aws

Administratorhandbuch

Amazon WorkDocs

Amazon WorkDocs: Administratorhandbuch

Table of Contents

Hinweis: Neukundenanmeldungen und Kontoerweiterungen sind für Amazon WorkDocs nicht mehr verfügbar. Erfahren Sie hier mehr über Migrationsschritte: So migrieren Sie Daten von Amazon 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 Service für die Speicherung und gemeinsame Nutzung von Unternehmen mit strengen administrativen Kontrollen und Feedback-Funktionen, die die Produktivität der Benutzer 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 Amazon- WorkDocs Clientanwendungen können verwendet werden, um viele verschiedene Arten von Dateien anzuzeigen, abhängig vom Internet-Medientyp der Datei. Amazon WorkDocs unterstützt alle gängigen Dokument- und Bildformate, und die Unterstützung für zusätzliche Medientypen wird ständig hinzugefügt.

Weitere Informationen finden Sie unter Amazon WorkDocs.

Zugriff auf Amazon WorkDocs

Administratoren verwenden die Amazon- WorkDocs Konsole, um Amazon- WorkDocs Standorte zu erstellen und zu deaktivieren. Mit der Administrator-Systemsteuerung können Sie Benutzer-, Speicher- und Sicherheitseinstellungen verwalten. Weitere Informationen finden Sie unter Verwalten von Amazon WorkDocs über die Website-Admin-Systemsteuerung und WorkDocs Amazon-Nutzer einladen und verwalten.

Benutzer ohne Administratorrolle verwenden die Client-Anwendungen für den Zugriff auf ihre Dateien. Sie verwenden niemals die Amazon- WorkDocs Konsole oder das Verwaltungs-Dashboard. Amazon 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
- Amazon WorkDocs Drive, eine App, die einen Ordner auf Ihrem macOS- oder Windows-Desktop mit Ihren Amazon- WorkDocs Dateien synchronisiert.

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

- Erste Schritte mit Amazon WorkDocs
- Arbeiten mit Dateien
- Arbeiten mit Ordnern

Preisgestaltung

Bei Amazon WorkDocsfallen keine Vorabgebühren oder Verpflichtungen an. Sie zahlen nur für aktive Benutzerkonten und den Speicher, den Sie verwenden. Weitere Informationen finden Sie unter -Preise.

Erste Schritte

Informationen zu den ersten Schritten mit Amazon WorkDocsfinden Sie unter Erstellen einer Amazon- WorkDocs Website.

Daten aus Amazon migrieren WorkDocs

Amazon WorkDocs bietet zwei Methoden für die Migration 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 Sie kontrollieren möchten, welche Dateien Sie migrieren, können Sie 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 Amazon 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 unter Herunterladen von Word-Dokumenten mit Feedback im WorkDocs Amazon-Benutzerhandbuch.
- Sie müssen Amazon WorkDocs Drive verwenden, um Dateien herunterzuladen, die größer als 5 GB sind.
- Wenn Sie Amazon WorkDocs Drive zum Herunterladen von Dateien und Ordnern verwenden, bleiben Ihre Verzeichnisstrukturen, Dateinamen und Dateiinhalte erhalten. Dateibesitz, Berechtigungen und Versionen werden nicht beibehalten.

Dateien aus dem Internet herunterladen

Sie verwenden diese Methode, um Dateien herunterzuladen, wenn:

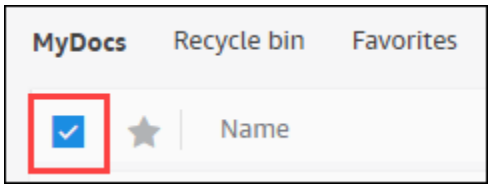
- Sie möchten nur einige Dateien von einer Site herunterladen.
- Sie möchten Word-Dokumente mit Kommentaren herunterladen und diese Kommentare in den jeweiligen Dokumenten beibehalten. Das Migrationstool lädt alle Kommentare herunter, schreibt sie jedoch in eine separate XML-Datei. Benutzer der Website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

Um Dateien aus dem Internet herunterzuladen

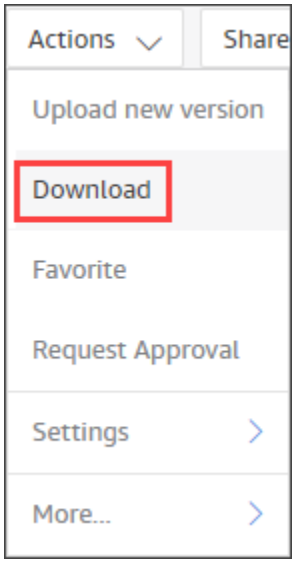
1. Melden Sie sich bei Amazon an WorkDocs.
2. Öffnen Sie bei Bedarf den Ordner, der die Dateien enthält, die Sie herunterladen möchten.
3. Aktivieren Sie das Kontrollkästchen neben den Dateien, die Sie herunterladen möchten.

   -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 bei Amazon an 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 Amazon WorkDocs Drive installieren, um die folgenden Schritte ausführen zu können. Weitere Informationen finden Sie unter Installation von Amazon WorkDocs Drive im Amazon 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 Amazon WorkDocs Drive.

Methode 2: Verwenden Sie das Migrationstool

Sie verwenden das WorkDocs Amazon-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 Amazon die WorkDocs Erlaubnis zu erteilen, Ihre Dateien hochzuladen, 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 Site. WorkDocs 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 für jeden Zeitraum von 24 Stunden 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 /workdocs/ site-alias/Created-Timestamp-UTC / skippedFiles.csv.*** 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 Amazon WorkDocs Developer Guide. 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 Dateien und/oder Ordner, deren Eigentümer er ist. Alle Dateien und/oder Ordner, die für den Benutzer freigegeben wurden, befinden sich in der Zip-Datei des Benutzers, dem die Dateien und/oder Ordner 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 Seite mit den Amazon S3 S3-Preisen.

Das Migrationstool ausführen

In den folgenden Schritten wird erklärt, wie Sie das WorkDocs Amazon-Migrationstool ausführen.

Um eine Site zu migrieren

1. Öffnen Sie die WorkDocs Amazon-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.

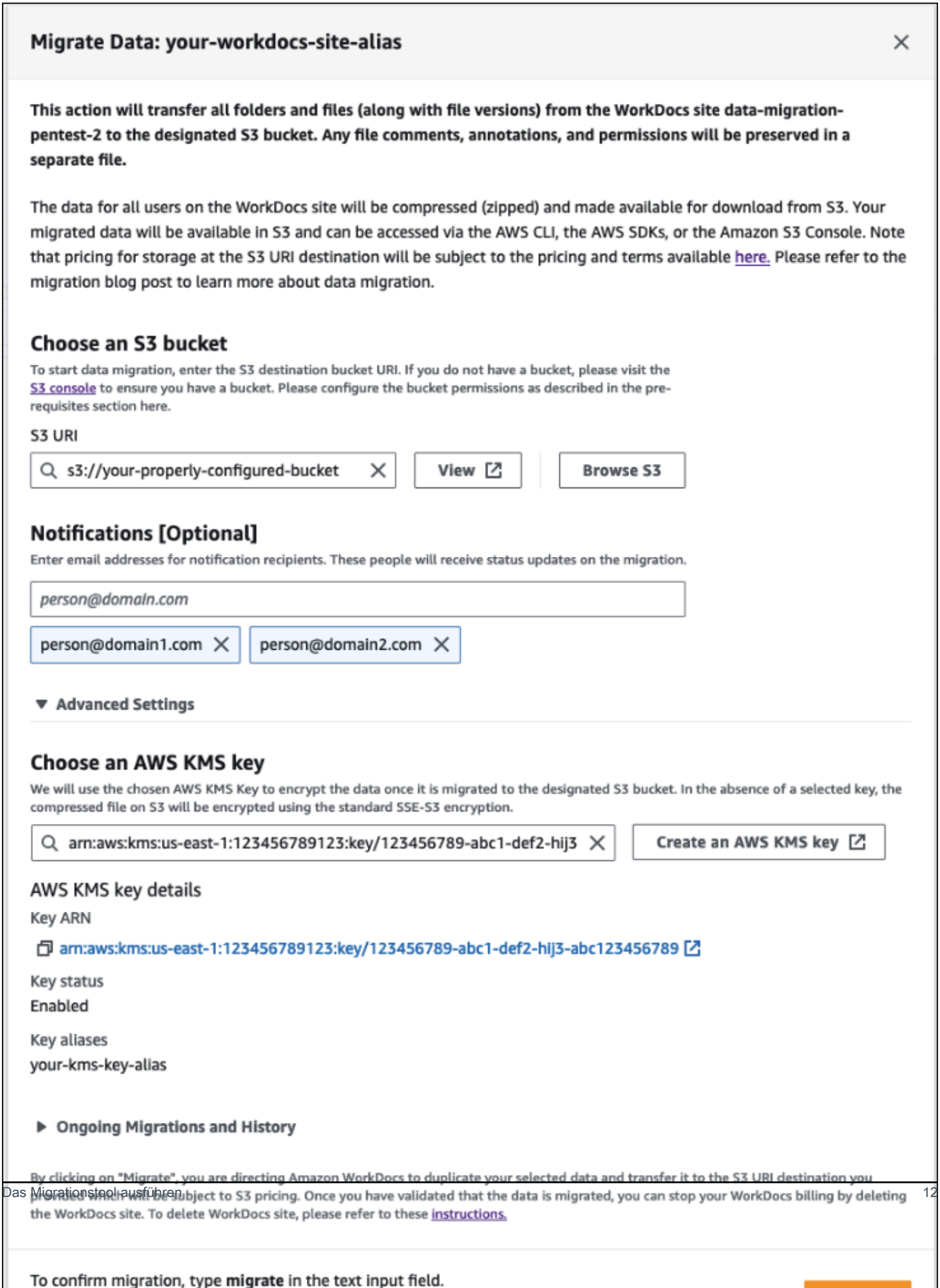
   -ODER-

   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 den Ordner /workdocs/ site-alias /created-timestamp-UTC/enthalten.*** 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-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 auf die 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

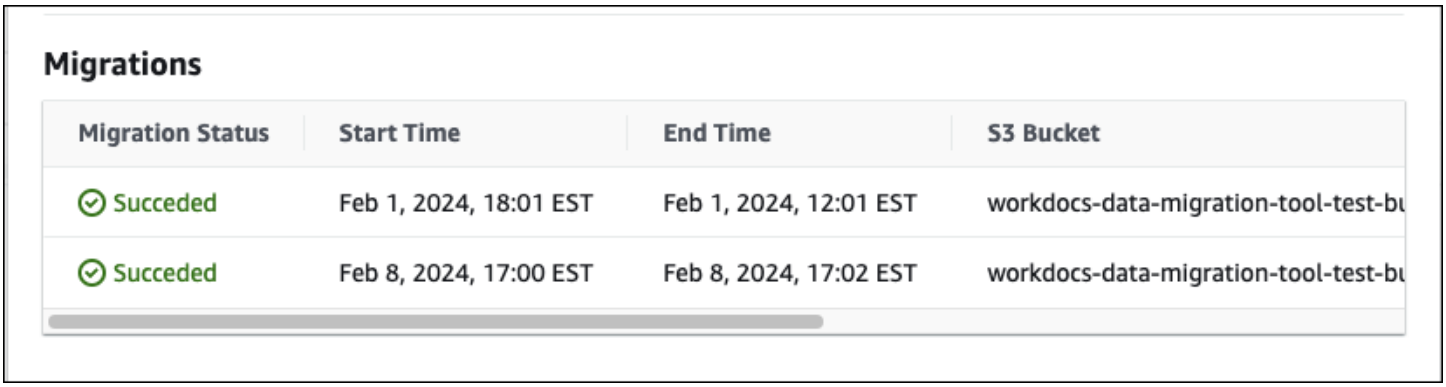
In den folgenden Schritten wird erklärt, wie Sie Ihren Migrationsverlauf einsehen können.

Um Ihren Verlauf einzusehen

1. Öffnen Sie die WorkDocs Amazon-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 Amazon-Websites einzurichten oder bestehende Websites zu verwalten, müssen Sie die folgenden Aufgaben ausführen.

Melden Sie sich an für ein AWS-Konto

Wenn Sie kein haben AWS-Konto, führen Sie die folgenden Schritte aus, um einen 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.

   Bei der Anmeldung müssen Sie auch einen Telefonanruf entgegennehmen und einen Verifizierungscode über die Telefontasten eingeben.

   Wenn Sie sich für eine anmelden AWS-Konto, ein Root-Benutzer des AWS-Kontoswird erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen im Konto. 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 sich Ihre Root-Benutzer des AWS-Kontos, aktivieren AWS IAM Identity Center, und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melde dich an bei AWS Management Consoleals Kontoinhaber wählen Sie Root-Benutzer und geben Sie Ihren AWS-Konto E-Mail-Adresse. Geben Sie auf der nächsten Seite Ihr Passwort ein.

Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter Als Root-Benutzer anmelden in der AWS-Anmeldung Benutzerleitfaden.

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

   Anweisungen finden Sie unter Aktivieren Sie ein virtuelles MFA Gerät für Ihr AWS-Konto Root-Benutzer (Konsole) im IAMBenutzerhandbuch.

Erstellen eines Benutzers mit Administratorzugriff

1. Aktivieren Sie IAM Identity Center.

   Anweisungen finden Sie unter Aktivieren AWS IAM Identity Center in der AWS IAM Identity Center Benutzerleitfaden.

2. Gewähren Sie einem Benutzer in IAM Identity Center Administratorzugriff.

   Für ein Tutorial zur Verwendung des IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie unter Benutzerzugriff mit der Standardeinstellung konfigurieren IAM-Identity-Center-Verzeichnis in der AWS IAM Identity Center Benutzerleitfaden.

Anmelden als Administratorbenutzer

- Um sich mit Ihrem IAM Identity Center-Benutzer anzumelden, verwenden Sie die Anmeldung, 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 unter Anmelden bei AWS Zugriffsportal im AWS-Anmeldung Benutzerleitfaden.

Weiteren Benutzern Zugriff zuweisen

1. Erstellen Sie in IAM Identity Center einen Berechtigungssatz, der der bewährten Methode zur Anwendung von Berechtigungen mit den geringsten Rechten folgt.

   Anweisungen finden Sie unter Einen Berechtigungssatz erstellen in der AWS IAM Identity Center Benutzerleitfaden.

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

Anweisungen finden Sie unter Gruppen hinzufügen im AWS IAM Identity Center Benutzerleitfaden.

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 von Amazon 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 Amazon konfigurieren WorkDocs , um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie lernen auch, wie Sie andere AWS Dienste nutzen können, die Ihnen helfen, Ihre WorkDocs Amazon-Ressourcen zu überwachen und zu sichern.

Themen

Identitäts- und Zugriffsmanagement für Amazon WorkDocs

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

Themen

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, die Sie bei Amazon erledigen WorkDocs.

Servicebenutzer — Wenn Sie den WorkDocs Amazon-Service für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen zur Verfügung, die Sie benötigen. Da Sie für Ihre Arbeit mehr WorkDocs Amazon-Funktionen verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Fuktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Wenn Sie auf eine Funktion in Amazon nicht zugreifen können WorkDocs, finden Sie weitere Informationen unterFehlerbehebung Amazon WorkDocs Amazon-Identität und -Zugriff.

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

IAMAdministrator — Wenn Sie ein IAM Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien schreiben können, um den Zugriff auf Amazon zu verwalten WorkDocs. Beispiele für WorkDocs identitätsbasierte Amazon-Richtlinien, die Sie in verwenden könnenIAM, 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 übernehmen. 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 (IAMIdentity Center-) Nutzer, die Single-Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als föderierte Identität anmelden, hat Ihr Administrator zuvor einen Identitätsverbund mithilfe von Rollen eingerichtet. IAM Wenn Sie AWS mithilfe eines Verbunds darauf zugreifen, übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console 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 darauf zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, mit der Sie Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch signieren können. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode, um Anfragen selbst zu signieren, finden Sie im IAMBenutzerhandbuch unter AWS API Anfragen signieren.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. 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 Verwenden der Multi-Faktor-Authentifizierung (MFA) AWS im IAM Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAMBenutzer ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wir empfehlen, sich nach Möglichkeit auf temporäre Anmeldeinformationen zu verlassen, anstatt IAM Benutzer mit langfristigen Anmeldeinformationen wie Passwörtern und Zugriffsschlüsseln zu erstellen. Wenn Sie jedoch spezielle Anwendungsfälle haben, für die langfristige Anmeldeinformationen von IAM Benutzern erforderlich sind, empfehlen wir, die Zugriffsschlüssel abwechselnd zu verwenden. Weitere Informationen finden Sie im Benutzerhandbuch unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, für die IAM langfristige Anmeldeinformationen erforderlich sind.

Eine IAMGruppe 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 Wann sollte ein IAM Benutzer (statt einer Rolle) erstellt werden? im IAMBenutzerhandbuch.

IAMRollen

Eine IAMRolle ist eine Identität innerhalb von Ihnen AWS-Konto , für die bestimmte Berechtigungen gelten. Sie ähnelt einem IAM Benutzer, ist jedoch keiner bestimmten Person zugeordnet. Sie können vorübergehend eine IAM Rolle in der übernehmen, AWS Management Console indem Sie die Rollen wechseln. Sie können eine Rolle übernehmen, indem Sie eine AWS CLI AWS API OR-Operation aufrufen oder eine benutzerdefinierte Operation verwendenURL. Weitere Informationen zu Methoden zur Verwendung von Rollen finden Sie unter Verwenden von IAM Rollen im IAMBenutzerhandbuch.

IAMRollen mit temporären Anmeldeinformationen sind in den folgenden Situationen nützlich:

- 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 im IAMBenutzerhandbuch unter Erstellen einer Rolle für einen externen Identitätsanbieter. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Um zu kontrollieren, 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 verschiedene Berechtigungen für eine bestimmte Aufgabe zu übernehmen.
- Kontoübergreifender Zugriff — Sie können eine IAM Rolle verwenden, um einer Person (einem vertrauenswürdigen Principal) 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 zum Unterschied zwischen Rollen und ressourcenbasierten Richtlinien für den kontenübergreifenden Zugriff finden Sie IAMim Benutzerhandbuch unter Kontoübergreifender Ressourcenzugriff. IAM
- Serviceübergreifender Zugriff — Einige AWS-Services verwenden Funktionen in anderen. AWS-Services Wenn Sie beispielsweise in einem Service einen Anruf tätigen, 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.
  - Zugriffssitzungen weiterleiten (FAS) — Wenn Sie einen IAM Benutzer oder eine 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. FASverwendet die Berechtigungen des Prinzipals, der an aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen AWS-Service an nachgelagerte Dienste zu stellen. FASAnfragen 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 beim Stellen von FAS Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

- Servicerolle — Eine Servicerolle ist eine IAMRolle, die ein Dienst übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM Administrator kann eine Servicerolle von innen heraus erstellen, ändern und löschenIAM. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Erstellen einer Rolle zum Delegieren von Berechtigungen AWS-Service an eine.
- Dienstbezogene Rolle — Eine dienstverknüpfte 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 dienstbezogene 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 IAMBenutzerhandbuch unter Verwenden einer IAM Rolle zur Erteilung von Berechtigungen für Anwendungen, die auf EC2 Amazon-Instances ausgeführt werden.

Informationen darüber, ob Sie IAM Rollen oder IAM Benutzer verwenden sollten, finden Sie im Benutzerhandbuch unter Wann sollte eine IAM Rolle (anstelle eines IAM Benutzers) erstellt werden.

Verwalten des Zugriffs mit Richtlinien

Sie steuern 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. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden in AWS Form von JSON Dokumenten gespeichert. Weitere Informationen zur Struktur und zum Inhalt von JSON Richtliniendokumenten finden Sie im IAMBenutzerhandbuch unter Überblick über JSON Richtlinien.

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

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Um Benutzern die Erlaubnis zu erteilen, Aktionen mit den Ressourcen durchzuführen, die sie benötigen, kann ein IAM Administrator IAM Richtlinien erstellen. Der Administrator kann dann die IAM Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen übernehmen.

IAMRichtlinien definieren Berechtigungen für eine Aktion, unabhängig von der Methode, mit der Sie den Vorgang ausführen. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen aus dem AWS Management Console AWS CLI, dem oder dem abrufen AWS API.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind Dokumente mit JSON Berechtigungsrichtlinien, die Sie an eine Identität anhängen können, z. B. an einen IAM Benutzer, eine Benutzergruppe oder eine Rolle. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen einer identitätsbasierten Richtlinie finden Sie unter IAMRichtlinien erstellen im Benutzerhandbuch. IAM

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 oder einer Inline-Richtlinie wählen können, finden Sie im IAMBenutzerhandbuch unter Auswahl zwischen verwalteten Richtlinien und Inline-Richtlinien.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON Richtliniendokumente, die Sie an eine Ressource anhängen. Beispiele für ressourcenbasierte Richtlinien sind IAM Rollenvertrauensrichtlinien und Amazon S3 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 nicht IAM in einer ressourcenbasierten Richtlinie verwenden.

Zugriffskontrolllisten

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

Amazon S3 und AWS WAF Amazon VPC sind Beispiele für Dienste, die Unterstützung bietenACLs. 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 eine erweiterte Funktion, mit der Sie die maximalen Berechtigungen festlegen, die eine identitätsbasierte Richtlinie einer IAM Entität (IAMBenutzer oder Rolle) gewähren 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 zu Berechtigungsgrenzen finden Sie im IAMBenutzerhandbuch unter Berechtigungsgrenzen für IAM Entitäten.
- 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 Geräte 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. Weitere Informationen zu Organizations und SCPs finden Sie unter Richtlinien zur Servicesteuerung 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 im IAMBenutzerhandbuch unter Sitzungsrichtlinien.

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

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zugelassen werden soll, wenn mehrere Richtlinientypen betroffen sind, findest du unter Bewertungslogik für Richtlinien im IAMBenutzerhandbuch.

So WorkDocs arbeitet Amazon mit IAM

Bevor Sie IAM den Zugriff auf Amazon verwalten WorkDocs, müssen Sie wissen, welche IAM Funktionen für Amazon verfügbar sind WorkDocs. Einen allgemeinen Überblick darüber, wie Amazon WorkDocs und andere AWS Dienste zusammenarbeitenIAM, finden Sie IAM im IAMBenutzerhandbuch unter AWS Services, die mit funktionieren.

Themen

- WorkDocsIdentitätsbasierte Richtlinien von Amazon
- WorkDocsRessourcenbasierte Richtlinien von Amazon
- Autorisierung basierend auf WorkDocs Amazon-Tags
- WorkDocs IAMRollen bei Amazon

WorkDocsIdentitätsbasierte Richtlinien von Amazon

Mit IAM identitätsbasierten Richtlinien können Sie zulässige oder abgelehnte Aktionen angeben. Amazon WorkDocs unterstützt bestimmte Aktionen. Weitere Informationen zu den Elementen,

die Sie in einer JSON Richtlinie verwenden, finden Sie in der Referenz zu den IAM JSON Richtlinienelementen im IAMBenutzerhandbuch.

Aktionen

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

Das `Action` Element 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, für die nur eine Genehmigung erforderlich ist und für die es keinen entsprechenden Vorgang gibt. API 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.

Richtlinienaktionen in Amazon WorkDocs verwenden vor der Aktion das folgende Präfix:`workdocs:`. Um beispielsweise jemandem die Erlaubnis zu erteilen, den WorkDocs `DescribeUsers` API Amazon-Vorgang auszuführen, nehmen Sie die `workdocs:DescribeUsers` Aktion in seine Richtlinie auf. Richtlinienanweisungen müssen entweder ein – `Action`oder ein `NotAction`-Element enthalten. Amazon WorkDocs definiert eigene Aktionen, die Aufgaben beschreiben, die Sie mit diesem Service ausführen 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. Beispielsweise:
>
> ```
> "Action": [
> "zocalo:*",
> "workdocs:*"
> ],
> ```

Eine Liste der WorkDocs Amazon-Aktionen finden Sie WorkDocs im IAMBenutzerhandbuch unter Von Amazon definierte Aktionen.

Ressourcen

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

Bedingungsschlüssel

Amazon WorkDocs stellt keine servicespezifischen Bedingungsschlüssel zur Verfügung, unterstützt jedoch die Verwendung einiger globaler Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAMBenutzerhandbuch.

Beispiele

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

WorkDocsRessourcenbasierte Richtlinien von Amazon

Amazon unterstützt WorkDocs keine ressourcenbasierten Richtlinien.

Autorisierung basierend auf WorkDocs Amazon-Tags

Amazon unterstützt WorkDocs weder das Markieren von Ressourcen noch das Steuern des Zugriffs auf der Grundlage von Tags.

WorkDocs IAMRollen bei Amazon

Eine IAMRolle ist eine Entität innerhalb Ihres AWS Kontos, die über bestimmte Berechtigungen verfügt.

Temporäre Anmeldeinformationen mit Amazon verwenden WorkDocs

Wir empfehlen dringend, temporäre Anmeldeinformationen zu verwenden, um sich bei Federation anzumelden, eine IAM Rolle zu übernehmen oder eine kontoübergreifende Rolle anzunehmen. Sie erhalten temporäre Sicherheitsanmeldedaten, indem Sie AWS STS API Operationen wie AssumeRoleoder GetFederationTokenaufrufen.

Amazon 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 durchzuführen. Mit Diensten verknüpfte Rollen werden in Ihrem IAM Konto angezeigt und gehören dem Dienst. Ein IAM Administrator kann die Berechtigungen für dienstbezogene Rollen anzeigen, aber nicht bearbeiten.

Amazon WorkDocs unterstützt keine servicebezogenen 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 dem Konto. Das bedeutet, dass ein IAM Administrator die Berechtigungen für diese Rolle ändern kann. Dies kann jedoch die Funktionalität des Dienstes beeinträchtigen.

Amazon 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.

Standardmäßig sind IAM Benutzer und Rollen nicht berechtigt, WorkDocs Amazon-Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben mit dem AWS Management Console AWS CLI, oder ausführen AWS API. Ein IAM Administrator muss IAM Richtlinien erstellen, die Benutzern und Rollen die Berechtigung gewähren, bestimmte API Operationen mit den angegebenen Ressourcen auszuführen, die sie benötigen. Der Administrator muss diese Richtlinien dann den IAM Benutzern oder Gruppen zuordnen, für die diese Berechtigungen erforderlich sind.

> **Note**
>
> Um die Abwärtskompatibilität sicherzustellen, sollten Sie die `zocalo` Aktion in Ihre Richtlinien aufnehmen. Beispielsweise:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Deny",
            "Action": [
            "zocalo:*",
            "workdocs:*"
            ],
            "Resource": "*"
        }
    ]
}
```

Informationen zum Erstellen einer IAM identitätsbasierten Richtlinie anhand dieser JSON Beispieldokumente finden Sie unter Richtlinien erstellen auf der JSON Registerkarte im IAM Benutzerhandbuch.

Themen

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

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand WorkDocs Amazon-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder diese 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 AWS im IAMBenutzerhandbuch unter AWS Verwaltete Richtlinien oder Verwaltete Richtlinien für Jobfunktionen.
- Berechtigungen mit den geringsten Rechten anwenden — Wenn Sie Berechtigungen mit IAM Richtlinien festlegen, gewähren Sie nur die Berechtigungen, die für die Ausführung 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 IAM zum Anwenden von Berechtigungen finden Sie IAMim Benutzerhandbuch unter Richtlinien und Berechtigungen. IAM
- Verwenden Sie Bedingungen in IAM Richtlinien, um den Zugriff weiter einzuschränken — Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen einzuschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um anzugeben, dass alle Anfragen mit gesendet werden müssenSSL. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese über einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter IAMJSONRichtlinienelemente: Bedingung.
- Verwenden Sie IAM Access Analyzer, um Ihre IAM Richtlinien zu validieren, um sichere und funktionale Berechtigungen zu gewährleisten. IAM Access Analyzer validiert neue und bestehende Richtlinien, sodass die Richtlinien der IAM Richtliniensprache (JSON) und den IAM bewährten Methoden entsprechen. IAMAccess Analyzer bietet mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen, um Sie bei der Erstellung sicherer und funktionaler Richtlinien zu unterstützen. Weitere Informationen finden Sie unter IAMAccess Analyzer-Richtlinienvalidierung im IAMBenutzerhandbuch.

- Multi-Faktor-Authentifizierung erforderlich (MFA) — Wenn Sie ein Szenario haben, in dem IAM Benutzer oder ein Root-Benutzer erforderlich sind AWS-Konto, aktivieren Sie die Option MFA für zusätzliche Sicherheit. Wenn Sie festlegen möchten, MFA wann API Operationen aufgerufen werden, fügen Sie MFA Bedingungen zu Ihren Richtlinien hinzu. Weitere Informationen finden Sie unter Konfiguration des MFA -geschützten API Zugriffs im IAMBenutzerhandbuch.

Weitere Informationen zu bewährten Methoden finden Sie unter Bewährte Sicherheitsmethoden IAM im IAM Benutzerhandbuch. IAM

Verwenden der WorkDocs Amazon-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 Amazon-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 Amazon-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 IAMBenutzerhandbuch.

- AmazonWorkDocsFullAccess
- AWSDirectoryServiceFullAccess
- Amazon EC2FullAccess

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

Sie müssen Benutzern, die nur Anrufe an den AWS CLI oder am tätigen, keine Mindestberechtigungen für die Konsole gewähren AWS API. Erlauben Sie stattdessen nur den Zugriff auf die Aktionen, die dem API Vorgang entsprechen, den Sie ausführen möchten.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

Dieses Beispiel zeigt, wie Sie eine Richtlinie erstellen könnten, die es IAM Benutzern ermöglicht, die Inline- und verwalteten Richtlinien einzusehen, die mit ihrer Benutzeridentität verknüpft sind.

Diese Richtlinie umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe von oder. AWS CLI AWS API

```
{
    "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 Amazon-Ressourcen WorkDocs

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

WorkDocs kann. Zugriff auf den AWS Directory Service `DescribeDirectories` Vorgang ist erforderlich, um Informationen über Ihre AWS 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 von Amazon

IAMAdministratoren können zusätzliche Richtlinien erstellen, um einer IAM Rolle oder einem Benutzer den Zugriff auf Amazon zu ermöglichen WorkDocs API. Weitere Informationen finden Sie unter Authentifizierung und Zugriffskontrolle für Verwaltungsanwendungen im Amazon WorkDocs Developer Guide.

Fehlerbehebung Amazon WorkDocs Amazon-Identität und -Zugriff

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit Amazon WorkDocs und auftreten könnenIAM.

Themen

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

Ich bin nicht berechtigt, eine Aktion in Amazon durchzuführen WorkDocs

Wenn Ihnen AWS Management Console 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 eine Fehlermeldung erhalten, dass Sie nicht berechtigt sind, die `iam:PassRole` Aktion durchzuführen, müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an Amazon weitergeben können WorkDocs.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Service zu übergeben, anstatt eine neue Servicerolle oder eine dienstbezogene 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 Amazon auszuführen WorkDocs. 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 Amazon-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 Amazon diese Funktionen WorkDocs unterstützt, finden Sie unterSo 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 anderen IAMBenutzer AWS-Konto , den Sie besitzen.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAMBenutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- Informationen dazu, wie Sie Zugriff über einen Identitätsverbund gewähren, finden Sie im Benutzerhandbuch unter Zugriff für extern authentifizierte Benutzer (Identitätsverbund). IAM
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontenübergreifenden Zugriff finden Sie IAMim Benutzerhandbuch unter Kontoübergreifender Ressourcenzugriff. IAM

Protokollierung und Überwachung in Amazon WorkDocs

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

Themen

Exportieren des seitenweiten Aktivitätsfeeds

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

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.

Wird AWS CloudTrail zum Protokollieren von WorkDocs API Amazon-Anrufen verwendet

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

Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Übermittlung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für Amazon 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 Amazon-Informationen in CloudTrail

CloudTrail ist in Ihrem AWS Konto aktiviert, wenn Sie das Konto erstellen. Wenn in Amazon Aktivitäten auftreten WorkDocs, wird diese Aktivität zusammen mit anderen AWS Serviceereignissen in der CloudTrail Ereignishistorie 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 Veranstaltungen für Amazon 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 SNS Amazon-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien von mehreren Konten

Alle WorkDocs Amazon-Aktionen werden von Amazon protokolliert CloudTrail und sind in der WorkDocs APIAmazon-Referenz 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:

- Ob die Anfrage mit Root- oder IAM Benutzeranmeldedaten gestellt 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 im CloudTrail userIdentityElement.

WorkDocs Amazon-Protokolldateieinträge 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 Bei Protokolldateien handelt es sich nicht um einen geordneten Stack-Trace der öffentlichen API Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Amazon WorkDocs generiert verschiedene Arten von CloudTrail Einträgen, solche aus der Steuerungsebene 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 Amazon-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 Protokollen als HIDDEN _ DUE _TO_ SECURITY _ REASONS angezeigt. CloudTrail

Das folgende Beispiel zeigt zwei CloudTrail Protokolleinträge für Amazon 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:

- Schnellstartanleitungen zu Sicherheit und Compliance — In diesen Bereitstellungsleitfäden werden architektonische Überlegungen erörtert und Schritte für die Implementierung von Basisumgebungen beschrieben AWS , bei denen Sicherheit und Compliance im Mittelpunkt stehen.
- Architecting for HIPAA Security and Compliance on Amazon Web Services — In diesem Whitepaper wird beschrieben, wie Unternehmen Anwendungen erstellen HIPAA können, die AWS für sie in Frage kommen.

  > **Note**
  >
  > Nicht alle sind berechtigt AWS-Services . HIPAA Weitere Informationen finden Sie in der Referenz für HIPAA qualifizierte Dienste.

- AWS Ressourcen zur AWS von Vorschriften — Diese Sammlung von Arbeitsmappen und Leitfäden kann auf Ihre Branche und Ihren Standort zutreffen.
- 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 für 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)) zusammengefasst.

- 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— 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. Eine Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerungsreferenz.
- 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 zu erfüllen PCIDSS, z. B. durch die Erfüllung der Anforderungen zur Erkennung von Eindringlingen, die in bestimmten Compliance-Frameworks vorgeschrieben sind.
- 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 IAMBenutzerhandbuch und Best Practices for Security, Identity, and Compliance im AWS Architecture Center.

Sie verwenden AWS veröffentlichte API Anrufe, um WorkDocs über das Netzwerk auf Amazon zuzugreifen. Kunden müssen Transport Layer Security (TLS) 1.2 unterstützen, und wir empfehlen die Verwendung von TLS 1.3. Die Kunden müssen außerdem Cipher Suites mit Perfect Forward Secrecy wie Ephemeral Diffie-Hellman oder Elliptic Curve Ephemeral Diffie-Hellman unterstützen. Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Darüber hinaus müssen Anfragen mithilfe einer Zugriffsschlüssel-ID und eines geheimen Zugriffsschlüssels, der einem Prinzipal zugeordnet ist, signiert werden. IAM Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Erste Schritte mit Amazon WorkDocs

Amazon WorkDocs verwendet ein Verzeichnis, um Organisationsinformationen für Ihre Benutzer und deren Dokumente zu speichern und zu verwalten. Im Gegenzug fügen Sie ein Verzeichnis an einen Standort an, wenn Sie diesen Standort bereitstellen. Wenn Sie dies tun, fügt eine Amazon- WorkDocs Funktion namens Automatische Aktivierung die Benutzer im Verzeichnis als verwaltete Benutzer zur Website hinzu, was bedeutet, dass sie keine separaten Anmeldeinformationen benötigen, um sich bei Ihrer Website anzumelden, und sie Dateien freigeben und an ihnen zusammenarbeiten können. Jeder Benutzer hat 1 TB Speicherplatz, es sei denn, er kauft mehr.

Sie müssen Benutzer nicht mehr manuell hinzufügen und aktivieren, obwohl Sie dies immer noch können. Sie können auch Benutzerrollen und Berechtigungen ändern, wenn Sie dies benötigen. Weitere Informationen dazu finden Sie unter weiter WorkDocs Amazon-Nutzer einladen und verwaltenunten in diesem Leitfaden.

Wenn Sie Verzeichnisse erstellen müssen, können Sie:

- Simple AD-Verzeichnis erstellen.
- Erstellen Sie ein AD-Connector-Verzeichnis, um eine Verbindung zu Ihrem On-Premises-Verzeichnis herzustellen.
- Aktivieren Sie Amazon WorkDocs , um mit einem vorhandenen AWS Verzeichnis zu arbeiten.
- Lassen Sie Amazon ein Verzeichnis für Sie WorkDocs erstellen.

Sie können auch eine Vertrauensstellung zwischen Ihrem AD-Verzeichnis und einem AWS Managed Microsoft AD-Verzeichnis erstellen.

> **Note**
>
> Wenn Sie zu einem Compliance-Programm wie PCI, FedRAMP oder DoD gehören, müssen Sie ein -AWS Managed Microsoft ADVerzeichnis einrichten, um die Compliance-Anforderungen zu erfüllen. In den Schritten in diesem Abschnitt wird erläutert, 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

Erstellen einer Amazon- WorkDocs Website

In den Schritten in den folgenden Abschnitten wird erläutert, wie Sie eine neue Amazon- WorkDocs Website einrichten.

Aufgaben

Bevor Sie beginnen

Sie müssen über die folgenden Elemente verfügen, bevor Sie eine Amazon- WorkDocs Website erstellen.

- Ein -AWSKonto zum Erstellen und Verwalten von Amazon- WorkDocs Standorten. Benutzer benötigen jedoch kein -AWSKonto, um eine Verbindung zu herzustellen und Amazon zu verwenden WorkDocs. Weitere Informationen finden Sie unter Voraussetzungen für Amazon WorkDocs.
- Wenn Sie Simple AD verwenden möchten, müssen Sie die Voraussetzungen erfüllen, die unter Voraussetzungen für Simple AD im AWS Directory Service -Administratorhandbuch aufgeführt sind.
- Ein -AWS Managed Microsoft ADVerzeichnis, wenn Sie zu einem Compliance-Programm wie PCI, FedRAMP oder DoD gehören. In den Schritten in diesem Abschnitt wird erläutert, 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.

Erstellen einer Amazon- WorkDocs Website

Gehen Sie wie folgt vor, um innerhalb weniger Minuten eine Amazon- WorkDocs Website zu erstellen.

So erstellen Sie die Amazon- WorkDocs Website

1. Öffnen Sie die Amazon- 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 Standorte und auf der Seite Ihre WorkDocs Standorte verwalten die Option WorkDocs Website erstellen aus.

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

   - Wenn Sie ein Verzeichnis haben, wird die Seite Verzeichnis auswählen angezeigt und ermöglicht Ihnen, ein vorhandenes Verzeichnis auszuwählen oder ein Verzeichnis zu erstellen.
   - Wenn Sie kein Verzeichnis haben, wird die Seite Einen Verzeichnistyp einrichten angezeigt und ermöglicht Ihnen, ein Simple-AD- oder AD-Connector-Verzeichnis zu erstellen

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

   So verwenden Sie ein vorhandenes Verzeichnis

   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 obigen Schritte 1 und 2.

      An dieser Stelle hängt das, was Sie tun, davon ab, ob Sie Simple AD verwenden oder einen AD Connector erstellen möchten.

So verwenden Sie Simple AD

a. Wählen Sie Simple AD und dann Weiter aus.

   Die Seite Simple-AD-Website erstellen wird angezeigt.

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

c. Geben Sie unter 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 Simple-AD-Website erstellen aus.

So erstellen Sie ein AD-Connector-Verzeichnis

a. Wählen Sie AD Connector und dann Weiter aus.

   Die Seite AD-Connector-Website erstellen wird angezeigt.

b. Füllen Sie alle Felder unter Verzeichnisdetails aus.

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

d. Füllen Sie wie gewünscht die optionalen Felder unter VPC-Konfiguration aus.

e. Wählen Sie AD-Connector-Website erstellen aus.

Amazon WorkDocs führt die folgenden Schritte aus:

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

> **Note**
>
> Amazon benachrichtigt Benutzer WorkDocs nicht über die neue Website. Sie müssen ihnen die URL mitteilen und sie darüber informieren, dass sie keine separate Anmeldung benötigen, um die Website zu verwenden.

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 Amazon registriert WorkDocs ist, ohne separate Anmeldeinformationen einzugeben. Amazon- WorkDocs Administratoren können Single Sign-On über die AWS Directory Service Konsole aktivieren. Weitere Informationen finden Sie unter Single Sign-On im AWS Directory Service -Administratorhandbuch.

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

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-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 branchenübliches Client/Server-Protokoll, das Authentifizierungs-, Autorisierungs- und Buchhaltungsverwaltung bereitstellt, damit Benutzer eine Verbindung zu -Netzwerkservices herstellen können. AWS Managed Microsoft AD enthält 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 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 Multi-Faktor-Authentifizierung für AWS Managed Microsoft AD aktivieren im AWS Directory Service Administration Guide.

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

Hochstufen eines Benutzers zum Administrator

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

So stufen Sie einen Benutzer zum Administrator hoch

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

   Die Seite Verwalten Ihrer WorkDocs Standorte wird angezeigt.
3. Wählen Sie die Schaltfläche neben dem gewünschten Standort, wählen Sie Aktionen und dann Administrator festlegen aus.

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

Sie können auch das Amazon WorkDocs Site Admin Control Panel verwenden, um einen Administrator zu degradieren. Weitere Informationen finden Sie unter Bearbeiten von Benutzern.

Verwalten von Amazon WorkDocs über die AWS Konsole

Sie verwenden diese Tools, um Ihre Amazon- WorkDocs Standorte zu verwalten:

- Die AWSKonsole unter https://console.aws.amazon.com/zocalo/.
- Die Website-Administrator-Systemsteuerung, die Administratoren auf allen Amazon- WorkDocs Standorten zur Verfügung steht.

Jedes dieser Tools bietet einen anderen Satz von Aktionen, und die Themen in diesem Abschnitt erklären die von der AWS Konsole bereitgestellten Aktionen. Weitere Informationen zur Website-Admin-Systemsteuerung finden Sie unter Verwalten von Amazon WorkDocs über die Website-Admin-Systemsteuerung.

Festlegen von Websiteadministratoren

Wenn Sie Administrator sind, können Sie Benutzern Zugriff auf die Website-Systemsteuerung und die von ihr bereitgestellten Aktionen gewähren.

So legen Sie einen Administrator fest

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

   Die Seite Ihre WorkDocs Standorte verwalten wird angezeigt und zeigt eine Liste Ihrer Standorte an.
3. Wählen Sie die Schaltfläche neben der Website, für die Sie einen Administrator festlegen möchten.
4. Öffnen Sie die Liste Aktionen und wählen Sie 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 Administrator festlegen aus.

Erneutes Senden von Einladungs-E-Mails

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

So senden Sie die Einladungs-E-Mail erneut

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

   Die Seite Ihre WorkDocs Standorte verwalten wird angezeigt und zeigt eine Liste Ihrer Standorte an.
3. Wählen Sie die Schaltfläche neben der Website, für die Sie die E-Mail erneut senden möchten.
4. Öffnen Sie die Liste Aktionen und wählen Sie Einladungs-E-Mail erneut senden aus.

   Oben auf der Seite wird eine Erfolgsmeldung in einem grünen Banner angezeigt.

Verwalten der Multifaktor-Authentifizierung

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

Festlegen von Website-URLs

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

So legen Sie eine Website-URL fest

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

Die Seite Ihre WorkDocs Standorte verwalten wird angezeigt und zeigt eine Liste Ihrer Standorte an.

3. Wählen Sie den Standort aus, den Sie in Amazon integriert haben WorkSpaces. Die URL enthält die Verzeichnis-ID Ihrer Amazon- WorkSpaces Instance, z. B. https://{directory_id}.awsapps.com.
4. Wählen Sie die Schaltfläche neben dieser URL, öffnen Sie die Liste Aktionen und wählen Sie Website-URL festlegen aus.

   Das Dialogfeld Website-URL festlegen wird angezeigt.
5. Geben Sie im Feld Website-URL die URL für die Website ein und wählen Sie dann Website-URL festlegen aus.
6. Wählen Sie auf der Seite Ihre WorkDocs Standorte verwalten die Option Aktualisieren aus, um die neue URL anzuzeigen.

Verwalten von Benachrichtigungen

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

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

Sie können Benachrichtigungen erstellen und löschen. In den folgenden Schritten wird erläutert, wie beide Aufgaben ausgeführt werden.

> **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 die IAM-Konsole unter https://console.aws.amazon.com/iam/.

2. Wählen Sie in der Navigationsleiste Benutzer aus.
3. Wählen Sie Ihren Benutzernamen aus.
4. Kopieren Sie unter Zusammenfassung Ihren ARN.

So erstellen Sie eine Benachrichtigung

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

   Die Seite Ihre WorkDocs Standorte verwalten wird angezeigt und zeigt eine Liste Ihrer Standorte an.
3. Wählen Sie die Schaltfläche neben dem gewünschten Standort.
4. Öffnen Sie die Liste Aktionen und wählen Sie Benachrichtigungen verwalten aus.

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

   Die Seite Ihre WorkDocs Standorte verwalten wird angezeigt und zeigt eine Liste Ihrer Standorte an.
3. Wählen Sie die Schaltfläche neben dem Standort mit der Benachrichtigung, die Sie löschen möchten.
4. Öffnen Sie die Liste Aktionen und wählen Sie Benachrichtigungen verwalten aus.
5. Wählen Sie auf der Seite Benachrichtigungen verwalten die Schaltfläche neben der Benachrichtigung aus, die Sie löschen möchten, und wählen Sie dann Benachrichtigungen löschen aus.

Löschen einer Website

Sie verwenden die Amazon- WorkDocs Konsole, um einen Standort zu löschen.

> **Warning**
>
> Sie verlieren alle Dateien, wenn Sie einen Standort 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 Amazon- WorkDocs Konsole unter https://console.aws.amazon.com/zocalo/.
2. Wählen Sie in der Navigationsleiste Meine Websites aus.

   Die Seite Ihre WorkDocs Standorte verwalten wird angezeigt.
3. Wählen Sie die Schaltfläche neben dem Standort, den Sie löschen möchten, und wählen Sie dann Löschen aus.

   Das Dialogfeld Website-URL löschen wird angezeigt.
4. Wählen Sie optional auch Benutzerverzeichnis löschen aus.

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

   Die Website wird sofort gelöscht und ist nicht mehr verfügbar.

Verwalten von Amazon WorkDocs über die Website-Admin-Systemsteuerung

Sie verwenden diese Tools, um Ihre Amazon- WorkDocs Standorte zu verwalten:

- Die Website-Administrator-Systemsteuerung, die Administratoren auf allen Amazon- WorkDocs Standorten zur Verfügung steht und in den folgenden Themen beschrieben wird.
- Die AWS Konsole unter https://console.aws.amazon.com/zocalo/.

Jedes dieser Tools bietet einen anderen Satz von Aktionen. In den Themen in diesem Abschnitt werden die Aktionen erläutert, die von der Website-Administrator-Systemsteuerung bereitgestellt werden. Informationen zu den in der Konsole verfügbaren Aufgaben finden Sie unter Verwalten von Amazon WorkDocs über die AWS Konsole.

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 Einstellungencom Online Editing und Office Online über die Admin-Systemsteuerung . 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

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

> **Note**
>
> Die IP Allow List (IP-Genehmigungsliste) funktioniert derzeit nur bei IPv4-Adressen. Die Sperrliste 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 für 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 ActiveDirectory Standorte

In diesem Thema werden die verschiedenen Sicherheitseinstellungen für einfache ActiveDirectory Standorte erläutert. Wenn Sie Standorte verwalten, die den ActiveDirectory Konnektor verwenden, lesen Sie den nächsten Abschnitt.

So verwenden Sie Sicherheitseinstellungen

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

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

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

Einstellung	Beschreibung
Wählen Sie unter Einstellung für gemeinsam nutzbare Links auswählen eine der folgenden Optionen aus:	
Erlauben Sie keine standortweiten oder öffentlich freigabefähigen Links	Deaktiviert die Linkfreigabe für alle Benutzer.
Benutzern erlauben, standortweite gemeinsam nutzbare Links zu erstellen, aber	Schränkt die Linkfreigabe nur auf Website-Mitglieder ein. Verwaltete Benutzer können diese Art von Link erstellen.

Einstellung	Beschreibung
ihnen nicht erlauben, öffentlich gemeinsam nutzbare Links zu erstellen	
Benutzern erlauben, standortweite gemeinsam nutzbare Links zu erstellen, aber nur Hauptbenutzer können öffentlich gemeinsam nutzbare Links erstellen	Verwaltete Benutzer können standortweite Links erstellen, aber nur Hauptbenutzer können öffentliche Links erstellen. Öffentliche Links ermöglichen jedem im Internet Zugriff.
Alle verwalteten Benutzer können standortweite und öffentlich gemeinsam nutzbare Links erstellen	Verwaltete Benutzer können öffentliche Links erstellen.

Aktivieren oder deaktivieren Sie unter Automatische Aktivierung das Kontrollkästchen.

Erlauben Sie allen Benutzern in Ihrem Verzeichnis, bei der ersten Anmeldung an Ihrer WorkDocs Website automatisch aktiviert zu werden.	Aktiviert Benutzer automatisch, wenn sie sich zum ersten Mal auf Ihrer Website anmelden.

Wählen Sie unter Wer sollte berechtigt sein, neue Benutzer zu Ihrer WorkDocs Website einzuladen 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 Dateien oder Ordner mit diesen Benutzern geteilt werden.
Benutzer können neue Benutzer aus einigen bestimmten Domänen einladen, indem sie Dateien oder Ordner für sie freigeben.	Benutzer können neue Personen aus den angegebenen Domänen einladen, indem sie Dateien oder Ordner für sie freigeben.

Aktivieren oder deaktivieren Sie unter Rolle für neue Benutzer konfigurieren das Kontrollkästchen.

Einstellung	Beschreibung
Neue Benutzer aus Ihrem Verzeichnis sind Verwaltete Benutzer (sie sind standardmäßig Gastbenutzer).	Konvertiert neue Benutzer automatisch aus Ihrem Verzeichnis in verwaltete Benutzer.

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

Sicherheit – ActiveDirectory Konnektor-Standorte

In diesem Thema werden die verschiedenen Sicherheitseinstellungen für ActiveDirectory Konnektor-Standorte erläutert. Wenn Sie Standorte verwalten, die Simple verwenden ActiveDirectory, lesen Sie den vorherigen Abschnitt.

So verwenden Sie Sicherheitseinstellungen

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

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

   Das Dialogfeld Richtlinieneinstellungen wird angezeigt. In der folgenden Tabelle sind die Sicherheitseinstellungen für ActiveDirectory Konnektor-Standorte aufgeführt und beschrieben.

Einstellung	Beschreibung
Wählen Sie unter Einstellung für gemeinsam nutzbare Links auswählen eine der folgenden Optionen aus:	
Site-weite oder öffentlich freigabefähige Links nicht zulassen	Wenn diese Option ausgewählt ist, wird die Linkfreigabe für alle Benutzer deaktiviert.
Benutzern erlauben, standortweite gemeinsam nutzbare Links zu erstellen, aber	Schränkt die Linkfreigabe nur auf Website-Mitglieder ein. Verwaltete Benutzer können diese Art von Link erstellen.

Einstellung	Beschreibung
ihnen nicht erlauben, öffentlich gemeinsam nutzbare Links zu erstellen	
Benutzern erlauben, standortweite gemeinsam nutzbare Links zu erstellen, aber nur Hauptbenutzer können öffentlich gemeinsam nutzbare Links erstellen	Verwaltete Benutzer können standortweite Links erstellen, aber nur Hauptbenutzer können öffentliche Links erstellen. Öffentliche Links ermöglichen jedem im Internet Zugriff.
Alle verwalteten Benutzer können standortweite und öffentliche gemeinsam nutzbare Links erstellen	Verwaltete Benutzer können öffentliche Links erstellen.

Aktivieren oder deaktivieren Sie unter Automatische Aktivierung das Kontrollkästchen.

Erlauben Sie allen Benutzern in Ihrem Verzeichnis, bei der ersten Anmeldung an Ihrer WorkDocs Website automatisch aktiviert zu werden.	Aktiviert Benutzer automatisch, wenn sie sich zum ersten Mal auf Ihrer Website anmelden.

Wählen Sie unter Wer sollte Verzeichnisbenutzer auf Ihrem WorkDocs Standort aktivieren dürfen? eine der folgenden Optionen aus:

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

Wählen Sie unter Wer sollte berechtigt sein, neue Benutzer zu Ihrer WorkDocs Website einzuladen? eine der folgenden Optionen aus:

Einstellung	Beschreibung
Mit externen Benutzern teilen **Note** Die folgenden Optionen werden erst angezeigt, nachdem Sie diese Einstellung ausgewählt haben.	Enables administrators and users to invite new external users to your Amazon WorkDocs site.
Nur Administratoren können neue externe Benutzer einladen	Nur Administratoren können externe Benutzer einladen.
Alle verwalteten Benutzer können neue Benutzer einladen	Ermöglicht es verwalteten Benutzern, externe Benutzer einzuladen.
Nur Hauptbenutzer können neue externe Benutzer einladen.	Ermöglicht nur Hauptbenutzern, neue externe Benutzer einzuladen.
Wählen Sie unter Rolle für neue Benutzer konfigurieren eine oder beide Optionen aus.	
Neue Benutzer aus Ihrem Verzeichnis sind Verwaltete Benutzer (standardmäßig Gastbenutzer).	Konvertiert neue Benutzer automatisch aus Ihrem Verzeichnis in verwaltete Benutzer.
Neue externer Benutzer sind verwaltete Benutzer (standardmäßig Gastbenutzer)	Konvertiert neue externe Benutzer automatisch in verwaltete Benutzer.

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

Aufbewahrung im Papierkorb

Wenn ein Benutzer eine Datei löscht, WorkDocs speichert Amazon die Datei 30 Tage lang im Papierkorb des Benutzers. Danach WorkDocs verschiebt Amazon die Dateien 60 Tage lang in einen temporären Wiederherstellungskorb und löscht sie dann dauerhaft. Nur Administratoren können den temporären Wiederherstellungs-Bin sehen. Durch die Änderung der standortweiten Datenaufbewahrungsrichtlinie können Site-Administratoren den Aufbewahrungszeitraum für den Wiederherstellungs-Bin auf ein Minimum von null Tagen und ein Maximum von 365 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 Wiederherstellungs-Bin aufbewahrt werden sollen, und wählen Sie Speichern aus.

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

Administratoren können Benutzerdateien aus dem Wiederherstellungs-Bin wiederherstellen, bevor Amazon sie dauerhaft WorkDocs löscht.

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 Amazon-Nutzer einladen und verwalten.

Bereitstellen von Amazon WorkDocs Drive auf mehreren Computern

Wenn Sie eine über eine Domäne verbundene Geräteflotte verfügen, können Sie den Amazon WorkDocs Drive--Client mit dem System Center Configuration Manager (SCCM) installieren. Sie können den -Client von herunterladenhttps://amazonworkdocs.com/en/clientsaus.

Denken Sie dabei daran, dass Amazon WorkDocs Drive HTTPS-Zugriff auf Port 443 für alle AWS-IP-Adressen benötigt. Sie möchten auch bestätigen, dass Ihre Zielsysteme die Installationsanforderungen für Amazon WorkDocs Drive erfüllen. Weitere Informationen finden Sie unterAmazon WorkDocs Drive installierenimAmazon WorkDocs User Guideaus.

> **Note**
>
> Installieren Sie den Amazon WorkDocs Drive-Client als Best Practice bei der Verwendung von GPO oder SCCM, nachdem sich Benutzer angemeldet haben.

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

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

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

```
msiexec /i "AWSWorkDocsDriveClient.msi" SITEID=Ihre_WorkDocs_Site_ID
DefaultDriveLetter=your_drive_letterREBOOT=REALLYSUPPRESS /norestart /qn
```

WorkDocs Amazon-Nutzer einladen und verwalten

Wenn Sie bei der Erstellung einer Website ein Verzeichnis anhängen, WorkDocs fügt die automatische Aktivierungsfunktion in Amazon standardmäßig alle Benutzer in diesem Verzeichnis der neuen Site als verwaltete Benutzer hinzu.

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

Darüber hinaus können Sie Benutzer einladen, aktivieren oder deaktivieren sowie Benutzerrollen und -einstellungen ändern. Außerdem können Sie einen Benutzer zum Administrator hochstufen. Weitere Informationen über das Hochstufen von Benutzern finden Sie unterHochstufen eines Benutzers zum Administrator.

Sie erledigen diese Aufgaben im Admin-Kontrollpanel im Amazon WorkDocs Web Client, und die Schritte in den folgenden Abschnitten erklären, wie das geht. Wenn Sie jedoch neu bei Amazon sind WorkDocs, nehmen Sie sich ein paar Minuten Zeit und informieren Sie sich über die verschiedenen Benutzerrollen, bevor Sie sich mit den administrativen Aufgaben befassen.

Inhalt

Übersicht: Benutzerrollen

Amazon 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.
- Poweruser: Ein bezahlter Benutzer, der über spezielle Administratorberechtigungen verfügt. Weitere Informationen zum Festlegen von Berechtigungen für einen Poweruser finden Sie unterSicherheit – Einfache ActiveDirectory Standorte undSicherheit – ActiveDirectory Konnektor-Standorte.
- Benutzer: Ein bezahlter Benutzer, der Dateien speichern und mit anderen auf einer WorkDocs Amazon-Website 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.

Amazon definiert WorkDocs auch diese zusätzlichen Benutzertypen.

WS-Benutzer

Ein Benutzer mit einem zugewiesenen WorkSpaces WorkSpace.

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

WorkDocs Amazon-Nutzer

Ein aktiver WorkDocs Amazon-Benutzer ohne zugewiesenen Benutzer WorkSpaces WorkSpace.

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

Das Admin-Kontrollpanel starten

Sie verwenden das administrative Kontrollfeld im Amazon WorkDocs Web Client, um die automatische Aktivierung aus- und einzuschalten und Benutzerrollen und -einstellungen zu ändern.

Um das Admin-Kontrollpanel zu öffnen

1. Wählen Sie oben rechts im WorkDocs Client das Profilsymbol aus.

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

> **Note**
>
> Einige Systemsteuerungsoptionen unterscheiden sich zwischen Cloud-Verzeichnissen und verbundenen Verzeichnissen.

Deaktivieren der automatischen Aktivierung

Sie deaktivieren die automatische Aktivierung, wenn Sie nicht alle Benutzer in einem Verzeichnis zu einer neuen Site hinzufügen möchten und wenn Sie unterschiedliche Berechtigungen und Rollen für

die Benutzer festlegen möchten, die Sie zu einer neuen Site einladen. Wenn Sie die automatische Aktivierung deaktivieren, können Sie auch entscheiden, wer neue Benutzer zur Site einladen darf — aktuelle Benutzer, Hauptbenutzer oder Administratoren. In diesen Schritten wird erläutert, wie Sie beide Aufgaben ausführen.

Deaktivieren der automatischen Aktivierung

1. Wählen Sie oben rechts im WorkDocs Client das Profilsymbol aus.

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

   Das Dialogfeld mit Richtlinieneinstellungen wird angezeigt.
4. Deaktivieren Sie unter Automatische Aktivierung das Kontrollkästchen neben Alle Benutzer in Ihrem Verzeichnis dürfen automatisch aktiviert werden, wenn sie sich zum ersten Mal auf Ihrer WorkDocs Site anmelden.

   Die Optionen ändern sich unter Wer sollte Verzeichnisbenutzer auf Ihrer WorkDocs Site aktivieren dürfen. Sie können aktuelle Benutzer neue Benutzer einladen lassen, oder Sie können diese Möglichkeit Power-Usern oder anderen Administratoren geben.
5. Wählen Sie eine Option aus und wählen Sie dann Änderungen speichern.

Wiederholen Sie die Schritte 1 bis 4, um die automatische Aktivierung erneut zu aktivieren.

Link-Sharing verwalten

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

Um das Teilen von Links zu aktivieren

1. Wählen Sie oben rechts im WorkDocs Client das Profilsymbol aus.

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

   Das Dialogfeld mit Richtlinieneinstellungen wird angezeigt.
4. Wählen Sie unter Wählen Sie Ihre Einstellung für teilbare Links eine Option aus:

   - Keine seitenweiten oder öffentlich teilbaren Links zulassen — Deaktiviert das Teilen von Links für alle Benutzer.
   - Erlaube Benutzern, Links zu erstellen, die auf der gesamten Website geteilt werden können, aber erlaube ihnen nicht, öffentlich teilbare Links zu erstellen — Beschränkt das Teilen von Links auf die Mitglieder der Website. Verwaltete Benutzer können diese Art von Link erstellen.
   - Erlauben Sie Benutzern, Links zu erstellen, die auf der gesamten Website geteilt werden können, aber nur Poweruser können öffentlich teilbare Links erstellen. Verwaltete Benutzer können Links für die gesamte Website erstellen, aber nur Poweruser können öffentliche Links erstellen. Öffentliche Links ermöglichen den Zugriff auf das Internet.
   - Alle verwalteten Benutzer können seitenweite und öffentlich teilbare Links erstellen — Verwaltete Benutzer können öffentliche Links erstellen.
5. Wählen Sie Save Changes.

Steuern 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 die Genehmigung für einen der folgenden Schritte erteilen:

- Alle Benutzer
- Power-User
- Administratoren.

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

Um Einladungsberechtigungen festzulegen

1. Wählen Sie oben rechts im WorkDocs Client das Profilsymbol aus.

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

   Das Dialogfeld mit Richtlinieneinstellungen wird angezeigt.
4. Aktivieren Sie unter Wer soll Verzeichnisbenutzer auf Ihrer WorkDocs Site aktivieren dürfen 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.

Einladen neuer Benutzer

Sie können neue Benutzer einladen, einem Verzeichnis beizutreten. Sie können auch vorhandenen Benutzern ermöglichen, neue Benutzer einzuladen. Weitere Informationen finden Sie unterSicherheit – Einfache ActiveDirectory Standorte undSicherheit – ActiveDirectory Konnektor-Standorte in diesem Handbuch.

Einladen von neuen Benutzern

1. Wählen Sie oben rechts im WorkDocs Client das Profilsymbol aus.

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

4. Im Dialogfeld Benutzer einladen für Wen möchten Sie einladen? , geben Sie die E-Mail-Adresse des Eingeladenen ein und wählen Sie Senden. Wiederholen Sie diesen Schritt für jede Einladung.

Amazon WorkDocs sendet eine Einladungs-E-Mail an jeden Empfänger. Die E-Mail enthält einen Link und Anweisungen zum Erstellen eines WorkDocs Amazon-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 oben rechts im WorkDocs Client das Profilsymbol aus.

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 ein Administrator ist. Sie können auch Benutzer heraufstufen oder herabstufen, denen eine WorkSpaces WorkSpace zugewiesen wurde. 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 oben rechts im WorkDocs Client das Profilsymbol aus.

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 Amazon-Website zugreifen.

> **Note**
>
> Wenn Sie einen Benutzer in den Status Inaktiv versetzen, werden seine Dateien, Ordner oder Feedback nicht von Ihrer WorkDocs Amazon-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 Amazon-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 Amazon-Website zugreift.

Übertragen der Dokumentenkontrolle

Sie können die Dateien und Ordner eines aktiven Benutzers auf einen inaktiven Benutzer übertragen. Weitere Informationen dazu, wie Sie einen Benutzer deaktivieren finden Sie unterDeaktivieren von Benutzern.

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

So übertragen Sie die Dokumentenkontrolle

1. Wählen Sie oben rechts im WorkDocs Client das Profilsymbol aus.

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 „Besitz des Dokuments übertragen“ und geben Sie die E-Mail-Adresse des neuen Besitzers ein.
6. Wählen Sie Save Changes.

Benutzerlisten herunterladen

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

So laden Sie eine Benutzerliste herunter

1. Wählen Sie oben rechts im WorkDocs Client das Profilsymbol aus.

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 in einem der folgenden Speicherorte ab:
   - Windows – `Downloads/WorkDocsDownloads`
   - macOS – *`hard drive`*`/users/`*`username`*`/WorkDocsDownloads/folder`

> **Note**
>
> Downloads können etwas Zeit in Anspruch nehmen. 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 die externe Freigabe aktivieren.

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

Inhalt

Freigeben von Links

Benutzer können Link teilen wählen, um Hyperlinks für Amazon- WorkDocs Inhalte schnell zu kopieren und mit Kollegen und externen Benutzern sowohl innerhalb als auch 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 Amazon- WorkDocs Website können nach der Datei suchen, sie anzeigen und kommentieren.
- Jeder Benutzer mit dem Link, auch Personen, die keine Mitglieder der Amazon- WorkDocs Website sind, kann die Datei anzeigen. 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 Verwalten von Amazon WorkDocs über die Website-Admin-Systemsteuerung.

Freigeben durch Einladen

Wenn Sie die Freigabe per Einladung aktivieren, können Ihre Website-Benutzer Dateien oder Ordner für einzelne Benutzer und für Gruppen freigeben, indem sie Einladungs-E-Mails senden. Die Einladungen enthalten Links zu den freigegebenen Inhalten, und Einladungen können die freigegebenen Dateien oder Ordner öffnen. Eingeladene können diese Dateien oder Ordner auch für andere Website-Mitglieder und für externe Benutzer freigeben.

Sie können Berechtigungsstufen für jeden eingeladenen Benutzer festlegen. Sie können auch Teamordner erstellen, die Sie freigeben können, indem Sie sie für von Ihnen erstellte Verzeichnisgruppen einladen.

> **Note**
>
> Freigabeeinladungen enthalten keine Mitglieder verschachtelter Gruppen. Um diese Mitglieder einzubeziehen, müssen Sie sie der Liste Freigabe nach Einladung hinzufügen.

Weitere Informationen finden Sie unter Verwalten von Amazon WorkDocs über die Website-Admin-Systemsteuerung.

Externe Freigaben

Die externe Freigabe ermöglicht es verwalteten Benutzern einer Amazon- WorkDocs Website, Dateien und Ordner gemeinsam zu nutzen und mit externen Benutzern zu arbeiten, ohne dass zusätzliche Kosten anfallen. Site-Benutzer können Dateien und Ordner für externe Benutzer freigeben, ohne dass Empfänger auf der Amazon- WorkDocs Website bezahlt werden müssen. Wenn Sie die externe Freigabe aktivieren, können Benutzer die E-Mail-Adresse des externen Benutzers eingeben, mit dem sie teilen möchten, und entsprechende Berechtigungen für die Freigabe von Viewern festlegen. Wenn externe Benutzer hinzugefügt werden, sind die Berechtigungen auf Betrachterrechte 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 Website weitergeleitet, auf der sie ihre Anmeldeinformationen eingeben, um sich bei Amazon 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 Verwalten von Amazon WorkDocs über die Website-Admin-Systemsteuerung.

Berechtigungen

Amazon 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 (nur Leseberechtigungen) auf die Datei.
- Anonymer Betrachter — Ein nicht registrierter Benutzer außerhalb der Organisation, der eine Datei ansehen kann, die über einen externen Link geteilt wurde. Wenn nicht anders angegeben, hat ein anonymer Betrachter die gleichen Berechtigungen wie ein Betrachter.

* 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 — Feedback von anderen Benutzern anzeigen.
- 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.

	Anmerk	Löschen	Umbenen	Hochlad	Herunte	Downloa	Freigeb	Teilen	Anzeige	Aktivi	Anmerk	Aktivitä	Version	Version	Versione	Alle privaten Kommentare anzeigen**
			n		laden	verhind		widerru	ansehe		anzeige	anzeige	anzeige	löschen	wiederh	
						n		n			n				stellen	
Besi der Date	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

	Anmerk	Löschen	Umbenen	Hochlad	Herunterladen	Download verhinder	Freigeben	Teilen widerrufen	Anzeige	Aktivitäten ansehen	Anmerkungen anzeigen	Aktivität anzeigen	Versionen anzeigen	Version löschen	Version wiederherstellen	Alle privaten Kommentare anzeigen**
Besitz des Ordn	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Miteig ümer des Ordn	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Mitwi 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 — Feedback von anderen Benutzern anzeigen.
- 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	Aktivitä 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 Online-Bearbeitungseinstellungen in Ihrem Admin-Steuerfeld, um die Optionen für die gemeinsame Bearbeitung zu aktivieren.

Inhalt

Aktivieren voncom ThinkFree

Sie könnencom ThinkFree für Ihre Amazon- WorkDocs Website aktivieren, sodass Benutzer Microsoft Office-Dateien über die Amazon WorkDocs -Webanwendung erstellen und gemeinsam bearbeiten können. Weitere Informationen finden Sie unter Bearbeiten mitcom ThinkFree.

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

So aktivieren Siecom ThinkFree

Aktivieren Siecom- ThinkFree Bearbeitung über die Admin-Systemsteuerung .

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.

So deaktivieren Siecom ThinkFree

Deaktivieren Siecom- ThinkFree Bearbeitung über die Admin-Systemsteuerung .

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 Open with Office Online für Ihre Amazon- WorkDocs Website, damit Benutzer Microsoft- Office-Dateien gemeinsam über die Amazon WorkDocs -Webanwendung bearbeiten können.

Open with Office Online ist für Amazon- WorkDocs Benutzer, die auch über ein Microsoft Office 365-Work- oder Bol-Konto mit einer Lizenz zur Bearbeitung in Office Online verfügen, ohne zusätzliche Kosten verfügbar. 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 zu Amazon migrieren WorkDocs

WorkDocs Amazon-Administratoren können den Amazon WorkDocs Migration Service verwenden, um eine umfangreiche Migration mehrerer Dateien und Ordner auf ihre WorkDocs Amazon-Website durchzuführen. Der Amazon WorkDocs Migration Service funktioniert mit Amazon Simple Storage Service (Amazon S3). Auf diese Weise können Sie abteilungsspezifische Dateifreigaben und private Festplattenfreigaben oder Benutzerdateifreigaben zu Amazon WorkDocs migrieren.

Während dieses Vorgangs WorkDocs bietet Amazon eine AWS Identity and Access Management (IAM) Richtlinie für Sie. Verwenden Sie diese Richtlinie, um eine neue IAM Rolle zu erstellen, die Zugriff auf den Amazon WorkDocs Migration Service gewährt, um Folgendes zu tun:

- Lesen Sie den Amazon S3 S3-Bucket, den Sie angeben, und listen Sie ihn auf.
- Lesen und schreiben Sie auf der von Ihnen angegebenen WorkDocs Amazon-Website.

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

- Administratorrechte für Ihre WorkDocs Amazon-Website
- Berechtigungen zum Erstellen von IAM-Rollen

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

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

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

Aufgaben

Schritt 1: Inhalte für die Migration vorbereiten

Um Ihre Inhalte für die Migration vorzubereiten

1. Erstellen Sie auf Ihrer WorkDocs Amazon-Website unter Meine Dokumente 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. Amazon 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 — Zum 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 einen neuen Amazon Simple Storage Service (Amazon S3) -Bucket in Ihrem AWS Konto, in das Sie Ihre Dateien und Ordner hochladen möchten. Der Amazon S3 S3-Bucket muss sich im selben befinden AWS Konto und AWS Region als Ihre WorkDocs Amazon-Website. 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 die Verwendung von AWS DataSync 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 Wie AWS DataSync funktioniert und Die Verwendung identitätsbasierter Richtlinien (IAMRichtlinien) für DataSync in der AWS DataSync Benutzerleitfaden.

Schritt 3: Planen einer Migration

Nachdem Sie die Schritte 1 und 2 abgeschlossen haben, verwenden Sie den Amazon WorkDocs Migration Service, 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 Amazon-Benutzerkontos automatisch auf Unbegrenzt.

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

Der Amazon WorkDocs Migration Service bietet eine AWS Identity and Access Management (IAM) Richtlinie, die Sie für die Migration verwenden können. Mit dieser Richtlinie erstellen Sie eine neue IAM Rolle, die dem Amazon WorkDocs Migration Service Zugriff auf den Amazon S3 S3-Bucket und die von Ihnen WorkDocs angegebene Amazon-Site gewährt. Sie abonnieren auch SNS E-Mail-Benachrichtigungen von Amazon, 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 Amazon-Konsole Apps, Migrationen aus.
   - Wenn Sie zum ersten Mal auf Amazon WorkDocs Migration Service zugreifen, werden Sie aufgefordert, SNS E-Mail-Benachrichtigungen von Amazon 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.
5. Kopieren Sie für Data Source & Validation unter Beispielrichtlinie die mitgelieferte 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 die IAM Konsole unter https://console.aws.amazon.com/iam/.
   b. Wählen Sie Policies (Richtlinien), Create policy (Richtlinie erstellen) aus.
   c. Wählen Sie die IAM Richtlinie aus, die Sie zuvor in Ihre Zwischenablage kopiert haben, JSONund fügen Sie sie ein.
   d. Wählen Sie Richtlinie prüfen. Geben Sie einen Namen und eine Beschreibung für die Richtlinie ein.
   e. Wählen Sie Create Policy (Richtlinie erstellen) aus.

f. Wählen Sie Roles (Rollen), Create role (Rolle erstellen) aus.

g. Wählen Sie 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) Folgendes 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) Folgendes 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.

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 API Sitzungsdauer CLI /auf 12 Stunden.

l. Kopieren Sie die Rolle ARN in Ihre Zwischenablage, um sie im nächsten Schritt zu verwenden.

7. Kehren Sie zum Amazon WorkDocs Migration Service zurück. Fügen Sie für Datenquelle und Validierung unter Rolle ARN die Rolle ARN aus der Rolle ein, die Sie im vorherigen Schritt kopiert haben. IAM
8. Wählen Sie für Bucket den Amazon S3 S3-Bucket aus, aus dem die Dateien migriert werden sollen.
9. Wählen Sie Weiter.
10. Wählen Sie unter WorkDocs Zielordner auswählen den Zielordner in Amazon WorkDocs aus, in den die Dateien migriert werden sollen.
11. Wählen Sie Weiter.
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 von der Amazon WorkDocs Migration Service-Landingpage aus verfolgen. Um von der WorkDocs Amazon-Website 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.

Um die IAM Richtlinie und Rolle zu löschen

1. Öffnen Sie die IAM Konsole unter https://console.aws.amazon.com/iam/.
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.
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 beginnt, wird die Speichereinstellung Ihres WorkDocs Amazon-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.

Fehlerbehebung für Amazon WorkDocsProblembereiche

Die folgenden Informationen können Ihnen helfen, Probleme mit Amazon zu beheben WorkDocs.

Problembereiche

Ich kann mein Amazon nicht einrichten WorkDocs Site in einer bestimmtenAWSRegion

Wenn Sie ein neues Amazon einrichten WorkDocs wählen Sie bei der Einrichtung die AWS-Region aus. Weitere Informationen finden Sie im Tutorial für Ihren speziellen Anwendungsfall unter Erste Schritte mit Amazon WorkDocs.

Willst du mein Amazon einrichten WorkDocs Site in einer vorhandenen Amazon VPC

Beim Einrichten Ihres neuen Amazon WorkDocs ein Verzeichnis mit der vorhandenen Virtual Private Cloud (VPC) erstellen Amazon 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 Amazon bereitstellen WorkDocs Drive oder Amazon WorkDocs Begleiter für mehrere Benutzer

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. Für spezifische Informationen über die Bereitstellung von Amazon WorkDocs Fahren Sie zu mehreren Benutzern, sieheBereitstellen von Amazon WorkDocs Drive auf mehreren Computern.

Online-Bearbeitung funktioniert nicht

Stellen Sie sicher, dass Sie Amazon haben WorkDocs Companion ist installiert. So installieren Sie Amazon WorkDocs Begleiter, sieheApps & Integrationen für Amazon WorkDocs.

Verwalten von Amazon WorkDocs für Amazon Business

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

Einladen eines neuen Benutzers zu Amazon WorkDocs für Amazon Business

1. Melden Sie sich unter https://workdocs.aws/ mit Ihren Amazon Business-Anmeldeinformationen an.
2. Öffnen Sie auf der -Startseite von Amazon 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 Done.

In Amazon WorkDocs für Amazon Business nach einem Benutzer suchen

1. Melden Sie sich unter https://workdocs.aws/ mit Ihren Amazon Business-Anmeldeinformationen an.
2. Öffnen Sie auf der -Startseite von Amazon 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`**.

Auswählen von Benutzerrollen in Amazon WorkDocs für Amazon Business

1. Melden Sie sich unter https://workdocs.aws/ mit Ihren Amazon Business-Anmeldeinformationen an.

2. Öffnen Sie auf der -Startseite von Amazon 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.

So löschen Sie einen Benutzer auf Amazon WorkDocs for Amazon Business

1. Melden Sie sich unter https://workdocs.aws/ mit Ihren Amazon Business-Anmeldeinformationen an.
2. Öffnen Sie auf der -Startseite von Amazon 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 Delete (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 Sie Ihrer Zulassungsliste hinzufügen möchten

Wenn Sie IP-Filterung auf Geräten implementieren, die auf Amazon zugreifen WorkDocs, fügen Sie die folgenden IP-Adressen und Domänen zu Ihrer Zulassungsliste hinzu. Dadurch wird Amazon aktiviert WorkDocs und Amazon WorkDocs Antrieb zur Verbindung mit dem WorkDocs Service.

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

Informationen zur Verwendung von IP-Adressbereichen finden Sie unterAWS-IP-Adressbereichein derAWSAllgemeine Hinweise.

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 Amazon-Datensicherung	Die Amazon WorkDocs Backup-Dokumentation wurde aus dem Amazon WorkDocs Administration Guide entfernt, da die Komponente nicht mehr unterstützt wird.	24. Juni 2021
Amazon WorkDocs für Amazon Business verwalten	Amazon WorkDocs for Amazon Business unterstützt die Benutzerverwaltung durch Administratoren. Weitere Informationen finden Sie unter Managing Amazon WorkDocs for Amazon Business im Amazon WorkDocs Administration Guide.	26. März 2020
Dateien zu Amazon migrieren WorkDocs	WorkDocs Amazon-Administratoren können den Amazon WorkDocs Migration Service verwenden, um eine	8. August 2019

	umfangreiche Migration mehrerer Dateien und Ordner auf ihre WorkDocs Amazon-Website durchzuführen. Weitere Informationen finden Sie unter Migrieren von Dateien zu Amazon WorkDocs im WorkDocs Amazon-Administratorhandbuch.	
Einstellungen für die IP-Zulassungsliste	Die Einstellungen für die IP-Zulassungsliste sind verfügbar, um den Zugriff auf Ihre WorkDocs Amazon-Website 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 Amazon-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 Amazon-We banwendung aus gemeinsam bearbeiten. Weitere Informati onen finden Sie unter Aktiviere n von Open with Office Online im WorkDocs Amazon-Ad ministratorhandbuch.	6. Juni 2018
Fehlersuche	Das Thema Fehlerbehebung wurde hinzugefügt. Weitere Informationen finden Sie unter Fehlerbehebung Amazon WorkDocs Amazon-Problemen im WorkDocs Amazon-Ad ministratorhandbuch.	23. Mai 2018
Ändern Sie den Aufbewahr ungszeitraum für den Aufbewahrungsbehälter	Der Aufbewahrungszeitr aum des Papierkorbs kann angepasst werden. Weitere Informationen finden Sie unter Aufbewahrungseinstellungen für den Wiederherstellungs korb im WorkDocs Amazon-Ad ministratorhandbuch.	27. Februar 2018