aws

Administratorhandbuch

Amazon WorkDocs

Amazon WorkDocs: Administratorhandbuch

Table of Contents

Hinweis: Neukundenanmeldungen und Kontoerweiterungen sind für Amazon WorkDocs nicht mehr verfügbar. Informationen zu den Migrationsschritten finden Sie hier: So migrieren Sie Daten von WorkDocs.

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.

Was ist Amazon WorkDocs?

Amazon WorkDocs ist ein vollständig verwalteter, sicherer Speicher- und Sharing-Service für Unternehmen mit starken administrativen Kontrollen und Feedback-Funktionen, die die Benutzerproduktivität verbessern. Dateien werden geschützt und sicher in der Cloud gespeichert. Die Dateien Ihrer Benutzer sind nur für diese sowie für ihre ausgewiesenen Beitragsleistenden und Betrachter sichtbar. Andere Mitglieder Ihrer Organisation haben auf Dateien anderer Benutzer keinen Zugriff, wenn ihnen nicht ausdrücklich Zugriff gewährt wurde.

Benutzer können ihre Dateien für andere Mitglieder Ihrer Organisation zur Zusammenarbeit oder Überprüfung freigeben. Die WorkDocs Client-Anwendungen können verwendet werden, um viele verschiedene Dateitypen anzuzeigen, abhängig vom Internet-Medientyp der Datei. WorkDocs unterstützt alle gängigen Dokument- und Bildformate, und Unterstützung für weitere Medientypen wird ständig hinzugefügt.

Weitere Informationen finden Sie auf Amazon WorkDocs.

Zugreifen WorkDocs

Administratoren verwenden die WorkDocs Konsole, um WorkDocs Websites zu erstellen und zu deaktivieren. Mit der Administrator-Systemsteuerung können Sie Benutzer-, Speicher- und Sicherheitseinstellungen verwalten. Weitere Informationen erhalten Sie unter Verwaltung WorkDocs über das Admin-Kontrollpanel der Website und WorkDocs Benutzer einladen und verwalten.

Benutzer ohne Administratorrolle verwenden die Client-Anwendungen für den Zugriff auf ihre Dateien. Sie verwenden niemals die WorkDocs Konsole oder das Administrations-Dashboard. WorkDocs bietet mehrere verschiedene Client-Anwendungen und Dienstprogramme:

- Eine Webanwendung für die Verwaltung und Anzeige von Dokumenten
- Native Apps für Mobilgeräte für das Prüfen von Dokumenten
- WorkDocs Drive, eine App, die einen Ordner auf Ihrem macOS- oder Windows-Desktop mit Ihren WorkDocs Dateien synchronisiert.

Weitere Informationen darüber, wie Benutzer WorkDocs Clients herunterladen, ihre Dateien bearbeiten und Ordner verwenden können, finden Sie unter den folgenden Themen im WorkDocs Benutzerhandbuch:

- Erste Schritte mit WorkDocs
- Mit Dateien arbeiten
- Mit Ordnern arbeiten

Preisgestaltung

Bei WorkDocs fallen keine Vorabgebühren oder Verpflichtungen an. Sie zahlen nur für aktive Benutzerkonten und den von Ihnen genutzten Speicherplatz. Weitere Informationen finden Sie unter Preise.

Erste Schritte

Informationen zu den ersten Schritten WorkDocs finden Sie unterEine WorkDocs Site erstellen.

Daten migrieren aus WorkDocs

WorkDocs bietet zwei Methoden zum Migrieren von Daten aus einer WorkDocs Site. Dieser Abschnitt bietet einen Überblick über diese Methoden und Links zu detaillierten Schritten zur Ausführung, Fehlerbehebung und Optimierung der einzelnen Migrationsmethoden.

Kunden haben zwei Möglichkeiten, ihre Daten von Amazon auszulagern WorkDocs: die bestehende Bulk-Download-Funktion (Methode 1) oder unser neues Datenmigrationstool (Methode 2). In den folgenden Themen wird erklärt, wie beide Methoden verwendet werden.

Themen

Methode 1: Dateien in großen Mengen herunterladen

Wenn du kontrollieren möchtest, welche Dateien du migrierst, kannst du sie manuell in großen Mengen herunterladen. Mit dieser Methode können Sie nur die gewünschten Dateien auswählen und sie an einen anderen Speicherort herunterladen, z. B. auf Ihr lokales Laufwerk. Sie können Dateien und Ordner von Ihrer WorkDocs Website oder von WorkDocs Drive herunterladen.

Beachten Sie Folgendes:

- Die Benutzer Ihrer Website können Dateien herunterladen, indem Sie die unten aufgeführten Schritte ausführen. Wenn Sie möchten, können Sie einen gemeinsamen Ordner einrichten, Ihre Benutzer die Dateien in diesen Ordner verschieben lassen und den Ordner dann an einen anderen Speicherort herunterladen. Sie können das Eigentum auch auf sich selbst übertragen und die Downloads durchführen.
- Informationen zum Herunterladen von Microsoft Word-Dokumenten mit Kommentaren finden Sie im WorkDocs Benutzerhandbuch unter Herunterladen von Word-Dokumenten mit Feedback.
- Sie müssen WorkDocs Drive verwenden, um Dateien herunterzuladen, die größer als 5 GB sind.
- Wenn Sie WorkDocs Drive zum Herunterladen von Dateien und Ordnern verwenden, bleiben Ihre Verzeichnisstrukturen, Dateinamen und Dateiinhalte erhalten. Dateieigentum, Berechtigungen und Versionen werden nicht beibehalten.

Dateien aus dem Internet herunterladen

Sie verwenden diese Methode, um Dateien herunterzuladen, wenn:

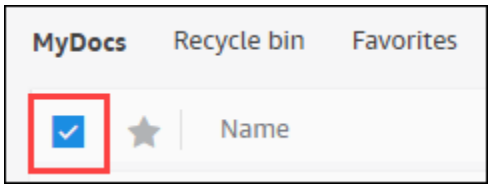
- Sie möchten nur einige Dateien von einer Site herunterladen.
- Sie möchten Word-Dokumente mit Kommentaren herunterladen und diese Kommentare in den jeweiligen Dokumenten beibehalten. Das Migrationstool lädt alle Kommentare herunter, schreibt sie jedoch in eine separate XML-Datei. Benutzer der Website haben dann möglicherweise Probleme, Kommentare ihren Word-Dokumenten zuzuordnen.

Um Dateien aus dem Internet herunterzuladen

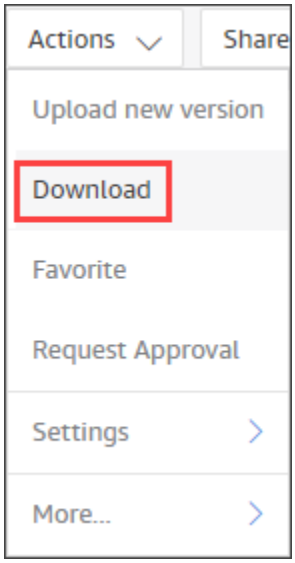
1. Melden Sie sich an bei WorkDocs.
2. Öffnen Sie bei Bedarf den Ordner, der die Dateien enthält, die Sie herunterladen möchten.
3. Aktivieren Sie das Kontrollkästchen neben den Dateien, die Sie herunterladen möchten.

   -ODER-

   Aktivieren Sie das Kontrollkästchen oben in der Liste, um alle Dateien im Ordner auszuwählen.



4. Öffnen Sie das Aktionsmenü und wählen Sie Herunterladen. .



Auf einem PC landen heruntergeladene Dateien standardmäßig im Ordnernamen Downloads/WorkDocsDownloads/. Auf einem Macintosh landen Dateien standardmäßig im Festplattennamen /Users/ user name/. WorkDocsDownloads

Ordner aus dem Internet werden heruntergeladen

> **Note**
>
> Wenn Sie Ordner herunterladen, laden Sie auch alle Dateien in den Ordnern herunter. Wenn Sie nur einige der Dateien in einem Ordner herunterladen möchten, verschieben Sie die unerwünschten Dateien an einen anderen Speicherort oder in den Papierkorb und laden Sie dann den Ordner herunter.

Um Ordner aus dem Internet herunterzuladen

1. Melden Sie sich an bei WorkDocs
2. Aktivieren Sie das Kontrollkästchen neben jedem Ordner, den Sie herunterladen möchten.

   -ODER-

   Öffnen Sie die Ordner und aktivieren Sie die Kontrollkästchen neben allen Unterordnern, die Sie herunterladen möchten.
3. Öffnen Sie das Aktionsmenü und wählen Sie Herunterladen. .

   Auf einem PC landen heruntergeladene Ordner standardmäßig unter Downloads/WorkDocsDownloads/Ordnername. Auf einem Macintosh landen Dateien standardmäßig unter dem Festplattennamen /Users/ user name/. WorkDocsDownloads

Verwenden von WorkDocs Drive zum Herunterladen von Dateien und Ordnern

> **Note**
>
> Sie müssen WorkDocs Drive installieren, um die folgenden Schritte ausführen zu können. Weitere Informationen finden Sie unter WorkDocs Drive-Installation im WorkDocs Drive-Benutzerhandbuch.

So laden Sie Dateien und Ordner von WorkDocs Drive herunter

1. Starten Sie den Datei-Explorer oder Finder und öffnen Sie Ihr Laufwerk W:.
2. Wählen Sie die Ordner oder Dateien aus, die Sie herunterladen möchten.
3. Tippen und halten Sie die ausgewählten Objekte (klicken Sie mit der rechten Maustaste) und wählen Sie Kopieren. Fügen Sie dann die kopierten Elemente an ihrem neuen Speicherort ein.

   -ODER-

   Ziehe die ausgewählten Objekte an ihre neue Position.
4. Löschen Sie die Originaldateien aus WorkDocs Drive.

Methode 2: Verwenden Sie das Migrationstool

Sie verwenden das WorkDocs Migrationstool, wenn Sie alle Daten von einer WorkDocs Site migrieren möchten.

Das Migrationstool verschiebt die Daten von einer Site in einen Amazon Simple Storage Service-Bucket. Das Tool erstellt für jeden Benutzer eine komprimierte ZIP-Datei. Die komprimierte Datei enthält alle Dateien und Ordner, Versionen, Berechtigungen, Kommentare und Anmerkungen für jeden Endbenutzer auf Ihrer WorkDocs Site.

Themen

- Migrierte Daten von Amazon S3 herunterladen
- Fehlerbehebung bei Migrationen
- Ihren Migrationsverlauf anzeigen

Voraussetzungen

Sie müssen über die folgenden Voraussetzungen verfügen, um das Migrationstool verwenden zu können.

- Ein Amazon-S3-Bucket Informationen zum Erstellen eines Amazon S3 S3-Buckets finden Sie unter Erstellen eines Buckets im Amazon S3 S3-Benutzerhandbuch. Ihr Bucket muss dasselbe IAM-Konto verwenden und sich in derselben Region wie Ihre WorkDocs Site befinden. Außerdem müssen Sie den öffentlichen Zugriff auf den Bucket blockieren. Weitere Informationen dazu finden Sie unter Sperren des öffentlichen Zugriffs auf Ihren Amazon S3 S3-Speicher im Amazon S3 S3-Benutzerhandbuch.

  Um die WorkDocs Erlaubnis zum Hochladen Ihrer Dateien zu erteilen, konfigurieren Sie die Bucket-Richtlinie wie im folgenden Beispiel gezeigt. Die Richtlinie verwendet die Schlüssel `aws:SourceAccount` und die `aws:SourceArn` Bedingungsschlüssel, um den Geltungsbereich der Richtlinie zu reduzieren. Dies ist eine bewährte Sicherheitsmethode.

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

```
            }
        }
    ]
}
```

> **Note**
>
> - *WORKDOCS-DIRECTORY-ID*ist die Organisations-ID Ihrer WorkDocs Site. Dies finden Sie in der Tabelle „Meine Websites“ in der WorkDocs AWS-Konsole.
> - Weitere Informationen zur Konfiguration einer Bucket-Richtlinie finden Sie unter Hinzufügen einer Bucket-Richtlinie mithilfe der Amazon S3 S3-Konsole

- Eine IAM-Richtlinie. Um eine Migration auf der WorkDocs Konsole zu starten, muss dem IAM-aufrufenden Principal die folgende Richtlinie an seinen Berechtigungssatz angehängt sein:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowStartWorkDocsMigration",
            "Effect": "Allow",
            "Action": [
                "workdocs:StartInstanceExport"
            ],
            "Resource": [
                "arn:aws:workdocs:REGION:AWS-ACCOUNT-ID:organization/WORKDOCS-
DIRECTORY-ID"
            ]
        },
        {
            "Sid": "AllowDescribeWorkDocsMigrations",
            "Effect": "Allow",
            "Action": [
                "workdocs:DescribeInstanceExports",
                "workdocs:DescribeInstances"
            ],
            "Resource": [
                "*"
            ]
        },
        {
```

```
            "Sid": "AllowS3Validations",
            "Effect": "Allow",
            "Action": [
                "s3:HeadBucket",
                "s3:ListBucket",
                "s3:GetBucketPublicAccessBlock",
                "kms:ListAliases"
            ],
            "Resource": [
                "arn:aws:s3:::BUCKET-NAME"
            ]
        },
        {
            "Sid": "AllowS3ListMyBuckets",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

- Optional können Sie einen AWS KMS Schlüssel verwenden, um die ruhenden Daten in Ihrem Bucket zu verschlüsseln. Wenn Sie keinen Schlüssel angeben, gilt die Standardverschlüsselungseinstellung des Buckets. Weitere Informationen finden Sie unter Schlüssel erstellen im AWS Key Management Service Developer Guide.

  Um einen AWS KMS Schlüssel zu verwenden, fügen Sie der IAM-Richtlinie die folgenden Anweisungen hinzu. Sie müssen einen aktiven Schlüssel vom Typ SYMMETRIC_DEFAULT verwenden.

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

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

Einschränkungen

Das Migrationstool hat die folgenden Einschränkungen:

- Das Tool schreibt alle Benutzerberechtigungen, Kommentare und Anmerkungen in separate CSV-Dateien. Sie müssen diese Daten manuell den entsprechenden Dateien zuordnen.
- Sie können nur aktive Websites migrieren.
- Das Tool ist auf eine erfolgreiche Migration pro Standort pro 24-Stunden-Zeitraum beschränkt.
- Sie können keine gleichzeitigen Migrationen derselben Site ausführen, aber Sie können gleichzeitige Migrationen für verschiedene Sites ausführen.
- Jede ZIP-Datei darf höchstens 50 GB groß sein. Benutzern mit mehr als 50 GB Daten WorkDocs werden mehrere ZIP-Dateien nach Amazon S3 exportiert.
- Das Tool exportiert keine Dateien, die größer als 50 GB sind. Das Tool listet alle Dateien, die größer als 50 GB sind, in einer CSV-Datei auf, die dasselbe Präfix wie die ZIP-Dateien hat. Zum Beispiel ***site-alias***/workdocs///skippedFiles.csv. ***created-timestamp-UTC*** Sie können die aufgelisteten Dateien programmgesteuert oder manuell herunterladen. Informationen zum programmgesteuerten Herunterladen finden Sie unterhttps://docs.aws.amazon.com/workdocs/latest/developerguide/download-documents.html, im Entwicklerhandbuch. WorkDocs Informationen zum manuellen Herunterladen der Dateien finden Sie in den Schritten unter Methode 1 weiter oben in diesem Thema.
- Die ZIP-Datei jedes Benutzers enthält nur and/or Dateiordner, deren Eigentümer er ist. Alle and/or Dateiordner, die für den Benutzer freigegeben wurden, befinden sich in der Zip-Datei des Benutzers, dem die and/or Dateiordner gehören.
- Wenn ein Ordner leer ist (enthält keine verschachtelten Dateien/Ordner) WorkDocs, wird er nicht exportiert.
- Es kann nicht garantiert werden, dass Daten (Dateien, Ordner, Versionen, Kommentare, Anmerkungen), die nach dem Initiieren des Migrationsauftrags erstellt wurden, in den exportierten Daten in S3 enthalten sind.
- Sie können mehrere Websites zu einem Amazon S3 S3-Bucket migrieren. Sie müssen nicht einen Bucket pro Site erstellen. Sie müssen jedoch sicherstellen, dass Ihre IAM- und Bucket-Richtlinien mehrere Websites zulassen.

- Die Migration erhöht Ihre Amazon S3 S3-Kosten, abhängig von der Datenmenge, die Sie in den Bucket migrieren. Weitere Informationen finden Sie auf der Amazon S3 S3-Preisseite.

Das Migrationstool ausführen

In den folgenden Schritten wird erklärt, wie das WorkDocs Migrationstool ausgeführt wird.

Um eine Site zu migrieren

1. Öffnen Sie die WorkDocs Konsole unter https://console.aws.amazon.com/zocalo/.
2. Wählen Sie im Navigationsbereich Meine Websites und anschließend das Optionsfeld neben der Site aus, die Sie migrieren möchten.
3. Öffnen Sie die Aktionsliste und wählen Sie Daten migrieren aus.
4. Geben Sie auf der Seite Migrate Data Site-Name die URI Ihres Amazon S3 S3-Buckets ein.

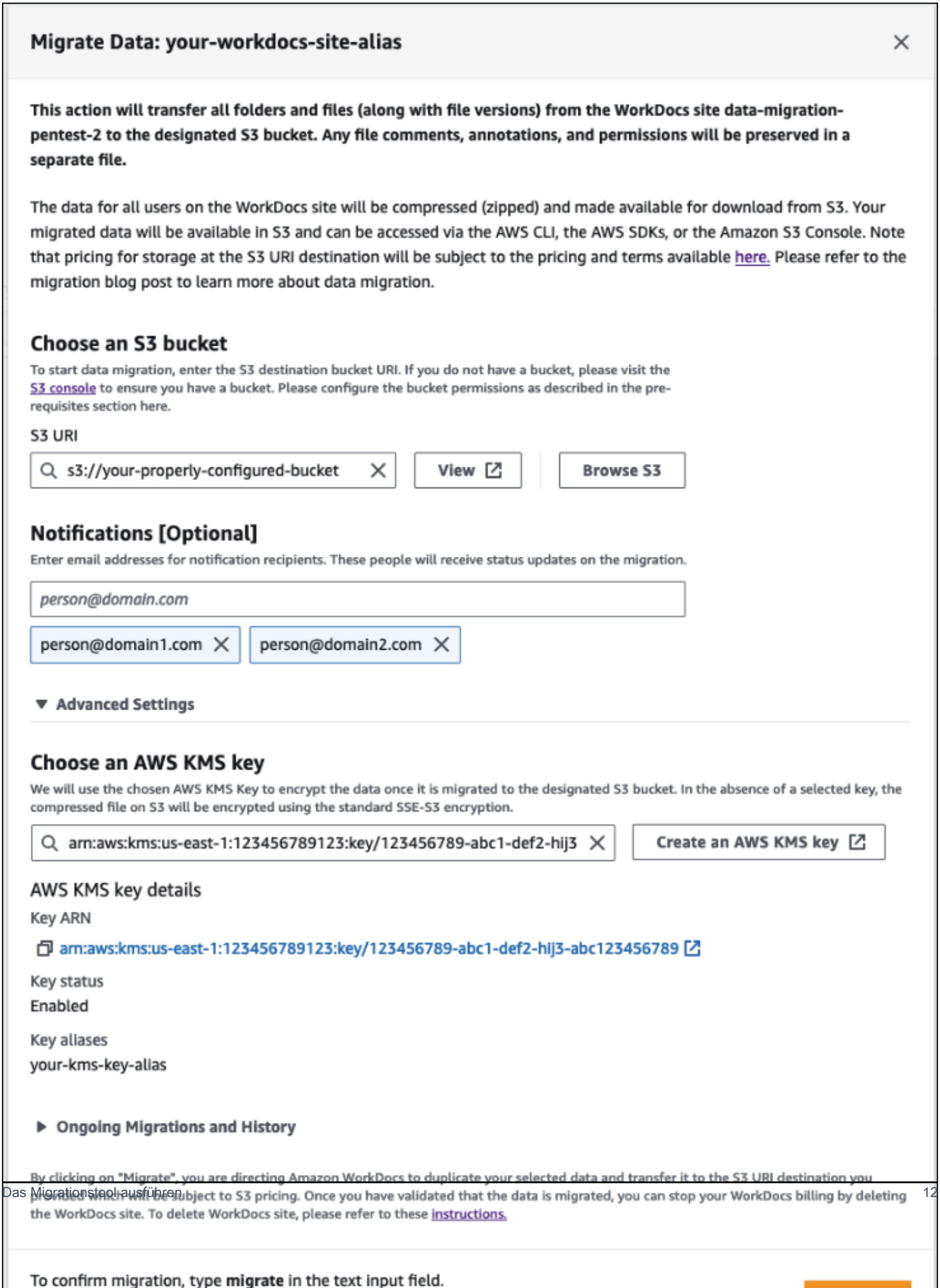
   -ODER-

   Wählen Sie Browse S3 und gehen Sie wie folgt vor:

   a. Suchen Sie bei Bedarf nach dem Bucket.

   b. Wählen Sie das Optionsfeld neben dem Bucket-Namen aus und wählen Sie dann Auswählen aus.
5. (Optional) Geben Sie unter Benachrichtigungen maximal fünf E-Mail-Adressen ein. Das Tool sendet E-Mails zum Migrationsstatus an jeden Empfänger.
6. (Optional) Wählen Sie unter Erweiterte Einstellungen einen KMS-Schlüssel aus, um Ihre gespeicherten Daten zu verschlüsseln.
7. Geben Sie **`migrate`** in das Textfeld ein, um die Migration zu bestätigen, und wählen Sie dann Migration starten aus.

   Ein Indikator wird angezeigt und zeigt den Status der Migration an. Die Migrationszeiten variieren je nach Datenmenge auf einer Site.


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

Wenn die Migration abgeschlossen ist:

- Das Tool sendet Erfolgs-E-Mails an die bei der Einrichtung eingegebenen Adressen, falls vorhanden.
- Ihr Amazon S3 S3-Bucket wird einen Ordner /workdocs///***site-alias***enthalten. ***created-timestamp-UTC*** Dieser Ordner enthält einen komprimierten Ordner für jeden Benutzer, der Daten auf der Site hatte. Jeder komprimierte Ordner enthält die Ordner und Dateien des Benutzers, einschließlich der Berechtigungen und Kommentare zur Zuordnung von CSV-Dateien.
- Wenn ein Benutzer vor der Migration alle seine Dateien entfernt, wird für diesen Benutzer kein komprimierter Ordner angezeigt.
- Versionen — Dokumente mit mehreren Versionen haben einen _ version _ Erstellungszeitstempel. Der Zeitstempel verwendet Epochen-Millisekunden. Ein Dokument mit dem Namen „TestFile.txt“ mit zwei Versionen sieht beispielsweise wie folgt aus:

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

- Berechtigungen — Das folgende Beispiel zeigt den Inhalt einer typischen CSV-Datei mit Berechtigungen.

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

- Kommentare — Das folgende Beispiel zeigt den Inhalt einer typischen CSV-Datei mit Kommentaren.

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

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

- Übersprungene Dateien — Das folgende Beispiel zeigt den Inhalt einer typischen CSV-Datei mit übersprungenen Dateien. Wir haben die ID gekürzt und die Ursachenwerte aus Gründen der besseren Lesbarkeit übersprungen.

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

Migrierte Daten von Amazon S3 herunterladen

Da die Migration Ihre Amazon S3-Kosten erhöht, können Sie die migrierten Daten von Amazon S3 auf eine andere Speicherlösung herunterladen. In diesem Thema wird erklärt, wie Sie Ihre migrierten Daten herunterladen können, und es enthält Vorschläge für das Hochladen von Daten in eine Speicherlösung.

> **Note**
>
> In den folgenden Schritten wird erklärt, wie Sie jeweils eine Datei oder einen Ordner herunterladen. Informationen zu anderen Möglichkeiten zum Herunterladen von Dateien finden Sie unter Objekte herunterladen im Amazon S3 S3-Benutzerhandbuch.

Um Daten herunterzuladen

1. Öffnen Sie die Amazon S3 S3-Konsole unter https://console.aws.amazon.com/s3/.

2. Wählen Sie den Ziel-Bucket aus und navigieren Sie zum Site-Alias.
3. Aktivieren Sie das Kontrollkästchen neben dem komprimierten Ordner.

   -ODER-

   Öffnen Sie den komprimierten Ordner und aktivieren Sie das Kontrollkästchen neben der Datei oder dem Ordner für einen einzelnen Benutzer.
4. Wählen Sie Herunterladen aus.

Vorschläge für Speicherlösungen

Für große Websites empfehlen wir, eine EC2 Instance mit einem kompatiblen Linux-basierten Amazon Machine Image bereitzustellen, um Ihre Daten programmgesteuert von Amazon S3 herunterzuladen, die Daten zu entpacken und sie dann auf Ihren Speicheranbieter oder Ihre lokale Festplatte hochzuladen.

Fehlerbehebung bei Migrationen

Gehen Sie wie folgt vor, um sicherzustellen, dass Sie Ihre Umgebung korrekt konfiguriert haben:

- Wenn eine Migration fehlschlägt, wird auf der Registerkarte Migrationsverlauf in der WorkDocs Konsole eine Fehlermeldung angezeigt. Überprüfen Sie die Fehlermeldung.
- Überprüfen Sie Ihre Amazon S3 S3-Bucket-Einstellungen.
- Führen Sie die Migration erneut aus.

Wenn das Problem weiterhin besteht, wenden Sie sich an den AWS Support. Geben WorkDocs Sie die Site-URL und die Migrationsjob-ID an, die sich in der Tabelle mit dem Migrationsverlauf befinden.

Ihren Migrationsverlauf anzeigen

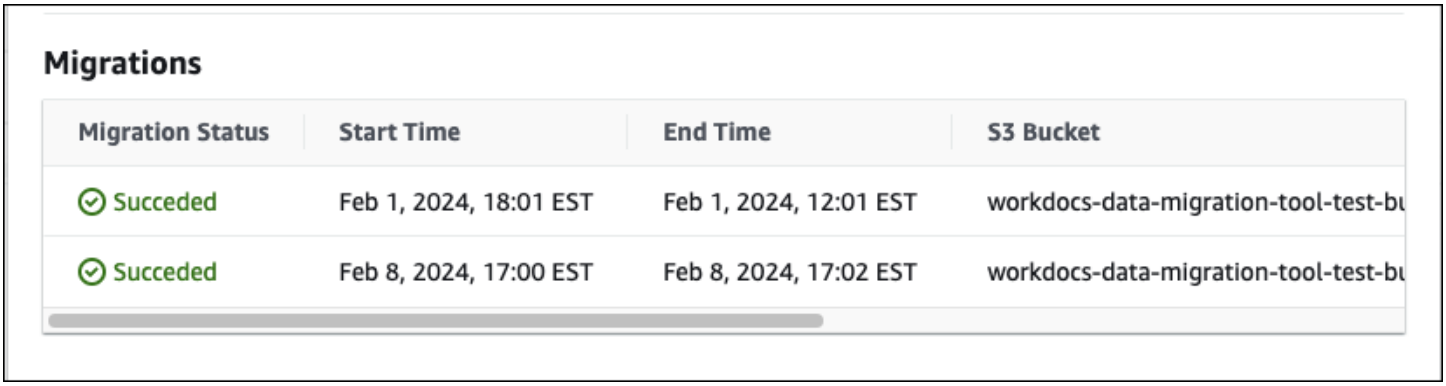
In den folgenden Schritten wird erklärt, wie Sie Ihren Migrationsverlauf einsehen können.

Um Ihren Verlauf einzusehen

1. Öffnen Sie die WorkDocs Konsole unter https://console.aws.amazon.com/zocalo/.
2. Wählen Sie das Optionsfeld neben der gewünschten WorkDocs Site aus.
3. Öffnen Sie die Aktionsliste und wählen Sie Daten migrieren aus.

4. Wählen Sie auf der Seite mit dem Namen der Migrate-Daten-Site die Option Laufende Migrationen und Verlauf aus.

Der Migrationsverlauf wird unter Migrationen angezeigt. Die folgende Abbildung zeigt einen typischen Verlauf.



Voraussetzungen für Amazon WorkDocs

Um neue WorkDocs Websites einzurichten oder bestehende Websites zu verwalten, müssen Sie die folgenden Aufgaben ausführen.

Melden Sie sich an für ein AWS-Konto

Wenn Sie noch keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um eine zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/die Anmeldung.
2. Folgen Sie den Online-Anweisungen.

   Ein Teil des Anmeldevorgangs umfasst den Empfang eines Telefonanrufs oder einer Textnachricht und die Eingabe eines Bestätigungscodes auf der Telefontastatur.

   Wenn Sie sich für eine anmelden AWS-Konto, wird eine Root-Benutzer des AWS-Kontoserstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Als bewährte Sicherheitsmethode weisen Sie einem Administratorbenutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Du kannst jederzeit deine aktuellen Kontoaktivitäten einsehen und dein Konto verwalten, indem du zu https://aws.amazon.com/gehst und Mein Konto auswählst.

Erstellen eines Benutzers mit Administratorzugriff

Nachdem Sie sich für einen angemeldet haben AWS-Konto, sichern Sie Ihren Root-Benutzer des AWS-Kontos AWS IAM Identity Center, aktivieren und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich AWS-Managementkonsoleals Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter Anmelden als Root-Benutzer im AWS-Anmeldung Benutzerhandbuch zu.

2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

   Anweisungen finden Sie unter Aktivieren eines virtuellen MFA-Geräts für Ihren AWS-Konto Root-Benutzer (Konsole) im IAM-Benutzerhandbuch.

Erstellen eines Benutzers mit Administratorzugriff

1. Aktivieren Sie das IAM Identity Center.

   Anweisungen finden Sie unter Aktivieren AWS IAM Identity Center im AWS IAM Identity Center Benutzerhandbuch.

2. Gewähren Sie einem Administratorbenutzer im IAM Identity Center Benutzerzugriff.

   Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie IAM-Identity-Center-Verzeichnis im Benutzerhandbuch unter Benutzerzugriff mit der Standardeinstellung konfigurieren.AWS IAM Identity Center

Anmelden als Administratorbenutzer

- Um sich mit Ihrem IAM-Identity-Center-Benutzer anzumelden, verwenden Sie die Anmelde-URL, die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM-Identity-Center-Benutzer erstellt haben.

  Hilfe bei der Anmeldung mit einem IAM Identity Center-Benutzer finden Sie im AWS-Anmeldung Benutzerhandbuch unter Anmeldung beim AWS Access-Portal.

Weiteren Benutzern Zugriff zuweisen

1. Erstellen Sie im IAM-Identity-Center einen Berechtigungssatz, der den bewährten Vorgehensweisen für die Anwendung von geringsten Berechtigungen folgt.

   Anweisungen hierzu finden Sie unter Berechtigungssatz erstellen im AWS IAM Identity Center Benutzerhandbuch.

2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

Eine genaue Anleitung finden Sie unter Gruppen hinzufügen im AWS IAM Identity Center Benutzerhandbuch.

Sicherheit bei Amazon WorkDocs

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS Dienste in der AWS Cloud ausführt. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der AWS -Compliance-Programme regelmäßig. Weitere Informationen zu den Compliance-Programmen, die für Amazon gelten WorkDocs, finden Sie unter AWS Services in Scope by Compliance Program.
- Sicherheit in der Cloud — Der AWS Service, den Sie nutzen, bestimmt Ihre Verantwortung. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, die Anforderungen Ihres Unternehmens und die geltenden Gesetze und Vorschriften. Die Themen in diesem Abschnitt helfen Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Nutzung anwenden können WorkDocs.

> **Note**
>
> Die Benutzer in einer WorkDocs Organisation können mit Benutzern außerhalb dieser Organisation zusammenarbeiten, indem sie einen Link oder eine Einladung zu einer Datei senden. Dies gilt jedoch nur für Websites, die einen Active Directory Connector verwenden. Sehen Sie sich die Einstellungen für gemeinsam genutzte Links für Ihre Site an und wählen Sie die Option aus, die den Anforderungen Ihres Unternehmens am besten entspricht.

In den folgenden Themen erfahren Sie, wie Sie die Konfiguration vornehmen WorkDocs , um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere AWS Dienste nutzen können, die Sie bei der Überwachung und Sicherung Ihrer WorkDocs Ressourcen unterstützen.

Themen

Identitäts- und Zugriffsmanagement für Amazon WorkDocs

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf Ressourcen sicher zu AWS kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Ressourcen zu verwenden. WorkDocs IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

Zielgruppe

Die Art und Weise, wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, in der Sie tätig sind. WorkDocs

Dienstbenutzer — Wenn Sie den WorkDocs Dienst für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die erforderlichen Anmeldeinformationen und Berechtigungen zur Verfügung. Wenn Sie für Ihre Arbeit mehr WorkDocs Funktionen verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Funktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anfordern müssen. Unter Fehlerbehebung Amazon WorkDocs Amazon-Identität und Zugriff finden Sie nützliche Informationen für den Fall, dass Sie keinen Zugriff auf eine Feature in WorkDocs haben.

Serviceadministrator — Wenn Sie in Ihrem Unternehmen für die WorkDocs Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf WorkDocs. Es ist Ihre Aufgabe, zu bestimmen, auf welche WorkDocs Funktionen und Ressourcen Ihre Servicebenutzer zugreifen sollen. Anschließend müssen Sie Anforderungen an Ihren IAM-Administrator senden, um die Berechtigungen der Servicebenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen darüber, wie Ihr Unternehmen IAM nutzen kann WorkDocs, finden Sie unterSo WorkDocs arbeitet Amazon mit IAM.

IAM-Administrator: Wenn Sie als IAM-Administrator fungieren, sollten Sie Einzelheiten dazu kennen, wie Sie Richtlinien zur Verwaltung des Zugriffs auf WorkDocs verfassen können. Beispiele für WorkDocs identitätsbasierte Richtlinien, die Sie in IAM verwenden können, finden Sie unter. Beispiele für WorkDocs identitätsbasierte Richtlinien von Amazon

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen als IAM-Benutzer authentifiziert (angemeldet AWS) sein oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAM Identity Center) -Benutzer, die Single Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie über den Verbund darauf zugreifen AWS , übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS-Managementkonsole oder beim AWS Zugangsportal anmelden. Weitere Informationen zur Anmeldung finden Sie AWS unter So melden Sie sich bei Ihrem an AWS-Konto im AWS-Anmeldung Benutzerhandbuch.

Wenn Sie AWS programmgesteuert zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, um Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch zu signieren. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode für die Selbstsignierung von Anforderungen finden Sie unter AWS Signature Version 4 für API-Anforderungen im IAM-Benutzerhandbuch.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen bereitstellen. AWS Empfiehlt beispielsweise, die Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter Multi-Faktor-Authentifizierung im AWS IAM Identity Center - Benutzerhandbuch und AWS Multi-Faktor-Authentifizierung (MFA) in IAM im IAM-Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Eine IAM-Gruppe ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise eine Gruppe benennen IAMAdminsund dieser Gruppe Berechtigungen zur Verwaltung von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter Anwendungsfälle für IAM-Benutzer im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität innerhalb von Ihnen AWS-Konto , die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, jedoch nicht mit einer bestimmten Person verknüpft. Um vorübergehend eine IAM-Rolle in der zu übernehmen AWS-Managementkonsole, können Sie von einer Benutzer- zu einer IAM-Rolle (Konsole) wechseln. Sie können eine Rolle übernehmen, indem Sie eine AWS CLI oder AWS API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter Methoden für die Übernahme einer Rolle im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter Erstellen von Rollen für externe Identitätsanbieter (Verbund) im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center -Benutzerhandbuch.
- Temporäre IAM-Benutzerberechtigungen – Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff — Einige AWS-Services verwenden Funktionen in anderen AWS-Services. Wenn Sie beispielsweise einen Service aufrufen, ist es üblich, dass dieser Service Anwendungen in Amazon ausführt EC2 oder Objekte in Amazon S3 speichert. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Forward Access Sessions (FAS) — Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.
  - Servicerolle – Eine Servicerolle ist eine IAM-Rolle, die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM

erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.

- Dienstbezogene Rolle — Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

- Auf Amazon ausgeführte Anwendungen EC2 — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2 Instance ausgeführt werden und AWS API-Anfragen stellen AWS CLI . Dies ist dem Speichern von Zugriffsschlüsseln innerhalb der EC2 Instance vorzuziehen. Um einer EC2 Instanz eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instanzprofil, das an die Instanz angehängt ist. Ein Instanzprofil enthält die Rolle und ermöglicht Programmen, die auf der EC2 Instanz ausgeführt werden, temporäre Anmeldeinformationen abzurufen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Verwenden einer IAM-Rolle, um Berechtigungen für Anwendungen zu gewähren, die auf EC2 Amazon-Instances ausgeführt werden.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Die Berechtigungen in den Richtlinien legen fest, ob eine Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen von der AWS-Managementkonsole AWS CLI, der oder der AWS API abrufen.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem System zuordnen können AWS-Konto. Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer Inline-Richtlinie wählen, finden Sie unter Auswählen zwischen verwalteten und eingebundenen Richtlinien im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Zugriffskontrolllisten

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLs ähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 und Amazon VPC sind Beispiele für Dienste, die Unterstützung ACLs bieten. AWS WAF Weitere Informationen finden Sie unter Übersicht über ACLs die Zugriffskontrollliste (ACL) im Amazon Simple Storage Service Developer Guide.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- Berechtigungsgrenzen – Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.
- Dienststeuerungsrichtlinien (SCPs) — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen. AWS Organizations AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Objekte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie alle Funktionen in einer Organisation aktivieren, können Sie Richtlinien zur Servicesteuerung (SCPs) auf einige oder alle Ihre Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Root-Benutzer des AWS-Kontos Entitäten. Weitere Informationen zu Organizations und SCPs finden Sie unter Richtlinien zur Servicesteuerung im AWS Organizations Benutzerhandbuch.
- Ressourcenkontrollrichtlinien (RCPs) — RCPs sind JSON-Richtlinien, mit denen Sie die maximal verfügbaren Berechtigungen für Ressourcen in Ihren Konten festlegen können, ohne die IAM-Richtlinien aktualisieren zu müssen, die jeder Ressource zugeordnet sind, deren Eigentümer Sie sind. Das RCP schränkt die Berechtigungen für Ressourcen in Mitgliedskonten ein und kann sich

auf die effektiven Berechtigungen für Identitäten auswirken, einschließlich der Root-Benutzer des AWS-Kontos, unabhängig davon, ob sie zu Ihrer Organisation gehören. Weitere Informationen zu Organizations RCPs, einschließlich einer Liste AWS-Services dieser Support-Leistungen RCPs, finden Sie unter Resource Control Policies (RCPs) im AWS Organizations Benutzerhandbuch.

- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

> **Note**
>
> WorkDocs unterstützt keine Service Control-Richtlinien für Slack-Organisationen.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, erfährst du unter Bewertungslogik für Richtlinien im IAM-Benutzerhandbuch.

So WorkDocs arbeitet Amazon mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf zu verwalten WorkDocs, müssen Sie wissen, mit welchen IAM-Funktionen Sie arbeiten können. WorkDocs Einen allgemeinen Überblick darüber, wie WorkDocs und andere AWS Dienste mit IAM funktionieren, finden Sie im AWS IAM-Benutzerhandbuch unter Dienste, die mit IAM funktionieren.

Themen

- Identitätsbasierte WorkDocs-Richtlinien
- Ressourcenbasierte WorkDocs-Richtlinien
- Autorisierung auf der Basis von WorkDocs -Tags
- WorkDocs IAM-Rollen

Identitätsbasierte WorkDocs-Richtlinien

Mit identitätsbasierten IAM-Richtlinien können Sie zulässige oder verweigerte Aktionen angeben. WorkDocs unterstützt bestimmte Aktionen. Informationen zu den Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Aktionen

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API-Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keinen passenden API-Vorgang gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Bei Richtlinienaktionen wird vor der Aktion das folgende Präfix WorkDocs verwendet:`workdocs:`. Um beispielsweise jemandem die Erlaubnis zu erteilen, den WorkDocs `DescribeUsers` API-Vorgang auszuführen, nehmen Sie die `workdocs:DescribeUsers` Aktion in seine Richtlinie auf. Richtlinienanweisungen müssen ein `Action`- oder `NotAction`-Element enthalten. WorkDocs definiert seinen eigenen Satz an Aktionen, die Aufgaben beschreiben, die Sie mit diesem Service durchführen können.

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie wie folgt durch Kommata:

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

Sie können auch Platzhalter verwenden, um mehrere Aktionen anzugeben. Beispielsweise können Sie alle Aktionen festlegen, die mit dem Wort `Describe` beginnen, einschließlich der folgenden Aktion:

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

> **Note**
>
> Um die Abwärtskompatibilität sicherzustellen, fügen Sie die `zocalo` Aktion hinzu. Zum Beispiel:
>
> ```
> "Action": [
> "zocalo:*",
> "workdocs:*"
> ],
> ```

Eine Liste der WorkDocs Aktionen finden Sie WorkDocs im IAM-Benutzerhandbuch unter Definierte Aktionen von.

Ressourcen

WorkDocs unterstützt die Angabe von Ressourcen ARNs in einer Richtlinie nicht.

Bedingungsschlüssel

WorkDocs stellt keine dienstspezifischen Bedingungsschlüssel bereit, unterstützt aber die Verwendung einiger globaler Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

Beispiele

Beispiele für WorkDocs identitätsbasierte Richtlinien finden Sie unter. Beispiele für WorkDocs identitätsbasierte Richtlinien von Amazon

Ressourcenbasierte WorkDocs-Richtlinien

WorkDocs unterstützt keine ressourcenbasierten Richtlinien.

Autorisierung auf der Basis von WorkDocs -Tags

WorkDocs unterstützt das Markieren von Ressourcen oder die Steuerung des Zugriffs anhand von Tags nicht.

WorkDocs IAM-Rollen

Eine IAM-Rolle ist eine Entität in Ihrem AWS Konto, die über bestimmte Berechtigungen verfügt.

Verwenden temporärer Anmeldeinformationen mit WorkDocs

Wir empfehlen dringend, temporäre Anmeldeinformationen zu verwenden, um sich bei einem Verbund anzumelden, eine IAM-Rolle anzunehmen oder eine kontoübergreifende Rolle anzunehmen. Sie erhalten temporäre Sicherheitsanmeldedaten, indem Sie AWS STS API-Operationen wie AssumeRoleoder aufrufen. GetFederationToken

WorkDocs unterstützt die Verwendung temporärer Anmeldeinformationen.

Service-verknüpfte Rollen

Mit dienstbezogenen Rollen können AWS Dienste auf Ressourcen in anderen Diensten zugreifen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem IAM-Konto angezeigt und gehören zum Service. Ein IAM-Administrator kann die Berechtigungen für serviceverknüpfte Rollen anzeigen, aber nicht bearbeiten.

WorkDocs unterstützt keine dienstbezogenen Rollen.

Servicerollen

Dieses Feature ermöglicht einem Service das Annehmen einer Servicerolle in Ihrem Namen. Diese Rolle gewährt dem Service Zugriff auf Ressourcen in anderen Diensten, um eine Aktion in Ihrem Namen auszuführen. Servicerollen werden in Ihrem IAM-Konto angezeigt und gehören zum Konto. Dies bedeutet, dass ein IAM-Administrator die Berechtigungen für diese Rolle ändern kann. Dies kann jedoch die Funktionalität des Dienstes beeinträchtigen.

WorkDocs unterstützt keine Servicerollen.

Beispiele für WorkDocs identitätsbasierte Richtlinien von Amazon

> **Note**
>
> Um die Sicherheit zu erhöhen, sollten Sie nach Möglichkeit Verbundbenutzer anstelle von IAM-Benutzern erstellen.

IAM-Benutzer besitzen keine Berechtigungen zum Erstellen oder Ändern von WorkDocs - Ressourcen. Sie können auch keine Aufgaben mit der AWS-Managementkonsole AWS CLI, oder

AWS API ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern und Rollen die Berechtigung zum Ausführen bestimmter API-Operationen für die angegebenen Ressourcen gewähren, die diese benötigen. Der Administrator muss diese Richtlinien anschließend den IAM-Benutzern oder -Gruppen anfügen, die diese Berechtigungen benötigen.

> **Note**
>
> Um die Abwärtskompatibilität zu gewährleisten, sollten Sie die `zocalo` Aktion in Ihre Richtlinien aufnehmen. Zum Beispiel:
>
> ```
> {
>     "Version": "2012-10-17",
>     "Statement": [
>         {
>             "Sid": "VisualEditor0",
>             "Effect": "Deny",
>             "Action": [
>             "zocalo:*",
>             "workdocs:*"
>             ],
>             "Resource": "*"
>         }
>     ]
> }
> ```

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von Richtlinien auf der JSON-Registerkarte im IAM-Benutzerhandbuch.

Themen

- Bewährte Methoden für Richtlinien
- Verwenden der WorkDocs -Konsole
- Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer
- Erlauben Sie Benutzern nur Lesezugriff auf Ressourcen WorkDocs
- Weitere Beispiele für WorkDocs identitätsbasierte Richtlinien

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand WorkDocs Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um Ihren Benutzern und Workloads zunächst Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien oder AWS -verwaltete Richtlinien für Auftrags-Funktionen im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. CloudFormation B. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung mit IAM Access Analyzer im IAM-Benutzerhandbuch.

- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Sicherer API-Zugriff mit MFA im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Verwenden der WorkDocs -Konsole

Um auf die WorkDocs Amazon-Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, die Details der WorkDocs Ressourcen in Ihrem AWS Konto aufzulisten und einzusehen. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die restriktiver ist als die erforderlichen Mindestberechtigungen, funktioniert die Konsole für IAM-Benutzer- oder Rollenentitäten nicht wie vorgesehen.

Um sicherzustellen, dass diese Entitäten die WorkDocs Konsole verwenden können, fügen Sie den Entitäten auch die folgenden AWS verwalteten Richtlinien hinzu. Weitere Informationen zum Anhängen von Richtlinien finden Sie unter Hinzufügen von Berechtigungen für einen Benutzer im IAM-Benutzerhandbuch.

- AmazonWorkDocsFullAccess
- AWSDirectoryServiceFullAccess
- AmazonEC2FullAccess

Diese Richtlinien gewähren einem Benutzer vollen Zugriff auf WorkDocs Ressourcen, AWS Directory Service Service-Operationen und die EC2 Amazon-Operationen, die Amazon WorkDocs benötigt, um ordnungsgemäß zu funktionieren.

Sie müssen Benutzern, die nur die API AWS CLI oder die AWS API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die den API-Operation entsprechen, die Sie ausführen möchten.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer

Benutzeridentität angefügt sind. Diese Richtlinie umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der API AWS CLI oder 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": "*"
        }
    ]
}
```

Erlauben Sie Benutzern nur Lesezugriff auf Ressourcen WorkDocs

Die folgende AWS verwaltete AmazonWorkDocsReadOnlyAccessRichtlinie gewährt einem IAM-Benutzer nur Lesezugriff auf Ressourcen. WorkDocs Die Richtlinie gewährt dem Benutzer Zugriff auf alle Operationen. WorkDocs `Describe` Der Zugriff auf die beiden EC2 Amazon-Operationen ist erforderlich, um eine Liste Ihrer VPCs und der Subnetze zu erhalten. WorkDocs Zugriff auf den

Directory Service `DescribeDirectories` Vorgang ist erforderlich, um Informationen über Ihre Directory Service Verzeichnisse zu erhalten.

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

Weitere Beispiele für WorkDocs identitätsbasierte Richtlinien

IAM-Administratoren können zusätzliche Richtlinien erstellen, um einer IAM-Rolle oder einem IAM-Benutzer den Zugriff auf die API zu ermöglichen. WorkDocs Weitere Informationen finden Sie unter Authentifizierung und Zugriffskontrolle für Verwaltungsanwendungen im WorkDocs Entwicklerhandbuch.

Fehlerbehebung Amazon WorkDocs Amazon-Identität und Zugriff

Mithilfe der folgenden Informationen können Sie häufig auftretende Probleme diagnostizieren und beheben, die bei der Arbeit mit WorkDocs IAM auftreten können.

Themen

- Ich bin nicht berechtigt, eine Aktion durchzuführen in WorkDocs
- Ich bin nicht berechtigt, iam auszuführen: PassRole
- Ich möchte Personen außerhalb meines AWS Kontos den Zugriff auf meine WorkDocs Ressourcen ermöglichen

Ich bin nicht berechtigt, eine Aktion durchzuführen in WorkDocs

Wenn Ihnen AWS-Managementkonsole mitgeteilt wird, dass Sie nicht berechtigt sind, eine Aktion durchzuführen, müssen Sie sich an Ihren Administrator wenden, um Unterstützung zu erhalten. Ihr Administrator ist die Person, die Ihnen Ihren Benutzernamen und Ihr Passwort bereitgestellt hat.

Ich bin nicht berechtigt, iam auszuführen: PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zum Durchführen der `iam:PassRole`-Aktion autorisiert sind, müssen Ihre Richtlinien aktualisiert werden, um eine Rolle an WorkDocs übergeben zu können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in WorkDocs auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

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

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb meines AWS Kontos den Zugriff auf meine WorkDocs Ressourcen ermöglichen

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Für Dienste, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (ACLs) unterstützen, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob diese Funktionen WorkDocs unterstützt werden, finden Sie unter. So WorkDocs arbeitet Amazon mit IAM
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs auf einen IAM-Benutzer in einem anderen AWS-Konto , den Sie besitzen.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Protokollierung und Überwachung in Amazon WorkDocs

Administratoren von WorkDocs Amazon-Websites können den Aktivitätsfeed für eine gesamte Website anzeigen und exportieren. Sie können ihn auch verwenden AWS CloudTrail , um Ereignisse von der WorkDocs Konsole aus zu erfassen.

Themen

- Exportieren des seitenweiten Aktivitätsfeeds
- Zum AWS CloudTrail Protokollieren von WorkDocs Amazon-API-Aufrufen verwenden

Exportieren des seitenweiten Aktivitätsfeeds

Administratoren können die Aktivitätenliste einer gesamten Website aufrufen und exportieren. Um diese Funktion nutzen zu können, müssen Sie zuerst WorkDocs Companion installieren. Informationen zur Installation von WorkDocs Companion finden Sie unter Apps und Integrationen für WorkDocs.

So rufen Sie die websiteweite Aktivitätenliste auf und exportieren sie

1. Wählen Sie in der Webanwendung Aktivität aus.

2. Wähle „Filter“ und bewege dann den Schieberegler „Aktivität für die gesamte Website“, um den Filter zu aktivieren.
3. Wählen Sie die Filter für den Aktivitätstyp, die gewünschten Einstellungen für Datum geändert und dann Anwenden aus.
4. Sie können die Ergebnisse in der Liste der gefilterten Aktivitäten mit einer Suche nach Datei-, Ordner- oder Benutzername weiter einschränken. Bei Bedarf lassen sich auch Filter hinzufügen oder entfernen.
5. Wählen Sie Export aus, um die Aktivitätenliste im CSV- (`.csv`) und JSON-Format (`.json`) auf Ihrem Computer zu speichern. Das System exportiert die Dateien an einen der folgenden Speicherorte:

   - Windows — WorkDocsDownloadsOrdner im Download-Ordner Ihres PCs
   - macOS – `/users/`**`username`**`/WorkDocsDownloads/folder`

   Die exportierte Datei spiegelt alle Filter wider, die Sie anwenden.

   > **Note**
   >
   > Benutzer ohne Administratorrechte können nur Aktivitätenlisten ihrer eigenen Inhalte aufrufen und exportieren. Weitere Informationen finden Sie unter Aktivitäts-Feed anzeigen im WorkDocs Amazon-Benutzerhandbuch.

Zum AWS CloudTrail Protokollieren von WorkDocs Amazon-API-Aufrufen verwenden

Sie können AWS CloudTrail; verwenden, um WorkDocs Amazon-API-Aufrufe zu protokollieren. CloudTrail bietet eine Aufzeichnung der Aktionen, die von einem Benutzer, einer Rolle oder einem AWS Dienst in ausgeführt wurden WorkDocs. CloudTrail erfasst alle API-Aufrufe WorkDocs als Ereignisse, einschließlich Aufrufe von der WorkDocs Konsole und von Codeaufrufen an die WorkDocs APIs.

Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für WorkDocs. Wenn Sie keinen Trail erstellen, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf anzeigen.

Zu den von gesammelten Informationen CloudTrail gehören Anfragen, die IP-Adressen, von denen aus die Anfragen gestellt wurden, die Benutzer, die die Anfragen gestellt haben, und das Datum der Anfrage.

Weitere Informationen zu CloudTrail finden Sie im AWS CloudTrail Benutzerhandbuch.

WorkDocs Informationen in CloudTrail

CloudTrail ist in Ihrem AWS Konto aktiviert, wenn Sie das Konto erstellen. Wenn eine Aktivität in stattfindet WorkDocs, wird diese Aktivität zusammen mit anderen CloudTrail AWS Serviceereignissen im Ereignisverlauf in einem Ereignis aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem AWS Konto ansehen, suchen und herunterladen. Weitere Informationen finden Sie unter Ereignisse mit CloudTrail Ereignisverlauf anzeigen.

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS Konto, einschließlich der Ereignisse für WorkDocs, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser standardmäßig für alle Regionen. Der Trail protokolliert Ereignisse aus allen Regionen der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie unter:

- Übersicht zum Erstellen eines Trails
- CloudTrail unterstützte Dienste und Integrationen
- Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien von mehreren Konten

Alle WorkDocs Aktionen werden von der Amazon WorkDocs API-Referenz protokolliert CloudTrail und sind in dieser dokumentiert. Beispielsweise generieren Aufrufe der `UpdateDocument` AbschnitteCreateFolder, `DeactivateUser` und Einträge in den CloudTrail Protokolldateien.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Gibt an, ob die Anforderung mit Root- oder IAM-Benutzer-Anmeldeinformationen ausgeführt wurde.

- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde.

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

WorkDocs Logdateieinträge verstehen

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

WorkDocs generiert verschiedene Arten von CloudTrail Einträgen, solche aus der Steuerebene und solche aus der Datenebene. Der wichtige Unterschied zwischen den beiden besteht darin, dass es sich bei der Benutzeridentität für Einträge auf der Kontrollebene um einen IAM-Benutzer handelt. Die Benutzeridentität für Einträge auf der Datenebene ist der WorkDocs Verzeichnisbenutzer.

> **Note**
>
> Um die Sicherheit zu erhöhen, sollten Sie nach Möglichkeit Verbundbenutzer anstelle von IAM-Benutzern erstellen.

Sensible Informationen, z. B. Kennwörter, Authentifizierungstoken, Dateikommentare und Dateiinhalt sind in den Protokolleinträgen geschwärzt. Diese werden in den Protokollen als HIDDEN_DUE_TO_SECURITY_REASONS angezeigt. CloudTrail Diese werden in den CloudTrail Protokollen als HIDDEN_DUE_TO_SECURITY_REASONS angezeigt.

Das folgende Beispiel zeigt zwei CloudTrail Protokolleinträge für WorkDocs: Der erste Datensatz bezieht sich auf eine Aktion auf der Steuerungsebene und der zweite auf eine Aktion auf der Datenebene.

```
{
  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"
    }
  ]
}
```

Konformitätsvalidierung für Amazon WorkDocs

Informationen darüber, ob AWS-Service ein AWS-Services in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter Umfang nach Compliance-Programm AWS-Services unter . Wählen Sie dort das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen unter .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- Compliance und Governance im Bereich Sicherheit – In diesen Anleitungen für die Lösungsimplementierung werden Überlegungen zur Architektur behandelt. Außerdem werden Schritte für die Bereitstellung von Sicherheits- und Compliance-Features beschrieben.
- Referenz für berechtigte HIPAA-Services – Listet berechtigte HIPAA-Services auf. Nicht alle AWS-Services sind HIPAA-fähig.
- AWS Compliance-Ressourcen — Diese Sammlung von Arbeitsmappen und Leitfäden gilt möglicherweise für Ihre Branche und Ihren Standort.
- AWS Leitfäden zur Einhaltung von Vorschriften für Kunden — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS-Services und die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zugeordnet.
- Evaluierung von Ressourcen anhand von Regeln im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.

- AWS Security Hub CSPM— Auf diese AWS-Service Weise erhalten Sie einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Die Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerelementreferenz.
- Amazon GuardDuty — Dies AWS-Service erkennt potenzielle Bedrohungen für Ihre Workloads AWS-Konten, Container und Daten, indem es Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedene Compliance-Anforderungen wie PCI DSS zu erfüllen, indem es die in bestimmten Compliance-Frameworks vorgeschriebenen Anforderungen zur Erkennung von Eindringlingen erfüllt.
- AWS Audit Manager— Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

Resilienz bei Amazon WorkDocs

Die AWS globale Infrastruktur basiert auf AWS Regionen und Availability Zones. AWS Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Availability Zones ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser hoch verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu AWS Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Infrastruktursicherheit bei Amazon WorkDocs

Als verwalteter Service WorkDocs ist Amazon durch die AWS globalen Netzwerksicherheitsverfahren geschützt. Weitere Informationen finden Sie unter Infrastruktursicherheit in AWS Identity and Access Management im IAM-Benutzerhandbuch und Best Practices for Security, Identity, & Compliance im AWS Architecture Center.

Sie verwenden AWS veröffentlichte API-Aufrufe für den Zugriff WorkDocs über das Netzwerk. Die Clients müssen Transport Layer Security (TLS) 1.2 unterstützen, und wir empfehlen die Verwendung

von TLS 1.3. Kunden müssen außerdem Cipher Suites mit Perfect Forward Secrecy wie Ephemeral Diffie-Hellman oder Elliptic Curve Ephemeral Diffie-Hellman unterstützen. Die meisten modernen Systemen wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS-Security-Token-Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Erste Schritte mit WorkDocs

WorkDocs verwendet ein Verzeichnis, um Organisationsinformationen für Ihre Benutzer und deren Dokumente zu speichern und zu verwalten. Im Gegenzug fügen Sie einer Site ein Verzeichnis hinzu, wenn Sie diese Site bereitstellen. Wenn Sie dies tun, fügt ein WorkDocs Feature namens Automatische Aktivierung die Benutzer im Verzeichnis der Site als verwaltete Benutzer hinzu. Sie benötigen also keine separaten Anmeldeinformationen, um sich bei Ihrer Site anzumelden, und sie können Dateien gemeinsam nutzen und gemeinsam daran arbeiten. Jeder Benutzer hat 1 TB Speicherplatz, sofern er nicht mehr kauft.

Sie müssen Benutzer nicht mehr manuell hinzufügen und aktivieren, können es aber immer noch. Sie können Benutzerrollen und Berechtigungen auch jederzeit ändern. Weitere Informationen dazu finden Sie weiter WorkDocs Benutzer einladen und verwalten unten in diesem Handbuch.

Wenn Sie Verzeichnisse erstellen müssen, können Sie:

- Simple AD-Verzeichnis erstellen.
- Erstellen Sie ein AD Connector Connector-Verzeichnis, um eine Verbindung zu Ihrem lokalen Verzeichnis herzustellen.
- Aktivieren Sie WorkDocs diese Option, um mit einem vorhandenen AWS Verzeichnis zu arbeiten.
- Habe ein Verzeichnis für dich WorkDocs erstellt.

Sie können auch eine Vertrauensbeziehung zwischen Ihrem AD-Verzeichnis und einem AWS Managed Microsoft AD Verzeichnis einrichten.

> **Note**
>
> Wenn Sie einem Compliance-Programm wie PCI, FedRAMP oder DoD angehören, müssen Sie ein AWS Managed Microsoft AD Verzeichnis einrichten, um die Compliance-Anforderungen zu erfüllen. In den Schritten in diesem Abschnitt wird erklärt, wie Sie ein vorhandenes Microsoft AD-Verzeichnis verwenden. Informationen zum Erstellen eines Microsoft AD-Verzeichnisses finden Sie unter AWS Managed Microsoft AD im AWS Directory Service Administration Guide.

Inhalt

- Aktivieren des einmaligen Anmeldens
- Aktivieren der Multifaktor-Authentifizierung
- Hochstufen eines Benutzers zum Administrator

Eine WorkDocs Site erstellen

Die Schritte in den folgenden Abschnitten erklären, wie Sie eine neue WorkDocs Site einrichten.

Aufgaben

- Bevor Sie beginnen
- Eine WorkDocs Site erstellen

Bevor Sie beginnen

Sie müssen über die folgenden Elemente verfügen, bevor Sie eine WorkDocs Site erstellen können.

- Ein AWS Konto zum Erstellen und Verwalten von WorkDocs Websites. Benutzer benötigen jedoch kein AWS Konto, um eine Verbindung herzustellen und sie zu verwenden WorkDocs. Weitere Informationen finden Sie unter Voraussetzungen für Amazon WorkDocs.
- Wenn Sie Simple AD verwenden möchten, müssen Sie die unter Simple AD AD-Voraussetzungen im AWS Directory Service Administratorhandbuch genannten Voraussetzungen erfüllen.
- Ein AWS Managed Microsoft AD Verzeichnis, wenn Sie einem Compliance-Programm wie PCI, FedRAMP oder DoD angehören. In den Schritten in diesem Abschnitt wird erklärt, wie Sie ein vorhandenes Microsoft AD-Verzeichnis verwenden. Informationen zum Erstellen eines Microsoft AD-Verzeichnisses finden Sie unter AWS Managed Microsoft AD im AWS Directory Service Administration Guide.
- Profilinformationen für den Administrator, einschließlich Vor- und Nachname sowie einer E-Mail-Adresse.

Eine WorkDocs Site erstellen

Folgen Sie diesen Schritten, um in wenigen Minuten eine WorkDocs Website zu erstellen.

Um die WorkDocs Site zu erstellen

1. Öffnen Sie die WorkDocs Konsole unter https://console.aws.amazon.com/zocalo/.

2. Wählen Sie auf der Startseite der Konsole unter WorkDocs Website erstellen die Option Jetzt starten aus.

   -ODER-

   Wählen Sie im Navigationsbereich Meine Websites und auf der Seite WorkDocs Websites verwalten die Option WorkDocs Website erstellen aus.

   Was als Nächstes passiert, hängt davon ab, ob Sie über ein Verzeichnis verfügen.

   - Wenn Sie über ein Verzeichnis verfügen, wird die Seite Verzeichnis auswählen angezeigt, auf der Sie ein vorhandenes Verzeichnis auswählen oder ein Verzeichnis erstellen können.
   - Wenn Sie kein Verzeichnis haben, wird die Seite Verzeichnistyp einrichten angezeigt, auf der Sie ein Simple AD- oder AD Connector Connector-Verzeichnis erstellen können.

   In den folgenden Schritten wird erklärt, wie Sie beide Aufgaben ausführen.

   Um ein vorhandenes Verzeichnis zu verwenden

   1. Öffnen Sie die Liste Verfügbare Verzeichnisse und wählen Sie das Verzeichnis aus, das Sie verwenden möchten.
   2. Klicken Sie auf Verzeichnis aktivieren.

   Erstellen eines -Verzeichnisses

   1. Wiederholen Sie die Schritte 1 und 2 oben.

      Was Sie jetzt tun, hängt davon ab, ob Sie Simple AD verwenden oder einen AD Connector erstellen möchten.

      Um Simple AD zu verwenden

      a. Wählen Sie Simple AD und dann Weiter.

         Die Seite Create Simple AD Site wird angezeigt.

      b. Geben Sie unter Zugriffspunkt im Feld Site-URL die URL für die Site ein.

c. Geben Sie unter Als WorkDocs Administrator festlegen die E-Mail-Adresse, den Vornamen und den Nachnamen des Administrators ein.

d. Füllen Sie bei Bedarf die Optionen unter Verzeichnisdetails und VPC-Konfiguration aus.

e. Wählen Sie Create Simple AD-Site aus.

So erstellen Sie ein AD Connector Connector-Verzeichnis

a. Wählen Sie AD Connector und dann Weiter.

Die Seite „AD Connector erstellen“ wird angezeigt.

b. Füllen Sie alle Felder unter Verzeichnisdetails aus.

c. Geben Sie unter Zugriffspunkt im Feld Site-URL die URL Ihrer Site ein.

d. Füllen Sie nach Bedarf die optionalen Felder unter VPC-Konfiguration aus.

e. Wählen Sie AD Connector-Site erstellen aus.

WorkDocs macht Folgendes:

- Wenn Sie in Schritt 4 oben „Eine VPC in meinem Namen einrichten“ ausgewählt haben, WorkDocs erstellt eine VPC für Sie. In einem Verzeichnis in der VPC werden Benutzer- und WorkDocs Standortinformationen gespeichert.
- Wenn Sie Simple AD verwendet haben, WorkDocs erstellt es einen Verzeichnisbenutzer und legt diesen Benutzer als WorkDocs Administrator fest. Wenn Sie ein AD Connector Connector-Verzeichnis erstellt haben, WorkDocs legt es den vorhandenen Verzeichnisbenutzer fest, den Sie als WorkDocs Administrator angegeben haben.
- Wenn Sie ein vorhandenes Verzeichnis verwendet haben, werden Sie WorkDocs aufgefordert, den Benutzernamen des WorkDocs Administrators einzugeben. Der Benutzer muss Mitglied des Verzeichnisses sein.

> **Note**
>
> WorkDocs benachrichtigt Benutzer nicht über die neue Site. Sie müssen ihnen die URL mitteilen und ihnen mitteilen, dass sie für die Nutzung der Website kein separates Login benötigen.

Aktivieren des einmaligen Anmeldens

AWS Directory Service ermöglicht Benutzern den Zugriff auf Amazon WorkDocs von einem Computer aus, der mit demselben Verzeichnis verbunden ist, in dem auch registriert WorkDocs ist, ohne dass die Anmeldeinformationen separat eingegeben werden müssen. WorkDocs Administratoren können Single Sign-On über die Directory Service Konsole aktivieren. Weitere Informationen finden Sie unter Single Sign-On im AWS Directory Service Administratorhandbuch.

Nachdem der WorkDocs Administrator Single Sign-On aktiviert hat, müssen die Benutzer der WorkDocs Site möglicherweise auch ihre Webbrowser-Einstellungen ändern, um Single Sign-On zuzulassen. Weitere Informationen finden Sie unter Single Sign-On für IE und Chrome und Single Sign-On für Firefox im Administratorhandbuch.AWS Directory Service

Aktivieren der Multifaktor-Authentifizierung

Sie verwenden die AWS Directory Services Console unter https://console.aws.amazon.com/directoryservicev2/, um die Multi-Faktor-Authentifizierung für Ihr AD Connector Connector-Verzeichnis zu aktivieren. Zum Aktivieren der MFA müssen Sie entweder über eine MFA-Lösung in Form eines Remote Authentication Dial-In User Service (RADIUS)-Servers verfügen oder über ein MFA-Plugin für einen RADIUS-Server, der bereits in Ihrer On-Premises-Infrastruktur vorhanden ist. Ihre MFA-Lösung sollte einmalige Sicherheitscodes (OTPs, One Time Passcodes) implementieren, die Benutzer von einem Hardwaregerät oder einer Software erhalten, die auf einem Gerät, beispielsweise einem Mobiltelefon, ausgeführt wird.

RADIUS ist ein client/server Industriestandardprotokoll, das Authentifizierung, Autorisierung und Kontoverwaltung ermöglicht, damit Benutzer eine Verbindung zu Netzwerkdiensten herstellen können. AWS Managed Microsoft AD umfasst einen RADIUS-Client, der eine Verbindung zu dem RADIUS-Server herstellt, auf dem Sie Ihre MFA-Lösung implementiert haben. Der RADIUS-Server überprüft den Benutzernamen und den OTP-Code. Wenn Ihr RADIUS-Server den Benutzer erfolgreich validiert, authentifiziert AWS Managed Microsoft AD den Benutzer anschließend gegenüber AD. Nach einer erfolgreichen AD-Authentifizierung können die Benutzer dann auf die AWS-Anwendung zugreifen. Für die Kommunikation zwischen dem AWS Managed Microsoft AD RADIUS-Client und Ihrem RADIUS-Server müssen Sie AWS-Sicherheitsgruppen konfigurieren, die die Kommunikation über Port 1812 ermöglichen.

Weitere Informationen finden Sie unter Aktivieren der Multi-Faktor-Authentifizierung für AWS Managed Microsoft AD im AWS Directory Service Administration Guide.

> **Note**
>
> Die Multi-Faktor-Authentifizierung ist für Simple AD AD-Verzeichnisse nicht verfügbar.

Hochstufen eines Benutzers zum Administrator

Sie verwenden die WorkDocs Konsole, um einen Benutzer zum Administrator heraufzustufen. Dazu gehen Sie wie folgt vor:

So stufen Sie einen Benutzer zum Administrator hoch

1. Öffnen Sie die WorkDocs Konsole unter https://console.aws.amazon.com/zocalo/.
2. Wählen Sie im Navigationsbereich Meine Websites aus.

   Die Seite „Ihre WorkDocs Websites verwalten“ wird angezeigt.
3. Wählen Sie die Schaltfläche neben der gewünschten Site aus, wählen Sie Aktionen und anschließend Administrator festlegen aus.

   Das Dialogfeld „ WorkDocs Administrator festlegen“ wird angezeigt.
4. Geben Sie im Feld Benutzername den Benutzernamen der Person ein, die Sie befördern möchten, und wählen Sie dann Als Administrator festlegen aus.

Du kannst auch das Admin-Kontrollpanel der WorkDocs Website verwenden, um einen Administrator herabzustufen. Weitere Informationen finden Sie unter Bearbeiten von Benutzern.

Verwaltung WorkDocs von der AWS Konsole aus

Sie verwenden diese Tools, um Ihre WorkDocs Websites zu verwalten:

- Die AWS Konsole bei https://console.aws.amazon.com/zocalo/.
- Das Site-Admin-Kontrollpanel, das Administratoren auf allen WorkDocs Websites zur Verfügung steht.

Jedes dieser Tools bietet eine andere Reihe von Aktionen, und in den Themen in diesem Abschnitt werden die von der AWS Konsole bereitgestellten Aktionen erläutert. Informationen zum Admin-Kontrollpanel der Site finden Sie unterVerwaltung WorkDocs über das Admin-Kontrollpanel der Website.

Site-Administratoren einrichten

Wenn Sie ein Administrator sind, können Sie Benutzern Zugriff auf das Site-Control-Panel und die darin enthaltenen Aktionen gewähren.

Um einen Administrator einzurichten

1. Öffnen Sie die WorkDocs Konsole unter https://console.aws.amazon.com/zocalo/.
2. Wählen Sie im Navigationsbereich Meine Websites aus.

   Die Seite „ WorkDocs Websites verwalten“ wird mit einer Liste Ihrer Websites angezeigt.
3. Wählen Sie die Schaltfläche neben der Site aus, für die Sie einen Administrator einrichten möchten.
4. Öffnen Sie die Aktionsliste und wählen Sie Als Administrator festlegen aus.

   Das Dialogfeld „ WorkDocs Administrator festlegen“ wird angezeigt.
5. Geben Sie im Feld Benutzername den Namen des neuen Administrators ein und wählen Sie dann Als Administrator festlegen aus.

Einladungs-E-Mails erneut senden

Sie können eine Einladungs-E-Mail jederzeit erneut senden.

Um die Einladungs-E-Mail erneut zu senden

1. Öffnen Sie die WorkDocs Konsole unter. https://console.aws.amazon.com/zocalo/
2. Wählen Sie im Navigationsbereich Meine Websites aus.

   Die Seite „ WorkDocs Websites verwalten“ wird mit einer Liste Ihrer Websites angezeigt.
3. Wählen Sie die Schaltfläche neben der Site aus, für die Sie die E-Mail erneut senden möchten.
4. Öffnen Sie die Aktionsliste und wählen Sie Einladungs-E-Mail erneut senden aus.

   Eine Erfolgsmeldung in einem grünen Banner wird oben auf der Seite angezeigt.

Verwaltung der Multifaktor-Authentifizierung

Sie können die Multi-Faktor-Authentifizierung aktivieren, nachdem Sie eine WorkDocs Site erstellt haben. Weitere Informationen über die Authentifizierung finden Sie unter Aktivieren der Multifaktor-Authentifizierung.

Website einrichten URLs

> **Note**
>
> Wenn Sie den Prozess zur Erstellung der Website unter verfolgt habenErste Schritte mit WorkDocs, haben Sie eine Site-URL eingegeben. Daher ist der Befehl WorkDocs „Site-URL festlegen“ nicht verfügbar, da Sie eine URL nur einmal festlegen können. Sie befolgen diese Schritte nur, wenn Sie Amazon bereitstellen WorkSpaces und in Amazon integrieren WorkDocs. Beim WorkSpaces Amazon-Integrationsprozess müssen Sie anstelle einer Site-URL eine Seriennummer eingeben, sodass Sie nach Abschluss der Integration eine URL eingeben müssen. Weitere Informationen zur Integration von Amazon WorkSpaces WorkDocs finden Sie unter Integrieren mit WorkDocs im WorkSpaces Amazon-Benutzerhandbuch.

Um eine Site-URL festzulegen

1. Öffnen Sie die WorkDocs Konsole unter https://console.aws.amazon.com/zocalo/.
2. Wählen Sie im Navigationsbereich Meine Websites aus.

Die Seite „ WorkDocs Websites verwalten“ wird mit einer Liste Ihrer Websites angezeigt.

3. Wählen Sie die Site aus, die Sie in Amazon integriert haben WorkSpaces. Die URL enthält die Verzeichnis-ID Ihrer WorkSpaces Amazon-Instance, z. https://{directory_id}.awsapps.comB.
4. Wählen Sie die Schaltfläche neben dieser URL, öffnen Sie die Aktionsliste und wählen Sie Site-URL festlegen aus.

   Das Dialogfeld „Site-URL festlegen“ wird angezeigt.
5. Geben Sie im Feld Site-URL die URL für die Site ein und wählen Sie dann Site-URL festlegen aus.
6. Wählen Sie auf der Seite „ WorkDocs Websites verwalten“ die Option Aktualisieren aus, um die neue URL zu sehen.

Benachrichtigungen verwalten

> **Note**
>
> Um die Sicherheit zu erhöhen, sollten Sie nach Möglichkeit Verbundbenutzer anstelle von IAM-Benutzern erstellen.

Benachrichtigungen ermöglichen es IAM-Benutzern oder -Rollen, die CreateNotificationSubscriptionAPI aufzurufen, mit der Sie Ihren eigenen Endpunkt für die Verarbeitung der gesendeten SNS-Nachrichten einrichten können. WorkDocs Weitere Informationen zu Benachrichtigungen finden Sie im Entwicklerhandbuch unter Benachrichtigungen für einen IAM-Benutzer oder eine IAM-Rolle einrichten. WorkDocs

Sie können Benachrichtigungen erstellen und löschen. In den folgenden Schritten wird erklärt, wie Sie beide Aufgaben ausführen.

> **Note**
>
> Um eine Benachrichtigung zu erstellen, benötigen Sie Ihren IAM- oder Rollen-ARN. Gehen Sie wie folgt vor, um Ihren IAM-ARN zu finden:
>
> 1. Öffnen Sie unter https://console.aws.amazon.com/iam/ die IAM-Konsole.
> 2. Wählen Sie in der Navigationsleiste Benutzer aus.

3. Wählen Sie Ihren Benutzernamen aus.
4. Kopieren Sie unter Zusammenfassung Ihren ARN.

Um eine Benachrichtigung zu erstellen

1. Öffnen Sie die WorkDocs Konsole unter https://console.aws.amazon.com/zocalo/.
2. Wählen Sie im Navigationsbereich Meine Websites aus.

   Die Seite „ WorkDocs Websites verwalten“ wird mit einer Liste Ihrer Websites angezeigt.
3. Wählen Sie die Schaltfläche neben der gewünschten Site aus.
4. Öffnen Sie die Aktionsliste und wählen Sie Benachrichtigungen verwalten.

   Die Seite „Benachrichtigungen verwalten“ wird angezeigt.
5. Wählen Sie Benachrichtigung erstellen aus.
6. Geben Sie im Dialogfeld „Neue Benachrichtigung“ Ihren IAM- oder Rollen-ARN ein und wählen Sie dann Benachrichtigungen erstellen aus.

So löschen Sie eine Benachrichtigung

1. Öffnen Sie die WorkDocs Konsole unter. https://console.aws.amazon.com/zocalo/
2. Wählen Sie im Navigationsbereich Meine Websites aus.

   Die Seite „ WorkDocs Websites verwalten“ wird mit einer Liste Ihrer Websites angezeigt.
3. Wählen Sie die Schaltfläche neben der Site aus, für die die Benachrichtigung angezeigt wurde, die Sie löschen möchten.
4. Öffnen Sie die Aktionsliste und wählen Sie Benachrichtigungen verwalten aus.
5. Wählen Sie auf der Seite Benachrichtigungen verwalten die Schaltfläche neben der Benachrichtigung, die Sie löschen möchten, und wählen Sie dann Benachrichtigungen löschen aus.

Löschen einer Website

Sie verwenden die WorkDocs Konsole, um eine Site zu löschen.

> **Warning**
>
> Sie verlieren alle Dateien, wenn Sie eine Site löschen. Löschen Sie eine Website nur dann, wenn Sie sich absolut sicher sind, dass Sie die Informationen nicht mehr benötigen.

So löschen Sie eine Website

1. Öffnen Sie die WorkDocs Konsole unter https://console.aws.amazon.com/zocalo/.
2. Wählen Sie in der Navigationsleiste Meine Websites aus.

   Die Seite „Meine WorkDocs Websites verwalten“ wird angezeigt.
3. Wählen Sie die Schaltfläche neben der Website, die Sie löschen möchten, und wählen Sie dann Löschen aus.

   Das Dialogfeld „Site-URL löschen“ wird angezeigt.
4. Wählen Sie optional Auch das Benutzerverzeichnis löschen.

   > **Important**
   >
   > Wenn Sie kein eigenes Verzeichnis für angeben WorkDocs, erstellen wir eines für Sie. Wenn Sie die WorkDocs Site löschen, wird Ihnen das von uns erstellte Verzeichnis in Rechnung gestellt, sofern Sie dieses Verzeichnis nicht löschen oder es für eine andere AWS-Anwendung verwenden. Preisinformationen finden Sie unter AWS Directory Service – Preise.
5. Geben Sie im Feld Site-URL die Site-URL ein und wählen Sie dann Löschen.

   Die Website wird sofort gelöscht und ist nicht mehr verfügbar.

Verwaltung WorkDocs über das Admin-Kontrollpanel der Website

Sie verwenden diese Tools, um Ihre WorkDocs Websites zu verwalten:

- Das Control Panel für Site-Administratoren, das Administratoren auf allen WorkDocs Websites zur Verfügung steht und in den folgenden Themen beschrieben wird.
- Die AWS Konsole unter https://console.aws.amazon.com/zocalo/.

Jedes dieser Tools bietet unterschiedliche Aktionen. In den Themen in diesem Abschnitt werden die Aktionen erläutert, die über das Control Panel für den Administrator der Website bereitgestellt werden. Informationen zu den in der Konsole verfügbaren Aufgaben finden Sie unterVerwaltung WorkDocs von der AWS Konsole aus.

Einstellungen der bevorzugten Sprache

Sie können die Sprache für E-Mail-Benachrichtigungen angeben.

So ändern Sie die Spracheinstellungen

1. Wählen Sie unter Mein Konto die Option Administrator-Systemsteuerung öffnen.
2. Wählen Sie für Einstellungen der bevorzugten Sprache die von Ihnen bevorzugte Sprache aus.

Hancom Online Editing und Office Online

Aktivieren oder deaktivieren Sie die Einstellungen für Hancom Online Editing und Office Online über das Admin-Bedienfeld. Weitere Informationen finden Sie unter Aktivieren der gemeinsamen Bearbeitung.

Speicher

Geben Sie die Speichermenge an, die neue Benutzer erhalten.

So ändern Sie die Speichereinstellungen

1. Wählen Sie unter Mein Konto die Option Administrator-Systemsteuerung öffnen.

2. Wählen Sie für Speicher die Option Änderung.
3. Legen Sie im Dialogfeld Speicherlimit fest, ob der neuen Benutzern zugewiesene Speicher unbegrenzt oder begrenzt sein soll.
4. Wählen Sie Save Changes.

Eine Änderung der Speichereinstellung wirkt sich nur auf Benutzer aus, die nach Ändern der Einstellung hinzugefügt werden. Die Speichermenge von vorhandenen Benutzern ist davon nicht betroffen. Informationen dazu, wie Sie die Speicherlimits von vorhandenen Benutzern ändern, finden Sie unter Bearbeiten von Benutzern.

IP-Genehmigungsliste

WorkDocs Site-Administratoren können Einstellungen für die IP-Zulassungsliste hinzufügen, um den Zugriff auf die Site auf einen zulässigen Bereich von IP-Adressen zu beschränken. Sie können bis zu 500 Einstellungen für die IP-Zulassungsliste pro Site hinzufügen.

> **Note**
>
> Die IP-Zulassungsliste funktioniert derzeit nur für IPv4 Adressen. Die Sperrung von IP-Adressen wird derzeit nicht unterstützt.

So fügen Sie einen IP-Bereich zur IP Allow List (IP-Genehmigungsliste) hinzu

1. Wählen Sie unter Mein Konto die Option Administrator-Systemsteuerung öffnen.
2. Wählen Sie unter IP Allow List (IP-Genehmigungsliste) die Option Change (Ändern).
3. Geben Sie unter CIDR-Wert eingeben den CIDR-Block (Classless Inter-Domain Routing) für die IP-Adressbereiche ein und wählen Sie Hinzufügen aus.
    - Um den Zugriff von einer einzigen IP-Adresse zu gewähren, geben Sie `/32` als CIDR-Präfix an:
4. Wählen Sie Save Changes.
5. Benutzer, die von den IP-Adressen auf der IP Allow List (IP-Genehmigungsliste) auf Ihre Website zugreifen, wird der Zugriff gewährt. Benutzer, die über eine nicht autorisierte IP-Adresse eine Verbindung herstellen möchten, erhalten die Antwort, dass sie nicht autorisiert sind.

> **Warning**
>
> Wenn Sie einen CIDR-Wert eingeben, der verhindert, dass Sie über Ihre aktuelle IP-Adresse auf die Website zugreifen können, wird eine Warnmeldung angezeigt. Wenn Sie mit dem aktuellen CIDR-Wert fortfahren möchten, können Sie mit Ihrer aktuellen IP-Adresse nicht auf die Website zugreifen. Diese Aktion kann nur rückgängig gemacht werden, wenn Sie sich an den AWS Support wenden.

Sicherheit — Einfache Websites ActiveDirectory

In diesem Thema werden die verschiedenen Sicherheitseinstellungen für einfache ActiveDirectory Websites erklärt. Informationen zur Verwaltung von Websites, die ActiveDirectory Connector verwenden, finden Sie im nächsten Abschnitt.

Um Sicherheitseinstellungen zu verwenden

1. Wählen Sie das Profilsymbol in der oberen rechten Ecke des WorkDocs Clients.

2. Wählen Sie unter Admin die Option Admin-Kontrollpanel öffnen.
3. Scrollen Sie nach unten zu Sicherheit und wählen Sie Ändern.

   Das Dialogfeld „Richtlinieneinstellungen“ wird angezeigt. In der folgenden Tabelle sind die Sicherheitseinstellungen für einfache ActiveDirectory Websites aufgeführt.

Einstellung	Beschreibung
Wählen Sie unter Wählen Sie Ihre Einstellung für gemeinsam nutzbare Links eine der folgenden Optionen aus:	
Erlauben Sie keine Links für die gesamte Website oder öffentliche, gemeinsam nutzbare Links	Deaktiviert das Teilen von Links für alle Benutzer.

Einstellung	Beschreibung
Erlaubt es Benutzern, Links für die gesamte Website zu erstellen, die gemeinsam genutzt werden können, aber nicht, dass sie öffentlich gemeinsam nutzbare Links erstellen	Beschränkt die gemeinsame Nutzung von Links auf Mitglieder der Website. Verwaltete Benutzer können diese Art von Link erstellen.
Erlauben Sie Benutzern, Links für die gesamte Website zu erstellen, aber nur Poweruser können öffentliche Links erstellen, die gemeinsam genutzt werden können	Verwaltete Benutzer können Links für die gesamte Website erstellen, aber nur Poweruser können öffentliche Links erstellen. Öffentliche Links ermöglichen den Zugriff auf alle Benutzer im Internet.
Alle verwalteten Benutzer können Links für die gesamte Website und öffentlich gemeinsam nutzbare Links erstellen	Verwaltete Benutzer können öffentliche Links erstellen.

Aktivieren oder deaktivieren Sie unter Automatische Aktivierung das Kontrollkästchen.

Erlauben Sie, dass alle Benutzer in Ihrem Verzeichnis bei ihrer ersten Anmeldung auf Ihrer WorkDocs Site automatisch aktiviert werden.	Aktiviert Benutzer automatisch, wenn sie sich zum ersten Mal auf Ihrer Site anmelden.

Wählen Sie unter Wer darf neue Nutzer auf Ihre WorkDocs Website einladen dürfen, eine der folgenden Optionen aus:

Nur Administratoren können neue Benutzer einladen.	Nur Administratoren können neue Benutzer einladen.
Benutzer können neue Benutzer von überall aus einladen, indem sie Dateien oder Ordner mit ihnen teilen.	Ermöglicht Benutzern, neue Benutzer einzuladen, indem sie Dateien oder Ordner mit diesen Benutzern teilen.
Benutzer können neue Benutzer aus bestimmten Domänen einladen, indem sie Dateien oder Ordner mit ihnen teilen.	Benutzer können neue Personen aus den angegebenen Domänen einladen, indem sie Dateien oder Ordner für sie freigeben.

Einstellung	Beschreibung
Aktivieren oder deaktivieren Sie unter Rolle für neue Benutzer konfigurieren das Kontrollk ästchen.	
Neue Benutzer aus Ihrem Verzeichnis werden zu verwalteten Benutzern (sie sind standardmäßig Gastbenutzer)	Konvertiert automatisch neue Benutzer aus Ihrem Verzeichnis in verwaltete Benutzer.

4. Wenn Sie fertig sind, wählen Sie Änderungen speichern.

Sicherheit — ActiveDirectory Connector-Sites

In diesem Thema werden die verschiedenen Sicherheitseinstellungen für ActiveDirectory Connector-Sites erklärt. Informationen zur Verwaltung von Websites, die Simple verwenden ActiveDirectory, finden Sie im vorherigen Abschnitt.

Um Sicherheitseinstellungen zu verwenden

1. Wählen Sie das Profilsymbol in der oberen rechten Ecke des WorkDocs Clients.

2. Wählen Sie unter Admin die Option Admin-Kontrollpanel öffnen.
3. Scrollen Sie nach unten zu Sicherheit und wählen Sie Ändern.

Das Dialogfeld „Richtlinieneinstellungen“ wird angezeigt. In der folgenden Tabelle werden die Sicherheitseinstellungen für ActiveDirectory Connector-Sites aufgeführt und beschrieben.

Einstellung	Beschreibung
Wählen Sie unter Wählen Sie Ihre Einstellung für gemeinsam nutzbare Links eine der folgenden Optionen aus:	
Erlauben Sie keine Links für die gesamte Website oder öffentliche, gemeinsam nutzbare Links	Wenn diese Option ausgewählt ist, wird die gemeinsame Nutzung von Links für alle Benutzer deaktiviert.

Einstellung	Beschreibung
Erlaubt es Benutzern, Links für die gesamte Website zu erstellen, die gemeinsam genutzt werden können, aber nicht, öffentliche Links zu erstellen	Beschränkt die gemeinsame Nutzung von Links auf Mitglieder der Website. Verwaltete Benutzer können diese Art von Link erstellen.
Erlauben Sie Benutzern, Links für die gesamte Website zu erstellen, aber nur Poweruser können öffentliche Links erstellen, die gemeinsam genutzt werden können	Verwaltete Benutzer können Links für die gesamte Website erstellen, aber nur Poweruser können öffentliche Links erstellen. Öffentliche Links ermöglichen den Zugriff auf alle Benutzer im Internet.
Alle verwalteten Benutzer können Links für die gesamte Website und öffentlich gemeinsam nutzbare Links erstellen	Verwaltete Benutzer können öffentliche Links erstellen.

Aktivieren oder deaktivieren Sie unter Automatische Aktivierung das Kontrollkästchen.

Erlauben Sie, dass alle Benutzer in Ihrem Verzeichnis bei ihrer ersten Anmeldung auf Ihrer WorkDocs Site automatisch aktiviert werden.	Aktiviert Benutzer automatisch, wenn sie sich zum ersten Mal auf Ihrer Site anmelden.

Unter Wer sollte Verzeichnisbenutzer auf Ihrer WorkDocs Site aktivieren dürfen? , wählen Sie eine der folgenden Optionen aus:

Nur Administratoren können neue Benutzer aus Ihrem Verzeichnis aktivieren.	Erlaubt nur Administratoren, neue Verzeichn isbenutzer zu aktivieren.
Benutzer können neue Benutzer aus Ihrem Verzeichnis aktivieren, indem sie Dateien oder Ordner mit ihnen teilen.	Ermöglicht Benutzern, Verzeichnisbenutzer zu aktivieren, indem sie Dateien oder Ordner mit den Verzeichnisbenutzern teilen.
Benutzer können neue Benutzer aus einigen bestimmten Domänen aktivieren, indem sie Dateien oder Ordner mit ihnen teilen.	Benutzer können nur Dateien oder Ordner von Benutzern in bestimmten Domänen teilen. Wenn Sie diese Option wählen, müssen Sie die Domänen eingeben.

Einstellung	Beschreibung
Unter Wer sollte neue Benutzer auf Ihre WorkDocs Website einladen dürfen? , wählen Sie eine der folgenden Optionen aus:	
Mit externen Benutzern teilen **Note** Die folgenden Optionen werden erst angezeigt, nachdem Sie diese Einstellung ausgewählt haben.	Ermöglicht Administratoren und Benutzern , neue externe Benutzer zu Ihrer WorkDocs Site einzuladen.
Nur Administratoren können neue externe Benutzer einladen	Nur Administratoren können externe Benutzer einladen.
Alle verwalteten Benutzer können neue Benutzer einladen	Ermöglicht verwalteten Benutzern, externe Benutzer einzuladen.
Nur Poweruser können neue externe Benutzer einladen.	Ermöglicht es nur Power-Usern, neue externe Benutzer einzuladen.
Wählen Sie unter Rolle für neue Benutzer konfigurieren eine oder beide Optionen aus.	
Neue Benutzer aus Ihrem Verzeichnis werden zu verwalteten Benutzern (sie sind standardmäßig Gastbenutzer)	Konvertiert automatisch neue Benutzer aus Ihrem Verzeichnis in verwaltete Benutzer.
Neue externer Benutzer sind verwaltete Benutzer (standardmäßig Gastbenutzer)	Konvertiert automatisch neue externe Benutzer in verwaltete Benutzer.

4. Wenn Sie fertig sind, wählen Sie Änderungen speichern.

Aufbewahrung im Papierkorb

Wenn ein Benutzer eine Datei löscht, wird die Datei 30 Tage lang im Papierkorb des Benutzers WorkDocs gespeichert. WorkDocs Verschiebt die Dateien anschließend für 60 Tage in einen temporären Wiederherstellungskorb und löscht sie anschließend dauerhaft. Nur Administratoren können den temporären Wiederherstellungsbehälter sehen. Durch Änderung der standortweiten

Datenaufbewahrungsrichtlinie können Site-Administratoren den Aufbewahrungszeitraum für den Wiederherstellungsordner auf mindestens null Tage und maximal 365 Tage ändern.

So ändern Sie den Aufbewahrungszeitraum des Papierkorbs

1. Wählen Sie unter Mein Konto die Option Administrator-Systemsteuerung öffnen.
2. Wählen Sie neben Aufbewahrung im Papierkorb die Option Änderung.
3. Geben Sie die Anzahl der Tage ein, für die Dateien im Wiederherstellungskorb aufbewahrt werden sollen, und wählen Sie Speichern.

> **Note**
>
> Der Standardaufbewahrungszeitraum beträgt 60 Tage. Sie können einen Zeitraum von 0 —365 Tagen verwenden.

Administratoren können Benutzerdateien aus dem Wiederherstellungsbehälter wiederherstellen, bevor sie dauerhaft WorkDocs gelöscht werden.

So stellen Sie eine Datei eines Benutzers wieder her

1. Wählen Sie unter Mein Konto die Option Administrator-Systemsteuerung öffnen.
2. Wählen Sie unter Benutzer verwalten das Ordnersymbol des Benutzers aus.
3. Wählen Sie unter Recovery bin (Papierkorb für Wiederherstellung) die wiederherzustellenden Dateien aus und wählen Sie anschließend das Symbol Recover (Wiederherstellen).
4. Wählen Sie unter Restore file (Datei wiederherstellen) den Speicherort zum Wiederherstellen der Datei aus und klicken Sie auf Restore (Wiederherstellen).

Verwalten von Benutzereinstellungen

Sie können Einstellungen für Benutzer verwalten, darunter Ändern von Benutzerrollen und Einladen, Aktivieren oder Deaktivieren von Benutzern. Weitere Informationen finden Sie unter WorkDocs Benutzer einladen und verwalten.

WorkDocs Drive auf mehreren Computern bereitstellen

Wenn Sie über eine Maschinenflotte verfügen, die einer Domäne angehört, können Sie Group Policy Objects (GPO) oder System Center Configuration Manager (SCCM) verwenden, um den Drive-Client zu installieren. WorkDocs Sie können den Client von den Clients herunterladen. https://amazonworkdocs.com/en/

Denken Sie dabei daran, dass WorkDocs Drive für alle AWS-IP-Adressen HTTPS-Zugriff auf Port 443 benötigt. Sie sollten auch sicherstellen, dass Ihre Zielsysteme die Installationsanforderungen für WorkDocs Drive erfüllen. Weitere Informationen finden Sie unter WorkDocs Drive-Installation im WorkDocs Amazon-Benutzerhandbuch.

> **Note**
>
> Als bewährte Methode bei der Verwendung von GPO oder SCCM empfiehlt es sich, den WorkDocs Drive-Client zu installieren, nachdem sich die Benutzer angemeldet haben.

Das MSI-Installationsprogramm für WorkDocs Drive unterstützt die folgenden optionalen Installationsparameter:

- **`SITEID`**— Füllt die WorkDocs Site-Informationen für Benutzer bei der Registrierung vorab aus. Beispiel, `SITEID=`*`site-name`*.
- **`DefaultDriveLetter`**— Füllt den Laufwerksbuchstaben, der für die Installation von Drive verwendet werden soll, vorab aus. WorkDocs Beispiel, `DefaultDriveLetter=`*`W`*. Denken Sie daran, dass jeder Benutzer einen anderen Laufwerksbuchstaben haben muss. Außerdem können Benutzer den Laufwerksnamen ändern, jedoch nicht den Laufwerksbuchstaben, nachdem sie WorkDocs Drive zum ersten Mal gestartet haben.

Im folgenden Beispiel wird WorkDocs Drive ohne Benutzeroberflächen und ohne Neustarts bereitgestellt. Beachten Sie, dass der Standardname der MSI-Datei verwendet wird:

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

WorkDocs Benutzer einladen und verwalten

Wenn Sie bei der Erstellung einer Website ein Verzeichnis anhängen, WorkDocs fügt die Funktion zur automatischen Aktivierung standardmäßig alle Benutzer in diesem Verzeichnis der neuen Site als verwaltete Benutzer hinzu.

WorkDocsIn müssen sich verwaltete Benutzer nicht mit separaten Anmeldeinformationen anmelden. Sie können Dateien teilen und gemeinsam daran arbeiten und verfügen automatisch über 1 TB Speicherplatz. Sie können die automatische Aktivierung jedoch deaktivieren, wenn Sie nur einige Benutzer in einem Verzeichnis hinzufügen möchten. In den nächsten Abschnitten wird beschrieben, wie das geht.

Darüber hinaus können Sie Benutzer einladen, aktivieren oder deaktivieren und Benutzerrollen und Einstellungen ändern. Außerdem können Sie einen Benutzer zum Administrator hochstufen. Weitere Informationen zur Beförderung von Benutzern finden Sie unterHochstufen eines Benutzers zum Administrator.

Sie erledigen diese Aufgaben im Admin-Kontrollpanel des WorkDocs Webclients. In den folgenden Abschnitten wird erklärt, wie das geht. Wenn Sie jedoch noch nicht damit vertraut sind WorkDocs, nehmen Sie sich ein paar Minuten Zeit und informieren Sie sich über die verschiedenen Benutzerrollen, bevor Sie sich mit administrativen Aufgaben befassen.

Inhalt

Übersicht: Benutzerrollen

WorkDocs definiert die folgenden Benutzerrollen. Sie können die Rollen von Benutzern ändern, indem Sie deren Benutzerprofile bearbeiten. Weitere Informationen finden Sie unter Bearbeiten von Benutzern.

- Admin: Ein bezahlter Benutzer mit Administratorberechtigungen für die gesamte Website, einschließlich Benutzerverwaltung und Konfiguration der Websiteeinstellung. Weitere Informationen zum Hochstufen eines Benutzers zum Administrator finden Sie unter Hochstufen eines Benutzers zum Administrator.
- Hauptbenutzer: Ein bezahlter Benutzer, der vom Administrator über spezielle Berechtigungen verfügt. Weitere Informationen zum Festlegen von Berechtigungen für einen Hauptbenutzer finden Sie unter Sicherheit — Einfache Websites ActiveDirectory undSicherheit — ActiveDirectory Connector-Sites.
- Benutzer: Ein kostenpflichtiger Benutzer, der Dateien speichern und mit anderen auf einer WorkDocs Site zusammenarbeiten kann.
- Gastbenutzer: Ein unbezahlter Benutzer, der nur Dateien anzeigen kann. Sie können Gastbenutzer auf die Rollen „Benutzer“, „Hauptbenutzer“ oder „Administrator“ hochstufen.

> **Note**
>
> Wenn Sie die Rolle eines Gastbenutzers ändern, führen Sie eine einmalige Aktion aus, die Sie nicht rückgängig machen können.

WorkDocs definiert auch diese zusätzlichen Benutzertypen.

WS-Benutzer

Ein Benutzer mit einem zugewiesenen WorkSpaces WorkSpace.

- Zugriff auf alle WorkDocs Funktionen
- Standardspeicher von 50 GB (kostenpflichtiges Upgrade auf 1 TB möglich)
- Keine monatliche Kosten

Hochgestufter WS-Benutzer

Ein Benutzer mit einem zugewiesenen WorkSpaces WorkSpace und aktualisierten Speicher.

- Zugriff auf alle WorkDocs Funktionen
- Standardspeicher von 1 TB (zusätzlicher Speicher auf pay-as-you-go Basis verfügbar)
- Monatliche Kosten

WorkDocs Benutzer

Ein aktiver WorkDocs Benutzer ohne zugewiesenen WorkSpaces WorkSpace.

- Zugriff auf alle WorkDocs Funktionen
- Standardspeicher von 1 TB (zusätzlicher Speicher auf pay-as-you-go Basis verfügbar)
- Monatliche Kosten

Das Admin-Kontrollpanel starten

Sie verwenden das administrative Bedienfeld im WorkDocs Webclient, um die automatische Aktivierung ein- und auszuschalten und Benutzerrollen und Einstellungen zu ändern.

Um das Admin-Kontrollpanel zu öffnen

1. Wählen Sie das Profilsymbol in der oberen rechten Ecke des WorkDocs Clients.

2. Wählen Sie unter Admin die Option Admin-Kontrollpanel öffnen aus.

> **Note**
>
> Einige Optionen in der Systemsteuerung unterscheiden sich zwischen Cloud-Verzeichnissen und verbundenen Verzeichnissen.

Automatische Aktivierung ausschalten

Sie deaktivieren die automatische Aktivierung, wenn Sie nicht alle Benutzer in einem Verzeichnis zu einer neuen Website hinzufügen möchten und wenn Sie den Benutzern, die Sie zu einer neuen

Website einladen, unterschiedliche Berechtigungen und Rollen zuweisen möchten. Wenn Sie die automatische Aktivierung deaktivieren, können Sie auch entscheiden, wer neue Benutzer zu der Site einladen darf — aktuelle Benutzer, Hauptbenutzer oder Administratoren. In diesen Schritten wird erklärt, wie Sie beide Aufgaben ausführen.

Um die automatische Aktivierung auszuschalten

1. Wählen Sie das Profilsymbol in der oberen rechten Ecke des WorkDocs Clients.

2. Wählen Sie unter Admin die Option Admin-Kontrollpanel öffnen aus.
3. Scrollen Sie nach unten zu Sicherheit und wählen Sie Ändern.

   Das Dialogfeld „Richtlinieneinstellungen“ wird angezeigt.
4. Deaktivieren Sie unter Automatische Aktivierung das Kontrollkästchen Automatische Aktivierung aller Benutzer in Ihrem Verzeichnis zulassen, wenn sie sich zum ersten Mal an Ihrer WorkDocs Site anmelden.

   Die Optionen ändern sich unter Wer sollte Verzeichnisbenutzer auf Ihrer WorkDocs Site aktivieren dürfen. Sie können aktuellen Benutzern die Möglichkeit geben, neue Benutzer einzuladen, oder Sie können diese Möglichkeit Hauptbenutzern oder anderen Administratoren geben.
5. Wählen Sie eine Option aus und wählen Sie dann Änderungen speichern.

Wiederholen Sie die Schritte 1—4, um die automatische Aktivierung wieder zu aktivieren.

Link-Sharing verwalten

In diesem Thema wird erklärt, wie Sie das Teilen von Links verwalten. WorkDocs Benutzer können ihre Dateien und Ordner teilen, indem sie Links mit ihnen teilen. Sie können Dateilinks innerhalb und außerhalb Ihrer Organisation teilen, aber sie können Ordnerlinks nur intern teilen. Als Administrator können Sie festlegen, wer Links teilen kann.

Um das Teilen von Links zu aktivieren

1. Wählen Sie das Profilsymbol in der oberen rechten Ecke des WorkDocs Clients.

2. Wählen Sie unter Admin die Option Admin-Kontrollpanel öffnen aus.
3. Scrollen Sie nach unten zu Sicherheit und wählen Sie Ändern.

   Das Dialogfeld „Richtlinieneinstellungen“ wird angezeigt.
4. Wählen Sie unter Wählen Sie Ihre Einstellung für gemeinsam nutzbare Links eine Option aus:

   - Keine Links für die gesamte Website oder öffentlich teilbare Links zulassen — Deaktiviert das Teilen von Links für alle Benutzer.
   - Erlauben Sie Benutzern, Links für die gesamte Website zu erstellen, die gemeinsam genutzt werden können, aber nicht, dass sie öffentlich gemeinsam nutzbare Links erstellen — Beschränkt die gemeinsame Nutzung von Links auf Mitglieder der Website. Verwaltete Benutzer können diese Art von Link erstellen.
   - Erlauben Sie Benutzern, für die gesamte Website gemeinsam nutzbare Links zu erstellen, aber nur Poweruser können öffentliche, gemeinsam nutzbare Links erstellen — Verwaltete Benutzer können Links für die gesamte Website erstellen, aber nur Poweruser können öffentliche Links erstellen. Öffentliche Links ermöglichen jedem Zugriff auf das Internet.
   - Alle verwalteten Benutzer können Links für die gesamte Website und öffentlich gemeinsam nutzbare Links erstellen. Verwaltete Benutzer können öffentliche Links erstellen.
5. Wählen Sie Save Changes.

Steuerung von Benutzereinladungen bei aktivierter automatischer Aktivierung

Wenn Sie die automatische Aktivierung aktivieren — und denken Sie daran, dass sie standardmäßig aktiviert ist —, können Sie Benutzern die Möglichkeit geben, andere Benutzer einzuladen. Sie können einer der folgenden Optionen die Erlaubnis erteilen:

- Alle Benutzer
- Power-User
- Administratoren.

Sie können Berechtigungen auch vollständig deaktivieren. In diesen Schritten wird erklärt, wie das geht.

So legen Sie Einladungsberechtigungen fest

1. Wählen Sie das Profilsymbol in der oberen rechten Ecke des WorkDocs Clients.

2. Wählen Sie unter Admin die Option Admin-Kontrollpanel öffnen aus.
3. Scrollen Sie nach unten zu Sicherheit und wählen Sie Ändern.

   Das Dialogfeld „Richtlinieneinstellungen“ wird angezeigt.
4. Aktivieren Sie unter Wer darf Verzeichnisbenutzer auf Ihrer WorkDocs Site aktivieren? Aktivieren Sie das Kontrollkästchen Für externe Benutzer freigeben, wählen Sie eine der Optionen unter dem Kontrollkästchen aus und wählen Sie dann Änderungen speichern aus.

   -ODER-

   Deaktivieren Sie das Kontrollkästchen, wenn Sie nicht möchten, dass jemand neue Benutzer einlädt, und wählen Sie dann Änderungen speichern aus.

Einladen neuer Benutzer

Sie können neue Benutzer einladen, einem Verzeichnis beizutreten. Sie können auch vorhandenen Benutzern ermöglichen, neue Benutzer einzuladen. Weitere Informationen finden Sie unter Sicherheit — Einfache Websites ActiveDirectory und Sicherheit — ActiveDirectory Connector-Sites in diesem Handbuch.

Einladen von neuen Benutzern

1. Wählen Sie das Profilsymbol in der oberen rechten Ecke des WorkDocs Clients.

2. Wählen Sie unter Admin die Option Admin-Kontrollpanel öffnen aus.
3. Wählen Sie unter Benutzer verwalten, die Option Benutzer einladen aus.

4. Wählen Sie im Dialogfeld „Benutzer einladen“ für Wen möchten Sie einladen? , geben Sie die E-Mail-Adresse der eingeladenen Person ein und wählen Sie Senden. Wiederholen Sie diesen Schritt für jede Einladung.

WorkDocs sendet eine Einladungs-E-Mail an jeden Empfänger. Die E-Mail enthält einen Link und Anweisungen zum Erstellen eines WorkDocs Kontos. Die Einladungs-Link läuft nach 30 Tagen ab.

Bearbeiten von Benutzern

Sie können Benutzerinformationen und Einstellungen ändern.

So bearbeiten Sie Benutzer

1. Wählen Sie das Profilsymbol in der oberen rechten Ecke des WorkDocs Clients.

2. Wählen Sie unter Admin die Option Admin-Kontrollpanel öffnen aus.
3. Wählen Sie unter Benutzer verwalten das Stiftsymbol (✎) neben dem Namen des Benutzers aus.
4. Im Dialogfeld Benutzer bearbeiten können Sie die folgenden Optionen bearbeiten:

   Vorname (nur Cloud-Verzeichnis)

   Der Vorname des Benutzers

   Nachname (nur Cloud-Verzeichnis)

   Der Nachname des Benutzers

   Status

   Gibt an, ob der Benutzer aktiv oder inaktiv ist. Weitere Informationen finden Sie unter Deaktivieren von Benutzern.

Rolle

Gibt an, ob jemand ein Benutzer oder Administrator ist. Sie können auch Benutzer, denen eine WorkSpaces WorkSpace zugewiesen wurde, auf- oder abstufen. Weitere Informationen finden Sie unter Übersicht: Benutzerrollen.

Speicherung

Legt das Speicherlimit für einen vorhandenen Benutzer fest.

5. Wählen Sie Save Changes.

Deaktivieren von Benutzern

Sie deaktivieren den Zugriff eines Benutzers, indem Sie seinen Status auf Inaktiv ändern.

So ändern Sie die Benutzerstatus in Inaktiv

1. Wählen Sie das Profilsymbol in der oberen rechten Ecke des WorkDocs Clients.

2. Wählen Sie unter Admin die Option Admin-Kontrollpanel öffnen aus.
3. Wählen Sie unter Benutzer verwalten das Stiftsymbol (✎) neben dem Namen des Benutzers aus.
4. Wählen Sie Inaktiv und danach Änderungen speichern.

Der inaktivierte Benutzer kann nicht auf Ihre WorkDocs Website zugreifen.

> **Note**
>
> Wenn Sie einen Benutzer in den Status Inaktiv ändern, werden seine Dateien, Ordner oder sein Feedback nicht von Ihrer WorkDocs Website gelöscht. Sie können jedoch die Dateien und Ordner eines inaktiven Benutzers auf einen aktiven Benutzer übertragen. Weitere Informationen finden Sie unter Übertragen der Dokumentenkontrolle.

Löschen ausstehender Benutzer

Sie können Simple AD-, AWS Managed Microsoft- und AD Connector Connector-Benutzer mit dem Status Ausstehend löschen. Um einen dieser Benutzer zu löschen, wählen Sie das Papierkorbsymbol (🗑) neben dem Namen des Benutzers.

Ihre WorkDocs Website muss immer mindestens einen aktiven Benutzer haben, der kein Gastbenutzer ist. Wenn Sie alle Benutzer löschen müssen, löschen Sie die gesamte Site.

Wir empfehlen, registrierte Benutzer nicht zu löschen. Stattdessen sollten Sie einen Benutzer vom Status Aktiv in den Status Inaktiv versetzen, um zu verhindern, dass er auf Ihre WorkDocs Site zugreift.

Übertragen der Dokumentenkontrolle

Sie können die Dateien und Ordner eines aktiven Benutzers auf einen inaktiven Benutzer übertragen. Weitere Informationen zum Deaktivieren eines Benutzers finden Sie unterDeaktivieren von Benutzern.

> ⚠ Warning
>
> Sie können diese Aktion nicht rückgängig machen.

So übertragen Sie die Dokumentenkontrolle

1. Wählen Sie das Profilsymbol in der oberen rechten Ecke des WorkDocs Clients.

2. Wählen Sie unter Admin die Option Admin-Kontrollpanel öffnen aus.
3. Suchen Sie unter Benutzer verwalten nach dem inaktiven Benutzer.
4. Wählen Sie das Stiftsymbol (✎) neben dem Namen des inaktiven Benutzers.
5. Wählen Sie Dokumentenbesitz übertragen aus und geben Sie die E-Mail-Adresse des neuen Besitzers ein.

6. Wählen Sie Save Changes.

Benutzerlisten werden heruntergeladen

Um eine Benutzerliste aus dem Admin-Kontrollpanel herunterzuladen, müssen Sie WorkDocs Companion installieren. Informationen zur Installation von WorkDocs Companion finden Sie unter Apps und Integrationen für WorkDocs.

So laden Sie eine Benutzerliste herunter

1. Wählen Sie das Profilsymbol in der oberen rechten Ecke des Clients. WorkDocs

2. Wählen Sie unter Admin die Option Admin-Kontrollpanel öffnen aus.
3. Wählen Sie unter Benutzer verwalten die Option Benutzer herunterladen.
4. Wählen Sie unter Download user (Benutzer herunterladen) die gewünschten Optionen (siehe unten) aus, um eine Benutzerliste im JSON-Format (`.json`) auf Ihrem Computer zu speichern:
   - Alle Benutzer
   - Gastbenutzer
   - WS-Benutzer
   - Benutzer
   - Hauptbenutzer
   - Admin.
5. WorkDocs speichert die Datei an einem der folgenden Speicherorte:
   - Windows – `Downloads/WorkDocsDownloads`
   - macOS – *`hard drive`*`/users/`*`username`*`/WorkDocsDownloads/folder`

> **Note**
>
> Das Herunterladen kann einige Zeit dauern. Außerdem landen heruntergeladene Dateien nicht in Ihrem `/~users` Ordner.

Weitere Informationen zu diesen Benutzerrollen finden Sie unter Übersicht: Benutzerrollen.

Freigabe und Zusammenarbeit

Ihre Benutzer können Inhalte teilen, indem sie einen Link oder eine Einladung senden. Benutzer können auch mit externen Benutzern zusammenarbeiten, wenn Sie das externe Teilen aktivieren.

WorkDocs steuert den Zugriff auf Ordner und Dateien mithilfe von Berechtigungen. Das System wendet Berechtigungen auf der Grundlage der Rolle eines Benutzers an.

Inhalt

Links teilen

Benutzer können „Link teilen“ auswählen, um Hyperlinks für WorkDocs Inhalte schnell zu kopieren und mit Kollegen und externen Benutzern innerhalb und außerhalb ihrer Organisation zu teilen. Wenn Benutzer einen Link freigeben, können sie ihn so konfigurieren, dass eine der folgenden Zugriffsoptionen zugelassen wird:

- Alle Mitglieder der WorkDocs Website können nach der Datei suchen, sie ansehen und kommentieren.
- Jeder, der über den Link verfügt, auch Personen, die keine Mitglieder der WorkDocs Website sind, kann die Datei ansehen. Diese Verknüpfungsoption schränkt die Berechtigungen auf das Anzeigen ein.

Empfänger mit Leseberechtigung können eine Datei nur ansehen. Die Kommentarberechtigung ermöglicht Benutzern, Kommentare abzugeben oder Dateien zu aktualisieren bzw. neu hochzuladen oder vorhandene Dateien zu löschen.

Standardmäßig können alle verwalteten Benutzer öffentliche Links erstellen. Um diese Einstellung zu ändern, aktualisieren Sie Ihre Einstellungen für Sicherheit über Ihre Administrator-Systemsteuerung.

Weitere Informationen finden Sie unter Verwaltung WorkDocs über das Admin-Kontrollpanel der Website.

Freigeben durch Einladen

Wenn Sie das Teilen per Einladung aktivieren, können die Benutzer Ihrer Website Dateien oder Ordner mit einzelnen Benutzern und mit Gruppen teilen, indem sie Einladungs-E-Mails senden. Die Einladungen enthalten Links zu den geteilten Inhalten, und Eingeladene können die geteilten Dateien oder Ordner öffnen. Eingeladene Personen können diese Dateien oder Ordner auch mit anderen Mitgliedern der Website und mit externen Benutzern teilen.

Sie können für jeden eingeladenen Benutzer Berechtigungsstufen festlegen. Sie können auch Teamordner erstellen, die Sie auf Einladung mit von Ihnen erstellten Verzeichnisgruppen teilen können.

> **Note**
>
> Beim Teilen von Einladungen sind Mitglieder verschachtelter Gruppen nicht enthalten. Um diese Mitglieder aufzunehmen, müssen Sie sie der Liste „Auf Einladung teilen“ hinzufügen.

Weitere Informationen finden Sie unter Verwaltung WorkDocs über das Admin-Kontrollpanel der Website.

Externe Freigaben

Externes Teilen ermöglicht verwalteten Benutzern einer WorkDocs Website, Dateien und Ordner gemeinsam zu nutzen und mit externen Benutzern zusammenzuarbeiten, ohne dass zusätzliche Kosten anfallen. Benutzer der Website können Dateien und Ordner für externe Benutzer freigeben, ohne dass es sich bei den Empfängern um kostenpflichtige Benutzer der WorkDocs Website handeln muss. Wenn Sie das externe Teilen aktivieren, können Benutzer die E-Mail-Adresse des externen Benutzers eingeben, mit dem sie Inhalte teilen möchten, und die entsprechenden Zugriffsberechtigungen für Zuschauer festlegen. Wenn externe Benutzer hinzugefügt werden, sind die Berechtigungen auf Zuschauer beschränkt, und andere Berechtigungen sind nicht verfügbar. Externe Benutzer erhalten eine E-Mail-Benachrichtigung mit einem Link auf die freigegebene Datei bzw. den freigegebenen Ordner. Wenn Sie den Link auswählen, werden externe Benutzer zur Site weitergeleitet, wo sie ihre Anmeldeinformationen eingeben, um sich dort anzumelden. WorkDocs Die freigegebenen Dateien und Ordner werden in der Ansicht Mit mir geteilt angezeigt.

Der Dateieigentümer kann jederzeit die Freigabeberechtigung ändern oder dem externen Benutzer den Zugriff auf Dateien und Ordner wieder entziehen. Die externe Freigabe muss für die Website vom Website-Administrator aktiviert werden, damit verwaltete Benutzer Inhalte für externe Benutzer freigeben können. Damit Gastbenutzer Beiträge erstellen oder Dateieigentümer werden können, müssen sie vom Website-Administrator auf Benutzer-Ebene hochgestuft werden. Weitere Informationen finden Sie unter Übersicht: Benutzerrollen.

Standardmäßig ist die externe Freigabe aktiviert und alle Benutzer können externe Benutzer einladen. Um diese Einstellung zu ändern, aktualisieren Sie Ihre Einstellungen für Sicherheit über Ihre Administrator-Systemsteuerung. Weitere Informationen finden Sie unter Verwaltung WorkDocs über das Admin-Kontrollpanel der Website.

Berechtigungen

WorkDocs verwendet Berechtigungen, um den Zugriff auf Ordner und Dateien zu kontrollieren. Berechtigungen werden auf der Grundlage von Benutzerrollen angewendet.

Inhalt

Benutzerrollen

Benutzerrollen steuern Ordner- und Dateiberechtigungen. Sie können die folgenden Benutzerrollen auf Ordnerebene anwenden:

- Ordnerbesitzer — Der Besitzer eines Ordners oder einer Datei.
- Miteigentümer eines Ordners — Ein Benutzer oder eine Gruppe, den oder die der Eigentümer als Miteigentümer eines Ordners oder einer Datei bestimmt.
- Mitwirkender eines Ordners — Jemand mit uneingeschränktem Zugriff auf einen Ordner.
- Ordnerbetrachter — Jemand mit eingeschränktem Zugriff (nur Leseberechtigungen) auf einen Ordner.

Sie können die folgenden Benutzerrollen auf individueller Dateiebene anwenden:

- Besitzer — Der Besitzer einer Datei.
- Miteigentümer — Ein Benutzer oder eine Gruppe, die der Eigentümer als Miteigentümer der Datei bestimmt.
- Mitwirkender* — Jemand, der Feedback zu einer Datei geben darf.
- Betrachter — Jemand mit eingeschränktem Zugriff (Schreibschutz und Zugriffsrechte für Aktivitäten zum Ansehen) auf die Datei.
- Anonymer Betrachter — Ein nicht registrierter Benutzer außerhalb der Organisation, der eine Datei ansehen kann, die über einen externen Link geteilt wurde. Sofern nicht anders angegeben, hat ein anonymer Betrachter dieselben Leseberechtigungen wie ein Betrachter. Anonyme Zuschauer können die Dateiaktivitäten nicht sehen.

* Mitwirkende können bestehende Dateiversionen nicht umbenennen. Sie können jedoch eine neue Version einer Datei mit einem anderen Namen hochladen.

Berechtigungen für freigegebene Ordner

Die folgenden Berechtigungen gelten für Benutzerrollen für geteilte Ordner:

> **Note**
>
> Die für einen Ordner angewendeten Berechtigungen gelten auch für die Unterordner und Dateien in diesem Ordner.

- Ansicht — Zeigt den Inhalt eines geteilten Ordners an.
- Unterordner anzeigen — Zeigt einen Unterordner an.
- Freigaben anzeigen — Zeigt die anderen Benutzer an, mit denen ein Ordner geteilt wird.
- Ordner herunterladen — Laden Sie einen Ordner herunter.
- Unterordner hinzufügen — Fügt einen Unterordner hinzu.
- Teilen — Teilen Sie den Ordner der obersten Ebene mit anderen Benutzern.
- Teilen widerrufen — Widerrufen Sie die gemeinsame Nutzung des Ordners auf oberster Ebene.
- Unterordner löschen — Löscht einen Unterordner.
- Ordner auf oberster Ebene löschen — Löscht den geteilten Ordner auf oberster Ebene.

	Anzeigen	Unterordner anzeigen	Aktien anzeigen	Ordner herunterladen	Unterordner hinzufügen	Freigeben	Teilen widerrufen	Unterordner löschen	Löschen Sie den Ordner auf oberster Ebene
Besitzer des Ordners	✓	✓	✓	✓	✓	✓	✓	✓	✓
Mitinhaber des Ordners	✓	✓	✓	✓	✓	✓	✓	✓	✓
Mitwirker der des Ordners	✓	✓	✓	✓	✓				
Ordnerbe rachter	✓	✓	✓	✓					

Berechtigungen für Dateien in geteilten Ordnern

Die folgenden Berechtigungen gelten für Benutzerrollen für Dateien in einem geteilten Ordner:

- Kommentieren — Fügt Feedback zu einer Datei hinzu.
- Löschen — Löscht eine Datei in einem geteilten Ordner.
- Umbenennen — Dateien umbenennen.
- Hochladen — Laden Sie neue Versionen einer Datei hoch.
- Herunterladen — Laden Sie eine Datei herunter. Dies ist die Standardberechtigung. Sie können die Dateieigenschaften verwenden, um das Herunterladen gemeinsam genutzter Dateien zuzulassen oder zu verweigern.
- Download verhindern — Verhindert, dass eine Datei heruntergeladen wird.

> **Note**
>
> - Wenn Sie diese Option auswählen, können Benutzer mit Anzeigeberechtigungen weiterhin Dateien herunterladen. Um dies zu verhindern, öffnen Sie den freigegebenen Ordner und deaktivieren Sie die Einstellung Downloads zulassen für alle Dateien, die diese Benutzer nicht herunterladen sollen.
> - Wenn der Eigentümer oder Miteigentümer einer MP4 Datei das Herunterladen dieser Datei verbietet, können Mitwirkende und Zuschauer sie nicht im Amazon WorkDocs Web Client abspielen.

- Teilen — Teilen Sie eine Datei mit anderen Benutzern.
- Teilen widerrufen — Widerrufen Sie die gemeinsame Nutzung einer Datei.
- Ansehen — Eine Datei in einem geteilten Ordner anzeigen.
- Freigaben anzeigen — Zeigt die anderen Benutzer an, mit denen eine Datei geteilt wurde.
- Anmerkungen anzeigen — Sehen Sie sich Feedback von anderen Benutzern an.
- Aktivität anzeigen — Zeigt den Aktivitätsverlauf einer Datei an.
- Versionen anzeigen — Frühere Versionen einer Datei anzeigen.
- Versionen löschen — Löscht eine oder mehrere Versionen einer Datei.
- Versionen wiederherstellen — Stellen Sie eine oder mehrere gelöschte Versionen einer Datei wieder her.
- Alle privaten Kommentare anzeigen — Der Eigentümer/Mitinhaber kann alle privaten Kommentare zu einem Dokument sehen, auch wenn es sich nicht um Antworten auf seinen Kommentar handelt.

	Anmerkungen	Löschen	Umbenennen	Hochladen	Herunterladen	Download verhindern	Freigeben	Teilen widerrufen	Anzeigen	Aktivität ansehen	Anmerkungen anzeigen	Aktivität anzeigen	Version anzeigen	Version löschen	Versionen wiederherstellen	Alle privaten Kommentare anzeigen**
Besitzer der Datei	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

	Anmerk	Löschen	Umbenen	Hochlad	Herunterladen	Download verhinde	Freigeb	Teilen widerrufen	Anzeige	Aktivität ansehe	Anmerkungen anzeige	Aktivität anzeigen	Versionen anzeigen	Version löschen	Version wiederherstellen	Alle privaten Kommentare anzeigen**
Besi des Ordn	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Mitei ümer des Ordn	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Mitw der des Ordn *	✓			✓	✓				✓	✓	✓	✓	✓			
Ordn rach					✓				✓	✓		✓				
Anon Betra r									✓	✓						

* In diesem Fall ist der Dateibesitzer die Person, die die Originalversion einer Datei in einen geteilten Ordner hochgeladen hat. Die Berechtigungen für diese Rolle gelten nur für die eigene Datei, nicht für alle Dateien im freigegebenen Ordner.

** Eigentümer und Miteigentümer können alle privaten Kommentare sehen. Beitragsleistende können nur Kommentare sehen, die Antworten auf ihre eigenen Kommentare sind.

*** Mitwirkende können bestehende Dateiversionen nicht umbenennen. Sie können jedoch eine neue Version einer Datei mit einem anderen Namen hochladen.

Berechtigungen für Dateien, die sich nicht in gemeinsam genutzten Ordnern befinden

Die folgenden Berechtigungen gelten für Benutzerrollen für Dateien, die sich nicht in einem gemeinsam genutzten Ordner befinden:

- Kommentieren — Fügt Feedback zu einer Datei hinzu.
- Löschen — Löscht eine Datei.
- Umbenennen — Dateien umbenennen.
- Hochladen — Laden Sie neue Versionen einer Datei hoch.
- Herunterladen — Laden Sie eine Datei herunter. Dies ist die Standardberechtigung. Sie können die Dateieigenschaften verwenden, um das Herunterladen gemeinsam genutzter Dateien zuzulassen oder zu verweigern.
- Download verhindern — Verhindert, dass eine Datei heruntergeladen wird.

> **Note**
>
> Wenn der Eigentümer oder Miteigentümer einer MP4 Datei das Herunterladen dieser Datei verbietet, können Mitwirkende und Zuschauer sie nicht im Amazon WorkDocs Web Client abspielen.

- Teilen — Teilen Sie eine Datei mit anderen Benutzern.
- Teilen widerrufen — Widerrufen Sie die gemeinsame Nutzung einer Datei.
- Ansehen — Eine Datei ansehen.
- Freigaben anzeigen — Sehen Sie sich die anderen Benutzer an, mit denen eine Datei geteilt wurde.
- Anmerkungen anzeigen — Sehen Sie sich Feedback von anderen Benutzern an.
- Aktivität anzeigen — Zeigt den Aktivitätsverlauf einer Datei an.
- Versionen anzeigen — Frühere Versionen einer Datei anzeigen.
- Versionen löschen — Löscht eine oder mehrere Versionen einer Datei.
- Versionen wiederherstellen — Stellen Sie eine oder mehrere gelöschte Versionen einer Datei wieder her.

	Anmerk	Löschen	Umbenen n	Hochlad	Herunte laden	Downloa verhinde n	Freigebe	Teilen widerruf n	Anzeige	Aktivit ansehe	Anmerku en anzeige	Aktivit anzeige	Versione anzeige	Versione löschen	Versionen wiederher stellen
Besit	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Mitinh r*	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Mitwi der**	✓			✓	✓				✓	✓	✓	✓	✓		
Betra r					✓				✓	✓		✓			
Anon Zusc									✓	✓					

* Dateibesitzer und Miteigentümer können alle privaten Kommentare sehen. Beitragsleistende können nur Kommentare sehen, die Antworten auf ihre eigenen Kommentare sind.

** Mitwirkende können bestehende Dateiversionen nicht umbenennen. Sie können jedoch eine neue Version einer Datei mit einem anderen Namen hochladen.

Aktivieren der gemeinsamen Bearbeitung

Sie verwenden den Abschnitt Einstellungen für die Online-Bearbeitung in Ihrem Admin-Kontrollpanel, um die Optionen für die gemeinsame Bearbeitung zu aktivieren.

Inhalt

Hancom aktivieren ThinkFree

Sie können Hancom ThinkFree für Ihre WorkDocs Site aktivieren, sodass Benutzer Microsoft Office-Dateien über die WorkDocs Webanwendung erstellen und gemeinsam bearbeiten können. Weitere Informationen finden Sie unter Bearbeiten mit Hancom. ThinkFree

Hancom ThinkFree ist ohne zusätzliche Kosten für WorkDocs Benutzer verfügbar. Sie benötigen weder zusätzliche Lizenzen noch müssen Sie neue Software installieren.

Um Hancom zu aktivieren ThinkFree

Aktivieren Sie die ThinkFree Hancom-Bearbeitung über das Admin-Bedienfeld.

1. Wählen Sie unter Mein Konto die Option Administrator-Systemsteuerung öffnen.
2. Wählen Sie unter Hancom Online Editing die Option Änderung aus.
3. Wählen Sie Hancom Online Editing-Funktion aktivieren aus, lesen Sie sich die Nutzungsbedingungen durch und klicken Sie dann auf Speichern.

Um Hancom zu deaktivieren ThinkFree

Deaktivieren Sie die ThinkFree Hancom-Bearbeitung über das Admin-Bedienfeld.

1. Wählen Sie unter Mein Konto die Option Administrator-Systemsteuerung öffnen.
2. Wählen Sie unter Hancom Online Editing die Option Änderung aus.
3. Deaktivieren Sie das Kontrollkästchen Hancom Online Editing-Funktion aktivieren und klicken Sie auf Speichern.

Aktivieren von Open with Office Online (Mit Office Online öffnen)

Aktivieren Sie Mit Office Online öffnen für Ihre WorkDocs Website, damit Benutzer Microsoft Office-Dateien von der WorkDocs Webanwendung aus gemeinsam bearbeiten können.

Open with Office Online ist ohne zusätzliche Kosten für WorkDocs Benutzer verfügbar, die auch über ein Microsoft Office 365 Work - oder School-Konto mit einer Lizenz zur Bearbeitung in Office Online verfügen. Weitere Informationen finden Sie unter Open with Office Online (Mit Office Online öffnen).

So aktivieren Sie Open with Office Online (Mit Office Online öffnen)

Sie aktivieren Open with Office Online (Mit Office Online öffnen) in der Administrator-Systemsteuerung.

1. Wählen Sie unter Mein Konto die Option Administrator-Systemsteuerung öffnen.
2. Wählen Sie unter Office Online die Option Änderung aus.
3. Wählen Sie Enable Office Online (Office Online aktivieren) aus und klicken Sie dann auf Speichern.

So deaktivieren Sie Open with Office Online (Mit Office Online öffnen)

Sie deaktivieren Open with Office Online (Mit Office Online öffnen) in der Administrator-Systemsteuerung.

1. Wählen Sie unter Mein Konto die Option Administrator-Systemsteuerung öffnen.
2. Wählen Sie unter Office Online die Option Änderung aus.
3. Deaktivieren Sie das Kontrollkästchen Enable Office Online (Office Online aktivieren) und klicken Sie auf Speichern.

Dateien migrieren zu WorkDocs

WorkDocs Administratoren können den WorkDocs Migrationsdienst verwenden, um eine umfangreiche Migration mehrerer Dateien und Ordner zu ihrer WorkDocs Site durchzuführen. Der WorkDocs Migrationsservice funktioniert mit Amazon Simple Storage Service (Amazon S3). Auf diese Weise können Sie abteilungsspezifische Dateifreigaben und Dateifreigaben auf das Home-Laufwerk oder Benutzerdateien migrieren. WorkDocs

WorkDocs Stellt während dieses Vorgangs eine AWS Identity and Access Management (IAM-) Richtlinie für Sie bereit. Verwenden Sie diese Richtlinie, um eine neue IAM-Rolle zu erstellen, die Zugriff auf den WorkDocs Migrationsdienst gewährt, um Folgendes zu tun:

- Lesen Sie den Amazon S3 S3-Bucket, den Sie angeben, und listen Sie ihn auf.
- Lese- und Schreibzugriff auf die von Ihnen angegebene WorkDocs Site.

Führen Sie die folgenden Schritte aus, um Ihre Dateien und Ordner zu WorkDocs zu migrieren. Stellen Sie zunächst sicher, dass Sie die folgenden Berechtigungen besitzen:

- Administratorrechte für Ihre Site WorkDocs
- Berechtigungen zum Erstellen einer IAM-Rolle

Wenn Ihre WorkDocs Site in demselben Verzeichnis wie Ihre WorkSpaces Flotte eingerichtet ist, müssen Sie die folgenden Anforderungen erfüllen:

- Verwenden Sie Admin nicht als Benutzernamen für Ihr WorkDocs Konto. Admin ist eine reservierte Benutzerrolle in WorkDocs.
- Ihr WorkDocs Administrator-Benutzertyp muss Upgraded WS User sein. Weitere Informationen erhalten Sie unter Übersicht: Benutzerrollen und Bearbeiten von Benutzern.

> **Note**
>
> Die Verzeichnisstruktur, die Dateinamen und der Dateiinhalt bleiben bei der Migration zu WorkDocs erhalten. Dateibesitz und -berechtigungen werden nicht bewahrt.

Aufgaben

Schritt 1: Inhalt für die Migration vorbereiten

So bereiten Sie Ihre Inhalte für die Migration vor

1. Erstellen Sie auf Ihrer WorkDocs Website unter Eigene Dateien einen Ordner, in den Sie Ihre Dateien und Ordner migrieren möchten.
2. Überprüfen Sie Folgendes:

   - Der Quellordner enthält nicht mehr als 100.000 Dateien und Unterordner. Migrationen schlagen fehl, wenn Sie dieses Limit überschreiten.
   - Keine einzelnen Dateien überschreiten 5 TB.
   - Jeder Dateiname enthält 255 Zeichen oder weniger. WorkDocs Drive zeigt nur Dateien mit einem vollständigen Verzeichnispfad von 260 Zeichen oder weniger an.

> **Warning**
>
> Wenn Sie versuchen, Dateien oder Ordner zu migrieren, die folgende Zeichen enthalten, kann dies zu Fehlern während der Migration führen. Wenn dies eintritt, wählen Sie Download report (Bericht herunterladen) aus, um ein Protokoll herunterzuladen, das die Fehler, alle Dateien, die nicht migriert wurden, und alle erfolgreich migrierten Dateien auflistet.

- Leerzeichen am Ende — Beispiel: ein zusätzliches Leerzeichen am Ende eines Dateinamens.
- Punkte am Anfang oder Ende — Zum Beispiel: `.file`, `.file.ppt`, `...`, oder `file.`
- Tilden am Anfang oder Ende — Zum Beispiel: `file.doc~`, `~file.doc`, oder `~$file.doc`
- Dateinamen, die auf **`.tmp`** — enden zum Beispiel: `file.tmp`
- Dateinamen, die genau diesen Begriffen entsprechen, bei denen Groß- und Kleinschreibung beachtet `Microsoft User Data` wird —`Outlook files`, `Thumbs.db`, oder `Thumbnails`

- Dateinamen, die eines der folgenden Zeichen enthalten — * (Sternchen), (Schrägstrich), / (umgekehrter Schrägstrich), \ (Doppelpunkt), : (kleiner als), < (größer als), > (Fragezeichen), ? (senkrechter Strich/senkrechter Strich), | (doppelte Anführungszeichen) oder " \202E (Zeichencode 202E).

Schritt 2: Dateien auf Amazon S3 hochladen

Um Dateien auf Amazon S3 hochzuladen

1. Erstellen Sie in Ihrem AWS Konto einen neuen Amazon Simple Storage Service (Amazon S3) -Bucket, in den Sie Ihre Dateien und Ordner hochladen möchten. Der Amazon S3 S3-Bucket muss sich in demselben AWS Konto und derselben AWS Region wie Ihre WorkDocs Site befinden. Weitere Informationen finden Sie unter Erste Schritte mit Amazon Simple Storage Service im Amazon Simple Storage Service-Benutzerhandbuch.
2. Laden Sie Ihre Dateien in den Amazon S3 S3-Bucket hoch, den Sie im vorherigen Schritt erstellt haben. Wir empfehlen AWS DataSync die Verwendung, um Ihre Dateien und Ordner in den Amazon S3 S3-Bucket hochzuladen. DataSync bietet zusätzliche Funktionen zur Nachverfolgung, Berichterstattung und Synchronisierung. Weitere Informationen finden Sie unter AWS DataSync Funktionsweise und Verwenden identitätsbasierter Richtlinien (IAM-Richtlinien) für DataSync im Benutzerhandbuch.AWS DataSync

Schritt 3: Planen einer Migration

Nachdem Sie die Schritte 1 und 2 abgeschlossen haben, verwenden Sie den WorkDocs Migrationsdienst, um die Migration zu planen. Es kann bis zu einer Woche dauern, bis der Migrationsservice Ihre Migrationsanfrage bearbeitet und Ihnen eine E-Mail mit dem Hinweis sendet, dass Sie mit der Migration beginnen können. Wenn Sie die Migration starten, bevor Sie die E-Mail erhalten haben, zeigt die Managementkonsole eine Meldung an, in der Sie aufgefordert werden, zu warten.

Wenn Sie die Migration planen, ändert sich die Speichereinstellung Ihres WorkDocs Benutzerkontos automatisch auf Unbegrenzt.

> **Note**
>
> Die Migration von Dateien, die Ihr WorkDocs Speicherlimit überschreiten, kann zu zusätzlichen Kosten führen. Weitere Informationen finden Sie unter WorkDocs – Preise.

Der WorkDocs Migrationsdienst stellt eine AWS Identity and Access Management (IAM-) Richtlinie bereit, die Sie für die Migration verwenden können. Mit dieser Richtlinie erstellen Sie eine neue IAM-Rolle, die dem WorkDocs Migrationsservice Zugriff auf den Amazon S3 S3-Bucket und die von Ihnen WorkDocs angegebene Site gewährt. Sie abonnieren auch E-Mail-Benachrichtigungen von Amazon SNS, um Updates zu erhalten, wann Ihre Migrationsanfrage geplant ist und wann sie beginnt und endet.

So planen Sie eine Migration

1. Wählen Sie in der WorkDocs Konsole Apps, Migrationen aus.
   - Wenn Sie zum ersten Mal auf den WorkDocs Migration Service zugreifen, werden Sie aufgefordert, Amazon SNS SNS-E-Mail-Benachrichtigungen zu abonnieren. Abonnieren und bestätigen Sie diese in der E-Mail-Nachricht, die Sie erhalten. Wählen Sie anschließend Continue (Weiter) aus.
2. Wählen Sie Create Migration (Migration erstellen) aus.
3. Wählen Sie in Source Type (Quelltyp) Amazon S3 aus.
4. Wählen Sie Weiter aus.
5. Kopieren Sie für Data Source & Validation unter Sample Policy die bereitgestellte IAM-Richtlinie.
6. Verwenden Sie die IAM-Richtlinie, die Sie im vorherigen Schritt kopiert haben, um eine neue IAM-Richtlinie und -Rolle wie folgt zu erstellen:
   a. Öffnen Sie unter https://console.aws.amazon.com/iam/ die IAM-Konsole.
   b. Wählen Sie Policies (Richtlinien), Create policy (Richtlinie erstellen) aus.
   c. Wählen Sie JSON und fügen Sie die IAM-Richtlinie ein, die Sie zuvor in Ihre Zwischenablage kopiert haben.
   d. Wählen Sie Richtlinie prüfen. Geben Sie einen Namen und eine Beschreibung für die Richtlinie ein.
   e. Wählen Sie Richtlinie erstellen aus.
   f. Wählen Sie Roles (Rollen), Create role (Rolle erstellen) aus.

g. Wählen Sie Another AWS account (Anderes AWS-Konto) aus. Geben Sie in Account ID (Konto-ID) eine der folgenden IDs ein:

   - Geben Sie für die Region USA Ost (Nord-Virginia) Folgendes ein `899282061130`
   - Geben Sie für die Region USA West (Oregon) Folgendes ein `814301586344`
   - Geben Sie für die Region Asien-Pazifik (Singapur) ein `900469912330`
   - Geben Sie für die Region Asien-Pazifik (Sydney) Folgendes ein `031131923584`
   - Geben Sie für die Region Asien-Pazifik (Tokio) Folgendes ein `178752524102`
   - Geben Sie für die Region Europa (Irland) ein `191921258524`

h. Wählen Sie die zuvor von Ihnen erstellte Richtlinie und anschließend Next: Review (Weiter: Überprüfen) aus. Wenn die neue Richtlinie nicht angezeigt wird, klicken Sie auf das Aktualisierungssymbol.

i. Geben Sie einen Namen und eine Beschreibung für die Rolle ein. Wählen Sie Rolle erstellen aus.

j. Wählen Sie auf der Seite Roles (Rollen) in Role name (Name der Rolle) die von Ihnen erstellte Rolle aus.

k. Ändern Sie auf der Übersichtsseite die maximale CLI/API Sitzungsdauer auf 12 Stunden.

l. Kopieren Sie den Wert in Role ARN (ARN der Rolle) in die Zwischenablage, um ihn im nächsten Schritt zu verwenden.

7. Kehren Sie zum WorkDocs Migration Service zurück. Fügen Sie für Datenquelle und Validierung unter Rollen-ARN den Rollen-ARN aus der IAM-Rolle ein, die Sie im vorherigen Schritt kopiert haben.
8. Wählen Sie für Bucket den Amazon S3 S3-Bucket aus, aus dem die Dateien migriert werden sollen.
9. Wählen Sie Weiter aus.
10. Wählen Sie unter WorkDocs Zielordner auswählen den Zielordner aus, in WorkDocs den die Dateien migriert werden sollen.
11. Wählen Sie Weiter aus.
12. Geben Sie unter Review (Prüfen) in Title (Titel) einen Namen für die Migration ein.
13. Wählen Sie Datum und Uhrzeit für die Migration aus.
14. Wählen Sie Send (Senden) aus.

Schritt 4: Nachverfolgen einer Migration

Sie können Ihre Migration auf der Startseite des WorkDocs Migrationsdienstes verfolgen. Um von der WorkDocs Website aus auf die Landingpage zuzugreifen, wählen Sie Apps, Migrationen. Wählen Sie Ihre Migration aus, um Details anzuzeigen und den Fortschritt zu überwachen. Sie können auch Cancel Migration (Migration abbrechen) auswählen, wenn Sie die Migration abbrechen müssen, oder Update (Aktualisieren), um den Zeitplan für die Migration zu aktualisieren. Nach Abschluss einer Migration können Sie Download report (Bericht herunterladen) auswählen, um ein Protokoll der erfolgreich migrierten Dateien, der nicht erfolgreich migrierten Dateien oder der Fehler herunterzuladen.

Die folgenden Angaben zum Migrationsstatus geben den Status Ihrer Migration an:

Scheduled (Geplant)

: Die Migration ist geplant, wurd jedoch noch nicht gestartet. Sie können bis zu fünf Minuten vor der geplanten Startzeit Migrationen abbrechen oder die Migrationsstartzeit aktualisieren.

Migrating

: Die Migration wird ausgeführt.

Herzlichen Glückwunsch

: Die Migration ist abgeschlossen.

Partial Success (Teilweise erfolgreich)

: Die Migration ist teilweise abgeschlossen. Zeigen Sie die Migrationsübersicht an oder laden Sie den bereitgestellten Bericht herunter, um weitere Details zu erhalten.

Fehlgeschlagen

: Die Migration war nicht erfolgreich. Zeigen Sie die Migrationsübersicht an oder laden Sie den bereitgestellten Bericht herunter, um weitere Details zu erhalten.

Canceled

: Die Migration wurde abgebrochen.

Schritt 5: Bereinigen von Ressourcen

Wenn Ihre Migration abgeschlossen ist, löschen Sie die Migrationsrichtlinie und die Rolle, die Sie in der IAM-Konsole erstellt haben.

So löschen Sie die IAM-Richtlinie und -Rolle

1. Öffnen Sie unter https://console.aws.amazon.com/iam/ die IAM-Konsole.
2. Wählen Sie Policies (Richtlinien).
3. Suchen Sie die von Ihnen erstellte Richtlinie und wählen Sie diese aus.
4. Wählen Sie in Policy actions (Richtlinienaktionen) Delete (Löschen) aus.
5. Wählen Sie Löschen aus.
6. Wählen Sie Roles.
7. Suchen Sie die von Ihnen erstellte Rolle und wählen Sie diese aus.
8. Wählen Sie Delete role (Rolle löschen), Delete (Löschen) aus.

Wenn eine geplante Migration gestartet wird, wird die Speichereinstellung Ihres WorkDocs Benutzerkontos automatisch auf Unbegrenzt geändert. Nach der Migration können Sie diese Einstellung über das Admin-Kontrollfeld ändern. Weitere Informationen finden Sie unter Bearbeiten von Benutzern.

WorkDocs-Fehlerbehebung

Die folgenden Informationen können Ihnen bei der Behebung von Problemen mit helfen WorkDocs.

Problembereiche

Ich kann meine WorkDocs Website nicht in einer bestimmten AWS Region einrichten

Wenn Sie eine neue WorkDocs Site einrichten, wählen Sie bei der Einrichtung die AWS-Region aus. Weitere Informationen finden Sie im Tutorial für Ihren speziellen Anwendungsfall unter Erste Schritte mit WorkDocs.

Ich möchte meine WorkDocs Site in einer vorhandenen Amazon VPC einrichten

Erstellen Sie beim Einrichten Ihrer neuen WorkDocs Site ein Verzeichnis mithilfe der vorhandenen Virtual Private Cloud (VPC). WorkDocs verwendet dieses Verzeichnis, um Benutzer zu authentifizieren.

Benutzer muss sein Passwort zurücksetzen

Benutzer können durch Wahl von Forgot password? (Passwort vergessen?) auf ihren Anmeldebildschirmen zurücksetzen.

Benutzer gab versehentlich vertrauliches Dokument frei

Um den Zugriff auf das Dokument aufzuheben, wählen Sie Freigeben durch Einladen neben dem Dokument. Entfernen Sie dann die Benutzer, die keinen Zugriff mehr haben sollen. Wenn das Dokument über einen Link freigegeben wurde, wählen Sie Link freigeben und deaktivieren Sie den Link.

Benutzer hat die Organisation verlassen und die Dokumentenkontrolle nicht übertragen

Übertragen Sie die Dokumentenkontrolle in der Administrator-Systemsteuerung auf einen anderen Benutzer. Weitere Informationen finden Sie unter Übertragen der Dokumentenkontrolle.

Sie müssen WorkDocs Drive oder WorkDocs Companion für mehrere Benutzer bereitstellen

Nehmen Sie die Bereitstellung an mehrere Benutzern in einem Unternehmen über eine Gruppenrichtlinie vor. Weitere Informationen finden Sie unter Identitäts- und Zugriffsmanagement für Amazon WorkDocs. Spezifische Informationen zur Bereitstellung von WorkDocs Drive für mehrere Benutzer finden Sie unterWorkDocs Drive auf mehreren Computern bereitstellen.

Online-Bearbeitung funktioniert nicht

Vergewissern Sie sich, dass WorkDocs Companion installiert ist. Informationen zur Installation von WorkDocs Companion finden Sie unter Apps und Integrationen für WorkDocs.

Verwaltung WorkDocs für Amazon Business

Wenn Sie Administrator WorkDocs für Amazon Business sind, können Sie Benutzer verwalten, indem Sie sich mit Ihren Amazon Business-Anmeldeinformationen bei https://workdocs.aws/ anmelden.

Um einen neuen Benutzer WorkDocs für Amazon Business einzuladen

1. Melden Sie sich unter https://workdocs.aws/ mit Ihren Amazon Business-Anmeldeinformationen an.
2. Öffnen Sie auf der Startseite WorkDocs für Amazon Business den Navigationsbereich auf der linken Seite.
3. Wählen Sie Admin Settings (Administrator-Einstellungen).
4. Wählen Sie Add people (Personen hinzufügen).
5. Geben Sie unter Recipients (Empfänger) die E-Mail-Adressen oder Benutzernamen der einzuladenden Benutzer ein.
6. (Optional) Passen Sie die Einladungsnachricht an.
7. Wählen Sie Erledigt aus.

Um auf WorkDocs Amazon Business nach einem Benutzer zu suchen

1. Melden Sie sich unter https://workdocs.aws/ mit Ihren Amazon Business-Anmeldeinformationen an.
2. Öffnen Sie auf der Startseite WorkDocs für Amazon Business den Navigationsbereich auf der linken Seite.
3. Wählen Sie Admin Settings (Administrator-Einstellungen).
4. Geben Sie unter Search users (Benutzer suchen) den Vornamen des Benutzers ein und drücken Sie **`Enter`**.

Um Benutzerrollen WorkDocs für Amazon Business auszuwählen

1. Melden Sie sich unter https://workdocs.aws/ mit Ihren Amazon Business-Anmeldeinformationen an.
2. Öffnen Sie auf der Startseite WorkDocs für Amazon Business den Navigationsbereich auf der linken Seite.

3. Wählen Sie Admin Settings (Administrator-Einstellungen).
4. Wählen Sie unter People (Personen) neben dem Benutzer die Rolle aus, die dem Benutzer zugewiesen werden soll.

Um einen Benutzer WorkDocs für Amazon Business zu löschen

1. Melden Sie sich unter https://workdocs.aws/ mit Ihren Amazon Business-Anmeldeinformationen an.
2. Öffnen Sie auf der Startseite WorkDocs für Amazon Business den Navigationsbereich auf der linken Seite.
3. Wählen Sie Admin Settings (Administrator-Einstellungen).
4. Wählen Sie unter People (Personen), die Auslassungspunkte (…) neben dem Benutzer.
5. Wählen Sie Löschen aus.
6. Wenn Sie dazu aufgefordert werden, geben Sie einen neuen Benutzer ein, an den die Dateien des Benutzers übertragen werden sollen, und wählen Sie Delete (Löschen).

IP-Adresse und Domains, die zu Ihrer Zulassungsliste hinzugefügt werden sollen

Wenn Sie IP-Filterung auf Geräten implementieren, die darauf zugreifen WorkDocs, fügen Sie Ihrer Zulassungsliste die folgenden IP-Adressen und Domänen hinzu. Dadurch kann WorkDocs WorkDocs Drive eine Verbindung mit dem WorkDocs Dienst herstellen.

- 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

Wenn Sie IP-Adressbereiche verwenden möchten, finden Sie in der allgemeinen Referenz weitere Informationen unter AWS IP-Adressbereiche.AWS

Dokumentverlauf

In der folgenden Tabelle werden wichtige Änderungen am Amazon WorkDocs Administration Guide ab Februar 2018 beschrieben. Um Benachrichtigungen über Aktualisierungen dieser Dokumentation zu erhalten, können Sie einen RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
Neue Rechte für Dateibesitzer	Administratoren können jetzt die Berechtigungen „Version löschen“ und „Version wiederherstellen“ vergeben. Die Berechtigungen sind Teil der DeleteDocumentVersionAPI-Version.	29. Juli 2022
WorkDocs Backup	Die WorkDocs Backup-Dokumentation wurde aus dem Amazon WorkDocs Administration Guide entfernt, da die Komponente nicht mehr unterstützt wird.	24. Juni 2021
Verwaltung WorkDocs für Amazon Business	WorkDocs for Amazon Business unterstützt die Benutzerverwaltung durch Administratoren. Weitere Informationen finden Sie unter Managing WorkDocs for Amazon Business im Amazon WorkDocs Administration Guide.	26. März 2020
Dateien zu Amazon migrieren WorkDocs	WorkDocs Administratoren können den WorkDocs Migrationsservice verwenden, um eine umfangreiche	8. August 2019

	Migration mehrerer Dateien und Ordner zu ihrer WorkDocs Site durchzuführen. Weitere Informationen finden Sie unter Dateien migrieren zu WorkDocs im WorkDocs Amazon-Administratorhandbuch.	
Einstellungen für die IP-Zulassungsliste	Die Einstellungen für die IP-Zulassungsliste sind verfügbar, um den Zugriff auf Ihre WorkDocs Site nach IP-Adressbereich zu filtern. Weitere Informationen finden Sie unter Einstellungen für die IP-Zulassungsliste im WorkDocs Amazon-Administratorhandbuch.	22. Oktober 2018
Hancom ThinkFree	Hancom ThinkFree ist verfügbar. Benutzer können Microsoft Office-Dateien von der WorkDocs Webanwendung aus erstellen und gemeinsam bearbeiten. Weitere Informationen finden Sie unter Enabling Hancom ThinkFree im Amazon WorkDocs Administration Guide.	21. Juni 2018

Mit Office Online öffnen	Open with Office Online (Mit Office Online öffnen) ist verfügbar. Benutzer können Microsoft Office-Dateien von der WorkDocs Webanwendung aus gemeinsam bearbeiten. Weitere Informationen finden Sie unter Aktivieren von Open with Office Online im WorkDocs Amazon-Administratorhandbuch.	6. Juni 2018
Fehlersuche	Das Thema Fehlerbehebung wurde hinzugefügt. Weitere Informationen finden Sie unter WorkDocs Problembehebung im WorkDocs Amazon-Administratorhandbuch.	23. Mai 2018
Ändern Sie den Aufbewahrungszeitraum für den Aufbewahrungsbehälter	Der Aufbewahrungszeitraum des Papierkorbs kann angepasst werden. Weitere Informationen finden Sie unter Aufbewahrungseinstellungen für den Wiederherstellungskorb im WorkDocs Amazon-Administratorhandbuch.	27. Februar 2018