aws

Panduan Administrasi

Amazon WorkDocs

Amazon WorkDocs: Panduan Administrasi

Table of Contents

Pemberitahuan: Pendaftaran pelanggan baru dan peningkatan akun tidak lagi tersedia untuk Amazon. WorkDocs Pelajari tentang langkah-langkah migrasi di sini: Cara memigrasi data dari WorkDocs.

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.

Apa itu Amazon WorkDocs?

Amazon WorkDocs adalah layanan penyimpanan dan berbagi perusahaan yang dikelola sepenuhnya dan aman dengan kontrol administratif yang kuat dan kemampuan umpan balik yang meningkatkan produktivitas pengguna. File tersimpan di dalam cloud, secara aman dan terlindungi. File pengguna Anda hanya terlihat oleh mereka, serta kontributor dan pemirsa mereka yang ditunjuk. Anggota lain dari organisasi Anda tidak memiliki akses ke file pengguna lain kecuali mereka secara khusus diberikan akses.

Pengguna dapat berbagi file mereka dengan anggota lain dari organisasi Anda untuk kolaborasi atau peninjauan. Aplikasi WorkDocs klien dapat digunakan untuk melihat berbagai jenis file, tergantung pada jenis media Internet dari file tersebut. WorkDocs mendukung semua format dokumen dan gambar umum, dan dukungan untuk jenis media tambahan terus ditambahkan.

Untuk informasi selengkapnya, lihat Amazon WorkDocs.

Mengakses WorkDocs

Administrator menggunakan WorkDocs konsol untuk membuat dan menonaktifkan situs WorkDocs . Dengan panel kontrol admin, mereka dapat mengelola pengguna, penyimpanan, dan pengaturan keamanan. Untuk informasi lebih lanjut, lihat Mengelola WorkDocs dari panel kontrol admin situs dan Mengundang dan mengelola pengguna WorkDocs .

Pengguna non-administratif menggunakan aplikasi klien untuk mengakses file mereka. Mereka tidak pernah menggunakan WorkDocs konsol atau dasbor administrasi. WorkDocs menawarkan beberapa aplikasi dan utilitas klien yang berbeda:

- Aplikasi web yang digunakan untuk pengelolaan dan peninjauan dokumen.
- Aplikasi native untuk perangkat seluler yang digunakan untuk peninjauan dokumen.
- WorkDocs Drive, aplikasi yang menyinkronkan folder di desktop macOS atau Windows dengan WorkDocs file Anda.

Untuk informasi selengkapnya tentang cara pengguna dapat mengunduh WorkDocs klien, mengedit file mereka, dan menggunakan folder, lihat topik berikut di Panduan WorkDocs Pengguna:

- Memulai dengan WorkDocs
- Bekerja dengan file

- Bekerja dengan folder

Harga

Dengan WorkDocs, tidak ada biaya atau komitmen di muka. Anda hanya membayar untuk akun pengguna aktif, dan penyimpanan yang Anda gunakan. Untuk informasi selengkapnya, lihat Harga.

Cara memulai

Untuk memulai WorkDocs, lihatMembuat WorkDocs situs.

Migrasi data keluar dari WorkDocs

WorkDocs menyediakan dua metode untuk memigrasikan data keluar dari WorkDocs situs. Bagian ini memberikan gambaran umum tentang metode ini dan tautan ke langkah-langkah terperinci untuk menjalankan, memecahkan masalah, dan mengoptimalkan setiap metode migrasi.

Pelanggan akan memiliki dua opsi untuk melepaskan data mereka dari Amazon WorkDocs: fungsionalitas Unduhan Massal yang ada (metode 1) atau Alat Migrasi Data baru kami (metode 2). Topik berikut menjelaskan cara menggunakan kedua metode tersebut.

Topik

Metode 1: Mengunduh file secara massal

Jika Anda ingin mengontrol file mana yang Anda migrasi, Anda dapat mengunduhnya secara manual secara massal. Metode ini memungkinkan Anda untuk memilih hanya file yang Anda inginkan dan mengunduhnya ke lokasi lain, seperti drive lokal Anda. Anda dapat mengunduh file dan folder dari situs WorkDocs web Anda atau dari WorkDocs Drive.

Ingat hal berikut:

- Pengguna situs Anda dapat mengunduh file dengan mengikuti langkah-langkah yang tercantum di bawah ini. Jika mau, Anda dapat mengatur folder bersama, meminta pengguna memindahkan file ke folder itu, lalu mengunduh folder ke lokasi lain. Anda juga dapat mentransfer kepemilikan kepada diri sendiri dan melakukan unduhan.
- Untuk mengunduh dokumen Microsoft Word dengan komentar, lihat Mengunduh dokumen Word dengan umpan balik, di Panduan WorkDocs Pengguna.
- Anda harus menggunakan WorkDocs Drive untuk mengunduh file yang lebih besar dari 5 GB.
- Saat Anda menggunakan WorkDocs Drive untuk mengunduh file dan folder, struktur direktori, nama file, dan konten file Anda tetap utuh. Kepemilikan file, izin, dan versi tidak dipertahankan.

Mengunduh file dari web

Anda menggunakan metode ini untuk mengunduh file ketika:

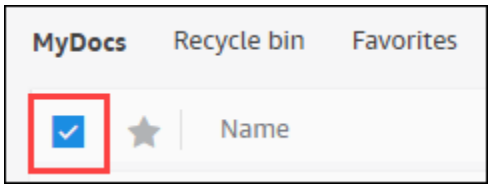
- Anda hanya ingin mengunduh beberapa file dari situs.
- Anda ingin mengunduh dokumen Word dengan komentar, dan meminta komentar tersebut tetap dengan dokumen masing-masing. Alat migrasi mengunduh semua komentar, tetapi menuliskannya ke file XHTML terpisah. Pengguna situs kemudian mungkin mengalami kesulitan mengaitkan komentar dengan dokumen Word mereka.

Untuk mengunduh file dari web

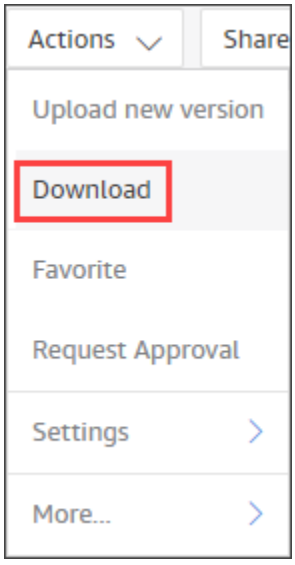
1. Masuk ke WorkDocs.
2. Sesuai kebutuhan, buka folder yang berisi file yang ingin Anda unduh.
3. Pilih kotak centang di sebelah file yang ingin Anda unduh.

   —ATAU—

   Pilih kotak centang di bagian atas daftar untuk memilih semua file di folder.



4. Buka menu Tindakan dan pilih Unduh. .



   Pada PC, file yang diunduh mendarat secara default di Unduhan/WorkDocsDownloads/nama folder. Pada Macintosh, file mendarat secara default dalam nama hard drive /Pengguna/nama pengguna/. WorkDocsDownloads

Mengunduh folder dari web

> **Note**
>
> Saat Anda mengunduh folder, Anda juga mengunduh semua file di folder. Jika Anda hanya ingin mengunduh beberapa file dalam folder, pindahkan file yang tidak diinginkan ke lokasi lain, atau ke Recycle Bin, lalu unduh folder tersebut.

Untuk mengunduh folder dari web

1. Masuk ke WorkDocs
2. Pilih kotak centang di sebelah setiap folder yang ingin Anda unduh.

   —ATAU—

   Buka folder dan pilih kotak centang di sebelah subfolder apa pun yang ingin Anda unduh.
3. Buka menu Tindakan dan pilih Unduh. .

   Pada PC, folder yang diunduh mendarat secara default di Unduhan/WorkDocsDownloads/nama folder. Pada Macintosh, file mendarat secara default dalam nama hard drive /Pengguna/nama pengguna/. WorkDocsDownloads

Menggunakan WorkDocs Drive untuk mengunduh file dan folder

> **Note**
>
> Anda harus menginstal WorkDocs Drive untuk menyelesaikan langkah-langkah berikut. Untuk informasi selengkapnya, lihat Menginstal WorkDocs Drive, di Panduan Pengguna WorkDocs Drive.

Untuk mengunduh file dan folder dari WorkDocs Drive

1. Mulai File Explorer atau Finder dan buka drive W: Anda.
2. Pilih folder atau file yang ingin Anda unduh.
3. Ketuk dan tahan (klik kanan) item yang dipilih dan pilih Salin, lalu tempel item yang disalin ke lokasi baru mereka.

—ATAU—

Seret item yang dipilih ke lokasi baru mereka.

4. Hapus file asli dari WorkDocs Drive.

Metode 2: Gunakan alat migrasi

Anda menggunakan alat WorkDocs migrasi saat ingin memigrasikan semua data dari WorkDocs situs.

Alat migrasi memindahkan data dari situs ke bucket Amazon Simple Storage Service. Alat ini membuat file ZIP terkompresi untuk setiap pengguna. File zip mencakup semua file dan folder, versi, izin, komentar, dan anotasi untuk setiap pengguna akhir di situs Anda. WorkDocs

Topik

Prasyarat

Anda harus memiliki item berikut untuk menggunakan alat migrasi.

- Bucket Amazon S3. Untuk informasi tentang membuat bucket Amazon S3, lihat Membuat bucket, di Panduan Pengguna Amazon S3. Bucket Anda harus menggunakan akun IAM yang sama dan berada di Wilayah yang sama dengan situs Anda WorkDocs . Selain itu, Anda harus memblokir akses publik ke ember. Untuk informasi selengkapnya tentang hal itu, lihat Memblokir akses publik ke penyimpanan Amazon S3 Anda, di Panduan Pengguna Amazon S3.

  Untuk memberikan WorkDocs izin untuk mengunggah file Anda, konfigurasikan kebijakan bucket seperti yang ditunjukkan pada contoh berikut. Kebijakan menggunakan kunci `aws:SourceAccount` dan `aws:SourceArn` kondisi untuk mengurangi ruang lingkup kebijakan, praktik terbaik keamanan.

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

> **Note**
>
> - *WORKDOCS-DIRECTORY-ID*adalah ID organisasi WorkDocs situs Anda. Ini dapat ditemukan di tabel “Situs Saya” di AWS WorkDocs Console
> - Untuk informasi selengkapnya tentang mengonfigurasi kebijakan bucket, lihat Menambahkan kebijakan bucket menggunakan konsol Amazon S3

- Kebijakan IAM. Untuk memulai migrasi di WorkDocs konsol, prinsipal panggilan IAM harus memiliki kebijakan berikut yang dilampirkan pada izinnya yang disetel:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowStartWorkDocsMigration",
            "Effect": "Allow",
```

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

```
}
```

- Secara opsional, Anda dapat menggunakan AWS KMS kunci untuk mengenkripsi data saat istirahat di bucket Anda. Jika Anda tidak memberikan kunci, setelan enkripsi standar bucket akan berlaku. Untuk informasi selengkapnya, lihat Membuat kunci, di Panduan Pengembang Layanan Manajemen AWS Kunci.

  Untuk menggunakan AWS KMS kunci, tambahkan pernyataan berikut ke kebijakan IAM. Anda harus menggunakan kunci aktif dari tipe SYMMETRIC_DEFAULT.

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

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

Batasan

Alat migrasi memiliki batasan berikut:

- Alat ini menulis semua izin pengguna, komentar, dan anotasi untuk memisahkan file CSV. Anda harus memetakan data itu ke file yang sesuai secara manual.
- Anda hanya dapat memigrasi situs aktif.
- Alat ini terbatas pada satu migrasi yang berhasil per situs untuk setiap periode 24 jam.
- Anda tidak dapat menjalankan migrasi bersamaan dari situs yang sama, tetapi Anda dapat menjalankan migrasi bersamaan untuk situs yang berbeda.
- Setiap file zip paling banyak 50GB. Pengguna dengan lebih dari 50GB data WorkDocs akan memiliki beberapa file zip yang diekspor ke Amazon S3.
- Alat ini tidak mengekspor file yang lebih besar dari 50 GB. Alat ini mencantumkan file apa pun yang lebih besar dari 50 GB dalam file CSV yang memiliki awalan yang sama dengan file ZIP. Misalnya, ***site-alias***/workdocs///skippedFiles.csv. ***created-timestamp-UTC*** Anda dapat mengunduh

file yang terdaftar secara terprogram atau manual. Untuk informasi tentang mengunduh secara terprogram, lihathttps://docs.aws.amazon.com/workdocs/latest/developerguide/download-documents.html, di Panduan WorkDocs Pengembang. Untuk informasi tentang mengunduh file secara manual, lihat langkah-langkah di Metode 1, sebelumnya dalam topik ini.

- Setiap file zip pengguna hanya akan berisi and/or folder file yang mereka miliki. Setiap and/or folder file yang telah dibagikan dengan pengguna akan berada di file zip pengguna yang memiliki and/or folder file.
- Jika folder kosong (tidak berisi file/folder bersarang) di WorkDocs, itu tidak akan diekspor.
- Tidak dijamin bahwa data apa pun (file, folder, versi, komentar, anotasi) yang dibuat setelah pekerjaan migrasi dimulai, akan dimasukkan dalam data yang diekspor di S3.
- Anda dapat memigrasikan beberapa situs ke bucket Amazon S3. Anda tidak perlu membuat satu ember per situs. Namun, Anda harus memastikan bahwa kebijakan IAM dan bucket Anda mengizinkan beberapa situs.
- Migrasi meningkatkan biaya Amazon S3, tergantung pada jumlah data yang Anda migrasi ke bucket. Untuk informasi selengkapnya, lihat halaman harga Amazon S3.

Menjalankan alat migrasi

Langkah-langkah berikut menjelaskan cara menjalankan alat WorkDocs migrasi.

Untuk memigrasi situs

1. Buka WorkDocs konsol di https://console.aws.amazon.com/zocalo/.
2. Di panel navigasi, pilih Situs saya, lalu pilih tombol radio di sebelah situs yang ingin Anda migrasi.
3. Buka daftar Tindakan dan pilih Migrasi Data.
4. Pada halaman nama situs Migrasi Data, masukkan URI bucket Amazon S3 Anda.

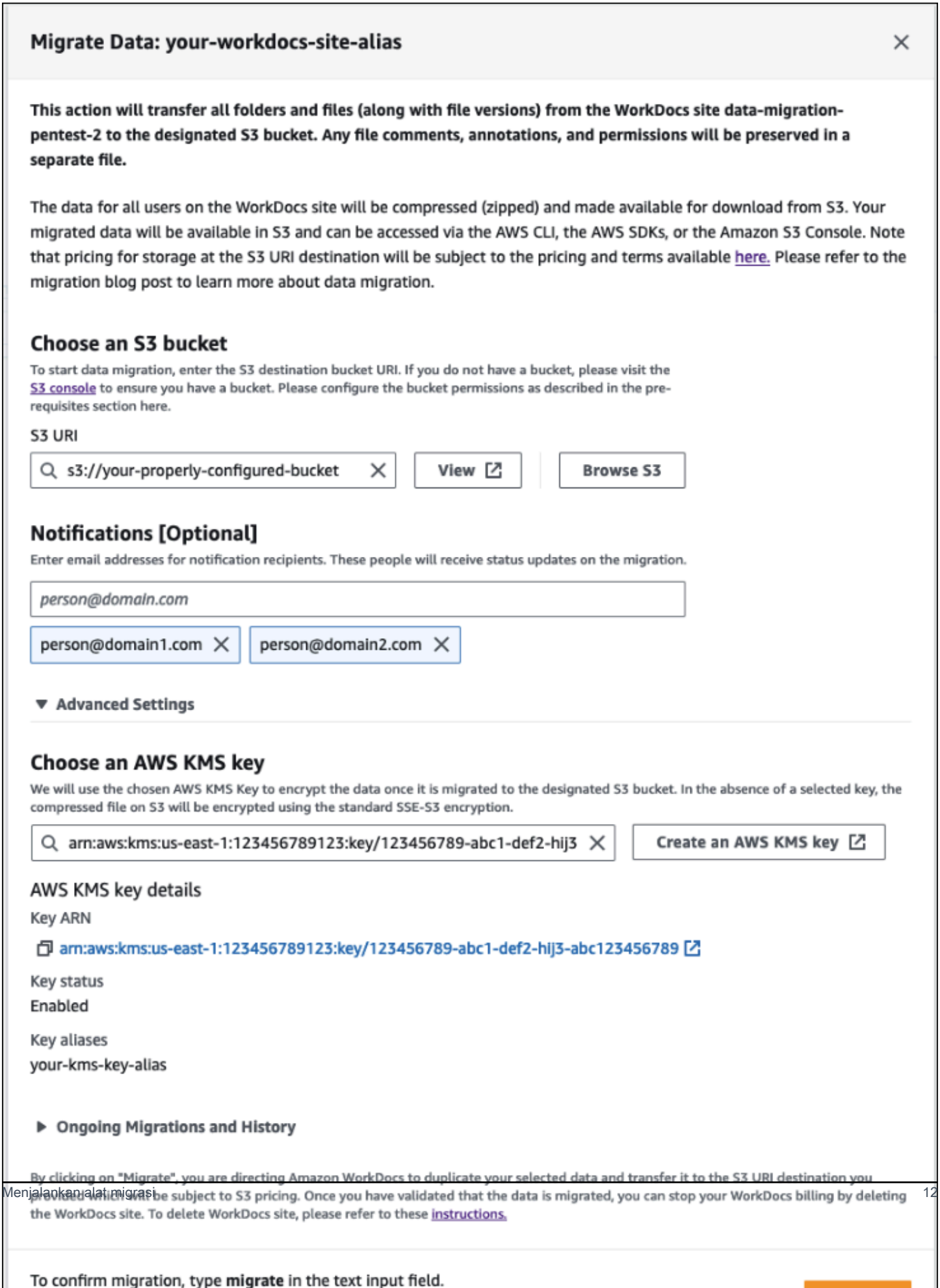
   —ATAU—

   Pilih Browse S3 dan ikuti langkah-langkah berikut:

   a. Sesuai kebutuhan, cari ember.
   b. Pilih tombol radio di sebelah nama bucket, lalu pilih Pilih.
5. (Opsional) Di bawah Pemberitahuan, masukkan maksimal lima alamat email. Alat ini mengirimkan email status migrasi ke setiap penerima.

6. (Opsional) Di bawah Pengaturan Lanjutan, pilih kunci KMS untuk mengenkripsi data yang Anda simpan.
7. Masukkan **`migrate`** di kotak teks untuk mengonfirmasi migrasi, lalu pilih Mulai Migrasi.

   Indikator muncul dan menampilkan status migrasi. Waktu migrasi bervariasi, tergantung pada jumlah data di situs.


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

Saat migrasi selesai:

- Alat ini mengirimkan email “sukses” ke alamat yang dimasukkan selama pengaturan, jika ada.
- Bucket Amazon S3 Anda akan berisi folder /workdocs///***site-alias***. ***created-timestamp-UTC*** Folder itu berisi folder zip untuk setiap pengguna yang memiliki data di situs. Setiap folder zip berisi folder dan file pengguna, termasuk izin dan komentar yang memetakan file CSV.
- Jika pengguna menghapus semua file mereka sebelum migrasi, tidak ada folder zip yang muncul untuk pengguna tersebut.
- Versi — Dokumen dengan beberapa versi memiliki pengidentifikasi stempel waktu pembuatan _ versi _. Stempel waktu menggunakan epoch milidetik. Misalnya, dokumen bernama “TestFile.txt” dengan 2 versi muncul sebagai berikut:

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

- Izin - Contoh berikut menunjukkan konten file CSV izin khas.

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

- Komentar - Contoh berikut menunjukkan isi dari file CSV komentar khas.

```
PathToFile,PrincipalName,PostedTimestamp,Text
/mydocs/Documentation/
Onboarding_Guide.xml,user1@domain.com,2023-12-28T20:57:40.781Z,TEST ANNOTATION 1
/mydocs/Documentation/
Onboarding_Guide.xml,user2@domain.com,2023-12-28T22:18:09.812Z,TEST ANNOTATION 2
/mydocs/Documentation/
Onboarding_Guide.xml,user3@domain.com,2023-12-28T22:20:04.099Z,TEST ANNOTATION 3
/mydocs/Documentation/
Onboarding_Guide.xml,user1@domain.com,2023-12-28T20:56:27.390Z,TEST COMMENT 1
```

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

- File yang dilewati - Contoh berikut menunjukkan konten file CSV file yang dilewati khas. Kami mempersingkat ID dan melewatkan nilai alasan untuk keterbacaan yang lebih baik.

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

Mengunduh data yang dimigrasi dari Amazon S3

Karena migrasi meningkatkan biaya Amazon S3, Anda dapat mengunduh data yang dimigrasi dari Amazon S3 ke solusi penyimpanan lain. Topik ini menjelaskan cara mengunduh data yang dimigrasi, dan memberikan saran untuk mengunggah data ke solusi penyimpanan.

> **Note**
>
> Langkah-langkah berikut menjelaskan cara mengunduh satu file atau folder sekaligus. Untuk informasi tentang cara lain untuk mengunduh file, lihat Mengunduh objek, di Panduan Pengguna Amazon S3.

Untuk mengunduh data

1. Buka konsol Amazon S3 di. https://console.aws.amazon.com/s3/
2. Pilih bucket target dan navigasikan ke alias situs.
3. Pilih kotak centang di sebelah folder zip.

   —ATAU—

   Buka folder zip dan pilih kotak centang di sebelah file atau folder untuk pengguna individu.

4. Pilih Unduh.

Saran untuk solusi penyimpanan

Untuk situs besar, sebaiknya sediakan EC2 instans menggunakan Amazon Machine Image berbasis Linux yang sesuai untuk mengunduh data Anda dari Amazon S3 secara terprogram, membuka zip data, lalu mengunggahnya ke penyedia penyimpanan atau disk lokal Anda.

Memecahkan masalah migrasi

Coba langkah-langkah ini untuk memastikan Anda telah mengonfigurasi lingkungan Anda dengan benar:

- Jika migrasi gagal, pesan galat akan muncul di tab Riwayat migrasi di WorkDocs konsol. Tinjau pesan kesalahan.
- Periksa pengaturan bucket Amazon S3 Anda.
- Jalankan kembali migrasi.

Jika masalah berlanjut, hubungi AWS Support. Sertakan URL WorkDocs Situs dan ID Pekerjaan Migrasi, yang terletak di tabel riwayat migrasi.

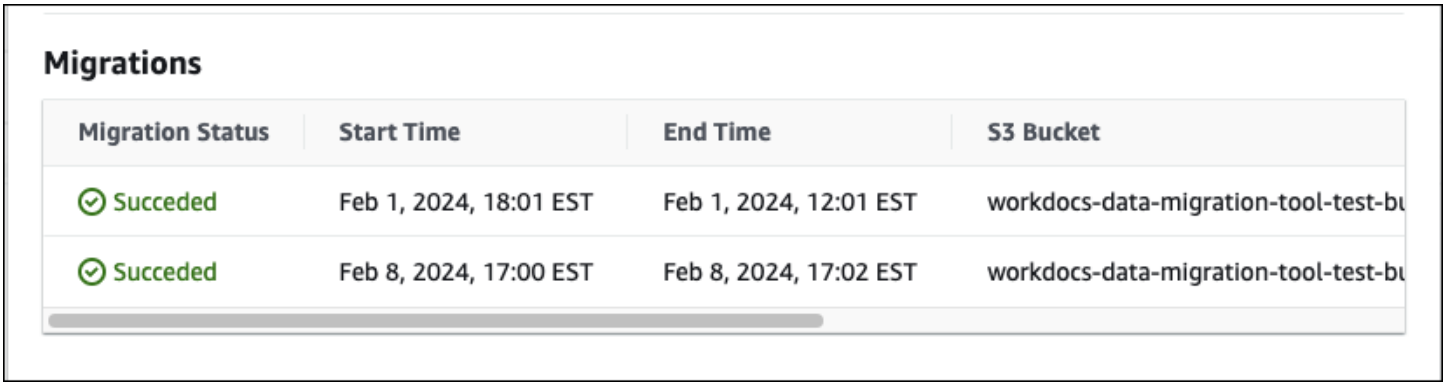
Melihat riwayat migrasi

Langkah-langkah berikut menjelaskan cara melihat riwayat migrasi Anda.

Untuk melihat riwayat Anda

1. Buka WorkDocs konsol di https://console.aws.amazon.com/zocalo/.
2. Pilih tombol radio di sebelah WorkDocs situs yang diinginkan.
3. Buka daftar Tindakan dan pilih Migrasi Data.
4. Pada halaman nama situs Migrasi Data, pilih Migrasi dan Riwayat Berlangsung.

Riwayat migrasi muncul di bawah Migrasi. Gambar berikut menunjukkan sejarah yang khas.


Migrations
Migration Status
Start Time
End Time
S3 Bucket
Succeded
Feb 1, 2024, 18:01 EST
Feb 1, 2024, 12:01 EST
workdocs-data-migration-tool-test-bu
Succeded
Feb 8, 2024, 17:00 EST
Feb 8, 2024, 17:02 EST
workdocs-data-migration-tool-test-bu

Prasyarat untuk Amazon WorkDocs

Untuk mengatur WorkDocs situs baru, atau mengelola situs yang ada, Anda harus menyelesaikan tugas-tugas berikut.

Mendaftar untuk Akun AWS

Jika Anda tidak memiliki Akun AWS, selesaikan langkah-langkah berikut untuk membuatnya.

Untuk mendaftar untuk Akun AWS

1. Buka https://portal.aws.amazon.com/billing/pendaftaran.
2. Ikuti petunjuk online.

   Bagian dari prosedur pendaftaran melibatkan menerima panggilan telepon atau pesan teks dan memasukkan kode verifikasi pada keypad telepon.

   Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWSdibuat. Pengguna root memiliki akses ke semua Layanan AWS dan sumber daya di akun. Sebagai praktik keamanan terbaik, tetapkan akses administratif ke pengguna, dan gunakan hanya pengguna root untuk melakukan tugas yang memerlukan akses pengguna root.

AWS mengirimi Anda email konfirmasi setelah proses pendaftaran selesai. Kapan saja, Anda dapat melihat aktivitas akun Anda saat ini dan mengelola akun Anda dengan masuk https://aws.amazon.comke/ dan memilih Akun Saya.

Buat pengguna dengan akses administratif

Setelah Anda mendaftar Akun AWS, amankan Pengguna root akun AWS, aktifkan AWS IAM Identity Center, dan buat pengguna administratif sehingga Anda tidak menggunakan pengguna root untuk tugas sehari-hari.

Amankan Anda Pengguna root akun AWS

1. Masuk ke AWS Management Consolesebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di laman berikutnya, masukkan kata sandi.

Untuk bantuan masuk dengan menggunakan pengguna root, lihat Masuk sebagai pengguna root di AWS Sign-In Panduan Pengguna.

2. Mengaktifkan autentikasi multi-faktor (MFA) untuk pengguna root Anda.

   Untuk petunjuk, lihat Mengaktifkan perangkat MFA virtual untuk pengguna Akun AWS root (konsol) Anda di Panduan Pengguna IAM.

Buat pengguna dengan akses administratif

1. Aktifkan Pusat Identitas IAM.

   Untuk mendapatkan petunjuk, silakan lihat Mengaktifkan AWS IAM Identity Center di Panduan Pengguna AWS IAM Identity Center .

2. Di Pusat Identitas IAM, berikan akses administratif ke pengguna.

   Untuk tutorial tentang menggunakan Direktori Pusat Identitas IAM sebagai sumber identitas Anda, lihat Mengkonfigurasi akses pengguna dengan default Direktori Pusat Identitas IAM di Panduan AWS IAM Identity Center Pengguna.

Masuk sebagai pengguna dengan akses administratif

- Untuk masuk dengan pengguna Pusat Identitas IAM, gunakan URL masuk yang dikirim ke alamat email saat Anda membuat pengguna Pusat Identitas IAM.

  Untuk bantuan masuk menggunakan pengguna Pusat Identitas IAM, lihat Masuk ke portal AWS akses di Panduan AWS Sign-In Pengguna.

Tetapkan akses ke pengguna tambahan

1. Di Pusat Identitas IAM, buat set izin yang mengikuti praktik terbaik menerapkan izin hak istimewa paling sedikit.

   Untuk petunjuknya, lihat Membuat set izin di Panduan AWS IAM Identity Center Pengguna.

2. Tetapkan pengguna ke grup, lalu tetapkan akses masuk tunggal ke grup.

   Untuk petunjuk, lihat Menambahkan grup di Panduan AWS IAM Identity Center Pengguna.

Keamanan di Amazon WorkDocs

Keamanan cloud di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. Model tanggung jawab bersama menggambarkan hal ini sebagai keamanan dari cloud dan keamanan di cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga secara berkala menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari Program kepatuhan AWS. Untuk mempelajari tentang program kepatuhan yang berlaku untuk Amazon WorkDocs, lihat AWS Layanan dalam Lingkup berdasarkan Program Kepatuhan.
- Keamanan di cloud — AWS Layanan yang Anda gunakan menentukan tanggung jawab Anda. Anda juga bertanggung jawab atas faktor-faktor lain, termasuk sensitivitas data Anda, persyaratan perusahaan Anda, dan hukum dan peraturan yang berlaku. Topik di bagian ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan WorkDocs.

> **Note**
>
> Pengguna dalam WorkDocs organisasi dapat berkolaborasi dengan pengguna di luar organisasi tersebut dengan mengirimkan tautan atau undangan ke file. Namun, ini hanya berlaku untuk situs yang menggunakan Konektor Direktori Aktif. Lihat pengaturan tautan bersama untuk situs Anda dan pilih opsi yang paling sesuai dengan persyaratan perusahaan Anda.

Topik berikut menunjukkan cara mengonfigurasi WorkDocs untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga belajar cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan WorkDocs sumber daya Anda.

Topik

- Validasi kepatuhan untuk Amazon WorkDocs
- Ketahanan di Amazon WorkDocs
- Keamanan infrastruktur di Amazon WorkDocs

Manajemen identitas dan akses untuk Amazon WorkDocs

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. Administrator IAM mengontrol siapa yang dapat diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber daya. WorkDocs IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik

- Audiens
- Mengautentikasi dengan identitas
- Mengelola akses menggunakan kebijakan
- Bagaimana Amazon WorkDocs bekerja dengan IAM
- Contoh WorkDocs kebijakan berbasis identitas Amazon
- Memecahkan masalah WorkDocs identitas dan akses Amazon

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda, tergantung pada pekerjaan yang Anda lakukan. WorkDocs

Pengguna layanan — Jika Anda menggunakan WorkDocs layanan untuk melakukan pekerjaan Anda, maka administrator Anda memberi Anda kredensi dan izin yang Anda butuhkan. Saat Anda menggunakan lebih banyak WorkDocs fitur untuk melakukan pekerjaan Anda, Anda mungkin memerlukan izin tambahan. Memahami cara mengelola akses dapat membantu Anda meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di WorkDocs, lihat Memecahkan masalah WorkDocs identitas dan akses Amazon.

Administrator layanan — Jika Anda bertanggung jawab atas WorkDocs sumber daya di perusahaan Anda, Anda mungkin memiliki akses penuh ke WorkDocs. Tugas Anda adalah menentukan WorkDocs fitur dan sumber daya mana yang harus diakses pengguna layanan Anda. Kemudian,

Anda harus mengirimkan permintaan kepada administrator IAM untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep dasar IAM. Untuk mempelajari lebih lanjut tentang bagaimana perusahaan Anda dapat menggunakan IAM WorkDocs, lihatBagaimana Amazon WorkDocs bekerja dengan IAM.

Administrator IAM – Jika Anda adalah administrator IAM, Anda mungkin ingin belajar dengan lebih detail tentang cara Anda menulis kebijakan untuk mengelola akses ke WorkDocs. Untuk melihat contoh kebijakan WorkDocs berbasis identitas yang dapat Anda gunakan di IAM, lihat. Contoh WorkDocs kebijakan berbasis identitas Amazon

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensyal identitas Anda. Anda harus diautentikasi (masuk ke AWS) sebagai Pengguna root akun AWS, sebagai pengguna IAM, atau dengan mengasumsikan peran IAM.

Anda dapat masuk AWS sebagai identitas federasi dengan menggunakan kredensyal yang disediakan melalui sumber identitas. AWS IAM Identity Center Pengguna (IAM Identity Center), autentikasi masuk tunggal perusahaan Anda, dan kredensi Google atau Facebook Anda adalah contoh identitas federasi. Saat Anda masuk sebagai identitas terfederasi, administrator Anda sebelumnya menyiapkan federasi identitas menggunakan peran IAM. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil peran.

Bergantung pada jenis pengguna Anda, Anda dapat masuk ke AWS Management Console atau portal AWS akses. Untuk informasi selengkapnya tentang masuk AWS, lihat Cara masuk ke Panduan AWS Sign-In Pengguna Anda Akun AWS.

Jika Anda mengakses AWS secara terprogram, AWS sediakan kit pengembangan perangkat lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara kriptografis dengan menggunakan kredensil Anda. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. Guna mengetahui informasi selengkapnya tentang penggunaan metode yang disarankan untuk menandatangani permintaan sendiri, lihat AWS Signature Version 4 untuk permintaan API dalam Panduan Pengguna IAM.

Apa pun metode autentikasi yang digunakan, Anda mungkin diminta untuk menyediakan informasi keamanan tambahan. Misalnya, AWS merekomendasikan agar Anda menggunakan otentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari selengkapnya, lihat Autentikasi multi-faktor dalam Panduan Pengguna AWS IAM Identity Center dan Autentikasi multi-faktor AWS di IAM dalam Panduan Pengguna IAM.

Pengguna dan grup IAM

Pengguna IAM adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, kami merekomendasikan untuk mengandalkan kredensial sementara, bukan membuat pengguna IAM yang memiliki kredensial jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan tertentu yang memerlukan kredensial jangka panjang dengan pengguna IAM, kami merekomendasikan Anda merotasi kunci akses. Untuk informasi selengkapnya, lihat Merotasi kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensial jangka panjang dalam Panduan Pengguna IAM.

Grup IAM adalah identitas yang menentukan sekumpulan pengguna IAM. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin bagi beberapa pengguna sekaligus. Grup mempermudah manajemen izin untuk sejumlah besar pengguna sekaligus. Misalnya, Anda dapat meminta kelompok untuk menyebutkan IAMAdmins dan memberikan izin kepada grup tersebut untuk mengelola sumber daya IAM.

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran dimaksudkan untuk dapat digunakan oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial sementara. Untuk mempelajari selengkapnya, lihat Kasus penggunaan untuk pengguna IAM dalam Panduan Pengguna IAM.

Peran IAM

Peran IAM adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus. Peran ini mirip dengan pengguna IAM, tetapi tidak terkait dengan orang tertentu. Untuk mengambil peran IAM sementara AWS Management Console, Anda dapat beralih dari pengguna ke peran IAM (konsol). Anda dapat mengambil peran dengan memanggil operasi AWS CLI atau AWS API atau dengan menggunakan URL kustom. Untuk informasi selengkapnya tentang cara menggunakan peran, lihat Metode untuk mengambil peran dalam Panduan Pengguna IAM.

Peran IAM dengan kredensial sementara berguna dalam situasi berikut:

- Akses pengguna terfederasi – Untuk menetapkan izin ke identitas terfederasi, Anda membuat peran dan menentukan izin untuk peran tersebut. Ketika identitas terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberi izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat Buat peran untuk penyedia identitas pihak ketiga dalam Panduan Pengguna IAM. Jika menggunakan Pusat Identitas IAM, Anda harus mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah identitas

tersebut diautentikasi, Pusat Identitas IAM akan mengorelasikan set izin ke peran dalam IAM. Untuk informasi tentang set izin, lihat Set izin dalam Panduan Pengguna AWS IAM Identity Center .

- Izin pengguna IAM sementara – Pengguna atau peran IAM dapat mengambil peran IAM guna mendapatkan berbagai izin secara sementara untuk tugas tertentu.
- Akses lintas akun – Anda dapat menggunakan peran IAM untuk mengizinkan seseorang (prinsipal tepercaya) di akun lain untuk mengakses sumber daya di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapa Layanan AWS, Anda dapat melampirkan kebijakan secara langsung ke sumber daya (alih-alih menggunakan peran sebagai proxy). Untuk mempelajari perbedaan antara peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM dalam Panduan Pengguna IAM.
- Akses lintas layanan — Beberapa Layanan AWS menggunakan fitur lain Layanan AWS. Misalnya, saat Anda melakukan panggilan dalam suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Sebuah layanan mungkin melakukannya menggunakan izin prinsipal yang memanggil, menggunakan peran layanan, atau peran terkait layanan.
  - Sesi akses teruskan (FAS) — Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses maju.
  - Peran layanan – Peran layanan adalah peran IAM yang dijalankan oleh layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Buat sebuah peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.
  - Peran terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke peran layanan. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.
- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan peran IAM untuk mengelola kredensi sementara untuk aplikasi yang berjalan pada EC2 instance dan membuat AWS CLI

atau AWS permintaan API. Ini lebih baik untuk menyimpan kunci akses dalam EC2 instance. Untuk menetapkan AWS peran ke EC2 instance dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instans yang dilampirkan ke instance. Profil instance berisi peran dan memungkinkan program yang berjalan pada EC2 instance untuk mendapatkan kredensi sementara. Untuk informasi selengkapnya, lihat Menggunakan peran IAM untuk memberikan izin ke aplikasi yang berjalan di EC2 instans Amazon di Panduan Pengguna IAM.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan adalah objek AWS yang, ketika dikaitkan dengan identitas atau sumber daya, menentukan izinnya. AWS mengevaluasi kebijakan ini ketika prinsipal (pengguna, pengguna root, atau sesi peran) membuat permintaan. Izin dalam kebijakan menentukan apakah permintaan diizinkan atau ditolak. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang struktur dan isi dokumen kebijakan JSON, lihat Gambaran umum kebijakan JSON dalam Panduan Pengguna IAM.

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Secara default, pengguna dan peran tidak memiliki izin. Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat mengambil peran.

Kebijakan IAM mendefinisikan izin untuk suatu tindakan terlepas dari metode yang Anda gunakan untuk melakukan operasinya. Misalnya, anggaplah Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole`. Pengguna dengan kebijakan tersebut bisa mendapatkan informasi peran dari AWS Management Console, API AWS CLI, atau AWS API.

Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas,

lihat Tentukan izin IAM kustom dengan kebijakan terkelola pelanggan dalam Panduan Pengguna IAM.

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan yang dikelola. Kebijakan inline disematkan langsung ke satu pengguna, grup, atau peran. Kebijakan terkelola adalah kebijakan mandiri yang dapat Anda lampirkan ke beberapa pengguna, grup, dan peran dalam. Akun AWS Kebijakan AWS terkelola mencakup kebijakan terkelola dan kebijakan yang dikelola pelanggan. Untuk mempelajari cara memilih antara kebijakan yang dikelola atau kebijakan inline, lihat Pilih antara kebijakan yang dikelola dan kebijakan inline dalam Panduan Pengguna IAM.

Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Kebijakan berbasis sumber daya merupakan kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan AWS terkelola dari IAM dalam kebijakan berbasis sumber daya.

Daftar kontrol akses

Access control lists (ACLs) mengontrol prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLs mirip dengan kebijakan berbasis sumber daya, meskipun mereka tidak menggunakan format dokumen kebijakan JSON.

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung. ACLs Untuk mempelajari selengkapnya ACLs, lihat Ringkasan daftar kontrol akses (ACL) di Panduan Pengembang Layanan Penyimpanan Sederhana Amazon.

Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang kurang umum. Jenis-jenis kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda oleh jenis kebijakan yang lebih umum.

- Batasan izin – Batasan izin adalah fitur lanjutan tempat Anda mengatur izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas ke entitas IAM (pengguna IAM atau peran IAM). Anda

dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas milik entitas dan batasan izinnya. Kebijakan berbasis sumber daya yang menentukan pengguna atau peran dalam bidang `Principal` tidak dibatasi oleh batasan izin. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya tentang batasan izin, lihat Batasan izin untuk entitas IAM dalam Panduan Pengguna IAM.

- Kebijakan kontrol layanan (SCPs) — SCPs adalah kebijakan JSON yang menentukan izin maksimum untuk organisasi atau unit organisasi (OU) di. AWS Organizations AWS Organizations adalah layanan untuk mengelompokkan dan mengelola secara terpusat beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur dalam suatu organisasi, maka Anda dapat menerapkan kebijakan kontrol layanan (SCPs) ke salah satu atau semua akun Anda. SCP membatasi izin untuk entitas di akun anggota, termasuk masing-masing. Pengguna root akun AWS Untuk informasi selengkapnya tentang Organizations dan SCPs, lihat Kebijakan kontrol layanan di Panduan AWS Organizations Pengguna.
- Kebijakan kontrol sumber daya (RCPs) — RCPs adalah kebijakan JSON yang dapat Anda gunakan untuk menetapkan izin maksimum yang tersedia untuk sumber daya di akun Anda tanpa memperbarui kebijakan IAM yang dilampirkan ke setiap sumber daya yang Anda miliki. RCP membatasi izin untuk sumber daya di akun anggota dan dapat memengaruhi izin efektif untuk identitas, termasuk Pengguna root akun AWS, terlepas dari apakah itu milik organisasi Anda. Untuk informasi selengkapnya tentang Organizations dan RCPs, termasuk daftar dukungan Layanan AWS tersebut RCPs, lihat Kebijakan kontrol sumber daya (RCPs) di Panduan AWS Organizations Pengguna.
- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter ketika Anda membuat sesi sementara secara programatis untuk peran atau pengguna terfederasi. Izin sesi yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya, lihat Kebijakan sesi dalam Panduan Pengguna IAM.

> **Note**
>
> WorkDocs tidak mendukung Kebijakan Kontrol Layanan untuk Slack Organizations.

Berbagai jenis kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan saat beberapa jenis kebijakan terlibat, lihat Logika evaluasi kebijakan di Panduan Pengguna IAM.

Bagaimana Amazon WorkDocs bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses WorkDocs, Anda perlu memahami fitur IAM mana yang tersedia untuk digunakan. WorkDocs Untuk mendapatkan pandangan tingkat tinggi tentang bagaimana WorkDocs dan AWS layanan lain bekerja dengan IAM, lihat AWS layanan yang bekerja dengan IAM di Panduan Pengguna IAM.

Topik

- Kebijakan berbasis identitas WorkDocs
- WorkDocs Kebijakan berbasis sumber daya
- Otorisasi berdasarkan tanda WorkDocs
- WorkDocs Peran IAM

Kebijakan berbasis identitas WorkDocs

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan tindakan yang diizinkan atau ditolak. WorkDocs mendukung tindakan tertentu. Untuk mempelajari semua elemen yang Anda gunakan dalam kebijakan JSON, lihat Referensi elemen kebijakan JSON IAM dalam Panduan Pengguna IAM.

Tindakan

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Tindakan kebijakan biasanya memiliki nama yang sama dengan operasi AWS API terkait. Ada beberapa pengecualian, misalnya tindakan hanya izin yang tidak memiliki operasi API yang cocok. Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam suatu kebijakan. Tindakan tambahan ini disebut tindakan dependen.

Sertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Tindakan kebijakan WorkDocs menggunakan awalan berikut sebelum tindakan:`workdocs:`. Misalnya, untuk memberikan izin kepada seseorang untuk menjalankan operasi WorkDocs `DescribeUsers` API, Anda menyertakan `workdocs:DescribeUsers` tindakan tersebut dalam kebijakan mereka. Pernyataan kebijakan harus menyertakan elemen `Action` atau `NotAction`. WorkDocs menentukan set tindakan sendiri yang menjelaskan tugas yang dapat Anda lakukan dengan layanan ini.

Untuk menetapkan beberapa tindakan dalam satu pernyataan, pisahkan dengan koma seperti berikut:

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

Anda dapat menentukan beberapa tindakan menggunakan wildcard (*). Misalnya, untuk menentukan semua tindakan yang dimulai dengan kata `Describe`, sertakan tindakan berikut:

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

> **Note**
>
> Untuk memastikan kompatibilitas dengan versi lama, sertakan tindakan `zocalo`. Misalnya:
>
> ```
> "Action": [
> "zocalo:*",
> "workdocs:*"
> ],
> ```

Untuk melihat daftar WorkDocs tindakan, lihat Tindakan yang ditentukan oleh WorkDocs dalam Panduan Pengguna IAM.

Sumber daya

WorkDocs tidak mendukung menentukan sumber daya ARNs dalam kebijakan.

Kunci syarat

WorkDocs tidak menyediakan kunci kondisi khusus layanan apa pun, tetapi mendukung penggunaan beberapa kunci kondisi global. Untuk melihat semua kunci kondisi AWS global, lihat kunci konteks kondisi AWS global di Panduan Pengguna IAM.

Contoh

Untuk melihat contoh kebijakan WorkDocs berbasis identitas, lihat. Contoh WorkDocs kebijakan berbasis identitas Amazon

WorkDocs Kebijakan berbasis sumber daya

WorkDocs tidak mendukung kebijakan berbasis sumber daya.

Otorisasi berdasarkan tanda WorkDocs

WorkDocs tidak mendukung penandaan sumber daya atau mengendalikan akses berdasarkan tag.

WorkDocs Peran IAM

Peran IAM adalah entitas dalam AWS akun Anda yang memiliki izin tertentu.

Menggunakan kredensi sementara dengan WorkDocs

Kami sangat menyarankan menggunakan kredensil sementara untuk masuk dengan federasi, mengambil peran IAM, atau untuk mengambil peran lintas akun. Anda memperoleh kredensil keamanan sementara dengan memanggil operasi AWS STS API seperti AssumeRoleatau. GetFederationToken

WorkDocs mendukung menggunakan kredensil sementara.

Peran terkait layanan

Peran terkait AWS layanan memungkinkan layanan mengakses sumber daya di layanan lain untuk menyelesaikan tindakan atas nama Anda. Peran terkait layanan muncul di akun IAM Anda dan dimiliki oleh layanan tersebut. Administrator IAM dapat melihat tetapi tidak dapat mengedit izin untuk peran terkait layanan.

WorkDocs tidak mendukung peran terkait layanan.

Peran layanan

Fitur ini memungkinkan layanan untuk menerima peran layanan atas nama Anda. Peran ini mengizinkan layanan untuk mengakses sumber daya di layanan lain untuk menyelesaikan tindakan atas nama Anda. Peran layanan muncul di akun IAM Anda dan dimiliki oleh akun tersebut. Ini berarti administrator IAM dapat mengubah izin untuk peran ini. Namun, melakukan hal itu dapat merusak fungsionalitas layanan.

WorkDocs tidak mendukung peran layanan.

Contoh WorkDocs kebijakan berbasis identitas Amazon

> **Note**
>
> Untuk keamanan yang lebih besar, buat pengguna federasi alih-alih pengguna IAM bila memungkinkan.

Secara default, pengguna dan IAM role tidak memiliki izin untuk membuat atau memodifikasi WorkDocs sumber daya. Mereka juga tidak dapat melakukan tugas menggunakan AWS Management Console, AWS CLI, atau AWS API. Administrator IAM harus membuat kebijakan IAM yang memberikan izin kepada pengguna dan peran untuk melakukan operasi API tertentu pada sumber daya yang diperlukan. Administrator kemudian harus melampirkan kebijakan tersebut ke pengguna IAM atau grup yang memerlukan izin tersebut.

> **Note**
>
> Untuk memastikan kompatibilitas dengan versi lama, sertakan tindakan `zocalo` dalam kebijakan Anda. Sebagai contoh:

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

```
            "Resource": "*"
        }
    ]
}
```

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM menggunakan contoh dokumen kebijakan JSON ini, lihat Membuat kebijakan di tab JSON dalam Panduan Pengguna IAM.

Topik

- Praktik terbaik kebijakan
- Menggunakan konsol WorkDocs
- Izinkan para pengguna untuk melihat izin mereka sendiri
- Izinkan pengguna akses hanya-baca ke sumber daya WorkDocs
- Lebih banyak WorkDocs contoh kebijakan berbasis identitas

Praktik terbaik kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus WorkDocs sumber daya di akun Anda. Tindakan ini membuat Akun AWS Anda dikenai biaya. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat Kebijakan yang dikelola AWS atau Kebijakan yang dikelola AWS untuk fungsi tugas dalam Panduan Pengguna IAM.
- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk mengajukan izin, lihat Kebijakan dan izin dalam IAM dalam Panduan Pengguna IAM.

- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti AWS CloudFormation. Untuk informasi selengkapnya, lihat Elemen kebijakan JSON IAM: Kondisi dalam Panduan Pengguna IAM.
- Gunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat Validasi kebijakan dengan IAM Access Analyzer dalam Panduan Pengguna IAM.
- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Anda, Akun AWS aktifkan MFA untuk keamanan tambahan. Untuk meminta MFA ketika operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat Amankan akses API dengan MFA dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat Praktik terbaik keamanan di IAM dalam Panduan Pengguna IAM.

Menggunakan konsol WorkDocs

Untuk mengakses WorkDocs konsol Amazon, Anda harus memiliki set izin minimum. Izin tersebut harus memungkinkan Anda untuk membuat daftar dan melihat detail sumber WorkDocs daya di AWS akun Anda. Jika Anda membuat kebijakan berbasis identitas yang lebih ketat dari izin minimum yang diperlukan, konsol tidak akan berfungsi sebagaimana dimaksudkan untuk entitas pengguna IAM atau IAM role.

Untuk memastikan bahwa entitas tersebut dapat menggunakan WorkDocs konsol, lampirkan juga kebijakan AWS terkelola berikut ke entitas. Untuk informasi tentang menyematkan kebijakan, lihat Menambahkan izin untuk pengguna dalam Panduan Pengguna IAM.

- AmazonWorkDocsFullAccess
- AWSDirectoryServiceFullAccess

- Amazon EC2 FullAccess

Kebijakan ini memberi pengguna akses penuh ke WorkDocs sumber daya, operasi AWS Directory Service, dan EC2 operasi Amazon yang WorkDocs dibutuhkan Amazon agar dapat berfungsi dengan baik.

Anda tidak perlu mengizinkan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau AWS API. Sebagai alternatif, hanya izinkan akses ke tindakan yang cocok dengan operasi API yang sedang Anda coba lakukan.

Izinkan para pengguna untuk melihat izin mereka sendiri

Contoh ini menunjukkan cara membuat kebijakan yang mengizinkan pengguna IAM melihat kebijakan inline dan terkelola yang dilampirkan ke identitas pengguna mereka. Kebijakan ini mencakup izin untuk menyelesaikan tindakan ini di konsol atau menggunakan API atau secara terprogram. AWS CLI AWS

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

```
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Izinkan pengguna akses hanya-baca ke sumber daya WorkDocs

AmazonWorkDocsReadOnlyAccessKebijakan AWS terkelola berikut memberikan akses hanya-baca pengguna IAM ke sumber daya. WorkDocs Kebijakan ini memberi pengguna akses ke semua WorkDocs `Describe` operasi. Akses ke dua EC2 operasi Amazon diperlukan sehingga WorkDocs dapat memperoleh daftar Anda VPCs dan subnet. Akses ke AWS Directory Service `DescribeDirectories` operasi diperlukan untuk mendapatkan informasi tentang AWS Directory Service direktori Anda.

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

Lebih banyak WorkDocs contoh kebijakan berbasis identitas

Administrator IAM dapat membuat kebijakan tambahan untuk mengizinkan peran IAM atau pengguna mengakses API. WorkDocs Untuk informasi selengkapnya, lihat Otentikasi dan kontrol akses untuk aplikasi administratif di Panduan WorkDocs Pengembang.

Memecahkan masalah WorkDocs identitas dan akses Amazon

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan WorkDocs dan IAM.

Topik

Saya tidak berwenang untuk melakukan tindakan di WorkDocs

Jika AWS Management Console memberitahu Anda bahwa Anda tidak berwenang untuk melakukan tindakan, maka Anda harus menghubungi administrator Anda untuk bantuan. Administrator Anda adalah orang yang memberikan nama pengguna dan kata sandi Anda.

Saya tidak berwenang untuk melakukan iam: PassRole

Jika Anda menerima kesalahan yang tidak diizinkan untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran WorkDocs.

Beberapa Layanan AWS memungkinkan Anda untuk meneruskan peran yang ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran terkait layanan. Untuk melakukannya, Anda harus memiliki izin untuk meneruskan peran ke layanan.

Contoh kesalahan berikut terjadi ketika pengguna IAM bernama `marymajor` mencoba menggunakan konsol tersebut untuk melakukan tindakan di WorkDocs. Namun, tindakan tersebut memerlukan layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

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

Dalam kasus ini, kebijakan Mary harus diperbarui agar dia mendapatkan izin untuk melakukan tindakan `iam:PassRole` tersebut.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya ingin mengizinkan orang di luar AWS akun saya untuk mengakses WorkDocs sumber daya saya

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau orang-orang di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACLs), Anda dapat menggunakan kebijakan tersebut untuk memberi orang akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mempelajari apakah WorkDocs mendukung fitur-fitur ini, lihatBagaimana Amazon WorkDocs bekerja dengan IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat Menyediakan akses ke pengguna IAM di pengguna lain Akun AWS yang Anda miliki di Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat Menyediakan akses ke pengguna terautentikasi eksternal (federasi identitas) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM.

Pencatatan dan pemantauan di Amazon WorkDocs

Administrator WorkDocs situs Amazon dapat melihat dan mengekspor umpan aktivitas untuk seluruh situs. Mereka juga dapat digunakan AWS CloudTrail untuk menangkap peristiwa dari WorkDocs konsol.

Topik

- Mengekspor umpan aktivitas di seluruh situs
- Menggunakan AWS CloudTrail untuk mencatat panggilan WorkDocs API Amazon

Mengekspor umpan aktivitas di seluruh situs

Admin dapat melihat dan mengekspor umpan aktivitas untuk seluruh situs. Untuk menggunakan fitur ini, Anda harus menginstal WorkDocs Companion terlebih dahulu. Untuk menginstal WorkDocs Companion, lihat Aplikasi & Integrasi untuk WorkDocs.

Untuk melihat dan mengekspor umpan aktivitas di seluruh situs

1. Dalam aplikasi web, pilih Aktivitas.
2. Pilih Filter, lalu gerakkan slider Aktivitas di seluruh situs untuk mengaktifkan filter.
3. Pilih filter Jenis Aktivitas dan pilih pengaturan Tanggal Diubah yang dibutuhkan, lalu pilih Terapkan.
4. Ketika hasil umpan aktivitas yang difilter muncul, cari berdasarkan file, folder, atau nama pengguna untuk mempersempit hasil Anda. Anda juga dapat menambahkan atau menghapus filter sesuai kebutuhan.
5. Pilih Ekspor untuk mengekspor umpan aktivitas menjadi file `.csv` dan `.json` pada desktop Anda. Sistem mengekspor file ke salah satu lokasi berikut:

   - Windows - WorkDocsDownloadsfolder di folder Unduhan PC Anda
   - macOS – `/users/`**`username`**`/WorkDocsDownloads/folder`

   File yang diekspor mencerminkan semua filter yang Anda terapkan.

   > **Note**
   >
   > Pengguna yang bukan administrator dapat melihat dan mengekspor umpan aktivitas hanya untuk konten mereka sendiri. Untuk informasi selengkapnya, lihat Melihat Umpan Aktivitas di Panduan WorkDocs Pengguna Amazon.

Menggunakan AWS CloudTrail untuk mencatat panggilan WorkDocs API Amazon

Anda dapat menggunakan AWS CloudTrail; untuk mencatat panggilan WorkDocs API Amazon. CloudTrail menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan

di WorkDocs. CloudTrail menangkap semua panggilan API untuk WorkDocs sebagai peristiwa, termasuk panggilan dari WorkDocs konsol dan dari panggilan kode ke WorkDocs APIs.

Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara berkelanjutan ke bucket Amazon S3, termasuk acara untuk. WorkDocs Jika Anda tidak membuat jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol dalam Riwayat acara.

Informasi yang dikumpulkan CloudTrail termasuk permintaan, alamat IP dari mana permintaan dibuat, pengguna yang membuat permintaan, dan tanggal permintaan.

Untuk informasi selengkapnya CloudTrail, lihat Panduan AWS CloudTrail Pengguna.

WorkDocs informasi di CloudTrail

CloudTrail diaktifkan di AWS akun Anda saat Anda membuat akun. Ketika aktivitas terjadi di WorkDocs, aktivitas tersebut dicatat dalam suatu CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam riwayat Acara. Anda dapat melihat, mencari, dan mengunduh acara terbaru di AWS akun Anda. Untuk informasi selengkapnya, lihat Melihat peristiwa dengan riwayat CloudTrail acara.

Untuk catatan peristiwa yang sedang berlangsung di AWS akun Anda, termasuk acara untuk WorkDocs, buat jejak. Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Secara default, ketika Anda membuat jejak di konsol, jejak ini diterapkan ke semua Wilayah. Trail mencatat peristiwa dari semua wilayah di AWS partisi dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasi AWS layanan lain untuk menganalisis lebih lanjut dan menindaklanjuti data peristiwa yang dikumpulkan dalam CloudTrail log. Untuk informasi selengkapnya, lihat:

- Ikhtisar untuk membuat jejak
- CloudTrail layanan dan integrasi yang didukung
- Mengonfigurasi notifikasi Amazon SNS untuk CloudTrail
- Menerima file CloudTrail log dari beberapa Wilayah dan Menerima file CloudTrail log dari beberapa akun

Semua WorkDocs tindakan dicatat oleh CloudTrail dan didokumentasikan dalam Referensi Amazon WorkDocs API. Misalnya, panggilan ke`CreateFolder`, `DeactivateUser` dan `UpdateDocument` bagian menghasilkan entri dalam file CloudTrail log.

Setiap entri peristiwa atau log berisi informasi tentang entitas yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan hal berikut ini:

- Apakah permintaan tersebut dibuat dengan kredensial root atau pengguna IAM.
- Apakah permintaan tersebut dibuat dengan kredensial keamanan sementara untuk satu peran atau pengguna terfederasi.
- Apakah permintaan itu dibuat oleh AWS layanan lain.

Untuk informasi selengkapnya, lihat Elemen userIdentity CloudTrail .

Memahami entri file WorkDocs log

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket Amazon S3 yang Anda tentukan. CloudTrail file log berisi satu atau lebih entri log. Peristiwa mewakili permintaan tunggal dari sumber manapun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, sehingga file tersebut tidak muncul dalam urutan tertentu.

WorkDocs menghasilkan berbagai jenis CloudTrail entri, yang berasal dari bidang kontrol dan yang dari bidang data. Perbedaan penting antara keduanya adalah bahwa identitas pengguna untuk entri bidang kontrol adalah pengguna IAM. Identitas pengguna untuk entri pesawat data adalah pengguna WorkDocs direktori.

> **Note**
>
> Untuk keamanan yang lebih besar, buat pengguna federasi alih-alih pengguna IAM bila memungkinkan.

Informasi sensitif, seperti kata sandi, token autentikasi, komentar file, dan konten file disunting dalam entri log. Ini muncul sebagai HIDDEN_DUE_TO_SECURITY_REASONS di log. CloudTrail Ini muncul sebagai HIDDEN_DUE_TO_SECURITY_REASONS di log. CloudTrail

Contoh berikut menunjukkan dua entri CloudTrail log untuk WorkDocs: catatan pertama adalah untuk tindakan bidang kontrol dan yang kedua adalah untuk tindakan bidang data.

```
{
  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"
    }
  ]
}
```

Validasi kepatuhan untuk Amazon WorkDocs

Untuk mempelajari apakah an Layanan AWS berada dalam lingkup program kepatuhan tertentu, lihat Layanan AWS di Lingkup oleh Program Kepatuhan Layanan AWS dan pilih program kepatuhan yang Anda minati. Untuk informasi umum, lihat Program AWS Kepatuhan Program AWS .

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat Mengunduh Laporan di AWS Artifact .

Tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan hukum dan peraturan yang berlaku. AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- Kepatuhan dan Tata Kelola Keamanan – Panduan implementasi solusi ini membahas pertimbangan arsitektur serta memberikan langkah-langkah untuk menerapkan fitur keamanan dan kepatuhan.
- Referensi Layanan yang Memenuhi Syarat HIPAA — Daftar layanan yang memenuhi syarat HIPAA. Tidak semua memenuhi Layanan AWS syarat HIPAA.
- AWS Sumber Daya AWS — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- AWS Panduan Kepatuhan Pelanggan - Memahami model tanggung jawab bersama melalui lensa kepatuhan. Panduan ini merangkum praktik terbaik untuk mengamankan Layanan AWS dan memetakan panduan untuk kontrol keamanan di berbagai kerangka kerja (termasuk Institut Standar dan Teknologi Nasional (NIST), Dewan Standar Keamanan Industri Kartu Pembayaran (PCI), dan Organisasi Internasional untuk Standardisasi (ISO)).
- Mengevaluasi Sumber Daya dengan Aturan dalam Panduan AWS Config Pengembang — AWS Config Layanan menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- AWS Security Hub— Ini Layanan AWS memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS. Security Hub menggunakan kontrol keamanan untuk sumber

daya AWS Anda serta untuk memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Untuk daftar layanan dan kontrol yang didukung, lihat Referensi kontrol Security Hub.

- Amazon GuardDuty — Ini Layanan AWS mendeteksi potensi ancaman terhadap beban kerja Akun AWS, kontainer, dan data Anda dengan memantau lingkungan Anda untuk aktivitas yang mencurigakan dan berbahaya. GuardDuty dapat membantu Anda mengatasi berbagai persyaratan kepatuhan, seperti PCI DSS, dengan memenuhi persyaratan deteksi intrusi yang diamanatkan oleh kerangka kerja kepatuhan tertentu.
- AWS Audit ManagerIni Layanan AWS membantu Anda terus mengaudit AWS penggunaan Anda untuk menyederhanakan cara Anda mengelola risiko dan kepatuhan terhadap peraturan dan standar industri.

Ketahanan di Amazon WorkDocs

Infrastruktur AWS global dibangun di sekitar AWS Wilayah dan Zona Ketersediaan. AWS Wilayah menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung dengan latensi rendah, throughput tinggi, dan jaringan yang sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang dan mengoperasikan aplikasi dan basis data yang secara otomatis melakukan failover di antara Zona Ketersediaan tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur biasa yang terdiri dari satu atau beberapa pusat data.

Untuk informasi selengkapnya tentang AWS Wilayah dan Availability Zone, lihat Infrastruktur AWS Global.

Keamanan infrastruktur di Amazon WorkDocs

Sebagai layanan terkelola, Amazon WorkDocs dilindungi oleh prosedur keamanan jaringan AWS global. Untuk informasi selengkapnya, lihat Keamanan infrastruktur di AWS Identity and Access Management di Panduan Pengguna IAM dan Praktik Terbaik untuk Keamanan, Identitas, & Kepatuhan di Pusat AWS Arsitektur.

Anda menggunakan panggilan API yang AWS dipublikasikan untuk mengakses WorkDocs melalui jaringan. Klien harus mendukung Transport Layer Security (TLS) 1.2, dan sebaiknya gunakan TLS 1.3. Klien juga harus mendukung cipher suite dengan kerahasiaan ke depan yang sempurna seperti Ephemeral Diffie-Hellman atau Elliptic Curve Ephemeral Diffie-Hellman. Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Selain itu, permintaan harus ditandatangani menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan prinsipal IAM. Atau Anda bisa menggunakan AWS Security Token Service (AWS STS) untuk membuat kredensial keamanan sementara guna menandatangani permintaan.

Memulai dengan WorkDocs

WorkDocs menggunakan direktori untuk menyimpan dan mengelola informasi organisasi untuk pengguna Anda dan dokumen mereka. Artinya, Anda melampirkan direktori ke situs ketika Anda menyediakan situs tersebut. Ketika Anda melakukannya, WorkDocs fitur yang disebut Aktivasi otomatis menambahkan pengguna di direktori ke situs sebagai pengguna terkelola, yang berarti mereka tidak memerlukan kredensi terpisah untuk masuk ke situs Anda, dan mereka dapat berbagi dan berkolaborasi pada file. Setiap pengguna memiliki 1 TB penyimpanan kecuali mereka membeli lebih banyak.

Anda tidak perlu lagi menambahkan dan mengaktifkan pengguna secara manual, meskipun hal itu masih bisa dilakukan. Anda juga dapat mengubah peran dan izin pengguna kapan pun diperlukan. Untuk informasi selengkapnya tentang cara melakukan hal itu, lihat Mengundang dan mengelola pengguna WorkDocs , di bagian berikutnya dalam panduan ini.

Jika Anda perlu membuat direktori, Anda dapat:

- Buat direktori Simple AD.
- Membuat direktori AD Connector untuk menghubungkan ke direktori on-premise Anda.
- Aktifkan WorkDocs untuk bekerja dengan AWS direktori yang ada.
- WorkDocs Buat direktori untuk Anda.

Anda juga dapat membuat hubungan kepercayaan antara direktori AD dan AWS Managed Microsoft AD Direktori.

> **Note**
>
> Jika Anda termasuk dalam program kepatuhan seperti PCI, FedRAMP, atau DoD, Anda harus menyiapkan Direktori AWS Managed Microsoft AD untuk memenuhi persyaratan kepatuhan. Langkah-langkah di bagian ini menjelaskan cara menggunakan Direktori Microsoft AD yang ada. Untuk informasi tentang membuat Direktori Microsoft AD, lihat AWS Managed Microsoft AD di Panduan Administrasi Layanan AWS Direktori.

Daftar Isi

- Mengaktifkan single sign-on
- Mengaktifkan autentikasi multi-faktor
- Mempromosikan pengguna ke administrator

Membuat WorkDocs situs

Langkah-langkah di bagian berikut menjelaskan cara menyiapkan WorkDocs situs baru.

Tugas

- Sebelum Anda mulai
- Membuat WorkDocs situs

Sebelum Anda mulai

Anda harus memiliki item berikut sebelum membuat WorkDocs situs.

- AWS Akun untuk membuat dan mengelola WorkDocs situs. Namun, pengguna tidak memerlukan AWS akun untuk terhubung dan menggunakan WorkDocs. Untuk informasi selengkapnya, lihat Prasyarat untuk Amazon WorkDocs.
- Jika Anda berencana untuk menggunakan Simple AD, Anda harus memenuhi prasyarat yang diidentifikasi dalam Prasyarat Simple AD dalam Panduan Administrasi.AWS Directory Service
- AWS Managed Microsoft AD Direktori jika Anda termasuk dalam program kepatuhan seperti PCI, FedRAMP, atau DoD. Langkah-langkah di bagian ini menjelaskan cara menggunakan Direktori Microsoft AD yang ada. Untuk informasi tentang membuat Direktori Microsoft AD, lihat AWS Managed Microsoft AD di Panduan Administrasi Layanan AWS Direktori.
- Informasi profil untuk administrator, termasuk nama depan dan belakang, dan alamat email.

Membuat WorkDocs situs

Ikuti langkah-langkah ini untuk membuat WorkDocs situs dalam hitungan menit.

Untuk membuat WorkDocs situs

1. Buka WorkDocs konsol di https://console.aws.amazon.com/zocalo/.
2. Di halaman Beranda konsol, di bawah Buat WorkDocs situs, pilih Mulai sekarang.

—ATAU—

Di panel navigasi, pilih Situs saya, dan pada halaman Kelola WorkDocs situs Anda, pilih Buat WorkDocs situs.

Apa yang terjadi selanjutnya tergantung pada apakah Anda memiliki direktori.

- Jika Anda memiliki direktori, halaman Pilih direktori muncul dan memungkinkan Anda untuk memilih direktori yang ada atau membuat direktori.
- Jika Anda tidak memiliki direktori, halaman Mengatur tipe direktori akan muncul dan memungkinkan Anda membuat direktori Simple AD atau AD Connector

Langkah-langkah berikut menjelaskan cara melakukan kedua tugas tersebut.

Untuk menggunakan direktori yang ada

1. Buka daftar direktori yang tersedia dan pilih direktori yang ingin Anda gunakan.
2. Pilih Aktifkan direktori.

Untuk membuat direktori

1. Ulangi langkah 1 dan 2 di atas.

   Pada titik ini, apa yang Anda lakukan tergantung pada apakah Anda ingin menggunakan Simple AD atau membuat AD Connector.

   Untuk menggunakan Simple AD

   a. Pilih Simple AD, lalu pilih Berikutnya.

      Halaman situs Create Simple AD muncul.

   b. Di bawah Access point, di kotak URL Situs, masukkan URL untuk situs tersebut.
   c. Di bawah Setel WorkDocs administrator, masukkan alamat email administrator, nama depan, dan nama belakang.
   d. Sesuai kebutuhan, lengkapi opsi di bawah Detail direktori dan konfigurasi VPC.
   e. Pilih Buat situs iklan sederhana.

Untuk membuat direktori AD Connector

a. Pilih AD Connector, lalu pilih Berikutnya.

   Halaman situs Create AD Connector akan muncul.

b. Lengkapi semua bidang di bawah Detail direktori.

c. Di bawah Access point, di kotak URL Situs, masukkan URL situs Anda.

d. Seperti yang diinginkan, lengkapi bidang opsional di bawah konfigurasi VPC.

e. Pilih situs Buat AD Connector.

WorkDocs melakukan hal berikut:

- Jika Anda memilih Siapkan VPC atas nama saya di langkah 4 di atas, WorkDocs buat VPC untuk Anda. Direktori di VPC menyimpan informasi pengguna dan WorkDocs situs.
- Jika Anda menggunakan Simple AD, WorkDocs buat Directory User dan tetapkan pengguna tersebut sebagai WorkDocs administrator. Jika Anda membuat direktori AD Connector, WorkDocs tetapkan pengguna direktori yang ada yang Anda berikan sebagai WorkDocs administrator.
- Jika Anda menggunakan direktori yang ada, WorkDocs meminta Anda untuk memasukkan nama pengguna WorkDocs administrator. Pengguna harus menjadi anggota direktori.

> **Note**
>
> WorkDocs tidak memberi tahu pengguna tentang situs baru. Anda perlu menginformasikan URL situs kepada mereka, dan memberi tahu bahwa mereka tidak memerlukan kredensial masuk berbeda untuk menggunakan situs ini.

Mengaktifkan single sign-on

AWS Directory Service memungkinkan pengguna untuk mengakses Amazon WorkDocs dari komputer yang bergabung ke direktori yang sama dengan yang WorkDocs terdaftar, tanpa memasukkan kredensional secara terpisah. WorkDocs administrator dapat mengaktifkan sistem masuk tunggal menggunakan konsol. AWS Directory Service Untuk informasi selengkapnya, lihat Single sign-on dalam Panduan Administrasi AWS Directory Service .

Setelah WorkDocs administrator mengaktifkan sistem masuk tunggal, pengguna WorkDocs situs mungkin juga perlu mengubah pengaturan browser web mereka untuk memungkinkan sistem masuk tunggal. Untuk informasi selengkapnya, lihat Single sign-on untuk IE dan Chrome dan Single sign-on untuk Firefox dalam Panduan Administrasi AWS Directory Service .

Mengaktifkan autentikasi multi-faktor

Anda menggunakan AWS Directory Services Console di https://console.aws.amazon.com/directoryservicev2/untuk mengaktifkan autentikasi multi-faktor untuk direktori AD Connector Anda. Untuk mengaktifkan MFA, Anda harus memiliki solusi MFA yang adalah server Layanan autentikasi jarak jauh panggilan masuk pengguna (RADIUS), atau Anda harus memiliki plugin MFA ke server RADIUS yang sudah diterapkan di infrastruktur on-premise Anda. Solusi MFA Anda harus menerapkan Kode Sandi Sekali Pakai (OTP) yang diperoleh pengguna dari perangkat keras atau dari perangkat lunak yang berjalan pada perangkat seperti ponsel.

RADIUS adalah client/server protokol standar industri yang menyediakan otentikasi, otorisasi, dan manajemen akuntansi untuk memungkinkan pengguna terhubung ke layanan jaringan. AWS Managed Microsoft AD menyertakan klien RADIUS yang terhubung ke server RADIUS tempat Anda menerapkan solusi MFA Anda. Server RADIUS Anda memvalidasi nama pengguna dan kode OTP. Jika server RADIUS Anda berhasil memvalidasi pengguna, AWS Managed Microsoft AD kemudian mengautentikasi pengguna terhadap AD. Setelah otentikasi AD berhasil, pengguna kemudian dapat mengakses aplikasi AWS. Komunikasi antara klien AWS Managed Microsoft AD RADIUS dan server RADIUS Anda mengharuskan Anda mengonfigurasi grup keamanan AWS yang memungkinkan komunikasi melalui port 1812.

Untuk informasi selengkapnya, lihat Mengaktifkan autentikasi multi-faktor untuk AWS Managed Microsoft AD di Panduan Administrasi Layanan AWS Direktori.

> **Note**
>
> Autentikasi multi-faktor tidak tersedia untuk direktori Simple AD.

Mempromosikan pengguna ke administrator

Anda menggunakan WorkDocs konsol untuk mempromosikan pengguna ke administrator. Ikuti langkah-langkah ini.

Untuk mempromosikan pengguna menjadi administrator

1. Buka WorkDocs konsol di https://console.aws.amazon.com/zocalo/.
2. Di panel navigasi, pilih Situs saya.

   Halaman Kelola WorkDocs Situs Anda muncul.
3. Pilih tombol di sebelah situs yang diinginkan, pilih Tindakan, lalu pilih Tetapkan administrator.

   Kotak dialog Set WorkDocs administrator muncul.
4. Di kotak Nama pengguna, masukkan nama pengguna orang yang ingin Anda promosikan, lalu pilih Tetapkan administrator.

Anda juga dapat menggunakan panel kontrol admin WorkDocs situs untuk menurunkan administrator. Lihat informasi yang lebih lengkap di Mengedit pengguna.

Mengelola WorkDocs dari AWS konsol

Anda menggunakan alat ini untuk mengelola WorkDocs situs Anda:

- AWS Konsol di https://console.aws.amazon.com/zocalo/.
- Panel kontrol admin situs, tersedia untuk administrator di semua WorkDocs situs.

Masing-masing alat tersebut menyediakan serangkaian tindakan yang berbeda, dan topik di bagian ini menjelaskan tindakan yang disediakan oleh AWS konsol. Untuk informasi tentang panel kontrol admin situs, lihatMengelola WorkDocs dari panel kontrol admin situs.

Mengatur administrator situs

Jika Anda seorang administrator, Anda dapat memberi pengguna akses ke panel kontrol situs dan tindakan yang disediakannya.

Untuk mengatur administrator

1. Buka WorkDocs konsol di https://console.aws.amazon.com/zocalo/.
2. Di panel navigasi, pilih Situs saya.

   Halaman Kelola WorkDocs situs Anda muncul dan menampilkan daftar situs Anda.
3. Pilih tombol di sebelah situs yang ingin Anda atur administrator.
4. Buka daftar Tindakan dan pilih Tetapkan administrator.

   Kotak dialog Set WorkDocs administrator muncul.
5. Di kotak Nama Pengguna, masukkan nama administrator baru, lalu pilih Tetapkan administrator.

Mengirim ulang email undangan

Anda dapat mengirim ulang email undangan kapan saja.

Untuk mengirim ulang email undangan

1. Buka WorkDocs konsol di https://console.aws.amazon.com/zocalo/.
2. Di panel navigasi, pilih Situs saya.

Halaman Kelola WorkDocs situs Anda muncul dan menampilkan daftar situs Anda.

3. Pilih tombol di sebelah situs yang ingin Anda kirim ulang emailnya.
4. Buka daftar Tindakan dan pilih Kirim ulang email undangan.

   Pesan sukses dalam spanduk hijau muncul di bagian atas halaman.

Mengelola otentikasi multifaktor

Anda dapat mengaktifkan otentikasi multi-faktor setelah membuat WorkDocs situs. Untuk informasi selengkapnya tentang otentikasi, lihatMengaktifkan autentikasi multi-faktor.

Mengatur situs URLs

> **Note**
>
> Jika Anda mengikuti proses pembuatan situsMemulai dengan WorkDocs, Anda memasukkan URL situs. Akibatnya, WorkDocs membuat perintah Setel URL situs tidak tersedia, karena Anda hanya dapat mengatur URL sekali. Anda hanya mengikuti langkah-langkah ini jika Anda menerapkan Amazon WorkSpaces dan mengintegrasikannya WorkDocs. Proses WorkSpaces integrasi Amazon meminta Anda memasukkan nomor seri alih-alih URL situs, jadi Anda harus memasukkan URL setelah Anda menyelesaikan integrasi. Untuk informasi selengkapnya tentang mengintegrasikan Amazon WorkSpaces dan WorkDocs lihat Mengintegrasikan dengan WorkDocs di Panduan WorkSpaces Pengguna Amazon.

Untuk menetapkan URL situs

1. Buka WorkDocs konsol di https://console.aws.amazon.com/zocalo/.
2. Di panel navigasi, pilih Situs saya.

   Halaman Kelola WorkDocs situs Anda muncul dan menampilkan daftar situs Anda.
3. Pilih situs yang Anda integrasikan dengan Amazon WorkSpaces. URL berisi ID direktori WorkSpaces instance Amazon Anda, seperti https://{directory_id}.awsapps.com.
4. Pilih tombol di sebelah URL tersebut, buka daftar Tindakan, dan pilih Setel URL situs.

   Kotak dialog Setel URL situs muncul.

5. Di kotak URL Situs, masukkan URL untuk situs, lalu pilih Tetapkan URL situs.
6. Pada halaman Kelola WorkDocs situs Anda, pilih Segarkan untuk melihat URL baru.

Mengelola notifikasi

> **Note**
>
> Untuk keamanan yang lebih besar, buat pengguna federasi alih-alih pengguna IAM bila memungkinkan.

Pemberitahuan memungkinkan pengguna atau peran IAM untuk memanggil CreateNotificationSubscriptionAPI, yang dapat Anda gunakan untuk mengatur titik akhir Anda sendiri untuk memproses pesan SNS yang dikirim. WorkDocs Untuk informasi selengkapnya tentang notifikasi, lihat Menyiapkan notifikasi untuk pengguna atau peran IAM di Panduan WorkDocs Pengembang.

Anda dapat membuat dan menghapus notifikasi, dan langkah-langkah berikut menjelaskan cara melakukan kedua tugas tersebut.

> **Note**
>
> Untuk membuat notifikasi, Anda harus memiliki IAM atau peran ARN Anda. Untuk menemukan ARN IAM Anda, lakukan hal berikut:
>
> 1. Buka konsol IAM di https://console.aws.amazon.com/iam/.
> 2. Di bilah navigasi, pilih Pengguna.
> 3. Pilih nama pengguna Anda.
> 4. Di bawah Ringkasan, salin ARN Anda.

Untuk membuat notifikasi

1. Buka WorkDocs konsol di https://console.aws.amazon.com/zocalo/.
2. Di panel navigasi, pilih Situs saya.

   Halaman Kelola WorkDocs situs Anda muncul dan menampilkan daftar situs Anda.

3. Pilih tombol di sebelah situs yang diinginkan.
4. Buka daftar Tindakan dan pilih Kelola pemberitahuan.

   Halaman Kelola pemberitahuan akan muncul.
5. Pilih Buat notifikasi.
6. Di kotak dialog Notifikasi baru, masukkan IAM atau ARN peran Anda, lalu pilih Buat pemberitahuan.

Untuk menghapus notifikasi

1. Buka WorkDocs konsol di https://console.aws.amazon.com/zocalo/.
2. Di panel navigasi, pilih Situs saya.

   Halaman Kelola WorkDocs situs Anda muncul dan menampilkan daftar situs Anda.
3. Pilih tombol di sebelah situs yang memiliki notifikasi yang ingin Anda hapus.
4. Buka daftar Tindakan dan pilih Kelola pemberitahuan.
5. Pada halaman Kelola pemberitahuan, pilih tombol di samping notifikasi yang ingin Anda hapus, lalu pilih Hapus pemberitahuan.

Menghapus situs

Anda menggunakan WorkDocs konsol untuk menghapus situs.

> **Warning**
>
> Anda kehilangan semua file ketika Anda menghapus situs. Hapus situs hanya jika Anda yakin bahwa informasi ini tidak lagi diperlukan.

Menghapus situs

1. Buka WorkDocs konsol di https://console.aws.amazon.com/zocalo/.
2. Di bilah navigasi, pilih Situs saya.

   Halaman Kelola WorkDocs situs Anda muncul.
3. Pilih tombol di sebelah situs yang ingin Anda hapus, lalu pilih Hapus.

Kotak dialog Hapus URL situs muncul.

4. Secara opsional, pilih Hapus juga direktori pengguna.

> **Important**
>
> Jika Anda tidak menyediakan direktori Anda sendiri WorkDocs, kami membuat satu untuk Anda. Ketika Anda menghapus WorkDocs situs, Anda dikenakan biaya untuk direktori yang kami buat kecuali Anda menghapus direktori itu atau menggunakannya untuk aplikasi AWS lain. Untuk informasi harga, lihat Harga AWS Directory Service.

5. Di kotak URL Situs, masukkan URL situs, lalu pilih Hapus.

Situs akan segera dihapus dan tidak lagi tersedia.

Mengelola WorkDocs dari panel kontrol admin situs

Anda menggunakan alat ini untuk mengelola WorkDocs situs Anda:

- Panel kontrol admin situs, tersedia untuk administrator di semua WorkDocs situs, dan dijelaskan dalam topik berikut.
- AWS Konsol di https://console.aws.amazon.com/zocalo/.

Masing-masing alat tersebut menyediakan serangkaian tindakan yang berbeda. Topik di bagian ini menjelaskan tindakan yang disediakan oleh panel kontrol admin situs. Untuk informasi tentang tugas yang tersedia di konsol, lihatMengelola WorkDocs dari AWS konsol.

Pengaturan bahasa pilihan

Anda dapat menentukan bahasa untuk pemberitahuan email.

Mengubah setelan bahasa

1. Di bawah Akun Saya, pilih Buka panel kontrol admin.
2. Untuk Pengaturan Bahasa Pilihan, pilih bahasa pilihan Anda.

Hancom Pengeditan Online dan Office Online

Mengaktifkan atau menonaktifkan pengaturan Hancom Pengeditan Online dan Office Online dari Panel kontrol admin. Untuk informasi selengkapnya, lihat Mengaktifkan pengeditan kolaboratif.

Penyimpanan

Tentukan jumlah penyimpanan yang diterima pengguna baru.

Mengubah setelan penyimpanan

1. Di bawah Akun Saya, pilih Buka panel kontrol admin.
2. Untuk Penyimpanan, pilih Perubahan.
3. Di kotak dialog Batas Penyimpanan, pilih apakah akan memberikan pengguna baru penyimpanan tidak terbatas atau terbatas.

4. Pilih Simpan Perubahan.

Mengubah pengaturan penyimpanan hanya memengaruhi pengguna yang ditambahkan setelah pengaturan berubah. Perubahan tersebut tidak mengubah jumlah penyimpanan yang dialokasikan untuk pengguna yang ada. Untuk mengubah batas penyimpanan untuk pengguna yang ada, lihat Mengedit pengguna.

Daftar IP diizinkan

WorkDocs administrator situs dapat menambahkan pengaturan IP Izinkan Daftar untuk membatasi akses situs ke rentang alamat IP yang diizinkan. Anda dapat menambahkan hingga 500 pengaturan IP Allow List per situs.

> **Note**
>
> Daftar Izinkan IP saat ini hanya berfungsi untuk IPv4 alamat. Daftar penolakan alamat IP saat ini tidak didukung.

Untuk menambahkan rentang IP ke Daftar IP Diizinkan

1. Di bawah Akun Saya, pilih Buka panel kontrol admin.
2. Untuk Daftar IP Diizinkan, pilih Perubahan.
3. Untuk Masukkan nilai CIDR, masukkan blok Classless Inter-Domain Routing (CIDR) untuk rentang alamat IP, dan pilih Tambah.
   - Untuk mengizinkan akses dari alamat IP tunggal, tentukan `/32` sebagai awalan CIDR.
4. Pilih Simpan Perubahan.
5. Pengguna yang terhubung ke situs Anda dari alamat IP pada Daftar IP Diizinkan memiliki akses. Pengguna yang mencoba terhubung ke situs Anda dari alamat IP yang tidak sah menerima respons yang tidak sah.

> **Warning**
>
> Jika Anda memasukkan nilai CIDR yang membatasi Anda menggunakan alamat IP saat ini untuk mengakses situs, pesan peringatan akan muncul. Jika Anda memilih untuk melanjutkan

dengan nilai CIDR saat ini, akses Anda ke situs dengan alamat IP Anda saat ini akan diblokir. Tindakan ini hanya dapat dibatalkan dengan menghubungi AWS Support.

Keamanan — ActiveDirectory Situs sederhana

Topik ini menjelaskan berbagai pengaturan keamanan untuk ActiveDirectory situs Sederhana. Jika Anda mengelola situs yang menggunakan ActiveDirectory konektor, lihat bagian selanjutnya.

Untuk menggunakan pengaturan keamanan

1. Pilih ikon profil di sudut kanan atas klien. WorkDocs

2. Di bawah Admin, pilih Buka panel kontrol admin.
3. Gulir turun ke Keamanan dan pilih Ubah.

   Kotak dialog Pengaturan Kebijakan akan muncul. Tabel berikut mencantumkan pengaturan keamanan untuk ActiveDirectory situs Sederhana.

Pengaturan	Deskripsi
Di bawah Pilih setelan Anda untuk tautan yang dapat dibagikan, pilih salah satu dari berikut ini:	
Jangan izinkan tautan di seluruh situs atau publik yang dapat dibagikan	Menonaktifkan berbagi tautan untuk semua pengguna.
Izinkan pengguna membuat tautan yang dapat dibagikan di seluruh situs, tetapi jangan izinkan mereka membuat tautan yang dapat dibagikan publik	Membatasi berbagi tautan hanya untuk anggota situs. Pengguna yang dikelola dapat membuat jenis tautan ini.
Memungkinkan pengguna membuat tautan yang dapat dibagikan di seluruh situs, tetapi hanya pengguna yang dapat membuat tautan publik yang dapat dibagikan	Pengguna yang dikelola dapat membuat tautan di seluruh situs, tetapi hanya pengguna yang dapat membuat tautan

Pengaturan	Deskripsi
	publik. Tautan publik memungkinkan akses ke siapa pun di internet.
Semua pengguna yang dikelola dapat membuat tautan di seluruh situs & publik yang dapat dibagikan	Pengguna yang dikelola dapat membuat tautan publik.

Di bawah Aktivasi otomatis, pilih atau kosongkan kotak centang.

Izinkan semua pengguna di direktori Anda diaktifkan secara otomatis saat login pertama mereka ke WorkDocs situs Anda.	Secara otomatis mengaktifkan pengguna ketika mereka pertama kali masuk ke situs Anda.

Di bawah Siapa yang diizinkan mengundang pengguna baru ke WorkDocs situs Anda, pilih salah satu dari berikut ini:

Hanya administrator yang dapat mengundang pengguna baru.	Hanya administrator yang dapat mengundang pengguna baru.
Pengguna dapat mengundang pengguna baru dari mana saja dengan berbagi file atau folder dengan mereka.	Memungkinkan pengguna untuk mengundang pengguna baru dengan berbagi file atau folder dengan pengguna tersebut.
Pengguna dapat mengundang pengguna baru dari beberapa domain tertentu dengan berbagi file atau folder dengan mereka.	Pengguna dapat mengundang orang baru dari domain yang ditentukan dengan berbagi file atau folder dengan mereka.

Di bawah Konfigurasi peran untuk pengguna baru, pilih atau kosongkan kotak centang.

Pengguna baru dari direktori Anda akan menjadi pengguna yang dikelola (mereka adalah pengguna Tamu secara default)	Secara otomatis mengonversi pengguna baru dari direktori Anda menjadi pengguna terkelola.

4. Setelah selesai, pilih Simpan Perubahan.

Keamanan - situs ActiveDirectory konektor

Topik ini menjelaskan berbagai pengaturan keamanan untuk situs ActiveDirectory konektor. Jika Anda mengelola situs yang menggunakan Simple ActiveDirectory, lihat bagian sebelumnya.

Untuk menggunakan pengaturan keamanan

1. Pilih ikon profil di sudut kanan atas klien. WorkDocs

2. Di bawah Admin, pilih Buka panel kontrol admin.
3. Gulir turun ke Keamanan dan pilih Ubah.

   Kotak dialog Pengaturan Kebijakan akan muncul. Tabel berikut mencantumkan dan menjelaskan pengaturan keamanan untuk situs ActiveDirectory konektor.

Pengaturan	Deskripsi
Di bawah Pilih setelan Anda untuk tautan yang dapat dibagikan, pilih salah satu dari berikut ini:	
Jangan izinkan tautan di seluruh situs atau publik yang dapat dibagikan	Saat dipilih, menonaktifkan berbagi tautan untuk semua pengguna.
Izinkan pengguna membuat tautan yang dapat dibagikan di seluruh situs, tetapi jangan izinkan mereka membuat tautan yang dapat dibagikan publik	Membatasi berbagi tautan hanya untuk anggota situs. Pengguna yang dikelola dapat membuat jenis tautan ini.
Memungkinkan pengguna membuat tautan yang dapat dibagikan di seluruh situs, tetapi hanya pengguna yang dapat membuat tautan publik yang dapat dibagikan	Pengguna yang dikelola dapat membuat tautan di seluruh situs, tetapi hanya pengguna yang dapat membuat tautan publik. Tautan publik memungkinkan akses ke siapa pun di internet.

Pengaturan	Deskripsi
Semua pengguna yang dikelola dapat membuat tautan di seluruh situs & publik yang dapat dibagikan	Pengguna yang dikelola dapat membuat tautan publik.

Di bawah Aktivasi otomatis, pilih atau kosongkan kotak centang.

Izinkan semua pengguna di direktori Anda diaktifkan secara otomatis saat login pertama mereka ke WorkDocs situs Anda.	Secara otomatis mengaktifkan pengguna ketika mereka pertama kali masuk ke situs Anda.

Di bawah Siapa yang harus diizinkan untuk mengaktifkan pengguna direktori di WorkDocs situs Anda? , pilih salah satu dari berikut ini:

Hanya administrator yang dapat mengaktif kan pengguna baru dari direktori Anda.	Hanya mengizinkan administrator untuk mengaktifkan pengguna direktori baru.
Pengguna dapat mengaktifkan pengguna baru dari direktori Anda dengan berbagi file atau folder dengan mereka.	Memungkinkan pengguna untuk mengaktif kan pengguna direktori dengan berbagi file atau folder dengan pengguna direktori.
Pengguna dapat mengaktifkan pengguna baru dari beberapa domain tertentu dengan berbagi file atau folder dengan mereka.	Pengguna hanya dapat berbagi file atau folder dari pengguna di domain tertentu. Ketika Anda memilih opsi ini, Anda harus memasukkan domain.

Di bawah Siapa yang harus diizinkan mengundang pengguna baru ke WorkDocs situs Anda? , pilih salah satu dari berikut ini:

Berbagi dengan pengguna eksternal **Note** Opsi di bawah ini hanya muncul setelah Anda memilih pengaturan ini.	Memungkinkan administrator dan pengguna untuk mengundang pengguna eksternal baru ke WorkDocs situs Anda.
Hanya administrator yang dapat mengundan g pengguna eksternal baru	Hanya administrator yang dapat mengundan g pengguna eksternal.

Pengaturan	Deskripsi
Semua pengguna terkelola dapat mengundang pengguna baru	Memungkinkan pengguna terkelola untuk mengundang pengguna eksternal.
Hanya pengguna daya yang dapat mengundang pengguna eksternal baru.	Memungkinkan hanya pengguna daya untuk mengundang pengguna eksternal baru.

Di bawah Konfigurasi peran untuk pengguna baru, pilih salah satu atau kedua opsi.

Pengguna baru dari direktori Anda akan menjadi pengguna yang dikelola (mereka adalah pengguna Tamu secara default)	Secara otomatis mengonversi pengguna baru dari direktori Anda menjadi pengguna terkelola.
Pengguna eksternal baru akan menjadi pengguna yang Dikelola (mereka adalah pengguna Tamu secara default)	Secara otomatis mengubah pengguna eksternal baru menjadi pengguna terkelola.

4. Setelah selesai, pilih Simpan Perubahan.

Penyimpanan kotak pemulihan

Ketika pengguna menghapus file, WorkDocs menyimpan file di recycle bin pengguna selama 30 hari. Setelah itu WorkDocs , pindahkan file ke tempat pemulihan sementara selama 60 hari, lalu hapus secara permanen. Hanya administrator yang dapat melihat tempat pemulihan sementara. Dengan mengubah kebijakan penyimpanan data di seluruh situs, administrator situs dapat mengubah periode retensi bin pemulihan menjadi minimum nol hari dan maksimum 365.

Mengubah periode penyimpanan kotak pemulihan

1. Di bawah Akun Saya, pilih Buka panel kontrol admin.
2. Di samping Penyimpanan kotak pemulihan, pilih Perubahan.
3. Masukkan jumlah hari untuk menyimpan file di tempat pemulihan, dan pilih Simpan.

> **Note**
>
> Periode penyimpanan default adalah 60 hari. Anda dapat menggunakan jangka waktu 0-365 hari.

Administrator dapat memulihkan file pengguna dari tempat pemulihan sebelum WorkDocs menghapusnya secara permanen.

Memulihkan file pengguna

1. Di bawah Akun Saya, pilih Buka panel kontrol admin.
2. Di bawah Kelola Pengguna, pilih ikon folder pengguna.
3. Di bawah Kotak pemulihan, pilih file yang akan dipulihkan, lalu pilih ikon Memulihkan.
4. Untuk Pemulihan file, pilih lokasi tempat untuk memulihkan file, lalu pilih Pemulihan.

Mengelola pengaturan pengguna

Anda dapat mengelola pengaturan untuk pengguna, termasuk mengubah peran pengguna dan mengundang, mengaktifkan, atau menonaktifkan pengguna. Lihat informasi yang lebih lengkap di Mengundang dan mengelola pengguna WorkDocs .

Menyebarkan WorkDocs Drive ke beberapa komputer

Jika Anda memiliki armada mesin yang bergabung dengan domain, Anda dapat menggunakan Objek Kebijakan Grup (GPO) atau Manajer Konfigurasi Pusat Sistem (SCCM) untuk menginstal klien Drive. WorkDocs Anda dapat mengunduh klien dari https://amazonworkdocs.com/en/klien.

Saat Anda pergi, ingatlah bahwa WorkDocs Drive memerlukan akses HTTPS pada port 443 untuk semua alamat IP AWS. Anda juga ingin mengonfirmasi bahwa sistem target Anda memenuhi persyaratan penginstalan untuk WorkDocs Drive. Untuk informasi selengkapnya, lihat Menginstal WorkDocs Drive di Panduan WorkDocs Pengguna Amazon.

> **Note**
>
> Sebagai praktik terbaik saat menggunakan GPO atau SCCM, instal klien WorkDocs Drive setelah pengguna masuk.

Penginstal MSI untuk WorkDocs Drive mendukung parameter instalasi opsional berikut:

- **`SITEID`**— Pra-mengisi informasi WorkDocs situs untuk pengguna selama pendaftaran. Misalnya, `SITEID=`*`site-name`*.
- **`DefaultDriveLetter`**- Pra-mengisi huruf drive yang akan digunakan untuk pemasangan WorkDocs Drive. Misalnya, `DefaultDriveLetter=`*`W`*. Ingat, setiap pengguna harus memiliki huruf drive yang berbeda. Selain itu, pengguna dapat mengubah nama drive, tetapi bukan huruf drive, setelah mereka memulai WorkDocs Drive untuk pertama kalinya.

Contoh berikut menyebarkan WorkDocs Drive tanpa antarmuka pengguna dan tidak ada restart. Perhatikan bahwa contoh tersebut menggunakan nama default file MSI:

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

Mengundang dan mengelola pengguna WorkDocs

Secara default, saat Anda melampirkan direktori selama pembuatan situs, fitur Aktivasi otomatis WorkDocs menambahkan semua pengguna di direktori itu ke situs baru sebagai pengguna terkelola.

Di WorkDocs, pengguna terkelola tidak perlu masuk dengan kredenal terpisah. Mereka dapat berbagi dan berkolaborasi pada file, dan mereka secara otomatis memiliki 1 TB penyimpanan. Namun, Anda dapat menonaktifkan Aktivasi otomatis ketika Anda hanya ingin menambahkan beberapa pengguna dalam direktori, dan langkah-langkah di bagian berikutnya menjelaskan cara melakukannya.

Selain itu, Anda dapat mengundang, mengaktifkan, atau menonaktifkan pengguna, serta mengubah peran dan pengaturan pengguna. Anda juga dapat mempromosikan pengguna menjadi administrator. Untuk informasi lebih lanjut tentang mempromosikan pengguna, lihat Mempromosikan pengguna ke administrator.

Anda melakukan tugas-tugas tersebut di panel kontrol admin di klien WorkDocs web, dan langkah-langkah di bagian berikut menjelaskan caranya. Namun, jika Anda baru mengenal WorkDocs, luangkan waktu beberapa menit dan pelajari tentang berbagai peran pengguna sebelum Anda menyelami tugas administratif.

Daftar Isi

Gambaran umum peran pengguna

WorkDocs mendefinisikan peran pengguna berikut. Anda dapat mengubah peran pengguna dengan mengedit profil pengguna mereka. Untuk informasi lebih lanjut, lihat Mengedit pengguna.

- Admin: Pengguna berbayar yang memiliki izin administratif untuk seluruh situs, termasuk manajemen pengguna dan konfigurasi pengaturan situs. Untuk informasi selengkapnya tentang cara mempromosikan pengguna menjadi administrator, lihat Mempromosikan pengguna ke administrator.
- Pengguna daya: Pengguna berbayar yang memiliki serangkaian izin khusus dari administrator. Untuk informasi selengkapnya tentang cara menyetel izin untuk pengguna daya, lihat Keamanan — ActiveDirectory Situs sederhana danKeamanan - situs ActiveDirectory konektor.
- Pengguna: Pengguna berbayar yang dapat menyimpan file dan berkolaborasi dengan orang lain di WorkDocs situs.
- Pengguna tamu: Pengguna non-berbayar yang hanya dapat melihat file. Anda dapat meningkatkan Pengguna tamu menjadi peran Pengguna, Power user, atau Administrator.

> **Note**
>
> Bila Anda mengubah peran pengguna tamu, Anda melakukan tindakan satu kali yang tidak dapat dibatalkan.

WorkDocs juga mendefinisikan jenis pengguna tambahan ini.

Pengguna WS

Seorang pengguna dengan yang ditugaskan WorkSpaces WorkSpace.

- Akses ke semua WorkDocs fitur
- Penyimpanan default sebesar 50 GB (dapat membayar untuk meningkatkan ke 1 TB)
- Tidak ada biaya bulanan

Pengguna WS yang ditingkatkan

Pengguna dengan penyimpanan yang ditetapkan WorkSpaces WorkSpace dan ditingkatkan.

- Akses ke semua WorkDocs fitur

- Penyimpanan default 1 TB (penyimpanan tambahan tersedia berdasarkan pay-as-you-go basis)
- Biaya bulanan berlaku

WorkDocs pengguna

WorkDocs Pengguna aktif tanpa ditugaskan WorkSpaces WorkSpace.

- Akses ke semua WorkDocs fitur
- Penyimpanan default 1 TB (penyimpanan tambahan tersedia berdasarkan pay-as-you-go basis)
- Biaya bulanan berlaku

Memulai panel kontrol admin

Anda menggunakan panel kontrol administratif di klien WorkDocs web untuk mematikan dan mengaktifkan Aktivasi otomatis, dan mengubah peran dan pengaturan pengguna.

Untuk membuka panel kontrol admin

1. Pilih ikon profil di sudut kanan atas klien. WorkDocs

2. Di bawah Admin, pilih Buka panel kontrol admin.

> **Note**
>
> Beberapa opsi panel kontrol berbeda antara direktori cloud dan direktori yang terhubung.

Menonaktifkan Aktivasi otomatis

Anda menonaktifkan Aktivasi otomatis ketika Anda tidak ingin menambahkan semua pengguna dalam direktori ke situs baru, dan ketika Anda ingin mengatur izin dan peran yang berbeda untuk pengguna yang Anda undang ke situs baru. Saat Anda menonaktifkan Aktivasi otomatis, Anda juga dapat memutuskan siapa yang memiliki kemampuan untuk mengundang pengguna baru ke situs

— pengguna saat ini, pengguna daya, atau administrator. Langkah-langkah ini menjelaskan cara melakukan kedua tugas tersebut.

Untuk menonaktifkan Aktivasi otomatis

1. Pilih ikon profil di sudut kanan atas klien. WorkDocs

2. Di bawah Admin, pilih Buka panel kontrol admin.
3. Gulir turun ke Keamanan dan pilih Ubah.

   Kotak dialog Pengaturan Kebijakan akan muncul.
4. Di bawah Aktivasi otomatis, kosongkan kotak centang di samping Izinkan semua pengguna di direktori Anda diaktifkan secara otomatis saat login pertama mereka ke WorkDocs situs Anda.

   Opsi berubah di bawah Siapa yang harus diizinkan untuk mengaktifkan pengguna direktori di WorkDocs situs Anda. Anda dapat membiarkan pengguna saat ini mengundang pengguna baru, atau Anda dapat memberikan kemampuan tersebut kepada power user atau administrator lainnya.
5. Pilih salah satu opsi, lalu pilih Simpan Perubahan.

Ulangi langkah 1-4 untuk mengaktifkan kembali Aktivasi otomatis.

Mengelola berbagi tautan

Topik ini menjelaskan cara mengelola berbagi tautan. WorkDocs pengguna dapat berbagi file dan folder mereka dengan berbagi tautan ke mereka. Mereka dapat berbagi tautan file di dalam dan di luar organisasi Anda, tetapi mereka hanya dapat berbagi tautan folder secara internal. Sebagai administrator, Anda mengelola siapa yang dapat berbagi tautan.

Untuk mengaktifkan berbagi tautan

1. Pilih ikon profil di sudut kanan atas klien. WorkDocs

2. Di bawah Admin, pilih Buka panel kontrol admin.
3. Gulir turun ke Keamanan dan pilih Ubah.

   Kotak dialog Pengaturan Kebijakan akan muncul.
4. Di bawah Pilih setelan Anda untuk tautan yang dapat dibagikan, pilih opsi:

   - Jangan izinkan tautan di seluruh situs atau publik yang dapat dibagikan - Menonaktifkan berbagi tautan untuk semua pengguna.
   - Izinkan pengguna membuat tautan yang dapat dibagikan di seluruh situs, tetapi jangan izinkan mereka membuat tautan yang dapat dibagikan publik — Batasi berbagi tautan hanya untuk anggota situs. Pengguna yang dikelola dapat membuat jenis tautan ini.
   - Izinkan pengguna membuat tautan yang dapat dibagikan di seluruh situs, tetapi hanya pengguna yang dapat membuat tautan yang dapat dibagikan publik - Pengguna yang dikelola dapat membuat tautan di seluruh situs, tetapi hanya pengguna yang dapat membuat tautan publik. Tautan publik memungkinkan akses ke siapa pun di internet.
   - Semua pengguna terkelola dapat membuat tautan di seluruh situs & dapat dibagikan publik - Pengguna yang dikelola dapat membuat tautan publik.
5. Pilih Simpan Perubahan.

Mengontrol undangan pengguna dengan Aktivasi otomatis diaktifkan

Saat Anda mengaktifkan Aktivasi otomatis—dan ingat, aktif secara default—Anda dapat memberi pengguna kemampuan untuk mengundang pengguna lain. Anda dapat memberikan izin kepada salah satu dari yang berikut:

- Semua pengguna
- Power user
- Administrator.

Anda juga dapat menonaktifkan izin sepenuhnya, dan langkah-langkah ini menjelaskan caranya.

Untuk mengatur izin undangan

1. Pilih ikon profil di sudut kanan atas klien. WorkDocs

2. Di bawah Admin, pilih Buka panel kontrol admin.
3. Gulir turun ke Keamanan dan pilih Ubah.

   Kotak dialog Pengaturan Kebijakan akan muncul.
4. Di bawah Siapa yang harus diizinkan untuk mengaktifkan pengguna direktori di WorkDocs situs Anda, pilih kotak centang Bagikan dengan pengguna eksternal, pilih salah satu opsi di bawah kotak centang, lalu pilih Simpan Perubahan.

   —ATAU—

   Kosongkan kotak centang jika Anda tidak ingin orang lain mengundang pengguna baru, lalu pilih Simpan Perubahan.

Mengundang pengguna baru

Anda dapat mengundang pengguna baru untuk bergabung dengan direktori. Anda juga dapat mengaktifkan pengguna yang ada untuk mengundang pengguna baru. Untuk informasi lebih lanjut, lihat Keamanan — ActiveDirectory Situs sederhana dan Keamanan - situs ActiveDirectory konektor di panduan ini.

Untuk mengundang pengguna baru

1. Pilih ikon profil di sudut kanan atas klien. WorkDocs

2. Di bawah Admin, pilih Buka panel kontrol admin.
3. Di bawah Kelola Pengguna, pilih Undang Pengguna.
4. Di kotak dialog Undang Pengguna, pada bagian Siapa yang ingin Anda undang?, masukkan alamat email undangan, lalu pilih Kirim. Ulangi langkah ini untuk setiap undangan.

WorkDocs mengirimkan email undangan ke setiap penerima. Surat berisi tautan dan instruksi tentang cara membuat WorkDocs akun. Tautan undangan berakhir setelah 30 hari.

Mengedit pengguna

Anda dapat mengubah informasi dan pengaturan pengguna.

Untuk mengedit pengguna

1. Pilih ikon profil di sudut kanan atas klien. WorkDocs

2. Di bawah Admin, pilih Buka panel kontrol admin.
3. Di bawah Kelola pengguna, pilih ikon pensil
(✎)
di sebelah nama pengguna.
4. Di kotak dialog Edit Pengguna, Anda dapat mengedit opsi berikut:

   Nama Depan (Hanya Cloud Directory)

   Nama depan pengguna.

   Nama Belakang (Hanya Cloud Directory)

   Nama belakang pengguna.

   Status

   Menentukan apakah pengguna Aktif atau Tidak Aktif. Untuk informasi lebih lanjut, lihat Menonaktifkan pengguna.

   Peran

   Menentukan apakah seseorang adalah pengguna atau administrator. Anda juga dapat memutakhirkan atau menurunkan versi pengguna yang telah WorkSpaces WorkSpace ditetapkan untuk mereka. Untuk informasi selengkapnya, lihat Gambaran umum peran pengguna.

   Penyimpanan

   Menentukan batas penyimpanan untuk pengguna yang ada.
5. Pilih Simpan Perubahan.

Menonaktifkan pengguna

Anda menonaktifkan akses pengguna dengan mengubah status mereka menjadi Tidak Aktif.

Untuk mengubah status pengguna menjadi Tidak Aktif

1. Pilih ikon profil di sudut kanan atas klien. WorkDocs

2. Di bawah Admin, pilih Buka panel kontrol admin.
3. Di bawah Kelola pengguna, pilih ikon pensil
   ( )
   di sebelah nama pengguna.
4. Pilih Aktifkan, dan pilih Simpan Perubahan

Pengguna yang tidak aktif tidak dapat mengakses WorkDocs situs Anda.

> **Note**
>
> Mengubah pengguna ke status Tidak Aktif tidak menghapus file, folder, atau umpan balik dari WorkDocs situs Anda. Namun, Anda dapat mentransfer file dan folder pengguna yang tidak aktif ke pengguna yang aktif. Untuk informasi selengkapnya, lihat Mentransfer kepemilikan dokumen.

Menghapus pengguna yang tertunda

Anda dapat menghapus pengguna Simple AD, AWS Managed Microsoft, dan AD Connector dalam status Pending. Untuk menghapus salah satu pengguna tersebut, pilih ikon tong sampah
( )
di sebelah nama pengguna.

WorkDocs Situs Anda harus selalu memiliki setidaknya satu pengguna aktif yang bukan pengguna tamu. Jika Anda perlu menghapus semua pengguna, hapus seluruh situs.

Kami tidak menyarankan Anda menghapus pengguna terdaftar. Sebagai gantinya, Anda harus mengalihkan pengguna dari status Aktif ke Tidak Aktif untuk mencegah mereka mengakses situs Anda WorkDocs .

Mentransfer kepemilikan dokumen

Anda dapat mentransfer file dan folder pengguna yang tidak aktif ke pengguna yang aktif. Untuk informasi selengkapnya tentang cara menonaktifkan pengguna, lihat Menonaktifkan pengguna.

> **Warning**
>
> Anda tidak dapat membatalkan tindakan ini.

Untuk mentransfer kepemilikan dokumen

1. Pilih ikon profil di sudut kanan atas klien. WorkDocs

2. Di bawah Admin, pilih Buka panel kontrol admin.
3. Di bawah Kelola Pengguna, cari pengguna yang tidak aktif.
4. Pilih ikon pensil
   (✎)
   di sebelah nama pengguna yang tidak aktif.
5. Pilih Transfer Kepemilikan Dokumen lalu masukkan alamat email pemilik baru.
6. Pilih Simpan Perubahan.

Mengunduh daftar pengguna

Untuk mengunduh daftar pengguna dari panel kontrol Admin, Anda harus menginstal WorkDocs Companion. Untuk menginstal WorkDocs Companion, lihat Aplikasi & Integrasi untuk WorkDocs.

Untuk mengunduh daftar pengguna

1. Pilih ikon profil di sudut kanan atas klien. WorkDocs

2. Di bawah Admin, pilih Buka panel kontrol admin.
3. Di bawah Kelola pengguna, pilih Unduh pengguna.
4. Pada Unduh pengguna, pilih salah satu opsi berikut untuk mengekspor daftar pengguna sebagai file `.json` ke desktop Anda:

   - Semua pengguna
   - Pengguna tamu
   - Pengguna WS
   - Pengguna
   - Power user
   - Admin
5. WorkDocs menyimpan file ke salah satu lokasi berikut:

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

   > **Note**
   >
   > Pengunduhan mungkin memakan waktu lama. Selain itu, file yang diunduh tidak masuk ke folder `/~users` Anda.

Untuk informasi selengkapnya tentang peran pengguna ini, lihat Gambaran umum peran pengguna.

Berbagi dan berkolaborasi

Pengguna Anda dapat berbagi konten dengan mengirimkan tautan atau undangan. Pengguna juga dapat berkolaborasi dengan pengguna eksternal jika Anda mengaktifkan berbagi eksternal.

WorkDocs mengontrol akses ke folder dan file melalui penggunaan izin. Sistem menerapkan izin berdasarkan peran pengguna.

Daftar Isi

Berbagi tautan

Pengguna dapat memilih Bagikan tautan untuk menyalin dan membagikan hyperlink dengan cepat untuk WorkDocs konten dengan rekan kerja dan pengguna eksternal baik di dalam maupun di luar organisasi mereka. Ketika pengguna berbagi tautan, mereka dapat mengonfigurasinya untuk mengizinkan salah satu opsi akses berikut:

- Semua anggota WorkDocs situs dapat mencari, melihat, dan mengomentari file tersebut.
- Siapa pun yang memiliki tautan, bahkan orang yang bukan anggota WorkDocs situs, dapat melihat file tersebut. Opsi link ini membatasi izin untuk hanya melihat file.

Penerima dengan izin hanya lihat hanya dapat melihat file. Izin mengomentari memungkinkan pengguna untuk berkomentar dan memperbarui atau menghapus operasi, seperti mengunggah file baru atau menghapus file yang ada.

Secara default, semua pengguna yang dikelola dapat membuat tautan publik. Untuk mengubah pengaturan ini, perbarui Keamanan dari panel kontrol admin Anda. Untuk informasi selengkapnya, lihat Mengelola WorkDocs dari panel kontrol admin situs.

Berbagi dengan undangan

Ketika Anda mengaktifkan berbagi dengan undangan, pengguna situs Anda dapat berbagi file atau folder dengan pengguna individu, dan dengan grup, dengan mengirim email undangan. Undangan berisi tautan ke konten bersama, dan undangan dapat membuka file atau folder bersama. Para undangan juga dapat berbagi file atau folder tersebut dengan anggota situs lain, dan dengan pengguna eksternal.

Anda dapat mengatur tingkat izin untuk setiap pengguna yang diundang. Anda juga dapat membuat folder tim untuk dibagikan dengan mengundang grup direktori yang Anda buat.

> **Note**
>
> Berbagi undangan tidak termasuk anggota grup bersarang. Untuk menyertakan anggota tersebut, Anda harus menambahkannya ke daftar Bagikan berdasarkan Undangan.

Untuk informasi selengkapnya, lihat Mengelola WorkDocs dari panel kontrol admin situs.

Berbagi eksternal

Berbagi eksternal memungkinkan pengguna WorkDocs situs yang dikelola untuk berbagi file dan folder, dan berkolaborasi dengan pengguna eksternal tanpa menimbulkan biaya tambahan. Pengguna situs dapat berbagi file dan folder dengan pengguna eksternal tanpa mengharuskan penerima untuk menjadi pengguna WorkDocs situs berbayar. Saat Anda mengaktifkan berbagi eksternal, pengguna dapat memasukkan alamat email pengguna eksternal yang ingin mereka bagikan dan menetapkan izin berbagi penampil yang sesuai. Ketika pengguna eksternal ditambahkan, izin dibatasi hanya untuk pemirsa, dan izin lainnya tidak tersedia. Pengguna eksternal menerima notifikasi email dengan tautan ke file atau folder yang dibagikan. Memilih tautan akan membawa pengguna eksternal ke situs, tempat mereka memasukkan kredensialnya untuk masuk. WorkDocs Mereka dapat melihat file atau folder yang dibagikan di tampilan Dibagikan dengan saya.

Pemilik file dapat mengubah izin berbagi atau menghapus akses untuk pengguna eksternal dari file atau folder kapan saja. Berbagi eksternal untuk situs harus diaktifkan oleh administrator situs agar pengguna terkelola bisa berbagi konten dengan pengguna eksternal. Untuk Pengguna tamu agar bisa menjadi kontributor atau pemilik bersama, mereka harus ditingkatkan ke tingkat Pengguna oleh administrator situs. Untuk informasi lebih lanjut, lihat Gambaran umum peran pengguna.

Secara default, berbagi eksternal diaktifkan dan semua pengguna dapat mengundang pengguna eksternal. Untuk mengubah pengaturan ini, perbarui Keamanan dari panel kontrol admin Anda. Untuk informasi selengkapnya, lihat Mengelola WorkDocs dari panel kontrol admin situs.

Izin

WorkDocs menggunakan izin untuk mengontrol akses ke folder dan file. Izin diterapkan berdasarkan peran pengguna.

Daftar Isi

Peran pengguna

Peran pengguna mengontrol folder dan izin file. Anda dapat menerapkan peran pengguna berikut di tingkat folder:

- Pemilik folder — Pemilik folder atau file.
- Pemilik bersama folder — Pengguna atau grup yang ditunjuk pemilik sebagai pemilik bersama folder atau file.
- Kontributor folder — Seseorang dengan akses tak terbatas ke folder.
- Penampil folder — Seseorang dengan akses terbatas (izin hanya-baca) ke folder.

Anda dapat menerapkan peran pengguna berikut di tingkat file individual:

- Pemilik — Pemilik file.
- Pemilik bersama — Pengguna atau grup yang ditunjuk pemilik sebagai pemilik bersama file.
- Kontributor* — Seseorang diizinkan untuk memberikan umpan balik pada file.
- Penampil — Seseorang dengan akses terbatas (hanya baca dan lihat izin aktivitas) ke file.
- Penampil anonim — Pengguna yang tidak terdaftar di luar organisasi yang dapat melihat file yang telah dibagikan menggunakan tautan tampilan eksternal. Kecuali dinyatakan lain, penampil

anonim memiliki izin hanya-baca yang sama dengan penampil. Pemirsa anonim tidak dapat melihat aktivitas file.

* Kontributor tidak dapat mengganti nama versi file yang ada. Namun, mereka dapat mengunggah versi baru file dengan nama yang berbeda.

Izin untuk folder yang dibagikan

Izin berikut berlaku untuk peran pengguna untuk folder bersama:

> **Note**
>
> Izin yang diterapkan untuk folder juga berlaku untuk sub-folder dan file di folder itu.

- Lihat - Lihat isi folder bersama.
- Lihat sub-folder - Lihat sub-folder.
- Lihat berbagi - Lihat pengguna lain folder yang dibagikan.
- Unduh folder - Unduh folder.
- Tambahkan sub-folder - Tambahkan sub-folder.
- Bagikan - Bagikan folder tingkat atas dengan pengguna lain.
- Cabut berbagi - Cabut berbagi folder tingkat atas.
- Hapus sub-folder - Hapus sub-folder.
- Hapus folder tingkat atas - Hapus folder bersama tingkat atas.

	Tayang	Lihat sub-folder	Lihat saham	Unduh folder	Tambahkan sub-folder	Bagikan	Cabut saham	Hapus sub-folder	Hapus folder tingkat atas
Pemilik folder	✓	✓	✓	✓	✓	✓	✓	✓	✓

	Tayang	Lihat sub-folder	Lihat saham	Unduh folder	Tambahkan sub-folder	Bagikan	Cabut saham	Hapus sub-folder	Hapus folder tingkat atas
Pemilik bersama folder	✓	✓	✓	✓	✓	✓	✓	✓	✓
Kontributor folder	✓	✓	✓	✓	✓				
Penampi folder	✓	✓	✓	✓					

Izin untuk file di folder bersama

Izin berikut berlaku untuk peran pengguna untuk file dalam folder bersama:

- Anotasi - Tambahkan umpan balik ke file.
- Hapus - Hapus file di folder bersama.
- Ganti nama - Ganti nama file.
- Unggah - Unggah versi baru file.
- Unduh - Unduh file. Ini adalah izin default. Anda dapat menggunakan properti file untuk mengizinkan atau menolak kemampuan mengunduh file bersama.
- Mencegah pengunduhan - Mencegah file diunduh.

> **Note**
>
> - Saat Anda memilih opsi ini, pengguna dengan izin Lihat masih dapat mengunduh file. Untuk mencegahnya, buka folder bersama dan hapus pengaturan Izinkan Unduhan untuk setiap file yang tidak ingin Anda unduh oleh pengguna tersebut.
> - Ketika pemilik atau pemilik bersama MP4 file melarang unduhan untuk file tersebut, kontributor dan pemirsa tidak dapat memutarnya di klien web Amazon. WorkDocs

- Bagikan — Bagikan file dengan pengguna lain.
- Mencabut berbagi - Mencabut berbagi file.
- Lihat - Lihat file di folder bersama.
- Lihat berbagi - Lihat pengguna lain yang berbagi file.
- Lihat anotasi - Lihat umpan balik dari pengguna lain.
- Lihat aktivitas - Melihat riwayat aktivitas file.
- Lihat versi - Lihat versi file sebelumnya.
- Hapus versi — Hapus satu atau beberapa versi file.
- Memulihkan versi - Memulihkan satu atau lebih versi file yang dihapus.
- Lihat semua komentar pribadi - Pemilik/pemilik bersama dapat melihat semua komentar pribadi untuk dokumen, bahkan jika mereka bukan balasan atas komentar mereka.

	Buat Anotasi	Hapus	Ubah Nama	Unggah	Unduh	Mencegah pengunduhan	Bagikan	Cabut saham	Tayang	Lihat saham	Lihat anotasi	Lihat aktivitas	Lihat versi	Hapus versi	Pulihkan versi	Lihat semua komentar pribadi**
Pem file*	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Pem folde	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Pem bers folde	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Kont or folde	✓			✓	✓				✓	✓	✓	✓	✓			
Pena folde					✓				✓	✓		✓				

	Buat Anotasi	Hapus	Ubah Nama	Unggah	Unduh	Mencegah pengunduhan	Bagikan	Cabut saham	Tayang	Lihat saham	Lihat anotasi	Lihat aktivitas	Lihat versi	Hapus versi	Pulihkan versi	Lihat semua komentar pribadi**
Penanor									✓	✓						

* Dalam hal ini, pemilik file adalah orang yang mengunggah versi asli file ke folder bersama. Izin untuk peran ini hanya berlaku untuk file yang dimiliki, bukan untuk semua file di folder bersama.

** Pemilik dan pemilik bersama dapat melihat semua komentar pribadi. Kontributor hanya dapat melihat komentar privat yang merupakan balasan atas komentar mereka.

*** Kontributor tidak dapat mengganti nama versi file yang ada. Namun, mereka dapat mengunggah versi baru file dengan nama yang berbeda.

Izin untuk file yang tidak ada di folder bersama

Izin berikut berlaku untuk peran pengguna untuk file yang tidak berada di folder bersama:

- Anotasi - Tambahkan umpan balik ke file.
- Hapus - Hapus file.
- Ganti nama - Ganti nama file.
- Unggah - Unggah versi baru file.
- Unduh - Unduh file. Ini adalah izin default. Anda dapat menggunakan properti file untuk mengizinkan atau menolak kemampuan mengunduh file bersama.
- Mencegah pengunduhan - Mencegah file diunduh.

> **Note**
>
> Ketika pemilik atau pemilik bersama MP4 file melarang unduhan untuk file tersebut, kontributor dan pemirsa tidak dapat memutarnya di klien web Amazon. WorkDocs

- Bagikan — Bagikan file dengan pengguna lain.
- Mencabut berbagi - Mencabut berbagi file.

- Lihat - Lihat file.
- Lihat berbagi - Lihat pengguna lain yang berbagi file.
- Lihat anotasi - Lihat umpan balik dari pengguna lain.
- Lihat aktivitas - Melihat riwayat aktivitas file.
- Lihat versi - Lihat versi file sebelumnya.
- Hapus versi — Hapus satu atau beberapa versi file.
- Memulihkan versi - Memulihkan satu atau lebih versi file yang dihapus.

	Buat Anotas	Hapus	Ubah Nama	Unggal	Undu	Mencegah pengundan	Bagikai	Cabut saham	Tayang	Lihat saham	Lihat anotas	Lihat aktivita	Lihat versi	Hapus versi	Pulihkan versi
Pemi	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Pemi bersa	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Kontı or**	✓			✓	✓				✓	✓	✓	✓	✓		
Pena					✓				✓	✓		✓			
Pena anon									✓	✓					

* Pemilik file dan pemilik bersama dapat melihat semua komentar pribadi. Kontributor hanya dapat melihat komentar privat yang merupakan balasan atas komentar mereka.

** Kontributor tidak dapat mengganti nama versi file yang ada. Namun, mereka dapat mengunggah versi baru file dengan nama yang berbeda.

Mengaktifkan pengeditan kolaboratif

Anda menggunakan bagian Pengaturan Pengeditan Online di panel kontrol Admin Anda untuk mengaktifkan opsi pengeditan kolaboratif.

Daftar Isi

Mengaktifkan Hancom ThinkFree

Anda dapat mengaktifkan Hancom ThinkFree untuk WorkDocs situs Anda, sehingga pengguna dapat membuat dan secara kolaboratif mengedit file Microsoft Office dari WorkDocs aplikasi web. Untuk informasi lebih lanjut, lihat Mengedit dengan Hancom ThinkFree.

Hancom ThinkFree tersedia tanpa biaya tambahan untuk WorkDocs pengguna. Lisensi atau instalasi perangkat lunak tambahan tidak diperlukan.

Untuk mengaktifkan Hancom ThinkFree

Aktifkan ThinkFree pengeditan Hancom dari panel kontrol Admin.

1. Di bawah Akun Saya, pilih Buka panel kontrol admin.
2. Untuk Pengeditan Hancom Online, pilih Ubah.
3. Pilih Aktifkan Fitur Edit Online Hancom, tinjau syarat penggunaan, lalu pilih Simpan.

Untuk menonaktifkan Hancom ThinkFree

Nonaktifkan ThinkFree pengeditan Hancom dari panel kontrol Admin.

1. Di bawah Akun Saya, pilih Buka panel kontrol admin.
2. Untuk Pengeditan Hancom Online, pilih Ubah.
3. Hapus Aktifkan Fitur Edit Online Hancom, lalu pilih Simpan.

Mengaktifkan Buka dengan Office Online

Aktifkan Buka dengan Office Online untuk WorkDocs situs Anda, sehingga pengguna dapat secara kolaboratif mengedit file Microsoft Office dari aplikasi WorkDocs web.

Buka dengan Office Online tersedia tanpa biaya tambahan bagi WorkDocs pengguna yang juga memiliki akun Microsoft Office 365 Work atau School dengan lisensi untuk mengedit di Office Online. Untuk informasi selengkapnya, lihat Buka dengan Office Online.

Untuk mengaktifkan Buka dengan Office Online

Aktifkan Buka dengan Office Online dari Panel kontrol admin.

1. Di bawah Akun Saya, pilih Buka panel kontrol admin.
2. Untuk Office Online, pilih Ubah.
3. Pilih Aktifkan Office Online, lalu pilih Simpan.

Untuk menonaktifkan Buka dengan Office Online

Nonaktifkan Buka dengan Office Online dari Panel kontrol admin.

1. Di bawah Akun Saya, pilih Buka panel kontrol admin.
2. Untuk Office Online, pilih Ubah.
3. Hapus Aktifkan Office Online, lalu pilih Simpan.

Migrasi file ke WorkDocs

WorkDocs administrator dapat menggunakan Layanan WorkDocs Migrasi untuk melakukan migrasi berskala besar dari beberapa file dan folder ke WorkDocs situs mereka. Layanan WorkDocs Migrasi berfungsi dengan Amazon Simple Storage Service (Amazon S3). Ini memungkinkan Anda memigrasikan berbagi file departemen dan home drive atau berbagi file pengguna ke. WorkDocs

Selama proses ini, WorkDocs berikan kebijakan AWS Identity and Access Management (IAM) untuk Anda. Gunakan kebijakan ini untuk membuat peran IAM baru yang memberikan akses ke Layanan WorkDocs Migrasi untuk melakukan hal berikut:

- Membaca dan membuat daftar bucket Amazon S3 yang Anda tentukan.
- Baca dan tulis ke WorkDocs situs yang Anda tunjuk.

Selesaikan tugas-tugas berikut untuk memigrasi file dan folder Anda. WorkDocs Sebelum memulai, konfirmasikan bahwa Anda memiliki izin berikut:

- Izin administrator untuk situs Anda WorkDocs
- Izin untuk membuat IAM role

Jika WorkDocs situs Anda diatur pada direktori yang sama dengan WorkSpaces armada Anda, Anda harus mengikuti persyaratan ini:

- Jangan gunakan Admin untuk nama pengguna WorkDocs akun Anda. Admin adalah peran pengguna yang dicadangkan di WorkDocs.
- Jenis pengguna WorkDocs administrator Anda harus Upgrade WS User. Untuk informasi selengkapnya, lihat Gambaran umum peran pengguna dan Mengedit pengguna.

> **Note**
>
> Struktur direktori, nama file, dan konten file dipertahankan saat bermigrasi ke WorkDocs. Kepemilikan file dan izin tidak dipertahankan.

Tugas

Langkah 1: Mempersiapkan konten untuk migrasi

Untuk mempersiapkan konten Anda untuk migrasi

1. Di WorkDocs situs Anda, di bawah My Documents, buat folder tempat Anda ingin memigrasikan file dan folder.
2. Konfirmasi hal berikut:
   - Folder sumber berisi tidak lebih dari 100.000 file dan subfolder. Migrasi gagal jika Anda melebihi batas itu.
   - Tidak ada file individual yang melebihi 5 TB.
   - Setiap nama file berisi 255 karakter atau kurang. WorkDocs Drive hanya menampilkan file dengan jalur direktori lengkap 260 karakter atau kurang.

> **Warning**
>
> Mencoba memigrasi file atau folder dengan nama yang berisi karakter berikut dapat menyebabkan kesalahan dan menghentikan proses migrasi. Jika ini terjadi, pilih Unduh laporan untuk mengunduh log daftar kesalahan, file yang gagal dimigrasi, dan file yang berhasil dimigrasi.

- Spasi tambahan — Misalnya: ruang tambahan di akhir nama file.
- Periode di awal atau akhir — Misalnya: `.file`,`.file.ppt`,`.`,`..`, atau `file.`
- Tildes di awal atau akhir — Misalnya:`file.doc~`,`~file.doc`, atau `~$file.doc`
- Nama file yang diakhiri dengan `.tmp` - Misalnya: `file.tmp`
- Nama file yang sama persis dengan istilah peka huruf besar/kecil ini —`Microsoft User Data`,,`Outlook files`, `Thumbs.db` atau `Thumbnails`

- Nama file yang berisi salah satu karakter ini - * (tanda bintang), / (garis miring), \ (garis miring belakang), : (titik dua), (kurang dari), < (lebih besar dari), > (tanda tanya), ? (bar/pipa vertikal), | (tanda kutip ganda), atau " \202E (kode karakter 202E).

Langkah 2: Mengunggah file ke Amazon S3

Untuk mengunggah file ke Amazon S3

1. Buat bucket Amazon Simple Storage Service (Amazon S3) baru di akun tempat AWS Anda ingin mengunggah file dan folder. Bucket Amazon S3 harus berada di AWS akun dan AWS Wilayah yang sama dengan situs Anda WorkDocs . Untuk informasi selengkapnya, lihat Memulai Layanan Penyimpanan Sederhana Amazon di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.
2. Unggah file Anda ke bucket Amazon S3 yang Anda buat pada langkah sebelumnya. Sebaiknya gunakan AWS DataSync untuk mengunggah file dan folder Anda ke bucket Amazon S3. DataSync menyediakan fitur pelacakan, pelaporan, dan sinkronisasi tambahan. Untuk informasi selengkapnya, lihat Cara AWS DataSync kerja dan Menggunakan kebijakan berbasis identitas (kebijakan IAM) DataSync di Panduan Pengguna.AWS DataSync

Langkah 3: Menjadwalkan migrasi

Setelah Anda menyelesaikan langkah 1 dan 2, gunakan Layanan WorkDocs Migrasi untuk menjadwalkan migrasi. Migaration Service dapat memakan waktu hingga seminggu untuk memproses permintaan migrasi dan mengirimkan email yang menyatakan bahwa Anda dapat memulai migrasi. Jika Anda memulai migrasi sebelum menerima email, konsol manajemen akan menampilkan pesan yang memberi tahu Anda untuk menunggu.

Saat Anda menjadwalkan migrasi, pengaturan Penyimpanan akun WorkDocs pengguna Anda secara otomatis berubah menjadi Tidak Terbatas.

> **Note**
>
> Migrasi file yang melebihi batas WorkDocs penyimpanan Anda dapat mengakibatkan biaya tambahan. Untuk informasi selengkapnya, silakan lihat Harga WorkDocs .

Layanan WorkDocs Migrasi menyediakan kebijakan AWS Identity and Access Management (IAM) untuk Anda gunakan untuk migrasi. Dengan kebijakan ini, Anda membuat peran IAM baru yang memberikan akses Layanan WorkDocs Migrasi ke bucket Amazon S3 WorkDocs dan situs yang Anda tentukan. Anda juga berlangganan notifikasi email Amazon SNS untuk menerima pembaruan saat permintaan migrasi dijadwalkan, serta kapan migrasi dimulai dan berakhir.

Untuk menjadwalkan migrasi

1. Dari WorkDocs konsol, pilih Aplikasi, Migrasi.
   - Jika ini adalah pertama kalinya Anda mengakses Layanan WorkDocs Migrasi, Anda diminta untuk berlangganan pemberitahuan email Amazon SNS. Berlangganan, konfirmasikan dalam pesan email yang Anda terima, lalu pilih Lanjutkan.
2. Pilih Buat Migrasi.
3. Untuk Jenis Sumber, pilih Amazon S3.
4. Pilih Selanjutnya.
5. Untuk Sumber Data & Validasi, di bawah Contoh Kebijakan, salin kebijakan IAM yang disediakan.
6. Gunakan kebijakan IAM yang Anda salin di langkah sebelumnya untuk membuat kebijakan dan IAM role baru, sebagai berikut:
   a. Buka konsol IAM di https://console.aws.amazon.com/iam/.
   b. Pilih Kebijakanh, kemudian Buat Kebijakan.
   c. Pilih JSON dan tempel kebijakan IAM yang Anda salin ke clipboard Anda sebelumnya.
   d. Pilih Tinjau kebijakan. Masukkan nama kebijakan dan deskripsi.
   e. Pilih Buat kebijakan.
   f. Pilih Peran, Buat peran.
   g. Pilih Akun AWS lainnya. Untuk ID Akun, masukkan salah satu langkah berikut:
      - Untuk Wilayah US East (N. Virginia), masukkan `899282061130`
      - Untuk Wilayah US West (Oregon), masukkan `814301586344`
      - Untuk Wilayah Asia Pacific (Singapore), masukkan `900469912330`
      - Untuk Wilayah Asia Pacific (Sydney), masukkan `031131923584`
      - Untuk Wilayah Asia Pacific (Tokyo), masukkan `178752524102`
      - Untuk Wilayah Eropa (Irlandia), masukkan `191921258524`

h. Pilih kebijakan yang Anda buat sebelumnya dan pilih Berikutnya: Tinjauan. Jika Anda tidak melihat kebijakan baru, pilih ikon refresh.

i. Masukkan nama peran dan deskripsi. Pilih Buat peran.

j. Pada halaman Peran, di bawah Nama peran, pilih nama peran yang Anda buat.

k. Pada halaman Ringkasan, ubah durasi CLI/API sesi maksimum menjadi 12 jam.

l. Salin ARN Peran Anda ke clipboard untuk digunakan di langkah berikutnya.

7. Kembali ke Layanan WorkDocs Migrasi. Untuk Sumber Data & Validasi, di bawah ARN Peran, tempel ARN peran dari IAM role yang Anda salin pada langkah sebelumnya.
8. Untuk Bucket, pilih bucket Amazon S3 untuk memigrasi file.
9. Pilih Berikutnya.
10. Untuk Pilih WorkDocs Folder tujuan, pilih folder tujuan WorkDocs untuk memigrasikan file ke.
11. Pilih Berikutnya.
12. Di bawah Ulasan, untuk Judul, masukkan nama untuk migrasi.
13. Pilih tanggal dan waktu untuk migrasi.
14. Pilih Kirim.

Langkah 4: Melacak migrasi

Anda dapat melacak migrasi Anda dari dalam halaman landing Layanan WorkDocs Migrasi. Untuk mengakses halaman arahan dari WorkDocs situs, pilih Aplikasi, Migrasi. Pilih migrasi Anda untuk melihat detailnya dan melacak kemajuannya. Anda juga dapat memilih Batalkan Migrasi jika Anda perlu membatalkannya, atau pilih Perbarui untuk memperbarui lini masa migrasi. Setelah migrasi selesai, Anda dapat memilih Unduh laporan untuk mengunduh log file yang berhasil atau gagal dimigrasi atau mengalami kesalahan.

Status migrasi berikut merupakan status migrasi Anda:

Terjadwal

Migrasi dijadwalkan tetapi tidak dimulai. Anda dapat membatalkan migrasi atau memperbarui waktu mulai migrasi hingga lima menit sebelum waktu mulai yang dijadwalkan.

Sedang Migrasi

Migrasi sedang berlangsung.

Sukses

Migrasi selesai.

Berhasil Sebagian

Migrasi sebagian selesai. Untuk detail lebih lanjut, lihat ringkasan migrasi dan unduh laporan yang disediakan.

Gagal

Migrasi gagal. Untuk detail lebih lanjut, lihat ringkasan migrasi dan unduh laporan yang disediakan.

Dibatalkan

Migrasi dibatalkan.

Langkah 5: Membersihkan sumber daya

Setelah migrasi selesai, hapus kebijakan migrasi dan peran yang Anda buat dari konsol IAM.

Untuk menghapus kebijakan IAM

1. Buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Pilih Kebijakan.
3. Cari dan pilih kebijakan yang Anda buat.
4. Dari Tindakan kebijakan, pilih Hapus.
5. Pilih Hapus.
6. Pilih Peran.
7. Cari dan pilih peran yang Anda buat.
8. Pilih Hapus peran, Hapus.

Saat migrasi terjadwal dimulai, pengaturan Penyimpanan akun WorkDocs pengguna Anda secara otomatis diubah menjadi Tidak Terbatas. Setelah migrasi, Anda dapat menggunakan panel kontrol admin untuk mengubah setelan itu. Lihat informasi yang lebih lengkap di Mengedit pengguna.

Masalah Pemecahan Masalah WorkDocs

Informasi berikut dapat membantu Anda memecahkan masalah. WorkDocs

Masalah

Tidak dapat mengatur WorkDocs situs saya di AWS Wilayah tertentu

Jika Anda menyiapkan WorkDocs situs baru, pilih Wilayah AWS selama penyiapan. Untuk informasi lebih lanjut, lihat tutorial untuk kasus penggunaan khusus Anda di bagian Memulai dengan WorkDocs.

Ingin mengatur WorkDocs situs saya di VPC Amazon yang ada

Saat menyiapkan WorkDocs situs baru Anda, buat direktori menggunakan virtual private cloud (VPC) yang ada. WorkDocs menggunakan direktori ini untuk mengautentikasi pengguna.

Pengguna perlu mengatur ulang kata sandi mereka

Pengguna dapat mengatur ulang kata sandi mereka dengan memilih Lupa kata sandi? di layar masuk mereka.

Pengguna secara tidak sengaja berbagi dokumen sensitif

Untuk mencabut akses ke dokumen tersebut, pilih Bagikan dengan undangan di samping dokumen, lalu hapus pengguna yang seharusnya tidak lagi memiliki akses. Jika dokumen dibagikan menggunakan tautan, pilih Bagikan tautan dan nonaktifkan tautan.

Pengguna meninggalkan organisasi dan tidak mentransfer kepemilikan dokumen

Transfer kepemilikan dokumen ke pengguna lain di panel kontrol admin. Untuk informasi selengkapnya, lihat Mentransfer kepemilikan dokumen.

Perlu menyebarkan WorkDocs Drive atau WorkDocs Companion ke beberapa pengguna

Deploy ke beberapa pengguna di korporasi dengan menggunakan kebijakan grup. Untuk informasi selengkapnya, lihat Manajemen identitas dan akses untuk Amazon WorkDocs. Untuk informasi spesifik tentang penerapan WorkDocs Drive ke beberapa pengguna, lihatMenyebarkan WorkDocs Drive ke beberapa komputer.

Pengeditan online tidak berfungsi

Verifikasi bahwa Anda telah menginstal WorkDocs Companion. Untuk menginstal WorkDocs Companion, lihat Aplikasi & Integrasi untuk WorkDocs.

Mengelola WorkDocs untuk Bisnis Amazon

Jika Anda adalah administrator WorkDocs untuk Amazon Business, Anda dapat mengelola pengguna dengan masuk ke https://workdocs.aws/ menggunakan kredensi Amazon Business Anda.

Untuk mengundang pengguna baru ke WorkDocs Amazon Business

1. Masuk dengan kredensial Amazon Business Anda di https://workdocs.aws/.
2. Di halaman beranda WorkDocs untuk Amazon Business, buka panel navigasi di sebelah kiri.
3. Pilih Pengaturan Admin.
4. Pilih Tambah pengguna.
5. Untuk Penerima, masukkan alamat email atau nama pengguna yang akan diundang.
6. (Opsional) Sesuaikan pesan undangan.
7. Pilih Selesai.

Untuk mencari pengguna di WorkDocs Amazon Business

1. Masuk dengan kredensial Amazon Business Anda di https://workdocs.aws/.
2. Di halaman beranda WorkDocs untuk Amazon Business, buka panel navigasi di sebelah kiri.
3. Pilih Pengaturan Admin.
4. Untuk Cari pengguna, masukkan nama pertama pengguna, dan tekan **`Enter`**.

Untuk memilih peran pengguna WorkDocs untuk Amazon Business

1. Masuk dengan kredensial Amazon Business Anda di https://workdocs.aws/.
2. Di halaman beranda WorkDocs untuk Amazon Business, buka panel navigasi di sebelah kiri.
3. Pilih Pengaturan Admin.
4. Di bawah Pengguna, di samping pengguna, pilih Peran yang akan diberikan kepada pengguna.

Untuk menghapus pengguna WorkDocs untuk Amazon Business

1. Masuk dengan kredensial Amazon Business Anda di https://workdocs.aws/.
2. Di halaman beranda WorkDocs untuk Amazon Business, buka panel navigasi di sebelah kiri.
3. Pilih Pengaturan Admin.

4. Di bawah Pengguna, pilih elipsis (...) di sebelah pengguna.
5. Pilih Hapus.
6. Jika diminta, masukkan pengguna baru yang akan menerima transfer file pengguna yang dihapus, dan pilih Hapus.

Alamat IP dan domain untuk ditambahkan ke daftar izin Anda

Jika Anda menerapkan pemfilteran IP pada perangkat yang mengakses WorkDocs, tambahkan alamat IP dan domain berikut ke daftar izin Anda. Melakukannya memungkinkan WorkDocs dan WorkDocs Drive untuk terhubung ke WorkDocs layanan.

- 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

Jika Anda ingin menggunakan rentang alamat IP, lihat rentang alamat AWS IP dalam referensi AWS umum.

Riwayat dokumen

Tabel berikut menjelaskan perubahan penting pada Panduan WorkDocs Administrasi Amazon, dimulai pada Februari 2018. Untuk notifikasi tentang pembaruan dokumentasi ini, Anda dapat berlangganan umpan RSS.

Perubahan	Deskripsi	Tanggal
Izin pemilik file baru	Administrator sekarang dapat memberikan izin Delete Version dan Recover Version. Izin adalah bagian dari rilis DeleteDocumentVersionAPI.	Juli 29, 2022
WorkDocs Cadangan	Dokumentasi WorkDocs Backup dihapus dari Panduan WorkDocs Administrasi Amazon karena komponen tidak lagi didukung.	24 Juni 2021
Mengelola WorkDocs untuk Bisnis Amazon	WorkDocs untuk Amazon Business mendukung manajemen pengguna oleh administrator. Untuk informasi selengkapnya, lihat Mengelola WorkDocs Bisnis Amazon di Panduan WorkDocs Administrasi Amazon.	26 Maret 2020
Migrasi file ke Amazon WorkDocs	WorkDocs administrator dapat menggunakan Layanan WorkDocs Migrasi untuk melakukan migrasi berskala besar dari beberapa file dan folder ke WorkDocs situs mereka. Untuk informasi selengkapnya, lihat Memigrasi	8 Agustus 2019

	file ke WorkDocs dalam Panduan WorkDocs Administrasi Amazon.	
IP memungkinkan pengaturan daftar	Pengaturan Daftar Izinkan IP tersedia untuk memfilter akses ke WorkDocs situs Anda berdasarkan rentang alamat IP. Untuk informasi selengkapnya, lihat IP mengizinkan pengaturan daftar di Panduan WorkDocs Administrasi Amazon.	22 Oktober 2018
Hancom ThinkFree	Hancom ThinkFree tersedia. Pengguna dapat membuat dan secara kolaboratif mengedit file Microsoft Office dari aplikasi WorkDocs web. Untuk informasi selengkapnya, lihat Mengaktifkan Hancom ThinkFree di Panduan WorkDocs Administrasi Amazon.	21 Juni 2018
Buka dengan Office Online	Open with Office Online tersedia. Pengguna dapat secara kolaboratif mengedit file Microsoft Office dari aplikasi WorkDocs web. Untuk informasi selengkapnya, lihat Mengaktifkan Buka dengan Office Online di Panduan WorkDocs Administrasi Amazon.	6 Juni 2018

Pemecahan Masalah	Topik pemecahan masalah ditambahkan. Untuk informasi selengkapnya, lihat Memecahkan WorkDocs masalah di Panduan WorkDocs Administrasi Amazon.	23 Mei 2018
Ubah periode retensi bin pemulihan	Periode penyimpanan kotak pemulihan dapat dimodifikasi. Untuk informasi selengkap nya, lihat Setelan retensi bin pemulihan di Panduan WorkDocs Administrasi Amazon.	27 Februari 2018