces WorkSpace compte est attribué. Pour plus d'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 sur Inactif.

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

1. Choisissez l'icône en forme d'icône en forme d'icône en forme d'icône en forme d'icône dans le coin supérieur droit du WorkDocs client.

2. Sous Administrateur, choisissez Ouvrir le panneau de configuration de l'administrateur.
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 désactivé ne peut pas accéder à votre WorkDocs site Amazon.

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

## Suppression 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 Amazon doit toujours avoir au moins un utilisateur actif qui n'est pas un utilisateur invité. Si vous devez supprimer tous les utilisateurs, supprimez le site dans son intégralité.

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

# Transfert de la propriété d'un document

Vous pouvez transférer les fichiers et les dossiers d'un utilisateur inactif à un utilisateur actif. Pour de plus amples 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 en forme d'icône en forme d'icône en forme d'icône en forme d'icône dans le coin supérieur droit du WorkDocs client.

2. Sous Administrateur, choisissez Ouvrir le panneau de configuration de l'administrateur.
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 la liste des utilisateurs depuis le panneau de configuration de l'administrateur, vous devez installer Amazon WorkDocs Companion. Pour installer Amazon WorkDocs Companion, consultez la section Applications et intégrations pour Amazon WorkDocs.

Pour télécharger une liste d'utilisateurs

1. Choisissez l'icône en forme d'icône en forme d'icône en forme d'icône en forme d'icône dans le coin supérieur droit du WorkDocs client.

   

2. Sous Administrateur, choisissez Ouvrir le panneau de configuration de l'administrateur.
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.

Amazon WorkDocs contrôle l'accès aux dossiers et aux fichiers par le biais d'autorisations. Le système applique les autorisations en fonction du rôle de l'utilisateur.

Table des matières


- Partage de liens
- Partage par invitation
- Partage externe
- Autorisations
- Activation de l'édition collaborative


## Partage de liens

Les utilisateurs peuvent choisir Partager un lien pour copier et partager rapidement des hyperliens vers le WorkDocs contenu Amazon avec des collègues et des utilisateurs externes au sein et en dehors 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 Amazon peuvent rechercher, consulter et commenter le fichier.
- Toute personne disposant du lien, même les personnes qui ne sont pas membres du WorkDocs site Amazon, 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 plus d'informations, consultez Gérer Amazon 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 plus d'informations, consultez Gérer Amazon WorkDocs depuis le panneau de configuration d'administration du site.

## Partage externe

Le partage externe permet aux utilisateurs gérés d'un WorkDocs site Amazon 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 Amazon. 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 à Amazon 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 plus d'informations, consultez 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 plus d'informations, consultez Gérer Amazon WorkDocs depuis le panneau de configuration d'administration du site.

# Autorisations

AmazonWorkDocsutilise 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
- Autorisations pour les dossiers partagés
- Autorisations pour les fichiers contenus dans des dossiers partagés
- Autorisations pour les fichiers ne figurant pas dans des dossiers partagés


## 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— Le propriétaire d'un dossier ou d'un fichier.
- Copropriétaire du dossier— Un utilisateur ou un groupe que le propriétaire désigne comme copropriétaire d'un dossier ou d'un fichier.
- Contributeur au dossier— Quelqu'un disposant d'un accès illimité à un dossier.
- Afficheur 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— Le propriétaire d'un fichier.
- Copropriétaire— Un utilisateur ou un groupe que le propriétaire désigne comme copropriétaire du fichier.
- Contributeur— Personne autorisée à donner des commentaires sur un dossier.
- Afficheur— Une personne disposant d'un accès limité (autorisations en lecture seule) au fichier.
- Afficheur anonyme— Un utilisateur non enregistré extérieur à l'organisation qui peut consulter un fichier qui a été partagé à l'aide d'un lien de consultation externe. Sauf mention contraire, un lecteur anonyme dispose des mêmes autorisations qu'un lecteur.

## 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— Afficher les autres utilisateurs avec lesquels un dossier est partagé.
- Dossier de téléchargement— Téléchargez un dossier.
- Ajouter un sous-dossier— Ajoutez un sous-dossier.
- Partager— Partagez le dossier de niveau supérieur avec d'autres utilisateurs.
- Révoquer le partage— Révoque le partage du dossier de niveau supérieur.
- Supprimer le sous-dossier— Supprime un sous-dossier
- Supprimer le dossier de niveau supérieur— Supprime le dossier partagé de niveau supérieur.

| | Vue | Afficher les sous-dossiers | Afficher les partages | Dossier de téléchargement | Ajouter un sous-dossier | Partage | Révoquer le partage | Supprimer le sous-dossier | Supprimer le dossier de niveau supérieur |
|---|---|---|---|---|---|---|---|---|---|
| Propriétaire du dossier | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Copropriétaire du dossier | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Contributeur au dossier | ✓ | ✓ | ✓ | ✓ | ✓ | | | | |
| Afficheur de dossiers | ✓ | ✓ | ✓ | ✓ | | | | | |

## Autorisations pour les fichiers contenus 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— Renomme les fichiers.
- Charger— Téléchargez les nouvelles versions d'un fichier.
- Télécharger— Téléchargez un fichier. Il s'agit de l'autorisation par défaut. Vous pouvez utiliser les propriétés du fichier pour autoriser ou refuser la possibilité de télécharger des fichiers partagés.
- Empêcher le téléchargement— Empêche le téléchargement d'un fichier.

> **Note**
>
> - Lorsque vous sélectionnez cette option, les utilisateurs ayantAfficherles autorisations peuvent toujours télécharger des fichiers. Pour éviter cela, ouvrez le dossier partagé et effacezAutoriser les téléchargementsparamètre pour chacun des fichiers que vous ne souhaitez pas que ces utilisateurs téléchargent.
> - Lorsque le propriétaire ou le copropriétaire d'un fichier MP4 interdit le téléchargement de ce fichier, les contributeurs et les spectateurs ne peuvent pas le lire sur AmazonWorkDocsclient Web.

- Partager— Partagez un fichier avec d'autres utilisateurs.
- Révoquer le partage— Révoque le partage d'un fichier.
- Afficher— Affiche un fichier dans un dossier partagé.
- Afficher les partages— Afficher les autres utilisateurs avec lesquels un fichier est partagé.
- Afficher les annotations— Consultez les commentaires des autres utilisateurs.
- Afficher l'activité— Afficher l'historique des activités d'un fichier.
- Afficher les versions— Afficher les versions précédentes d'un fichier.
- Supprimer des versions— Supprime une ou plusieurs versions d'un fichier.
- Récupérer des versions— Récupérez 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 son commentaire.

| | Annote | Delete | Renam | Charge | Téléch ement | Empêch le téléch ement | Partag | Révoqu le partag | Vue | Affiche les partag | Affiche les annotat ns | Affiche l'activit é | Affiche les version | Supprim des version | Récupér des version | Voir tous les commentai res privés** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Prop ire du fichi | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

| | Annote | Delete | Renam | Charge | Téléch ement | Empêch le téléch ement | Partag | Révoqu le partag | Vue | Affiche les partag | Affiche les annotat ns | Affiche l'activi é | Affiche les versio | Supprim des versio | Récupér des versio | Voir tous les commentai res privés** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Prop ire du doss | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Copr taire du doss | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Cont eur au doss | ✓ | | | ✓ | ✓ | | | | ✓ | ✓ | ✓ | ✓ | ✓ | | | |
| Affic de doss | | | | | ✓ | | | | ✓ | ✓ | | | | | | |
| Affic anor | | | | | | | | | ✓ | ✓ | | | | | | |

* - Dans ce cas, le propriétaire du fichier est la personne qui a téléchargé la version d'origine d'un fichier dans un dossier partagé. Les autorisations pour ce rôle s'appliquent uniquement au fichier dont il est propriétaire, et non pas à tous les fichiers du dossier partagé.

** Le propriétaire/copropriétaire du fichier peut afficher tous les commentaires privés. Les participants peuvent uniquement afficher les commentaires privés qui sont des réponses à leurs propres commentaires.

# Autorisations pour les fichiers ne figurant pas dans des dossiers partagés

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

- Annoter— Ajoutez des commentaires à un fichier.
- Supprimer— Supprime un fichier
- Renommer— Renomme les fichiers.
- Charger— Téléchargez les nouvelles versions d'un fichier.
- Télécharger— Téléchargez un fichier. Il s'agit de l'autorisation par défaut. Vous pouvez utiliser les propriétés du fichier pour autoriser ou refuser la possibilité de télécharger des fichiers partagés.
- Empêcher le téléchargement— Empêche le téléchargement d'un fichier.

> **Note**
>
> Lorsque le propriétaire ou le copropriétaire d'un fichier MP4 interdit le téléchargement de ce fichier, les contributeurs et les spectateurs ne peuvent pas le lire sur AmazonWorkDocsclient Web.

- Partager— Partagez un fichier avec d'autres utilisateurs.
- Révoquer le partage— Révoque le partage d'un fichier.
- Afficher— Affiche un fichier.
- Afficher les partages— Afficher les autres utilisateurs avec lesquels un fichier est partagé.
- Afficher les annotations— Consultez les commentaires des autres utilisateurs.
- Afficher l'activité— Afficher l'historique des activités d'un fichier.
- Afficher les versions— Afficher les versions précédentes d'un fichier.
- Supprimer des versions— Supprime une ou plusieurs versions d'un fichier.
- Récupérer des versions— Récupérez une ou plusieurs versions supprimées d'un fichier.

| | Annote | Delete | Renam | Charge | Téléch ement | Empêch le téléchar ement | Partag | Révoqu le partag | Vue | Affiche les partag | Affiche les annotati ns | Affiche l'activit é | Affiche les versio | Supprir des versio | Récupérer des versions |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Prop ire | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Copr taire | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Parti nt | ✓ | | | ✓ | ✓ | | | | ✓ | ✓ | ✓ | ✓ | ✓ | | |
| Lecte | | | | | ✓ | | | | ✓ | ✓ | | | | | |
| Affich anon | | | | | | | | | ✓ | ✓ | | | | | |

# 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
- Activation d'Ouvrir avec Office Online


## Activation de Hancom ThinkFree

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

Hancom ThinkFree est disponible sans frais supplémentaires pour les WorkDocs utilisateurs d'Amazon. 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 Amazon, afin que les utilisateurs puissent modifier des fichiers Microsoft Office de manière collaborative à partir de l'application WorkDocs Web Amazon.

Open with Office Online est disponible sans frais supplémentaires pour WorkDocs les utilisateurs d'Amazon 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 Amazon WorkDocs

WorkDocs Les administrateurs Amazon peuvent utiliser Amazon WorkDocs Migration Service pour effectuer une migration à grande échelle de plusieurs fichiers et dossiers vers leur WorkDocs site Amazon. Amazon WorkDocs Migration Service fonctionne avec Amazon Simple Storage Service (Amazon S3). Cela vous permet de migrer les partages de fichiers départementaux et les partages de fichiers personnels ou utilisateurs vers Amazon WorkDocs.

Au cours de ce processus, Amazon vous WorkDocs propose une politiqueAWS Identity and Access Management (IAM). Utilisez cette politique pour créer un nouveau rôle IAM qui autorise l'accès à Amazon WorkDocs Migration Service afin d'effectuer les opérations suivantes :

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

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

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

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

- N'utilisez pas Admin comme nom d'utilisateur de votre WorkDocs compte Amazon. L'administrateur est un rôle d'utilisateur réservé sur Amazon WorkDocs.
- Votre type d'utilisateur WorkDocs administrateur Amazon doit être un utilisateur WS amélioré. Pour en savoir plus, consultez les sections 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 Amazon WorkDocs. La propriété des fichiers et les autorisations ne sont pas préservées.

Tâches


- Étape 1 : Préparation du contenu pour la migration
- Étape 2 : Chargement de fichiers sur Amazon S3
- Étape 3 : Planification d'une migration
- Étape 4 : Suivi d'une migration
- Étape 5 : Nettoyage des ressources


# Étape 1 : Préparation du contenu pour la migration

Pour préparer votre contenu à la migration

1. Sur votre WorkDocs site Amazon, 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. Amazon 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 d'un nom de 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`
- Noms de fichiers correspondant exactement à ces termes sensibles aux majuscules et minuscules —`Microsoft User DataOutlook files`,`Thumbs.db`,, ou`Thumbnails`
- Noms de fichiers contenant l'un des caractères suivants :`*` (astérisque),`/` (barre oblique vers l'avant),`\` (barre oblique arrière),`:`< (deux-points),> (inférieur à),`?` (point d'interrogation),`|` (barre verticale ou barre verticale),`"` (guillemets doubles), ou `\202E`(code de caractère 202E).

# Étape 2 : Chargement de fichiers sur Amazon S3

Chargement de fichiers sur Amazon S3

1. Créez un compartiment Amazon Simple Storage Service (Amazon S3) dans votreAWS compte dans lequel charger vos fichiers et dossiers. Le compartiment Amazon S3 doit se trouver dans le mêmeAWS compte etAWS la même région que votre WorkDocs site Amazon. Pour en savoir plus, consulter Prise en main Amazon Simple Storage Service dans le Guide de l'utilisateur d'Amazon Simple Storage Service.
2. Chargez vos fichiers dans le compartiment Amazon S3 créé à l'étape précédente. Nous vous recommandonsAWS DataSync de charger vos fichiers et dossiers dans le compartiment Amazon S3. DataSync fournit des fonctionnalités supplémentaires de suivi, de génération de rapports et de synchronisation. Pour plus d'informations, voir AWS DataSyncFonctionnement et Utilisation de politiques basées sur l'identité (politiques IAM) DataSync dans le Guide deAWS DataSync l'utilisateur.

# Étape 3 : Planification d'une migration

Après avoir effectué les étapes 1 et 2, utilisez le service de WorkDocs migration Amazon 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 vous 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 Amazon passe automatiquement à Illimité.

> **Note**
>
> La migration de fichiers dépassant votre limite WorkDocs de stockage Amazon peut entraîner des coûts supplémentaires. Pour en savoir plus, consulter WorkDocs Tarification Amazon.

Le service de WorkDocs migration Amazon fournit une politiqueAWS Identity and Access Management (IAM) que vous pouvez utiliser pour la migration. Avec cette politique, vous créez un nouveau rôle IAM qui accorde à Amazon WorkDocs Migration Service l'accès au compartiment Amazon S3 et au WorkDocs site Amazon 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 ses dates de début et de fin.

Pour planifier une migration

1. Dans la WorkDocs console Amazon, choisissez Apps, Migrations.
   - Si c'est la première fois que vous accédez à Amazon WorkDocs Migration Service, vous êtes invité à vous abonner aux notifications par e-mail d'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 Next (Suivant).
5. Pour la source de données et la validation, sous Exemple de politique, copiez la politique IAM fournie.
6. Utilisez la politique IAM que vous avez copiée à l'étape précédente pour créer une nouvelle politique 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 Review policy (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 US East (N. Virginia), sélectionnez`899282061130`
- Pour la région USA Ouest (Oregon), sélectionnez`814301586344`
- Pour la région Asie-Pacifique (Singapour), sélectionnez`900469912330`
- Pour la région Asie-Pacifique (Sydney), sélectionnez`031131923584`
- Pour la région Asie-Pacifique (Tokyo), sélectionnez`178752524102`
- Pour la région Europe (Irlande), sélectionnez`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. Sélectionnez Create role (Créer un rôle).

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

k. Sur la page Récapitulatif, changez la valeur de Durée maximum de session de CLI/API en 12 heures.

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

7. Revenez au service de WorkDocs migration Amazon. Pour Source de données et validation, sous Role ARN, collez l'ARN du rôle à partir du rôle IAM que vous avez copié à l'étape précédente.
8. Dans Bucket, sélectionnez le compartiment Amazon S3 à partir duquel migrer les fichiers.
9. Choisissez Next (Suivant).
10. Pour Sélectionner un WorkDocs dossier de destination, sélectionnez le dossier de destination sur Amazon WorkDocs vers lequel migrer les fichiers.
11. Choisissez Next (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 Amazon WorkDocs Migration Service. Pour accéder à la page de destination depuis le WorkDocs site Amazon, choisissez 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 (Migration)

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 depuis la console IAM.

Pour supprimer la stratégie et le rôle IAM

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Choisissez Policies (Politiques).

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 commence, le paramètre de stockage de votre compte WorkDocs utilisateur Amazon passe automatiquement à Illimité. Après la migration, vous pouvez modifier vos paramètres Storage (Stockage) en éditant votre compte utilisateur à partir du panneau de configuration d'administration. Pour plus d'informations, consultez Modification d'utilisateurs.

# Dépannage d'Amazon WorkDocsProblèmes

Les informations suivantes peuvent vous aider à résoudre les problèmes rencontrés avec Amazon. WorkDocs.

Problèmes


- Impossible de configurer mon Amazon WorkDocs site dans unAWSRégion
- Je veux configurer mon Amazon WorkDocs site dans un Amazon VPC existant
- Les utilisateurs doivent réinitialiser leur mot de passe
- Un utilisateur a partagé par erreur un document sensible
- L'utilisateur a quitté l'organisation et n'a pas transféré la propriété du document
- Nécessité de déployer Amazon WorkDocs Drive ou Amazon WorkDocs Accessoire pour plusieurs utilisateurs
- La modification en ligne est inopérante


## Impossible de configurer mon Amazon WorkDocs site dans unAWSRégion

Si vous configurez un nouvel Amazon 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 à utiliser Amazon WorkDocs.

## Je veux configurer mon Amazon WorkDocs site dans un Amazon VPC existant

Lors de la configuration de votre nouvel Amazon WorkDocs site, créez un répertoire à l'aide du cloud privé virtuel (VPC) existant. Amazon 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 plus d'informations, consultez Transfert de la propriété d'un document.

## Nécessité de déployer Amazon WorkDocs Drive ou Amazon WorkDocs Accessoire pour plusieurs utilisateurs

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

## La modification en ligne est inopérante

Vérifiez que vous avez Amazon WorkDocs Companion installé. Pour installer Amazon WorkDocs Compagnon, consultezApplications et intégrations pour Amazon WorkDocs.

# Gestion d'Amazon WorkDocs pour Amazon Business

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

Pour inviter un nouvel utilisateur dans Amazon WorkDocs pour Amazon Business

1. Connectez-vous avec vos informations d'identification Amazon Business à l'adresse https://workdocs.aws/.
2. Sur la page d'accueil d'Amazon WorkDocs pour 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 Done (Exécuté).

Pour rechercher un utilisateur sur Amazon WorkDocs pour Amazon Business

1. Connectez-vous avec vos informations d'identification Amazon Business à l'adresse https://workdocs.aws/.
2. Sur la page d'accueil d'Amazon WorkDocs pour 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 utilisateur sur Amazon WorkDocs pour Amazon Business

1. Connectez-vous avec vos informations d'identification Amazon Business à l'adresse https://workdocs.aws/.

2. Sur la page d'accueil d'Amazon WorkDocs pour 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 utilisateur sur Amazon WorkDocs for Amazon Business

1. Connectez-vous avec vos informations d'identification Amazon Business à l'adresse https://workdocs.aws/.
2. Sur la page d'accueil d'Amazon WorkDocs pour 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. Choisissez 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'autorisation

Si vous implémentez le filtrage IP sur les appareils qui accèdent à Amazon WorkDocs, ajoutez les adresses IP et les domaines suivants à votre liste d'autorisation. Cela permet à Amazon WorkDocs et Amazon WorkDocs Drive pour vous connecter au WorkDocs web.

- 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, voirAWSPlages d'adresses IPdans leAWSweb.

# 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 |
| Amazon WorkDocs Backup | Suppression de la documentation Amazon WorkDocs Backup du guide d' WorkDocs administration Amazon car le composant n'est plus pris en charge. | 24 juin 2021 |
| Gérer Amazon WorkDocs pour Amazon Business | Amazon WorkDocs pour Amazon Business prend en charge la gestion des utilisateurs par les administrateurs. Pour plus d'informations, consultez Managing Amazon WorkDocs for Amazon Business dans le guide d' WorkDocs administration Amazon. | 26 mars 2020 |
| Migration de fichiers vers Amazon WorkDocs | WorkDocs Les administrateurs Amazon peuvent utiliser Amazon WorkDocs Migration | 8 août 2019 |

| | | |
|---|---|---|
| | Service pour effectuer une migration à grande échelle de plusieurs fichiers et dossiers vers leur WorkDocs site Amazon. Pour plus d'informations, consultez la section Migration de fichiers vers Amazon WorkDocs dans 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 Amazon par plage d'adresses IP. Pour plus d'informations, consultez la section Paramètres des listes d'adresses IP autorisées dans le Guide WorkDocs d'administration 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 Amazon. Pour plus d'informations, consultez la section Enabling Hancom ThinkFree dans le guide d' WorkDocs administration 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 Amazon. 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 liés à Amazon 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 |

# Glossaire AWS

Pour connaître la terminologie la plus récente d'AWS, consultez le Glossaire AWS dans la Référence Glossaire AWS.