aws

Administratorhandbuch

# Amazon WorkDocs

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

# Amazon WorkDocs: Administratorhandbuch

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Handelsmarken und Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

# Table of Contents

Sie müssen ein WorkDocs Amazon-Systemadministrator sein, um die Schritte in diesem Handbuch ausführen zu können. Wenn Sie Hilfe bei der Nutzung von Amazon benötigen WorkDocs, finden Sie weitere Informationen unter Erste Schritte mit Amazon WorkDocs im WorkDocs Amazon-Benutzerhandbuch.

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.

# Voraussetzungen für Amazon WorkDocs

Um neue Amazon- WorkDocs Standorte einzurichten oder vorhandene Standorte zu verwalten, müssen Sie die folgenden Aufgaben ausführen.

## So melden Sie sich für ein AWS-Konto an

Wenn Sie kein AWS-Konto haben, führen Sie die folgenden Schritte zum Erstellen durch.

Anmeldung für ein AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/signup.
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 ein AWS-Konto anmelden, wird ein Root-Benutzer des AWS-Kontos erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Als bewährte Sicherheitsmethode weisen Sie einem Administratorbenutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

AWS sendet Ihnen eine Bestätigungs-E-Mail, sobald die Anmeldung abgeschlossen ist. Sie können jederzeit Ihre aktuelle Kontoaktivität anzeigen und Ihr Konto verwalten. Rufen Sie dazu https://aws.amazon.com/ auf und klicken Sie auf Mein Konto.

## Erstellen eines Administratorbenutzers

Nachdem Sie sich für ein AWS-Kontoangemeldet haben, sichern Sie Ihr Root-Benutzer des AWS-Kontos, aktivieren Sie AWS IAM Identity Centerund erstellen Sie einen administrativen Benutzer, damit Sie nicht den Root-Benutzer für alltägliche Aufgaben verwenden.

Schützen Ihres Root-Benutzer des AWS-Kontos

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

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

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

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

## Erstellen eines Administratorbenutzers

1. Aktivieren von IAM Identity Center.

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

2. Im IAM Identity Center gewähren Sie einem administrativen Benutzer administrativen Zugriff.

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

## Anmelden als Administratorbenutzer

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

  Hilfe bei der Anmeldung mit einem IAM-Identity-Center-Benutzer finden Sie unter Anmelden beim AWS-Zugangsportal im AWS-Anmeldung Benutzerhandbuch zu.

# Sicherheit in Amazon WorkDocs

Die Sicherheit in der Cloud hat für AWS höchste Priorität. Als AWS-Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die zur Erfüllung der Anforderungen von Organisationen entwickelt wurden, für die Sicherheit eine kritische Bedeutung hat.

Sicherheit gilt zwischen AWS und Ihnen eine geteilte Verantwortung. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud: AWS ist dafür verantwortlich, die Infrastruktur zu schützen, mit der AWS-Services in der AWS-Cloud ausgeführt werden. AWS stellt Ihnen außerdem Services bereit, die Sie sicher nutzen können. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der AWS-Compliance-Programme regelmäßig. Informationen zu den Compliance-Programmen, die für Amazon gelten WorkDocs, finden Sie unter AWS Im Rahmen des Compliance-Programms zugelassene -Services.
- Sicherheit in der Cloud – Der AWS Service, den Sie verwenden, 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 geteilten Verantwortung bei der Verwendung von Amazon einsetzen können WorkDocs.

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

Die folgenden Themen zeigen Ihnen, wie Sie Amazon WorkDocs zur Erfüllung Ihrer Sicherheits- und Compliance-Ziele konfigurieren. Sie erfahren auch, wie Sie andere -AWSServices verwenden, die Sie bei der Überwachung und Sicherung Ihrer Amazon- WorkDocs Ressourcen unterstützen.

Themen

- Identity and Access Management für Amazon WorkDocs

# Identity and Access Management für Amazon WorkDocs

AWS Identity and Access Management (IAM) ist ein AWS-Service, mit dem Administratoren den Zugriff auf AWS-Ressourcen sicher steuern können. IAM-Administratoren steuern, wer für die Nutzung von Amazon- WorkDocs Ressourcen authentifiziert (angemeldet) und autorisiert (im Besitz von Berechtigungen) werden kann. IAM ist ein AWS-Service, den Sie ohne zusätzliche Kosten verwenden können.

Themen



## Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, unterscheidet sich je nach Ihrer Arbeit in Amazon WorkDocs.

Service-Benutzer – Wenn Sie den Amazon- WorkDocs Service zur Ausführung von Aufgaben verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen bereit, die Sie benötigen. Wenn Sie für Ihre Arbeit weitere Amazon- WorkDocs Funktionen ausführen, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Featuresweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Wenn Sie nicht auf ein Feature in Amazon zugreifen können WorkDocs, finden Sie weitere Informationen unter Fehlerbehebung für Amazon- WorkDocs Identität und -Zugriff.

Service-Administrator – Wenn Sie in Ihrem Unternehmen für die Amazon- WorkDocs Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollständigen Zugriff auf Amazon WorkDocs. Ihre Aufgabe besteht darin, zu bestimmen, auf welche Amazon- WorkDocs Funktionen und -Ressourcen Ihre Service-Benutzer zugreifen sollen. Sie müssen dann Anträge an Ihren IAM-Administrator stellen, um die Berechtigungen Ihrer Servicenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen dazu, wie Ihr Unternehmen IAM mit Amazon verwenden kann WorkDocs, finden Sie unter Funktionsweise WorkDocs von Amazon mit IAM.

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

## Authentifizierung mit Identitäten

Authentifizierung ist die Art, wie Sie sich mit Ihren Anmeldeinformationen bei AWS anmelden. Die Authentifizierung (Anmeldung bei AWS) muss als Root-Benutzer des AWS-Kontos, als IAM-Benutzer oder durch Übernahme einer IAM-Rolle erfolgen.

Sie können sich bei AWS als Verbundidentität mit Anmeldeinformationen anmelden, die über eine Identitätsquelle bereitgestellt werden. Benutzer von AWS IAM Identity Center (IAM Identity Center), die Single-Sign-on-Authentifizierung Ihres Unternehmens und Anmeldeinformationen für Google oder Facebook sind Beispiele für Verbundidentitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie auf AWS mithilfe des Verbunds zugreifen, übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich bei der AWS Management Console oder beim AWS-Zugriffsportal anmelden. Weitere Informationen zum Anmelden bei AWS finden Sie unter So melden Sie sich bei Ihrem AWS-Konto an im Benutzerhandbuch von AWS-Anmeldung.

Bei programmgesteuertem Zugriff auf AWS bietet AWS ein Software Development Kit (SDK) und eine Command Line Interface (CLI, Befehlszeilenschnittstelle) zum kryptographischen Signieren Ihrer Anfragen mit Ihren Anmeldeinformationen. Wenn Sie keine AWS-Tools verwenden, müssen Sie Anforderungen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode zum eigenen Signieren von Anforderungen finden Sie unter Signieren von AWS-API-Anforderungen im IAM-Benutzerhandbuch.

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

## IAM-Benutzer und -Gruppen

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

Eine IAM-Gruppe ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise einer Gruppe mit dem Namen IAMAdmins Berechtigungen zum Verwalten 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 Erstellen eines IAM-Benutzers (anstatt einer Rolle) im IAM-Benutzerhandbuch.

## IAM-Rollen

Eine IAM-Rolle ist eine Identität in Ihrem AWS-Konto mit spezifischen Berechtigungen. Sie ist einem IAM-Benutzer vergleichbar, ist aber nicht mit einer bestimmten Person verknüpft. Sie können vorübergehend eine IAM-Rolle in der AWS Management Console übernehmen, indem Sie Rollen wechseln. Sie können eine Rolle annehmen, indem Sie eine AWS CLI oder AWS-API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter Verwenden von IAM-Rollen im IAM-Benutzerhandbuch.

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

- Verbundbenutzerzugriff: Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter Erstellen von Rollen für externe Identitätsanbieter im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center-Benutzerhandbuch.
- Temporäre IAM-Benutzerberechtigungen: Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. In einigen AWS-Services können Sie jedoch eine Richtlinie direkt an eine Ressource anfügen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff: Einige AWS-Services verwenden Features in anderen AWS-Services. Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon EC2 aus oder speichert Objekte in Amazon S3. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Forward access sessions (FAS) – Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle zum Ausführen von Aktionen in AWS verwenden, gelten Sie als Prinzipal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service auslösen. FAS verwendet die Berechtigungen des Prinzipals, der einen AWS-Service aufruft, in Kombination mit der Anforderung an den AWS-Service, Anforderungen an nachgelagerte Services zu stellen. FAS-Anfragen werden nur dann gestellt, wenn ein Service eine Anfrage erhält, die eine Interaktion mit anderen AWS-Services oder -Ressourcen erfordert. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

  - Servicerolle: Eine Servicerolle ist eine IAM-Rolle, die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.
  - Serviceverknüpfte Rolle: Eine serviceverknüpfte Rolle ist ein Typ von Servicerolle, die mit einem AWS-Service verknüpft ist. Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem AWS-Konto angezeigt und gehören zum Service. Ein IAM-Administrator kann die Berechtigungen für serviceverbundene Rollen anzeigen, aber nicht bearbeiten.
- Anwendungen in Amazon EC2: Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und AWS CLI- oder AWS-API-Anforderungen durchführen. Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Erstellen Sie ein Instance-Profil, das an die Instance angefügt ist, um eine AWS-Rolle einer EC2-Instance zuzuweisen und die Rolle für sämtliche Anwendungen der Instance bereitzustellen. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon EC2-Instances ausgeführt werden im IAM-Benutzerhandbuch.

Informationen dazu, wann Sie IAM-Rollen oder IAM-Benutzer verwenden sollten, finden Sie unter Erstellen einer IAM-Rolle (anstatt eines Benutzers) im IAM-Benutzerhandbuch.

## Verwalten des Zugriffs mit Richtlinien

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

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

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

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

## Identitätsbasierte Richtlinien

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

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

## Ressourcenbasierte Richtlinien

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

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

## Zugriffskontrolllisten

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3, AWS WAF und Amazon VPC sind Beispiele für Dienste, die ACLs unterstützen. Weitere Informationen“ zu ACLs finden Sie unter Zugriffskontrollliste (ACL) – Übersicht (Access Control List) im Amazon-Simple-Storage-Service-Entwicklerhandbuch.

## Weitere Richtlinientypen

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

- Berechtigungsgrenzen:Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.
- Service-Kontrollrichtlinien (SCPs) – SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OE) in AWS Organizations angeben. AWS Organizations ist ein Dienst für die Gruppierung und zentrale Verwaltung mehrerer AWS-Konten Ihres Unternehmens. Wenn Sie innerhalb einer Organisation alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. SCPs schränken Berechtigungen für Entitäten in Mitgliedskonten einschließlich des jeweiligen Root-Benutzer des AWS-Kontos ein. Weitere Informationen zu Organizations und SCPs finden Sie unter Funktionsweise von SCPs im AWS Organizations-Benutzerhandbuch.
- Sitzungsrichtlinien:Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen

Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

> **Note**
>
> Amazon unterstützt WorkDocs keine Service-Kontrollrichtlinien für Slack Organizations.

### Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen dazu, wie AWS die Zulässigkeit einer Anforderung ermittelt, wenn mehrere Richtlinientypen beteiligt sind, finden Sie unter Logik für die Richtlinienauswertung im IAM-Benutzerhandbuch.

## Funktionsweise WorkDocs von Amazon mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf Amazon zu verwalten WorkDocs, müssen Sie verstehen, welche IAM-Funktionen für die Verwendung mit Amazon verfügbar sind WorkDocs. Einen Überblick über das Zusammenwirken von Amazon WorkDocs und anderen -AWSServices mit IAM finden Sie unter -AWSServices, die mit IAM funktionieren im IAM-Benutzerhandbuch.

Themen

- Identitätsbasierte Amazon WorkDocs-Richtlinien
- Ressourcenbasierte Amazon WorkDocs-Richtlinien
- Autorisierung basierend auf Amazon- WorkDocs Tags
- Amazon WorkDocs -IAM-Rollen

### Identitätsbasierte Amazon WorkDocs-Richtlinien

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

### Aktionen

Administratoren können mit AWS-JSON-Richtlinien festlegen, welche Personen zum Zugriff auf welche Ressourcen berechtigt sind. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

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

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

Richtlinienaktionen in Amazon WorkDocs verwenden das folgende Präfix vor der Aktion: `workdocs:`. Um beispielsweise jemandem die Berechtigung zum Ausführen des Amazon WorkDocs `DescribeUsers`-API-Vorgangs zu erteilen, fügen Sie die `workdocs:DescribeUsers` Aktion in seine Richtlinie ein. Richtlinienanweisungen müssen entweder ein `Action`- oder ein `NotAction`-Element enthalten. Amazon WorkDocs definiert eine eigene Gruppe von Aktionen, die Aufgaben beschreiben, die Sie mit diesem Service durchführen können.

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

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

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

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

> **Note**
>
> Um die Abwärtskompatibilität zu gewährleisten, schließen Sie die `zocalo` Aktion ein. Beispielsweise:
>
> ```
> "Action": [
> "zocalo:*",
> "workdocs:*"
> ],
> ```

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

Ressourcen

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

Bedingungsschlüssel

Amazon WorkDocs stellt keine servicespezifischen Bedingungsschlüssel bereit, unterstützt jedoch die Verwendung einiger globaler Bedingungsschlüssel. Eine Liste aller globalen AWS-Bedingungsschlüssel finden Sie unter Globale AWS-Bedingungskontextschlüssel im IAM-Benutzerhandbuch.

Beispiele

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

## Ressourcenbasierte Amazon WorkDocs-Richtlinien

Amazon unterstützt WorkDocs keine ressourcenbasierten Richtlinien.

## Autorisierung basierend auf Amazon- WorkDocs Tags

Amazon unterstützt WorkDocs nicht das Markieren von Ressourcen oder das Steuern des Zugriffs auf der Grundlage von Tags.

### Amazon WorkDocs -IAM-Rollen

Eine IAM-Rolle ist eine Entität in Ihrem AWS-Konto mit spezifischen Berechtigungen.

Verwenden temporärer Anmeldeinformationen mit Amazon WorkDocs

Wir empfehlen dringend, temporäre Anmeldeinformationen zu verwenden, um sich mit einem Verbund anzumelden, eine IAM-Rolle anzunehmen oder eine kontoübergreifende Rolle anzunehmen. Sie erhalten temporäre Sicherheitsanmeldeinformationen, indem Sie AWS STS -API-Operationen wie AssumeRole oder aufrufenGetFederationToken.

Amazon WorkDocs unterstützt die Verwendung temporärer Anmeldeinformationen.

Serviceverknüpfte Rollen

Serviceverknüpfte Rollen erlauben AWS-Services den Zugriff auf Ressourcen in anderen Services, um eine Aktion in Ihrem Auftrag auszuführen. Serviceverknüpfte Rollen werden in Ihrem IAM-Konto angezeigt und gehören zum Service. Ein IAM-Administrator kann die Berechtigungen für serviceverknüpfte Rollen anzeigen, aber nicht bearbeiten.

Amazon unterstützt WorkDocs keine serviceverknüpften Rollen.

Servicerollen

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

Amazon unterstützt WorkDocs keine Servicerollen.

## Beispiele für WorkDocs identitätsbasierte Amazon-Richtlinien

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

Standardmäßig haben IAM-Benutzer und -Rollen keine Berechtigungen zum Erstellen oder Ändern von Amazon- WorkDocs Ressourcen. Sie können auch keine Aufgaben ausführen, die die AWS

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

> **Note**
>
> Um die Abwärtskompatibilität sicherzustellen, fügen Sie die `-zocalo`Aktion in Ihre Richtlinien ein. Beispielsweise:

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

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

Themen

- Bewährte Methoden für Richtlinien
- Verwenden der Amazon- WorkDocs Konsole
- Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer
- Benutzern schreibgeschützten Zugriff auf Amazon- WorkDocs Ressourcen gewähren
- Weitere Beispiele für WorkDocs identitätsbasierte Amazon-Richtlinien

## Bewährte Methoden für Richtlinien

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

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

- Bedarf einer Multi-Faktor-Authentifizierung (MFA):Wenn Sie ein Szenario haben, das IAM-Benutzer oder Root-Benutzer in Ihrem AWS-Konto erfordert, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Konfigurieren eines MFA-geschützten API-Zugriffs im IAM-Benutzerhandbuch.

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

## Verwenden der Amazon- WorkDocs Konsole

Um auf die Amazon- WorkDocs Konsole zugreifen zu können, müssen Sie über einen Mindestsatz von Berechtigungen verfügen. Diese Berechtigungen müssen es Ihnen ermöglichen, die Details der Amazon- WorkDocs Ressourcen in Ihrem AWS Konto aufzulisten und anzuzeigen. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die restriktiver ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole für IAM-Benutzer- oder -Rollen-Entitäten nicht wie vorgesehen.

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

- AmazonWorkDocsFullAccess
- AWSDirectoryServiceFullAccess
- AmazonEC2FullAccess

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

Für Benutzer, die nur Aufrufe an die AWS CLI oder AWS-API durchführen, müssen Sie keine Mindestberechtigungen in der Konsole erteilen. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die den API-Operation entsprechen, die Sie ausführen möchten.

## Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie enthält Berechtigungen für die Ausführung dieser Aktion auf der Konsole oder für die programmgesteuerte Ausführung über die AWS CLI oder die 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": "*"
        }
    ]
}
```

### Benutzern schreibgeschützten Zugriff auf Amazon- WorkDocs Ressourcen gewähren

Die folgende AWS verwaltete AmazonWorkDocsReadOnlyAccess Richtlinie gewährt einem IAM-Benutzer schreibgeschützten Zugriff auf Amazon- WorkDocs Ressourcen. Die Richtlinie gewährt dem Benutzer Zugriff auf alle Amazon WorkDocs `Describe`-Operationen. Der Zugriff auf die beiden Amazon EC2-Operationen ist erforderlich, damit Amazon eine Liste Ihrer VPCs und Subnetze abrufen WorkDocs kann. Zugriff auf die AWS Directory Service-Operation `DescribeDirectories` wird benötigt, um Informationen zu Ihren AWS Directory Service-Verzeichnissen abrufen zu können.

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

### Weitere Beispiele für WorkDocs identitätsbasierte Amazon-Richtlinien

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

## Fehlerbehebung für Amazon- WorkDocs Identität und -Zugriff

Verwenden Sie die folgenden Informationen, um häufige Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit Amazon WorkDocs und IAM auftreten können.

Themen

- Ich bin nicht autorisiert, eine Aktion in Amazon auszuführen WorkDocs
- Ich bin nicht autorisiert, iam durchzuführen:PassRole

- Ich möchte Personen außerhalb meines -AWSKontos Zugriff auf meine Amazon- WorkDocs Ressourcen gewähren

## Ich bin nicht autorisiert, eine Aktion in Amazon auszuführen WorkDocs

Wenn die AWS Management Console Ihnen mitteilt, dass Sie nicht zur Ausführung einer Aktion autorisiert sind, 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 autorisiert, iam durchzuführen:PassRole

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

Einige AWS-Services erlauben die Übergabe einer vorhandenen Rolle an diesen Dienst, sodass keine neue Servicerolle oder serviceverknüpfte Rolle erstellt werden muss. 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.

Wenden Sie sich an Ihren AWS-Administrator, falls Sie weitere Unterstützung benötigen. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

## Ich möchte Personen außerhalb meines -AWSKontos Zugriff auf meine Amazon-WorkDocs Ressourcen gewähren

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. Im Fall von Diensten, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen dazu, ob Amazon diese Funktionen WorkDocs unterstützt, finden Sie unter Funktionsweise WorkDocs von Amazon mit IAM.
- Informationen zum Gewähren des Zugriffs auf Ihre Ressourcen für alle Ihre AWS-Konten finden Sie unter Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen Ihrer AWS-Konto im IAM-Benutzerhandbuch.
- Informationen dazu, wie Sie AWS-Konten-Drittanbieter Zugriff auf Ihre Ressourcen bereitstellen, finden Sie unter Gewähren des Zugriffs auf AWS-Konten von externen Benutzern im IAM-Benutzerhandbuch.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.

# Protokollierung und Überwachung in Amazon WorkDocs

Amazon- WorkDocs Site-Administratoren können den Aktivitäts-Feed für eine gesamte Site anzeigen und exportieren. Sie können auch verwendenAWS CloudTrail, um Ereignisse aus der Amazon-WorkDocs Konsole zu erfassen.

Themen

- Exportieren des seitenweiten Aktivitäts-Feeds
- Verwenden von AWS CloudTrail zum Protokollieren von Amazon WorkDocs -API-Aufrufen

## Exportieren des seitenweiten Aktivitäts-Feeds

Administratoren können die Aktivitätenliste einer gesamten Website aufrufen und exportieren. Um diese Funktion verwenden zu können, müssen Sie zunächst 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. Wählen Sie Filter aus und verschieben Sie dann den Schieberegler für die seitenweite Aktivität, 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 – WorkDocsDownloads Ordner im Ordner Downloads 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 Anzeigen des Aktivitäts-Feeds im Amazon- WorkDocs Benutzerhandbuch.

## Verwenden von AWS CloudTrail zum Protokollieren von Amazon WorkDocs -API-Aufrufen

Sie können verwendenAWS CloudTrail, um Amazon WorkDocs -API-Aufrufe zu protokollieren. CloudTrail bietet eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem -AWSService in Amazon durchgeführten Aktionen WorkDocs. CloudTrail erfasst alle API-Aufrufe für Amazon

WorkDocs als Ereignisse, einschließlich Aufrufen von der Amazon- WorkDocs Konsole und von Code-Aufrufen an die Amazon- WorkDocs APIs.

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

Zu den von gesammelten Informationen CloudTrail gehören Anforderungen, die IP-Adressen, von denen die Anforderungen gestellt wurden, die Benutzer, die die Anforderungen gestellt haben, und die Anforderungsdaten.

Weitere Informationen zu CloudTrailfinden Sie im AWS CloudTrail -Benutzerhandbuch.

## Amazon- WorkDocs Informationen in CloudTrail

CloudTrail wird beim Erstellen des AWS Kontos in Ihrem Konto aktiviert. Wenn eine Aktivität in Amazon auftritt WorkDocs, wird diese Aktivität in einem - CloudTrail Ereignis zusammen mit anderen -AWSServiceereignissen im Ereignisverlauf aufgezeichnet. Sie können die neusten Ereignisse in Ihr AWS-Konto herunterladen und dort suchen und anzeigen. Weitere Informationen finden Sie unter Anzeigen von Ereignissen mit dem CloudTrail Ereignisverlauf .

Erstellen Sie für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS Konto, einschließlich Ereignissen für Amazon WorkDocs, einen Trail. Ein Trail ermöglicht CloudTrail die Bereitstellung von Protokolldateien an einen Amazon S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser standardmäßig für alle Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS-Partition und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon-S3-Bucket bereit. Darüber hinaus können Sie andere -AWSServices konfigurieren, um die in den CloudTrail Protokollen erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie hier:

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

Alle Amazon- WorkDocs Aktionen werden von protokolliert CloudTrail und sind in der Amazon WorkDocs -API-Referenz dokumentiert. Aufrufe der `UpdateDocument` Abschnitte `CreateFolder`, `DeactivateUser` und erzeugen beispielsweise Einträge in den CloudTrail Protokolldateien.

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

- Gibt an, ob die Anforderung mit Root- oder IAM-Benutzer-Anmeldeinformationen ausgeführt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anforderung aus einem anderen AWS-Service gesendet wurde

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

## Grundlegendes zu Amazon- WorkDocs Protokolldateieinträgen

Ein Trail ist eine Konfiguration, die die Bereitstellung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der Aktion, die Anfrageparameter usw. CloudTrail Protokolldateien sind kein geordnetes Stacktrace der öffentlichen API-Aufrufe und erscheinen daher nicht in einer bestimmten Reihenfolge.

Amazon WorkDocs generiert verschiedene Arten von CloudTrail Einträgen, diejenigen von der Steuerebene und diejenigen von der Datenebene. Der wichtige Unterschied zwischen den beiden besteht darin, dass die Benutzeridentität für Einträge auf Steuerebene ein IAM-Benutzer ist. Die Benutzeridentität für Einträge auf Datenebene ist der Amazon- WorkDocs Verzeichnisbenutzer.

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

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

Das folgende Beispiel zeigt zwei CloudTrail Protokolleinträge für Amazon WorkDocs: Der erste Datensatz ist für eine Aktion auf Steuerebene und der zweite für eine Aktion auf 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"
    }
  ]
}
```

# Compliance-Validierung für Amazon WorkDocs

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

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

Ihre Compliance-Verantwortung bei der Verwendung von AWS-Services ist von der Sensibilität Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften abhängig. AWS stellt die folgenden Ressourcen zur Unterstützung der Compliance bereit:

- Kurzanleitungen für Sicherheit und Compliance: In diesen Bereitstellungsleitfäden werden Überlegungen zur Architektur erörtert und Schritte zum Bereitstellen von Basisumgebungen auf AWS zur Verfügung gestellt, die auf Sicherheit und Compliance ausgerichtet sind.
- Erstellung einer Architektur mit HIPAA-konformer Sicherheit und Compliance in Amazon Web Services – In diesem Whitepaper wird beschrieben, wie Unternehmen mithilfe von AWS HIPAA-berechtigte Anwendungen erstellen können.

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

- AWS-Compliance-Ressourcen – Diese Arbeitsbücher und Leitfäden könnten für Ihre Branche und Ihren Standort relevant sein.
- AWS-Compliance-Leitfäden für Kunden: Verstehen Sie das Modell der geteilten Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Methoden zum Schutz von AWS-Services zusammengefasst und die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zugeordnet.
- Auswertung von Ressourcen mit Regeln im AWS ConfigEntwicklerhandbuch – Der AWS Config-Service bewertet, wie gut Ihre Ressourcenkonfigurationen mit internen Praktiken, Branchenrichtlinien und Vorschriften übereinstimmen.
- AWS Security Hub: Dieser AWS-Service bietet einen umfassenden Überblick über Ihren Sicherheitsstatus innerhalb von 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.
- AWS Audit Manager: Dieser AWS-Service hilft Ihnen, Ihre AWS-Nutzung kontinuierlich zu überprüfen, um den Umgang mit Risiken und die Compliance von Branchenstandards zu vereinfachen.

## Ausfallsicherheit in Amazon WorkDocs

Im Zentrum der globalen AWS Infrastruktur stehen die AWS-Regionen und Availability Zones (Verfügbarkeitszonen, AZs). AWS Regionen stellen mehrere physisch getrennte und isolierte Availability Zones bereit, die mit Netzwerken mit geringer Latenz, hohem Durchsatz und hochredundanten Vernetzungen 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 über AWS-Regionen und -Availability Zones finden Sie unter AWS Globale Infrastruktur.

# Infrastruktursicherheit in Amazon WorkDocs

Als verwalteter Service WorkDocs ist Amazon durch die AWS globalen Verfahren zur Gewährleistung der Netzwerksicherheit von geschützt. Weitere Informationen finden Sie unter Infrastruktursicherheit in AWS Identity and Access Management im IAM-Benutzerhandbuch und unter Bewährte Methoden für Sicherheit, Identität und Compliance im AWS Architecture Center.

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

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

# Erste Schritte mit 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<br><br>**Note**<br>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

AmazonasWorkDocsverwendet Berechtigungen, um den Zugriff auf Ordner und Dateien zu kontrollieren. Berechtigungen werden auf der Grundlage von Benutzerrollen vergeben.

Inhalt



## Benutzerrollen

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

- Besitzer des Ordners— Der Besitzer eines Ordners oder einer Datei.
- Mitinhaber des Ordners— Ein Benutzer oder eine Gruppe, den oder die der Besitzer als Miteigentümer eines Ordners oder einer Datei benennt.
- Mitwirkender Ordner— Jemand mit unbegrenztem Zugriff auf einen Ordner.
- Ordnerbetrachter— Jemand mit eingeschränktem Zugriff (nur Leserechte) auf einen Ordner.

Sie können die folgenden Benutzerrollen auf der Ebene der einzelnen Dateien anwenden:

- Besitzer— Der Besitzer einer Datei.

- Mitinhaber— Ein Benutzer oder eine Gruppe, den oder die der Eigentümer als Miteigentümer der Datei benennt.
- Mitwirkender— Jemand hat die Erlaubnis, Feedback in der Datei zu geben.
- Zuschauer— Jemand mit eingeschränktem Zugriff (nur Leserechte) auf die Datei.
- Anonymer Zuschauer— 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.

## Berechtigungen für freigegebene Ordner

Die folgenden Berechtigungen gelten für Benutzerrollen für gemeinsam genutzte Ordner:

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

- Ansehen— Zeigt den Inhalt eines geteilten Ordners an.
- Unterordner anzeigen— Zeigt einen Unterordner an.
- Aktien ansehen— Zeigt die anderen Benutzer an, mit denen ein Ordner geteilt wurde.
- Ordner herunterladen— Laden Sie einen Ordner herunter.
- Unterordner hinzufügen— Fügt einen Unterordner hinzu.
- Teilen— Teilen Sie den Ordner auf oberster Ebene mit anderen Benutzern.
- Aktie widerrufen— Widerrufen Sie die Freigabe 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 ansehen | Ordner herunterladen | Unterordner hinzufügen | Freigeben | Aktie widerrufen | Unterordner löschen | Ordner auf oberster Ebene löschen |
|---|---|---|---|---|---|---|---|---|---|
| Besitzer des Ordners | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Mitinhaber des Ordners | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Mitwirker der Ordner | ✓ | ✓ | ✓ | ✓ | ✓ | | | | |
| Ordnerbe rachter | ✓ | ✓ | ✓ | ✓ | | | | | |

## Berechtigungen für Dateien in geteilten Ordnern

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

- Kommentieren— Fügt einer Datei Feedback hinzu.
- Löschen— Löscht eine Datei in einem geteilten Ordner.
- Umbenennen— Benennen Sie Dateien um.
- hochladen— Laden Sie neue Versionen einer Datei hoch.
- Herunterladen— Laden Sie eine Datei herunter. Dies ist die Standardberechtigung. Sie können 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 mitAnsehenBerechtigungen können weiterhin Dateien herunterladen. Um dies zu verhindern, öffnen Sie den geteilten Ordner und löschen Sie denDownloads zulassenEinstellung für jede der 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 auf Amazon abspielenWorkDocsWebclient.

- 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.
- Aktien ansehen— Zeigt die anderen Benutzer an, mit denen eine Datei geteilt wurde.
- Anmerkungen anzeigen— Feedback von anderen Benutzern anzeigen.
- Aktivität ansehen— Zeigt den Aktivitätsverlauf einer Datei an.
- Versionen ansehen— 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 ansehen— Besitzer/Mitinhaber kann alle privaten Kommentare zu einem Dokument sehen, auch wenn es sich nicht um Antworten auf seinen Kommentar handelt.

| | Anmerk | Lösch | Uhe | Hoch | Herun | Down | Freig | Aktie | Anzeig | Aktien | Anmerk | Aktivit | Versio | Versio | Versio | Alle privaten Kommentare anzeigen** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | n | | ader | verhind | n | widerru | n | ansehe | anzeige | ansehe | anzeig | lösche | stelle | |
| Date tzer* | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

| | Anmerk | Löschen | Umbenennen | Hochladen | Herunterladen | Downloads verhindern | Freigeben | Aktien widerrufen | Anzeigen | Aktivitäten ansehen | Anmerkungen anzeigen | Aktivität ansehen | Versionen anzeigen | Versionen löschen | Version wiederherstellen | Alle privaten Kommentare anzeigen* |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Besitzer des Ordners | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Mitinhaber des Ordners | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Mitwirkender Ordner | ✓ | | | ✓ | ✓ | | | | ✓ | ✓ | ✓ | ✓ | ✓ | | | |
| Ordnerrechte | | | | | ✓ | | | | ✓ | ✓ | | | | | | |
| Anonyme Zuschauer | | | | | | | | | ✓ | ✓ | | | | | | |

* In diesem Fall ist der Eigentümer der Datei die Person, die die Originalversion eines für sie freigegebenen Ordners hochgeladen hat. Die Berechtigungen für diese Rolle gelten nur für die eigene Datei, nicht für alle Dateien in einem freigegebenen Ordner.

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

## Berechtigungen für Dateien, die sich nicht in geteilten Ordnern befinden

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

- Kommentieren— Fügt einer Datei Feedback hinzu.
- Löschen— Löscht eine Datei.
- Umbenennen— Benennen Sie Dateien um.
- hochladen— Laden Sie neue Versionen einer Datei hoch.
- Herunterladen— Laden Sie eine Datei herunter. Dies ist die Standardberechtigung. Sie können 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 auf Amazon abspielenWorkDocsWebclient.

- Teilen— Teilen Sie eine Datei mit anderen Benutzern.
- Aktie widerrufen— Widerrufen Sie die gemeinsame Nutzung einer Datei.
- Ansehen— Eine Datei anzeigen.
- Aktien ansehen— Zeigt die anderen Benutzer an, mit denen eine Datei geteilt wurde.
- Anmerkungen anzeigen— Feedback von anderen Benutzern anzeigen.
- Aktivität ansehen— Zeigt den Aktivitätsverlauf einer Datei an.
- Versionen ansehen— 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 | Lösch | Umbenen n | Hochlad | Herunte aden | Downlo verhind n | Freigebe | Aktie widerruf n | Anzeige | Aktien ansehe | Anmerku en anzeige | Aktivitä ansehe | Versione anzeige | Versione löschen | Versionen wiederher stellen |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Eigen r | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

| | Anmerk | Lösch | Umben | Hochlad | Herunte | Downlo | Freigebe | Aktie widerruf | Anzeige | Aktion ansehe | Anmerku anzeige | Aktivitä ansehe | Versione anzeige | Versione lösche | Versionen wiederher stellen |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Mitei ümer | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Beitra der | ✓ | | | ✓ | ✓ | | | | ✓ | ✓ | ✓ | ✓ | ✓ | | |
| Betra r | | | | | ✓ | | | | ✓ | ✓ | | | | | |
| Anon Zusc | | | | | | | | | ✓ | ✓ | | | | | |

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

## 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 groß angelegte 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 abteilungsinterne Dateifreigaben und Home-Drive- oder Benutzerdateifreigaben zu Amazon migrieren WorkDocs.

Während dieses Vorgangs WorkDocs stellt Amazon eineAWS Identity and Access Management (IAM-) Richtlinie für Sie bereit. 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.

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

- Administratorberechtigungen für Ihre WorkDocs Amazon-Website
- Berechtigungen zum Erstellen einer IAM-Rolle

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

- Verwenden Sie Admin nicht für den Benutzernamen Ihres WorkDocs Amazon-Kontos. Admin ist eine reservierte Benutzerrolle in 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 erhalten WorkDocs. Dateibesitz und -berechtigungen werden nicht bewahrt.

Aufgaben

# Schritt 1: Inhalte für die Migration vorbereiten

So bereiten Sie Ihre Inhalte für die Migration vor

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.
- Perioden 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 mit der Endung **`.tmp`** — Zum Beispiel: `file.tmp`
- Dateinamen, die genau diesen Begriffen entsprechen, die zwischen Groß- und Kleinschreibung unterscheiden — `Microsoft User Data`, `Outlook files`, `Thumbs.db`, , oder `Thumbnails`

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

## Schritt 2: Hochladen von Dateien in Amazon S3

Hochladen von Dateien in Amazon S3

1. Erstellen Sie in IhremAWS -Konto einen neuen Amazon Simple Storage Service (Amazon S3) -Bucket, in den Sie Ihre Dateien und Ordner hochladen möchten. Der Amazon-S3-Bucket muss sich im gleichenAWS -Konto und in derselbenAWS -Region wie Ihre WorkDocs Amazon-Website befinden. Weitere Informationen finden Sie unter Erste Schritte mit Amazon Simple Storage Service im Benutzerhandbuch von Amazon Simple Storage Service.
2. Laden Sie Ihre Dateien in den Amazon S3 S3-Bucket hoch, den Sie im vorherigen Schritt erstellt haben. Wir empfehlenAWS DataSync die Verwendung, um Ihre Dateien und Ordner in den Amazon S3 S3-Bucket hochzuladen. DataSync bietet zusätzliche Tracking-, Berichts- und Synchronisierungsfunktionen. Weitere Informationen finden Sie unter AWS DataSyncFunktionsweise und Verwendung identitätsbasierter Richtlinien (IAM-Richtlinien) DataSync im AWS DataSyncBenutzerhandbuch.

## 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 Migrationsdienst Ihre Migrationsanfrage bearbeitet und Ihnen eine E-Mail mit der Information sendet, dass Sie mit der Migration beginnen können. Wenn Sie die Migration starten, bevor Sie die E-Mail erhalten, zeigt die Management-Konsole 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 Amazon — WorkDocs Preise.

Der Amazon WorkDocs Migration Service bietet eineAWS 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-Bucket und die WorkDocs Amazon-Website gewährt, die Sie angeben. Sie abonnieren auch Amazon SNS SNS-E-Mail-Benachrichtigungen, um Updates zu erhalten, wenn 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, Amazon SNS SNS-E-Mail-Benachrichtigungen zu abonnieren. Abonnieren und bestätigen Sie diese in der E-Mail-Nachricht, die Sie erhalten. Wählen Sie anschließend Continue (Weiter) aus.
2. Wählen Sie Create Migration (Migration erstellen) aus.
3. Wählen Sie in Source Type (Quelltyp) Amazon S3 aus.
4. Wählen Sie Next (Weiter).
5. Kopieren Sie für Datenquelle und Validierung 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 JSON und fügen Sie die IAM-Richtlinie ein, die Sie zuvor in Ihre Zwischenablage kopiert haben.
   d. Wählen Sie Review policy (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 Another AWS account (Anderes AWS-Konto) aus. Geben Sie in Account ID (Konto-ID) eine der folgenden IDs ein:
      - Geben Sie für Region USA East (N. Virginia)`899282061130`
      - Geben Sie für Region USA West (Oregon)`814301586344`

- Geben Sie für Region Asien-Pazifik (Singapur)`900469912330`
- Geben Sie für Region Asien-Pazifik (Sydney)`031131923584`
- Geben Sie für Region Asien-Pazifik (Tokio)`178752524102`
- Geben Sie für Region Europa (Irland)`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 Create role (Rolle erstellen) aus.

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

k. Ändern Sie auf der Seite Summary (Übersicht) den Wert für Maximum CLI/API session duration (Maximale Dauer der CLI/API-Sitzung) in 12 Stunden.

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

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

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 Rolle, die Sie in der IAM-Konsole erstellt haben.

Löschen Sie die IAM-Richtlinie und -Rolle wie folgt:

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 die Speichereinstellungen ändern, indem Sie Ihr Benutzerkonto in der Administrator-Systemsteuerung bearbeiten. 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 Identity and Access Management 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 |

# AWS-Glossar

Die neueste AWS-Terminologie finden Sie im AWS-Glossar in der AWS-Glossar-Referenz.