



Guida di amministrazione

Amazon WorkDocs



Amazon WorkDocs: Guida di amministrazione

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

I marchi e l'immagine commerciale di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in una qualsiasi modalità che possa causare confusione tra i clienti o in una qualsiasi modalità che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà delle rispettive aziende, che possono o meno essere associate, collegate o sponsorizzate da Amazon.

Table of Contents

.....	vi
Che cos'è Amazon WorkDocs?	1
Accesso ad Amazon WorkDocs	1
Prezzi	2
Come iniziare	2
Migrazione dei dati da WorkDocs	3
Metodo 1: scaricare file in blocco	3
Scaricamento di file dal Web	3
Scaricamento di cartelle dal Web	5
Utilizzo di WorkDocs Drive per scaricare file e cartelle	5
Metodo 2: utilizza lo strumento di migrazione	6
Prerequisiti	6
Limitazioni	9
Esecuzione dello strumento di migrazione	10
Scaricamento di dati migrati da Amazon S3	14
Risoluzione dei problemi relativi alle migrazioni	15
Visualizzazione della cronologia delle migrazioni	15
Prerequisiti	17
Registrati per un Account AWS	17
Crea un utente con accesso amministrativo	17
Sicurezza	19
Gestione dell'identità e degli accessi	20
Destinatari	20
Autenticazione con identità	21
Gestione dell'accesso con policy	24
Come WorkDocs funziona Amazon con IAM	26
Esempi di policy basate su identità	29
Risoluzione dei problemi	34
Registrazione di log e monitoraggio	36
Esportazione del feed di attività a livello di sito	36
CloudTrail registrazione	37
Convalida della conformità	40
Resilienza	41
Sicurezza dell'infrastruttura	42

Nozioni di base	43
Creare un WorkDocs sito Amazon	44
Prima di iniziare	44
Creare un WorkDocs sito Amazon	44
Abilitazione di Single Sign-On	46
Abilitazione dell'autenticazione a più fattori	47
Promozione di un utente ad amministratore	47
Gestione di Amazon WorkDocs dalla AWS console	49
Impostazione degli amministratori del sito	49
Reinvio delle email di invito	49
Gestione dell'autenticazione a più fattori	50
Impostazione degli URL dei siti	50
Gestione delle notifiche	51
Eliminazione di un sito	52
Gestione di Amazon WorkDocs dal pannello di controllo di amministrazione del sito	54
Distribuzione di Amazon WorkDocs Drive su più computer	62
Invito e gestione di utenti	63
Ruoli utente	63
Avvio del pannello di controllo amministrativo	65
Disattivazione dell'attivazione automatica	65
Gestire la condivisione dei link	66
Controllo degli inviti degli utenti con attivazione automatica abilitata	67
Invito di nuovi utenti	68
Modifica di utenti	68
Disabilitazione di utenti	69
Eliminazione di utenti in sospeso	70
Trasferimento della proprietà del documento	70
Scaricamento di elenchi utenti	71
Condivisione e collaborazione	73
Collegamenti di condivisione	73
Condivisione mediante invito	74
Condivisione esterna	74
Autorizzazioni	75
Ruoli utente	75
Autorizzazioni per le cartelle condivise	76
Autorizzazioni per i file nelle cartelle condivise	77

Autorizzazioni per i file che non si trovano nelle cartelle condivise	80
Abilitazione della modifica collaborativa	81
Attivazione di Hancom ThinkFree	82
Abilitazione di Open with Office Online	82
Migrazione dei file	84
Fase 1: Preparazione dei contenuti per la migrazione	85
Fase 2: Caricamento di file su Amazon S3	86
Fase 3: pianificazione di una migrazione	86
Fase 4: tracciamento di una migrazione	88
Fase 5: pulizia delle risorse	89
Risoluzione dei problemi	91
Non riesco a configurare il mio Amazon WorkDocs sito in uno specificoAWSRegion	91
Voglio configurare il mio Amazon WorkDocs sito in un Amazon VPC esistente	91
È necessario che gli utenti resettino la propria password	91
Un utente ha condiviso accidentalmente un documento sensibile	92
L'utente ha lasciato l'organizzazione e non ha trasferito la proprietà del documento.	92
Necessità di implementare Amazon WorkDocs Drive o Amazon WorkDocs Compagno per utenti multipli	92
L'editing online non funziona	54
Gestione di Amazon WorkDocs per Amazon Business	93
Indirizzo IP e domini da aggiungere all'elenco degli indirizzi consentiti	95
Cronologia dei documenti	96

Avviso: le registrazioni di nuovi clienti e gli upgrade degli account non sono più disponibili per Amazon WorkDocs. Scopri le fasi di migrazione qui: [Come migrare i dati da Amazon WorkDocs](#).

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.

Che cos'è Amazon WorkDocs?

Amazon WorkDocs è un servizio di condivisione e archiviazione aziendale completamente gestito e sicuro con solidi controlli amministrativi e funzionalità di feedback che migliorano la produttività degli utenti. I tuoi file vengono archiviati nel [cloud](#), in modo sicuro. I file dei tuoi utenti sono visibili solo a loro e ai collaboratori e visualizzatori designati. Gli altri membri dell'organizzazione non hanno accesso ai file degli altri utenti, a meno che non gli venga concesso l'accesso specificamente.

Gli utenti possono condividere i loro file con altri membri dell'organizzazione a scopi di collaborazione o revisione. Le applicazioni WorkDocs client Amazon possono essere utilizzate per visualizzare diversi tipi di file, a seconda del tipo di supporto Internet del file. Amazon WorkDocs supporta tutti i formati di documenti e immagini più comuni e il supporto per tipi di file multimediali aggiuntivi viene costantemente aggiunto.

Per ulteriori informazioni, consulta [Amazon WorkDocs](#).

Accesso ad Amazon WorkDocs

Gli amministratori utilizzano la [WorkDocs console Amazon](#) per creare e disattivare siti Amazon WorkDocs. Con il pannello di controllo admin si possono gestire le impostazioni di utenti, storage e sicurezza. Per ulteriori informazioni, consultare [Gestione di Amazon WorkDocs dal pannello di controllo di amministrazione del sito](#) e [Invitare e gestire WorkDocs gli utenti Amazon](#).

Gli utenti non amministrativi usano le applicazioni client per accedere ai file. Non usano mai la WorkDocs console Amazon o il pannello di amministrazione. Amazon WorkDocs offre diverse applicazioni e utilità client:

- Un'applicazione Web usata per la gestione e la revisione dei documenti.
- App native per dispositivi mobili usate per la revisione dei documenti.
- Amazon WorkDocs Drive, un'app che sincronizza una cartella sul desktop macOS o Windows con i tuoi file Amazon WorkDocs.

Per ulteriori informazioni su come gli utenti possono scaricare WorkDocs i client Amazon, modificare i propri file e utilizzare le cartelle, consulta i seguenti argomenti nella Amazon WorkDocs User Guide:

- [Guida introduttiva ad Amazon WorkDocs](#)
- [Lavorare con i file](#)

- [Lavorare con le cartelle](#)

Prezzi

Con Amazon WorkDocs, non ci sono commissioni o impegni iniziali. Pagi solo per gli account utente attivi e lo spazio di archiviazione che utilizzi. Per ulteriori informazioni, consulta la [pagina Prezzi](#).

Come iniziare

Per iniziare a usare Amazon WorkDocs, consulta [Creare un WorkDocs sito Amazon](#).

Migrazione dei dati da Amazon WorkDocs

Amazon WorkDocs offre due metodi per la migrazione dei dati da un WorkDocs sito. Questa sezione fornisce una panoramica di questi metodi e collegamenti a passaggi dettagliati per eseguire, risolvere i problemi e ottimizzare ciascun metodo di migrazione.

I clienti avranno a disposizione due opzioni per trasferire i propri dati da Amazon WorkDocs: la funzionalità Bulk Download esistente (metodo 1) o il nostro nuovo Data Migration Tool (metodo 2). I seguenti argomenti spiegano come utilizzare entrambi i metodi.

Argomenti

- [Metodo 1: scaricare file in blocco](#)
- [Metodo 2: utilizza lo strumento di migrazione](#)

Metodo 1: scaricare file in blocco

Se desideri controllare quali file migrare, puoi scaricarli manualmente in blocco. Questo metodo consente di selezionare solo i file desiderati e di scaricarli in un'altra posizione, ad esempio l'unità locale. Puoi scaricare file e cartelle dal tuo sito WorkDocs Web o da Amazon WorkDocs Drive.

Ricorda quanto segue:

- Gli utenti del tuo sito possono scaricare i file seguendo i passaggi elencati di seguito. Se preferisci, puoi configurare una cartella condivisa, chiedere agli utenti di spostare i file in quella cartella, quindi scaricare la cartella in un'altra posizione. Puoi anche [trasferire la proprietà a te stesso](#) ed eseguire i download.
- Per scaricare documenti Microsoft Word con commenti, consulta [Downloading Word documents with feedback](#), nella Amazon WorkDocs User Guide.
- È necessario utilizzare Amazon WorkDocs Drive per scaricare file di dimensioni superiori a 5 GB.
- Quando usi Amazon WorkDocs Drive per scaricare file e cartelle, le strutture di directory, i nomi dei file e il contenuto dei file rimangono intatti. La proprietà, le autorizzazioni e le versioni dei file non vengono mantenute.

Scaricamento di file dal Web

Questo metodo viene utilizzato per scaricare file quando:

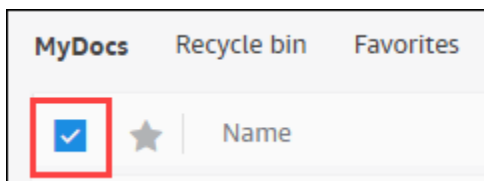
- Vuoi scaricare solo alcuni file da un sito.
- Vuoi scaricare documenti Word con commenti e fare in modo che tali commenti rimangano nei rispettivi documenti. Lo strumento di migrazione scarica tutti i commenti, ma li scrive in un file XML separato. Gli utenti del sito potrebbero quindi avere problemi ad associare i commenti ai propri documenti Word.

Per scaricare file dal Web

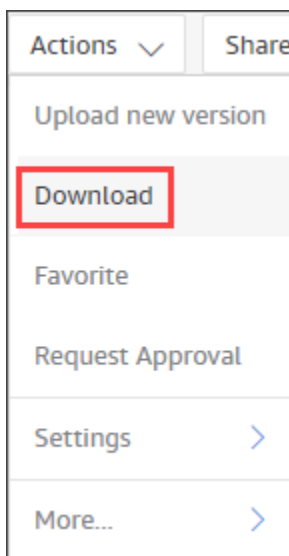
1. Accedi ad Amazon WorkDocs.
2. Se necessario, apri la cartella che contiene i file che desideri scaricare.
3. Seleziona la casella di controllo accanto ai file che desideri scaricare.

- OPPURE -

Seleziona la casella di controllo nella parte superiore dell'elenco per scegliere tutti i file nella cartella.



4. Apri il menu Azioni e scegli Scarica. .



Su un PC, per impostazione predefinita, i file scaricati si trovano nel nome della cartella Downloads/WorkDocsDownloads/. Su un Macintosh, per impostazione predefinita, i file vengono inseriti nel nome del disco rigido /Users/ nome utente/. WorkDocsDownloads

Scaricamento di cartelle dal Web

Note

Quando scarichi delle cartelle, scarichi anche tutti i file in esse contenuti. Se desideri scaricare solo alcuni file di una cartella, sposta i file indesiderati in un'altra posizione o nel Cestino, scarica la cartella.

Per scaricare cartelle dal Web

1. Accedi ad Amazon WorkDocs
2. Seleziona la casella di controllo accanto a ciascuna delle cartelle che desideri scaricare.

- OPPURE -

Apri le cartelle e seleziona le caselle di controllo accanto alle sottocartelle che desideri scaricare.

3. Apri il menu Azioni e scegli Scarica. .

Su un PC, per impostazione predefinita, le cartelle scaricate si trovano nel nome della cartella Downloads/WorkDocsDownloads/. Su un Macintosh, per impostazione predefinita, i file vengono inseriti nel nome del disco rigido /Users/ nome utente/. WorkDocsDownloads

Utilizzo di WorkDocs Drive per scaricare file e cartelle

Note

Devi installare Amazon WorkDocs Drive per completare i seguenti passaggi. Per ulteriori informazioni, consulta [Installazione di Amazon WorkDocs Drive](#), nella Guida per l'utente di Amazon WorkDocs Drive.

Per scaricare file e cartelle da WorkDocs Drive

1. Avvia File Explorer o Finder e apri l'unità W:.
2. Seleziona le cartelle o i file che desideri scaricare.
3. Tocca e tieni premuti (fai clic con il pulsante destro del mouse) sugli elementi selezionati e scegli Copia, quindi incolla gli elementi copiati nella nuova posizione.

- OPPURE -

Trascina gli elementi selezionati nella nuova posizione.

4. Elimina i file originali da Amazon WorkDocs Drive.

Metodo 2: utilizza lo strumento di migrazione

Utilizzi lo strumento di WorkDocs migrazione Amazon quando desideri migrare tutti i dati da un WorkDocs sito.

Lo strumento di migrazione sposta i dati da un sito a un bucket Amazon Simple Storage Service. Lo strumento crea un file ZIP compresso per ogni utente. Il file compresso include tutti i file e le cartelle, le versioni, le autorizzazioni, i commenti e le annotazioni per ciascuno degli utenti finali del sito.

WorkDocs

Argomenti

- [Prerequisiti](#)
- [Limitazioni](#)
- [Esecuzione dello strumento di migrazione](#)
- [Scaricamento di dati migrati da Amazon S3](#)
- [Risoluzione dei problemi relativi alle migrazioni](#)
- [Visualizzazione della cronologia delle migrazioni](#)

Prerequisiti

È necessario disporre dei seguenti elementi per utilizzare lo strumento di migrazione.

- Un bucket Amazon S3. Per informazioni sulla creazione di un bucket Amazon S3, consulta [Creating a bucket](#), nella Amazon S3 User Guide. Il tuo bucket deve utilizzare lo stesso account IAM

e risiedere nella stessa regione del tuo sito. WorkDocs Inoltre, devi bloccare l'accesso pubblico al bucket. Per ulteriori informazioni su questa operazione, consulta [Bloccare l'accesso pubblico allo storage Amazon S3](#), nella Amazon S3 User Guide.

Per concedere ad Amazon WorkDocs l'autorizzazione a caricare i tuoi file, configura la bucket policy come mostrato nell'esempio seguente. La policy utilizza i tasti `aws:SourceAccount` e `aws:SourceArn` condition per ridurre l'ambito della policy, una best practice di sicurezza.

```
{
  "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** è l'**ID** dell'organizzazione del tuo sito. WorkDocs È possibile trovarlo nella tabella «I miei siti» nella WorkDocs console AWS
- Per ulteriori informazioni sulla configurazione di una policy bucket, consulta [Aggiungere una bucket policy utilizzando la console Amazon S3](#)

- Una policy IAM. Per avviare una migrazione sulla WorkDocs console, il principale chiamante IAM deve avere la seguente policy allegata al set di autorizzazioni:

```
{
  "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": [
            "*"
        ]
    }
]
}

```

- Facoltativamente, puoi utilizzare una AWS KMS chiave per crittografare i dati inattivi nel tuo bucket. Se non fornisci una chiave, si applica l'impostazione di crittografia standard del bucket. Per ulteriori informazioni, consulta [Creating keys](#), nella AWS Key Management Service Developer Guide.

Per utilizzare una AWS KMS chiave, aggiungi le seguenti istruzioni alla policy IAM. È necessario utilizzare una chiave attiva di tipo SYMMETRIC_DEFAULT.

```

{
  "Sid": "AllowKMSMigration",
  "Effect": "Allow",
  "Action": [
    "kms:CreateGrant",
    "kms:DescribeKey"
  ],
  "Resource": [
    "arn:aws:kms:REGION:AWS-ACCOUNT-ID:key/KEY-RESOURCE-ID"
  ]
}

```

Limitazioni

Lo strumento di migrazione presenta le seguenti limitazioni:

- Lo strumento scrive tutte le autorizzazioni, i commenti e le annotazioni degli utenti in file CSV separati. È necessario mappare manualmente tali dati ai file corrispondenti.
- È possibile migrare solo i siti attivi.
- Lo strumento è limitato a una migrazione riuscita per sito per ogni periodo di 24 ore.

- Non è possibile eseguire migrazioni simultanee dello stesso sito, ma è possibile eseguire migrazioni simultanee per siti diversi.
- Ogni file zip avrà una dimensione massima di 50 GB. Gli utenti con più di 50 GB di dati WorkDocs avranno più file zip esportati in Amazon S3.
- Lo strumento non esporta file di dimensioni superiori a 50 GB. Lo strumento elenca tutti i file di dimensioni superiori a 50 GB in un file CSV con lo stesso prefisso dei file ZIP. **Ad esempio, /workdocs/ site-alias/Created-Timestamp-UTC /skippedFiles.csv.** È possibile scaricare i file elencati a livello di codice o manualmente. Per informazioni sul download programmatico <https://docs.aws.amazon.com/workdocs/latest/developerguide/download-documents.html>, consulta la Amazon WorkDocs Developer Guide. Per informazioni sul download manuale dei file, consulta la procedura descritta nel Metodo 1, più avanti in questo argomento.
- Il file zip di ogni utente conterrà solo file e/o cartelle di sua proprietà. Tutti i file e/o le cartelle che sono stati condivisi con l'utente saranno contenuti nel file zip dell'utente proprietario dei file e/o delle cartelle.
- Se una cartella è vuota (non contiene file/cartelle annidati) in WorkDocs, non verrà esportata.
- Non è garantito che i dati (file, cartelle, versioni, commenti, annotazioni) creati dopo l'avvio del processo di migrazione vengano inclusi nei dati esportati in S3.
- Puoi migrare più siti in un bucket Amazon S3. Non è necessario creare un bucket per sito. Tuttavia, devi assicurarti che le tue policy IAM e bucket consentano più siti.
- La migrazione aumenta i costi di Amazon S3, a seconda della quantità di dati da migrare nel bucket. Per ulteriori informazioni, consulta la pagina dei [prezzi di Amazon S3](#).

Esecuzione dello strumento di migrazione

I passaggi seguenti spiegano come eseguire lo strumento di WorkDocs migrazione Amazon.

Per migrare un sito

1. Apri la WorkDocs console Amazon all'[indirizzo https://console.aws.amazon.com/zocalo/](https://console.aws.amazon.com/zocalo/).
2. Nel riquadro di navigazione, scegli I miei siti, quindi seleziona il pulsante di opzione accanto al sito che desideri migrare.
3. Apri l'elenco Azioni e scegli Migra dati.
4. Nella pagina Migrate Data site-name, inserisci l'URI del tuo bucket Amazon S3.

- OPPURE -

Scegli Browse S3 e segui questi passaggi:

- a. Se necessario, cerca il bucket.
 - b. Seleziona il pulsante di opzione accanto al nome del bucket, quindi seleziona Scegli.
5. (Facoltativo) In Notifiche, inserisci un massimo di cinque indirizzi email. Lo strumento invia e-mail sullo stato della migrazione a ciascun destinatario.
 6. (Facoltativo) In Impostazioni avanzate, seleziona una chiave KMS per crittografare i dati archiviati.
 7. Inserisci **migrate** nella casella di testo per confermare la migrazione, quindi scegli Avvia migrazione.

Viene visualizzato un indicatore che mostra lo stato della migrazione. I tempi di migrazione variano a seconda della quantità di dati in un sito.

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 prerequisites section here.

S3 URI

 ✕ View [↗](#) Browse S3

Notifications [Optional]

Enter email addresses for notification recipients. These people will receive status updates on the migration.

 ✕ ✕

▼ 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.

 ✕ 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 when using the migration tool. Pricing for storage at the S3 URI destination will be subject to the pricing and terms available [here](#). 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.

Al termine della migrazione:

- Lo strumento invia e-mail di «operazione riuscita» agli indirizzi immessi durante la configurazione, se presenti.
- ***Il tuo bucket Amazon S3 conterrà una cartella /workdocs/ site-alias/ Created-Timestamp-UTC /.*** Questa cartella contiene una cartella zippata per ogni utente che aveva dati sul sito. Ogni cartella compressa contiene le cartelle e i file dell'utente, incluse le autorizzazioni e i commenti relativi alla mappatura dei file CSV.
- Se un utente rimuove tutti i propri file prima della migrazione, non viene visualizzata alcuna cartella compressa per quell'utente.
- Versioni: i documenti con più versioni hanno un identificatore di data e ora di creazione `_version_`. Il timestamp utilizza millisecondi di epoca. Ad esempio, un documento denominato «TestFile.txt» con 2 versioni viene visualizzato come segue:

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

- Autorizzazioni: l'esempio seguente mostra il contenuto di un tipico file CSV di autorizzazioni.

```
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
```

- Commenti: l'esempio seguente mostra il contenuto di un tipico file CSV di commenti.

```
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 ignorati: l'esempio seguente mostra il contenuto di un tipico file CSV con file ignorati. Abbiamo abbreviato l'ID e omesso i valori del motivo per una migliore leggibilità.

```
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...
```

Scaricamento di dati migrati da Amazon S3

Poiché la migrazione aumenta i costi di Amazon S3, puoi scaricare i dati migrati da Amazon S3 a un'altra soluzione di storage. Questo argomento spiega come scaricare i dati migrati e fornisce suggerimenti per il caricamento dei dati su una soluzione di storage.

Note

I passaggi seguenti spiegano come scaricare un file o una cartella alla volta. Per informazioni su altri modi per scaricare file, consulta [Downloading objects](#), nella Amazon S3 User Guide.

Per scaricare dati

1. Apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Seleziona il bucket di destinazione e accedi all'alias del sito.
3. Seleziona la casella di controllo accanto alla cartella compressa.

- OPPURE -

Apri la cartella compressa e seleziona la casella di controllo accanto al file o alla cartella per un singolo utente.

4. Scegli Download (Scarica).

Suggerimenti per soluzioni di archiviazione

Per siti di grandi dimensioni, consigliamo di effettuare il provisioning di un'istanza EC2 utilizzando un'[Amazon Machine Image conforme basata su Linux](#) per scaricare programmaticamente i dati da Amazon S3, decomprimerli e caricarli sul provider di storage o sul disco locale.

Risoluzione dei problemi relativi alle migrazioni

Prova questi passaggi per assicurarti di aver configurato correttamente il tuo ambiente:

- Se una migrazione non riesce, viene visualizzato un messaggio di errore nella scheda Cronologia delle migrazioni della WorkDocs console. Controlla il messaggio di errore.
- Controlla le impostazioni del bucket Amazon S3.
- Esegui nuovamente la migrazione.

Se il problema persiste, contatta AWS Support. Includi l'URL del WorkDocs sito e il Migration Job ID, che si trovano nella tabella della cronologia delle migrazioni.

Visualizzazione della cronologia delle migrazioni

I passaggi seguenti spiegano come visualizzare la cronologia delle migrazioni.

Per visualizzare la cronologia

1. Apri la WorkDocs console Amazon all'[indirizzo https://console.aws.amazon.com/zocalo/](https://console.aws.amazon.com/zocalo/).
2. Seleziona il pulsante radio accanto al WorkDocs sito desiderato.
3. Apri l'elenco Azioni e scegli Migra dati.
4. Nella pagina del nome del sito Migrate Data, scegli Migrazioni e cronologia in corso.

La cronologia delle migrazioni viene visualizzata in Migrazioni. L'immagine seguente mostra una cronologia tipica.

Migrations

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

Prerequisiti per Amazon WorkDocs

Per configurare nuovi WorkDocs siti Amazon o gestire siti esistenti, devi completare le seguenti attività.

Registrati per un Account AWS

Se non hai un Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti a un Account AWS

1. Apri la <https://portal.aws.amazon.com/billing/registrazione>.
2. Segui le istruzioni online.

Nel corso della procedura di registrazione riceverai una telefonata, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.

Quando ti iscrivi a un Account AWS, un Utente root dell'account AWS viene creato. L'utente root ha accesso a tutti Servizi AWS e le risorse presenti nell'account. Come best practice di sicurezza, assegna l'accesso amministrativo a un utente e utilizza solo l'utente root per eseguire [attività che richiedono l'accesso di un utente root](#).

AWS ti invia un'email di conferma dopo il completamento della procedura di registrazione. In qualsiasi momento, puoi visualizzare l'attività corrente del tuo account e gestirlo accedendo a <https://aws.amazon.com/> e scegliendo Il mio account.

Crea un utente con accesso amministrativo

Dopo esserti registrato per un Account AWS, proteggi il tuo Utente root dell'account AWS, abilita AWS IAM Identity Center e crea un utente amministrativo in modo da non utilizzare l'utente root per le attività quotidiane.

Proteggi i tuoi Utente root dell'account AWS

1. Accedi a [AWS Management Console](#) come proprietario dell'account selezionando Utente root e inserendo il Account AWS indirizzo email. Nella pagina successiva, inserisci la password.

Per informazioni [sull'accesso tramite utente root, consulta Accesso come utente root](#) in Accedi ad AWS Guida per l'utente.

2. Attiva l'autenticazione a più fattori (MFA) per il tuo utente root.

Per istruzioni, consulta [Abilitare un MFA dispositivo virtuale per il Account AWS utente root \(console\)](#) nella Guida per l'IAMutente.

Crea un utente con accesso amministrativo

1. Abilita IAM Identity Center.

Per istruzioni, vedi [Abilitazione AWS IAM Identity Center](#) nella AWS IAM Identity Center Guida per l'utente.

2. In IAM Identity Center, concedi l'accesso amministrativo a un utente.

Per un tutorial sull'utilizzo di IAM Identity Center directory come fonte di identità, vedi [Configurare l'accesso utente con l'impostazione predefinita IAM Identity Center directory](#) nella AWS IAM Identity Center Guida per l'utente.

Accesso come utente amministratore

- Per accedere con il tuo utente IAM Identity Center, utilizza l'accesso URL che ti è stato inviato al tuo indirizzo e-mail quando hai creato l'utente IAM Identity Center.

Per informazioni sull'accesso tramite un utente di IAM Identity Center, vedi [Accesso a AWS accedere al portale](#) in Accedi ad AWS Guida per l'utente.

Assegna l'accesso a ulteriori utenti

1. In IAM Identity Center, crea un set di autorizzazioni che segua la migliore pratica di applicazione delle autorizzazioni con privilegi minimi.

Per istruzioni, vedere [Creare](#) un set di autorizzazioni nella AWS IAM Identity Center Guida per l'utente.

2. Assegna al gruppo prima gli utenti e poi l'accesso con autenticazione unica (Single Sign-On).

Per istruzioni, consulta [Aggiungere gruppi](#) nella AWS IAM Identity Center Guida per l'utente.

Sicurezza in Amazon WorkDocs

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di un data center e di un'architettura di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra AWS te e te. Il [modello di responsabilità condivisa](#) descrive questo come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi nel AWS cloud. AWS ti fornisce anche servizi che puoi utilizzare in modo sicuro. I revisori di terze parti testano e verificano regolarmente l'efficacia della sicurezza come parte dei [programmi di conformitàAWS](#). Per maggiori informazioni sui programmi di conformità applicabili ad Amazon WorkDocs, consulta [AWS Services in Scope by Compliance Program](#).
- Sicurezza nel cloud: il AWS servizio che utilizzi determina la tua responsabilità. L'utente è anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti dell'azienda e le leggi e le normative applicabili. Gli argomenti di questa sezione ti aiutano a capire come applicare il modello di responsabilità condivisa quando usi Amazon WorkDocs.

Note

Gli utenti di un' WorkDocs organizzazione possono collaborare con utenti esterni all'organizzazione inviando un link o un invito a un file. Tuttavia, questo vale solo per i siti che utilizzano un connettore Active Directory. Consulta [le impostazioni dei link condivisi](#) per il tuo sito e seleziona l'opzione che meglio soddisfa i requisiti della tua azienda.

I seguenti argomenti mostrano come configurare Amazon per WorkDocs soddisfare i tuoi obiettivi di sicurezza e conformità. Scopri anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le tue WorkDocs risorse Amazon.

Argomenti

- [Gestione delle identità e degli accessi per Amazon WorkDocs](#)
- [Registrazione e monitoraggio in Amazon WorkDocs](#)
- [Convalida della conformità per Amazon WorkDocs](#)
- [Resilienza in Amazon WorkDocs](#)

- [Sicurezza dell'infrastruttura in Amazon WorkDocs](#)

Gestione delle identità e degli accessi per Amazon WorkDocs

AWS Identity and Access Management (IAM) è un sistema Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. IAM gli amministratori controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse Amazon. WorkDocs IAM è un software Servizio AWS che puoi utilizzare senza costi aggiuntivi.

Argomenti

- [Destinatari](#)
- [Autenticazione con identità](#)
- [Gestione dell'accesso con policy](#)
- [Come WorkDocs funziona Amazon con IAM](#)
- [Esempi di policy WorkDocs basate sull'identità di Amazon](#)
- [Risoluzione dei problemi relativi all' WorkDocs identità e all'accesso ad Amazon](#)

Destinatari

Il modo in cui usi AWS Identity and Access Management (IAM) varia a seconda del lavoro che svolgi in Amazon WorkDocs.

Utente del servizio: se utilizzi il WorkDocs servizio Amazon per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più WorkDocs funzionalità di Amazon per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni aggiuntive. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità di Amazon WorkDocs, consulta [Risoluzione dei problemi relativi all' WorkDocs identità e all'accesso ad Amazon](#).

Amministratore del servizio: se sei responsabile delle WorkDocs risorse Amazon della tua azienda, probabilmente hai pieno accesso ad Amazon WorkDocs. È tuo compito determinare a quali WorkDocs funzionalità e risorse di Amazon devono accedere gli utenti del servizio. Devi quindi inviare richieste all'IAM amministratore per modificare le autorizzazioni degli utenti del servizio. Consulta le informazioni contenute in questa pagina per comprendere i concetti di base di IAM. Per ulteriori informazioni su come la tua azienda può utilizzare IAM Amazon WorkDocs, consulta [Come WorkDocs funziona Amazon con IAM](#).

IAM amministratore: se sei un IAM amministratore, potresti voler saperne di più su come scrivere politiche per gestire l'accesso ad Amazon WorkDocs. Per visualizzare esempi di policy WorkDocs basate sull'identità di Amazon che puoi utilizzare, consulta IAM. [Esempi di policy WorkDocs basate sull'identità di Amazon](#)

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. È necessario autenticarsi (accedere a AWS) come Utente root dell'account AWS, come IAM utente o assumendo un ruolo. IAM

È possibile accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAM Identity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Quando accedi come identità federata, l'amministratore aveva precedentemente configurato la federazione delle identità utilizzando i ruoli. IAM Quando si accede AWS utilizzando la federazione, si assume indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi [Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente](#).

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando () per firmare crittograficamente le tue richieste utilizzando le tue credenziali. CLI Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, consulta [AWS Signature Version 4 per API le richieste](#) nella Guida per l'IAM utente.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta [Autenticazione a più fattori](#) nella Guida per l'AWS IAM Identity Center utente e [Autenticazione a AWS più fattori IAM nella Guida per l'IAM utente](#).

IAM users and groups

Un [IAM utente](#) è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Laddove possibile, consigliamo di fare affidamento su credenziali temporanee anziché creare IAM utenti con credenziali a lungo termine come password

e chiavi di accesso. Tuttavia, se hai casi d'uso specifici che richiedono credenziali a lungo termine con IAM gli utenti, ti consigliamo di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta [Ruotare regolarmente le chiavi di accesso per i casi d'uso che richiedono credenziali a lungo termine](#) nella Guida per l'utente. IAM

Un [IAMgruppo](#) è un'identità che specifica un insieme di utenti. IAM Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, potresti avere un gruppo denominato IAMAdminse concedere a quel gruppo le autorizzazioni per IAM amministrare le risorse.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta [Casi d'uso per IAM gli utenti nella Guida per l'IAMutente](#).

IAMruoli

Un [IAMruolo](#) è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un IAM utente, ma non è associato a una persona specifica. Per assumere temporaneamente un IAM ruolo in AWS Management Console, puoi [passare da un utente a un IAM ruolo \(console\)](#). È possibile assumere un ruolo chiamando un' AWS APIoperazione AWS CLI or o utilizzando un'operazione personalizzataURL. Per ulteriori informazioni sui metodi di utilizzo dei ruoli, vedere [Metodi per assumere un ruolo](#) nella Guida per l'IAMutente.

IAMI ruoli con credenziali temporanee sono utili nelle seguenti situazioni:

- **Accesso utente federato:** per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per informazioni sui ruoli per la federazione, consulta [Creare un ruolo per un provider di identità di terze parti \(federazione\)](#) nella Guida per l'IAMutente. Se utilizzi IAM Identity Center, configuri un set di autorizzazioni. Per controllare a cosa possono accedere le identità dopo l'autenticazione, IAM Identity Center correla il set di autorizzazioni a un ruolo in. IAM Per informazioni sui set di autorizzazioni, consulta [Set di autorizzazioni](#) nella Guida per l'utente di AWS IAM Identity Center .
- **Autorizzazioni IAM utente temporanee:** un IAM utente o un ruolo può assumere il IAM ruolo di assumere temporaneamente autorizzazioni diverse per un'attività specifica.

- **Accesso su più account:** puoi utilizzare un IAM ruolo per consentire a qualcuno (un responsabile fidato) di un altro account di accedere alle risorse del tuo account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per conoscere la differenza tra ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta la [sezione Accesso alle risorse su più account IAM nella Guida per l'utente](#). IAM
- **Accesso tra servizi:** alcuni Servizi AWS utilizzano funzionalità in altri. Servizi AWS Ad esempio, quando effettui una chiamata in un servizio, è normale che quel servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
- **Sessioni di accesso diretto (FAS):** quando utilizzi un IAM utente o un ruolo per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama un Servizio AWS, in combinazione con la richiesta di effettuare richieste Servizio AWS ai servizi downstream. FAS le richieste vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli FAS delle politiche relative alle richieste, consulta [Forward access sessions](#).
- **Ruolo di servizio:** un ruolo di servizio è un [IAM ruolo](#) che un servizio assume per eseguire azioni per conto dell'utente. Un IAM amministratore può creare, modificare ed eliminare un ruolo di servizio dall'internal IAM. Per ulteriori informazioni, consulta [Creare un ruolo per delegare le autorizzazioni a un utente Servizio AWS nella Guida per l'utente](#).
- **Ruolo collegato al servizio:** un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un Servizio AWS. Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un IAM amministratore può visualizzare, ma non modificare le autorizzazioni per i ruoli collegati al servizio.
- **Applicazioni in esecuzione su Amazon EC2:** puoi utilizzare un IAM ruolo per gestire le credenziali temporanee per le applicazioni in esecuzione su un'EC2 istanza e che effettuano AWS CLI o effettuano AWS API richieste. È preferibile archiviare le chiavi di accesso all'interno dell'EC2 istanza. Per assegnare un AWS ruolo a un'EC2 istanza e renderlo disponibile per tutte le sue applicazioni, create un profilo di istanza collegato all'istanza. Un profilo di istanza contiene il ruolo e consente ai programmi in esecuzione sull'EC2 istanza di ottenere credenziali temporanee.

Per ulteriori informazioni, consulta [Utilizzare un IAM ruolo per concedere le autorizzazioni alle applicazioni in esecuzione su EC2 istanze Amazon nella Guida](#) per l'IAMutente.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e associandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come JSON documenti. Per ulteriori informazioni sulla struttura e il contenuto dei documenti relativi alle JSON politiche, vedere [Panoramica delle JSON politiche](#) nella Guida per l'IAMutente.

Gli amministratori possono utilizzare AWS JSON le politiche per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un IAM amministratore può creare IAM politiche. L'amministratore può quindi aggiungere le IAM politiche ai ruoli e gli utenti possono assumerli.

IAMle politiche definiscono le autorizzazioni per un'azione indipendentemente dal metodo utilizzato per eseguire l'operazione. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale criterio può ottenere informazioni sul ruolo da AWS Management Console, da o da. AWS CLI AWS API

Policy basate su identità

I criteri basati sull'identità sono documenti relativi alle politiche di JSON autorizzazione che è possibile allegare a un'identità, ad esempio un IAM utente, un gruppo di utenti o un ruolo. Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una politica basata sull'identità, consulta [Definire le IAM autorizzazioni personalizzate con](#) le politiche gestite dal cliente nella Guida per l'utente. IAM

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli all'interno del tuo Account AWS. Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per

informazioni su come scegliere tra una politica gestita o una politica in linea, consulta [Scegliere tra politiche gestite e politiche in linea nella Guida](#) per l'IAMutente.

Policy basate su risorse

Le politiche basate sulle risorse sono documenti di JSON policy allegati a una risorsa. Esempi di politiche basate sulle risorse sono le policy di trust dei IAM ruoli e le policy dei bucket di Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario [specificare un principale](#) in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non è possibile utilizzare le policy AWS gestite contenute IAM in una policy basata sulle risorse.

Liste di controllo accessi

Le liste di controllo degli accessi (ACLs) controllano quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLs sono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy. JSON

Amazon S3 e Amazon VPC sono esempi di servizi che supportano. AWS WAF ACLs Per ulteriori informazioni ACLs, consulta la [panoramica di Access control list \(ACL\)](#) nella Amazon Simple Storage Service Developer Guide.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite di autorizzazioni è una funzionalità avanzata in cui si impostano le autorizzazioni massime che una politica basata sull'identità può concedere a un'entità (utente o ruolo). IAM IAM È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal` sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. [Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità nella Guida per l'utente. IAM IAM](#)

- Politiche di controllo del servizio (SCPs): SCPs sono JSON politiche che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in AWS Organizations. AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più Account AWS di proprietà dell'azienda. Se abiliti tutte le funzionalità di un'organizzazione, puoi applicare le politiche di controllo del servizio (SCPs) a uno o tutti i tuoi account. SCP limita le autorizzazioni per le entità negli account dei membri, inclusa ciascuna Utente root dell'account AWS. Per ulteriori informazioni su Organizations and SCPs, consulta [le politiche di controllo dei servizi](#) nella Guida AWS Organizations per l'utente.
- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta [le politiche di sessione](#) nella Guida IAM per l'utente.

Note

Amazon WorkDocs non supporta le politiche di controllo dei servizi per Slack Organizations.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per sapere come si AWS determina se consentire una richiesta quando sono coinvolti più tipi di policy, consulta [Logica di valutazione delle politiche](#) nella Guida per l'IAM utente.

Come WorkDocs funziona Amazon con IAM

Prima di utilizzare IAM per gestire l'accesso ad Amazon WorkDocs, devi capire quali IAM funzionalità sono disponibili per l'uso con Amazon WorkDocs. Per avere una panoramica generale del funzionamento di Amazon WorkDocs e di altri AWS servizi IAM, consulta [AWS i servizi con cui funzionano IAM](#) nella Guida per l'IAM utente.

Argomenti

- [WorkDocs Politiche basate sull'identità di Amazon](#)
- [Politiche basate WorkDocs sulle risorse di Amazon](#)

- [Autorizzazione basata sui WorkDocs tag Amazon](#)
- [WorkDocs IAMRuoli Amazon](#)

WorkDocs Politiche basate sull'identità di Amazon

Con le politiche IAM basate sull'identità, puoi specificare azioni consentite o negate. Amazon WorkDocs supporta azioni specifiche. Per maggiori informazioni sugli elementi utilizzati in una JSON policy, consulta il [riferimento agli elementi della IAM JSON policy](#) nella Guida per l'IAM utente.

Azioni

Gli amministratori possono utilizzare AWS JSON le policy per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'Action elemento di una JSON policy descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a una policy. Le azioni politiche in genere hanno lo stesso nome dell' AWS API operazione associata. Esistono alcune eccezioni, come le azioni basate solo sulle autorizzazioni che non hanno un'operazione corrispondente. API Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Le azioni politiche in Amazon WorkDocs utilizzano il seguente prefisso prima dell'azione: `workdocs:`. Ad esempio, per concedere a qualcuno l'autorizzazione a eseguire l' WorkDocs `DescribeUsers` API operazione Amazon, includi l'`workdocs:DescribeUsers` azione nella sua politica. Le istruzioni della policy devono includere un elemento `Action` o `NotAction`. Amazon WorkDocs definisce il proprio set di azioni che descrivono le attività che puoi eseguire con questo servizio.

Per specificare più azioni in una sola istruzione, separa ciascuna di esse con una virgola come mostrato di seguito:

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

È possibile specificare più azioni tramite caratteri jolly (*). Ad esempio, per specificare tutte le azioni che iniziano con la parola `Describe`, includi la seguente azione:

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

Note

Per garantire la compatibilità con le versioni precedenti, includi l'allocazione. Per esempio:

```
"Action": [  
  "zocalo:*",  
  "workdocs:*"  
],
```

Per visualizzare un elenco di WorkDocs azioni Amazon, consulta [Actions defined by Amazon WorkDocs](#) nella IAMUser Guide.

Risorse

Amazon WorkDocs non supporta la specificazione della risorsa ARNs in una politica.

Chiavi di condizione

Amazon WorkDocs non fornisce chiavi di condizione specifiche del servizio, ma supporta l'utilizzo di alcune chiavi di condizione globali. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di [contesto delle condizioni AWS globali nella Guida](#) per l'IAMutente.

Esempi

Per visualizzare esempi di politiche WorkDocs basate sull'identità di Amazon, consulta. [Esempi di policy WorkDocs basate sull'identità di Amazon](#)

Politiche basate WorkDocs sulle risorse di Amazon

Amazon WorkDocs non supporta politiche basate sulle risorse.

Autorizzazione basata sui WorkDocs tag Amazon

Amazon WorkDocs non supporta l'etichettatura delle risorse o il controllo dell'accesso in base ai tag.

WorkDocs IAMRuoli Amazon

Un [IAMruolo](#) è un'entità all'interno del tuo AWS account che dispone di autorizzazioni specifiche.

Utilizzo di credenziali temporanee con Amazon WorkDocs

Consigliamo vivamente di utilizzare credenziali temporanee per accedere con la federazione, assumere un IAM ruolo o assumere un ruolo per più account. È possibile ottenere credenziali di sicurezza temporanee chiamando AWS STS API operazioni come o.

[AssumeRoleGetFederationToken](#)

Amazon WorkDocs supporta l'utilizzo di credenziali temporanee.

Ruoli collegati ai servizi

[I ruoli collegati ai](#) AWS servizi consentono ai servizi di accedere alle risorse di altri servizi per completare un'azione per tuo conto. I ruoli collegati ai servizi vengono visualizzati nell'IAMaccount e sono di proprietà del servizio. Un IAM amministratore può visualizzare ma non modificare le autorizzazioni per i ruoli collegati al servizio.

Amazon WorkDocs non supporta ruoli collegati ai servizi.

Ruoli dei servizi

Questa caratteristica consente a un servizio di assumere un [ruolo di servizio](#) per conto dell'utente. Questo ruolo consente al servizio di accedere alle risorse in altri servizi per completare un'azione per conto dell'utente. I ruoli di servizio vengono visualizzati nel tuo IAM account e sono di proprietà dell'account. Ciò significa che un IAM amministratore può modificare le autorizzazioni per questo ruolo. Tuttavia, il farlo potrebbe pregiudicare la funzionalità del servizio.

Amazon WorkDocs non supporta i ruoli di servizio.

Esempi di policy WorkDocs basate sull'identità di Amazon

Note

Per una maggiore sicurezza, crea utenti federati anziché IAM utenti quando possibile.

Per impostazione predefinita, IAM gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare WorkDocs risorse Amazon. Inoltre, non possono eseguire attività utilizzando AWS Management Console AWS CLI, o AWS API. Un IAM amministratore deve creare IAM politiche che concedano a utenti e ruoli l'autorizzazione a eseguire API operazioni specifiche sulle risorse specifiche di cui ha bisogno. L'amministratore deve quindi allegare tali politiche agli IAM utenti o ai gruppi che richiedono tali autorizzazioni.

Note

Per garantire la compatibilità con le versioni precedenti, includi l'allocazione nelle tue politiche. Per esempio:

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

Per informazioni su come creare una politica IAM basata sull'identità utilizzando questi documenti di esempio JSON, consulta [Creazione di politiche nella JSON scheda della Guida per l'utente](#). IAM

Argomenti

- [Best practice per le policy](#)
- [Utilizzo della WorkDocs console Amazon](#)
- [Consentire agli utenti di visualizzare le loro autorizzazioni](#)
- [Consenti agli utenti l'accesso in sola lettura alle risorse Amazon WorkDocs](#)
- [Altri esempi di policy WorkDocs basate sull'identità di Amazon](#)

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare WorkDocs risorse Amazon nel tuo account. Queste azioni possono comportare costi aggiuntivi per l' Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono le autorizzazioni per molti casi d'uso comuni. AWS Sono disponibili nel tuo Account AWS. Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta [le politiche AWS gestite o le politiche AWS gestite per le funzioni lavorative](#) nella Guida per l'IAM utente.
- Applica le autorizzazioni con privilegi minimi: quando imposti le autorizzazioni con le IAM politiche, concedi solo le autorizzazioni necessarie per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo per applicare le autorizzazioni, consulta [Politiche](#) e autorizzazioni nella Guida IAM per l'utente. IAM IAM
- Utilizza le condizioni nelle IAM politiche per limitare ulteriormente l'accesso: puoi aggiungere una condizione alle tue politiche per limitare l'accesso ad azioni e risorse. Ad esempio, puoi scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. È inoltre possibile utilizzare condizioni per concedere l'accesso alle azioni di servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta [Elementi IAM JSON della politica: Condizione](#) nella Guida IAM per l'utente.
- Usa IAM Access Analyzer per convalidare IAM le tue policy e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio delle IAM policy () e alle best practice. JSON IAM IAM Access Analyzer fornisce più di 100 controlli delle politiche e consigli pratici per aiutarti a creare policy sicure e funzionali. Per ulteriori informazioni, consulta [Convalida delle politiche con IAM Access Analyzer](#) nella Guida per l'utente. IAM
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede l'utilizzo di IAM utenti o di un utente root Account AWS, attiva questa opzione MFA per una maggiore sicurezza. Per richiedere MFA quando vengono richiamate API le operazioni, aggiungi MFA delle condizioni alle tue politiche. Per ulteriori informazioni, consulta [Secure API access with MFA](#) nella Guida IAM per l'utente.

Per ulteriori informazioni sulle best practice in IAM, consulta la sezione [Procedure consigliate in materia di sicurezza IAM](#) nella Guida IAM per l'utente.

Utilizzo della WorkDocs console Amazon

Per accedere alla WorkDocs console Amazon, devi disporre di un set minimo di autorizzazioni. Tali autorizzazioni devono consentirti di elencare e visualizzare i dettagli delle WorkDocs risorse Amazon

nel tuo AWS account. Se crei una politica basata sull'identità più restrittiva delle autorizzazioni minime richieste, la console non funzionerà come previsto per le entità utente o di ruolo. IAM

Per garantire che tali entità possano utilizzare la WorkDocs console Amazon, allega anche le seguenti politiche AWS gestite alle entità. Per ulteriori informazioni su come allegare le politiche, consulta [Aggiungere autorizzazioni a un utente nella Guida](#) per l'IAMutente.

- AmazonWorkDocsFullAccess
- AWSDirectoryServiceFullAccess
- Amazon EC2FullAccess

Queste politiche garantiscono all'utente l'accesso completo alle WorkDocs risorse di Amazon, alle operazioni di AWS Directory Service e alle EC2 operazioni Amazon di WorkDocs cui Amazon ha bisogno per funzionare correttamente.

Non è necessario consentire autorizzazioni minime per la console agli utenti che effettuano chiamate solo verso il AWS CLI o il AWS API. Consenti invece l'accesso solo alle azioni che corrispondono all'APIoperazione che stai cercando di eseguire.

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra come è possibile creare una politica che consenta IAM agli utenti di visualizzare le politiche in linea e gestite allegate alla loro identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando o a livello di codice. AWS CLI
AWS API

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",
        "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": "*"
    }
  ]
}

```

Consenti agli utenti l'accesso in sola lettura alle risorse Amazon WorkDocs

La seguente `AmazonWorkDocsReadOnlyAccess` politica AWS gestita concede a un IAM utente l'accesso in sola lettura alle risorse Amazon WorkDocs. La policy consente all'utente di accedere a tutte le WorkDocs Describe operazioni di Amazon. L'accesso alle due EC2 operazioni di Amazon è necessario per consentire ad Amazon di WorkDocs ottenere un elenco delle tue VPCs sottoreti. L'accesso all' AWS Directory Service DescribeDirectoriesoperazione è necessario per ottenere informazioni sulle tue AWS Directory Service directory.

```

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

```

}

Altri esempi di policy WorkDocs basate sull'identità di Amazon

IAM gli amministratori possono creare politiche aggiuntive per consentire a un IAM ruolo o a un utente di accedere ad Amazon WorkDocs API. Per ulteriori informazioni, consulta [Autenticazione e controllo degli accessi per applicazioni amministrative](#) nella Amazon WorkDocs Developer Guide.

Risoluzione dei problemi relativi all' WorkDocs identità e all'accesso ad Amazon

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare lavorando con Amazon WorkDocs e IAM.

Argomenti

- [Non sono autorizzato a eseguire un'azione in Amazon WorkDocs](#)
- [Non sono autorizzato a eseguire iam: PassRole](#)
- [Voglio consentire a persone esterne al mio AWS account di accedere alle mie WorkDocs risorse Amazon](#)

Non sono autorizzato a eseguire un'azione in Amazon WorkDocs

Se ti AWS Management Console dice che non sei autorizzato a eseguire un'azione, devi contattare l'amministratore per ricevere assistenza. L'amministratore è la persona da cui si sono ricevuti il nome utente e la password.

Non sono autorizzato a eseguire iam: PassRole

Se ricevi un messaggio di errore indicante che non sei autorizzato a eseguire l'`iam:PassRole` azione, le tue politiche devono essere aggiornate per consentirti di trasferire un ruolo ad Amazon WorkDocs.

Alcuni Servizi AWS consentono di trasferire un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

Il seguente errore di esempio si verifica quando un IAM utente denominato `marymajor` tenta di utilizzare la console per eseguire un'azione in Amazon WorkDocs. Tuttavia, l'azione richiede che

il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare il ruolo al servizio.

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

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire a persone esterne al mio AWS account di accedere alle mie WorkDocs risorse Amazon

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per i servizi che supportano politiche basate sulle risorse o liste di controllo degli accessi (ACLs), puoi utilizzare tali politiche per consentire alle persone di accedere alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se Amazon WorkDocs supporta queste funzionalità, consulta [Come WorkDocs funziona Amazon con IAM](#).
- Per sapere come fornire l'accesso alle tue risorse su Account AWS un sito di tua proprietà, consulta [Fornire l'accesso a un IAM utente di un altro Account AWS utente di tua proprietà](#) nella Guida per l'IAMutente.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta [Fornire l'accesso a persone Account AWS di proprietà di terzi](#) nella Guida per l'IAMutente.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta [Fornire l'accesso agli utenti autenticati esternamente \(federazione delle identità\)](#) nella Guida per l'IAMutente.
- Per conoscere la differenza tra l'utilizzo di ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta la sezione Accesso alle [risorse tra account nella Guida per l'utente](#). IAM IAM

Registrazione e monitoraggio in Amazon WorkDocs

Gli amministratori dei WorkDocs siti Amazon possono visualizzare ed esportare il feed delle attività per un intero sito. Possono anche essere utilizzati AWS CloudTrail per acquisire eventi dalla WorkDocs console Amazon.

Argomenti

- [Esportazione del feed di attività a livello di sito](#)
- [Utilizzo AWS CloudTrail per registrare WorkDocs API le chiamate Amazon](#)

Esportazione del feed di attività a livello di sito

Gli amministratori possono visualizzare ed esportare il feed attività per un intero sito. Per utilizzare questa funzionalità, devi prima installare Amazon WorkDocs Companion. Per installare Amazon WorkDocs Companion, consulta [App e integrazioni per Amazon WorkDocs](#).

Per visualizzare ed esportare il feed attività a livello di sito

1. Nell'applicazione web, scegli Attività.
2. Scegli Filtro, quindi sposta il cursore delle attività a livello di sito per attivare il filtro.
3. Selezionare i filtri Activity Type (Tipo di attività) e scegliere le impostazioni Date Modified (Data di modifica) come richiesto, quindi Apply (Applica).
4. Quando vengono visualizzati i risultati di feed attività filtrati, effettuare la ricerca per file, cartella o nome utente per ridurre i risultati. È inoltre possibile aggiungere o rimuovere filtri in base alle esigenze.
5. Scegliere Export (Esporta) per esportare i feed attività in file .csv e .json sul desktop. Il sistema esporta i file in una delle seguenti posizioni:
 - Windows: WorkDocsDownloadscartella nella cartella Download del PC
 - macOS – /users/**username**/WorkDocsDownloads/folder

Il file esportato riflette tutti i filtri applicati.

Note

Gli utenti che non sono amministratori possono visualizzare ed esportare il feed attività solo per i loro contenuti. Per ulteriori informazioni, consulta [Visualizzazione del feed delle attività](#) nella Amazon WorkDocs User Guide.

Utilizzo AWS CloudTrail per registrare WorkDocs API le chiamate Amazon

Puoi usare AWS CloudTrail; per registrare WorkDocs API le chiamate Amazon. CloudTrail fornisce un registro delle azioni intraprese da un utente, un ruolo o un AWS servizio in Amazon WorkDocs. CloudTrail acquisisce tutte le API chiamate per Amazon WorkDocs come eventi, incluse le chiamate dalla WorkDocs console Amazon e le chiamate in codice verso Amazon WorkDocs APIs.

Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per Amazon. WorkDocs Se non crei un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi.

Le informazioni raccolte da CloudTrail includono le richieste, gli indirizzi IP da cui sono state effettuate le richieste, gli utenti che hanno effettuato le richieste e le date della richiesta.

Per ulteriori informazioni in merito CloudTrail, consulta la [Guida AWS CloudTrail per l'utente](#).

WorkDocs Informazioni su Amazon in CloudTrail

CloudTrail è abilitato sul tuo AWS account al momento della creazione dell'account. Quando si verifica un'attività in Amazon WorkDocs, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi AWS di servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare gli eventi recenti nel tuo AWS account. Per ulteriori informazioni, consulta [Visualizzazione degli eventi con cronologia degli CloudTrail eventi](#).

Per una registrazione continua degli eventi nel tuo AWS account, inclusi gli eventi per Amazon WorkDocs, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando crei un trail nella console, il trail sarà valido in tutte le regioni. Il trail registra gli eventi da tutte le regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consultare:

- [Panoramica della creazione di un percorso](#)

- [CloudTrail servizi e integrazioni supportati](#)
- [Configurazione delle SNS notifiche Amazon per CloudTrail](#)
- [Ricezione di file di CloudTrail registro da più regioni](#) e [ricezione di file di CloudTrail registro da più account](#)

Tutte le WorkDocs azioni di Amazon vengono registrate CloudTrail e documentate in [Amazon WorkDocs API Reference](#). Ad esempio, le chiamate alle `CreateFolder` `UpdateDocument` sezioni `DeactivateUser` e generano voci nei file di CloudTrail registro.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali root o IAM utente.
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio.

Per ulteriori informazioni, vedete l'[CloudTrail userIdentityelemento](#).

Comprendere le voci dei file di WorkDocs log di Amazon

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle API chiamate pubbliche, quindi non vengono visualizzati in un ordine specifico.

Amazon WorkDocs genera diversi tipi di CloudTrail voci, quelle dal piano di controllo e quelle dal piano dati. La differenza importante tra i due è che l'identità utente per le voci del piano di controllo è un IAM utente. L'identità utente per le voci del piano dati è l'utente della WorkDocs directory Amazon.

Note

Per una maggiore sicurezza, crea utenti federati anziché IAM utenti quando possibile.

Le informazioni sensibili, ad esempio le password, i token di autenticazione, i commenti e i contenuti dei file, vengono incluse nelle voci di log. Questi vengono visualizzati come `HIDDEN _ DUE _ TO _ SECURITY _ REASONS` nei log. CloudTrail Questi vengono visualizzati come `HIDDEN _ DUE SECURITY _ TO _ _` nei log. REASONS CloudTrail

L'esempio seguente mostra due voci di CloudTrail registro per Amazon WorkDocs: il primo record è per un'azione del piano di controllo e il secondo è per un'azione del piano dati.

```
{
  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"
}
]
```

Convalida della conformità per Amazon WorkDocs

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione [Scope by Compliance Program Servizi AWS](#) e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di [AWS conformità Programmi](#) di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta [Scaricamento dei report in AWS Artifact](#) .

La vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- [Guide introduttive su sicurezza e conformità](#): queste guide all'implementazione illustrano considerazioni sull'architettura e forniscono passaggi per implementare ambienti di base incentrati sulla AWS sicurezza e la conformità.
- [Architettura per la HIPAA sicurezza e la conformità su Amazon Web Services](#): questo white paper descrive in che modo le aziende possono utilizzare AWS per creare applicazioni idonee. HIPAA

Note

Non tutte sono idonee. Servizi AWS HIPAA Per ulteriori informazioni, consulta la [Guida ai servizi HIPAA idonei](#).

- [AWS Risorse per AWS](#) per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe riguardare il tuo settore e la tua località.
- [AWS Guide alla conformità dei clienti](#): comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione Servizi AWS e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization ()). ISO
- [Evaluating Resources with Rules](#) nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida del settore e alle normative.
- [AWS Security Hub](#)— Ciò Servizio AWS fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina [Documentazione di riferimento sui controlli della Centrale di sicurezza](#).
- [Amazon GuardDuty](#): Servizio AWS rileva potenziali minacce ai tuoi carichi di lavoro Account AWS, ai contenitori e ai dati monitorando l'ambiente alla ricerca di attività sospette e dannose. GuardDuty può aiutarti a soddisfare vari requisiti di conformità, ad esempio PCI DSS soddisfacendo i requisiti di rilevamento delle intrusioni imposti da determinati framework di conformità.
- [AWS Audit Manager](#)— Ciò Servizio AWS consente di verificare continuamente AWS l'utilizzo per semplificare la gestione del rischio e la conformità alle normative e agli standard di settore.

Resilienza in Amazon WorkDocs

L'infrastruttura AWS globale è costruita attorno a AWS regioni e zone di disponibilità. AWS Le regioni forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità, è possibile progettare e gestire applicazioni e database che eseguono il failover automatico tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture tradizionali a data center singolo o multiplo.

[Per ulteriori informazioni su AWS regioni e zone di disponibilità, consulta Global Infrastructure.AWS](#)

Sicurezza dell'infrastruttura in Amazon WorkDocs

In quanto servizio gestito, Amazon WorkDocs è protetto dalle procedure di sicurezza della rete AWS globale. Per ulteriori informazioni, consulta la sezione [Sicurezza dell'infrastruttura in AWS Identity and Access Management](#) nella Guida per l'IAMutente e [Best practice for Security, Identity e Compliance](#) nell' AWS Architecture Center.

Utilizzi API le chiamate AWS pubblicate per accedere ad Amazon WorkDocs tramite la rete. I client devono supportare Transport Layer Security (TLS) 1.2 e consigliamo di utilizzare TLS 1.3. I client devono inoltre supportare suite di crittografia con perfetta segretezza di inoltrare, come Ephemeral Diffie-Hellman o Elliptic Curve Ephemeral Diffie-Hellman. La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale. IAM In alternativa, è possibile utilizzare [AWS Security Token Service](#) (AWS STS) per generare le credenziali di sicurezza temporanee per sottoscrivere le richieste.

Guida introduttiva ad Amazon WorkDocs

Amazon WorkDocs utilizza una directory per archiviare e gestire le informazioni sull'organizzazione per gli utenti e i relativi documenti. A sua volta, alleggi una directory a un sito quando esegui il provisioning di quel sito. Quando lo fai, una WorkDocs funzionalità di Amazon chiamata Attivazione automatica aggiunge gli utenti della directory al sito come utenti gestiti, il che significa che non hanno bisogno di credenziali separate per accedere al tuo sito e possono condividere e collaborare sui file. Ogni utente dispone di 1 TB di spazio di archiviazione a meno che non ne acquisti altro.

Non è più necessario aggiungere e attivare gli utenti manualmente, ma è comunque possibile. Puoi anche modificare i ruoli e le autorizzazioni degli utenti ogni volta che ne hai bisogno. Per ulteriori informazioni su questa operazione [Invitare e gestire WorkDocs gli utenti Amazon](#), consulta più avanti in questa guida.

Se hai bisogno di creare delle directory, puoi:

- Creazione di una directory Simple AD
- Crea una directory AD Connector per connetterti alla tua directory locale.
- Consenti WorkDocs ad Amazon di lavorare con una AWS directory esistente.
- Chiedi ad Amazon di WorkDocs creare una directory per te.

Puoi anche creare una relazione di trust tra la directory AD e una directory AWS Managed Microsoft AD.

Note

Se si appartiene a un programma di conformità come PCI, FedRAMP o DoD, è necessario configurare una directory per soddisfare i requisiti di conformità. AWS Managed Microsoft AD I passaggi di questa sezione spiegano come utilizzare una directory Microsoft AD esistente. Per informazioni sulla creazione di una directory Microsoft AD, consulta [AWS Managed Microsoft AD](#) nella AWS Directory Service Administration Guide.

Indice

- [Creare un WorkDocs sito Amazon](#)
- [Abilitazione di Single Sign-On](#)

- [Abilitazione dell'autenticazione a più fattori](#)
- [Promozione di un utente ad amministratore](#)

Creare un WorkDocs sito Amazon

I passaggi nelle sezioni seguenti spiegano come configurare un nuovo WorkDocs sito Amazon.

Attività

- [Prima di iniziare](#)
- [Creare un WorkDocs sito Amazon](#)

Prima di iniziare

È necessario disporre dei seguenti articoli prima di creare un WorkDocs sito Amazon.

- Un AWS account per creare e amministrare WorkDocs siti Amazon. Tuttavia, gli utenti non hanno bisogno di un AWS account per connettersi e utilizzare Amazon WorkDocs. Per ulteriori informazioni, consulta [Prerequisiti per Amazon WorkDocs](#).
- Se si prevede di utilizzare Simple AD, è necessario soddisfare i prerequisiti identificati in [Simple AD Prerequisites](#) nella AWS Directory Service Administration Guide.
- Una AWS Managed Microsoft AD directory se si appartiene a un programma di conformità come PCI, FedRAMP o DoD. I passaggi di questa sezione spiegano come utilizzare una directory Microsoft AD esistente. Per informazioni sulla creazione di una directory Microsoft AD, consulta [AWS Managed Microsoft AD](#) nella AWS Directory Service Administration Guide.
- Informazioni sul profilo dell'amministratore, inclusi nome e cognome e un indirizzo e-mail.

Creare un WorkDocs sito Amazon

Segui questi passaggi per creare un WorkDocs sito Amazon in pochi minuti.

Per creare il WorkDocs sito Amazon

1. Apri la WorkDocs console Amazon all'[indirizzo https://console.aws.amazon.com/zocalo/](https://console.aws.amazon.com/zocalo/).
2. Nella home page della console, in Crea un WorkDocs sito, scegli Inizia subito.

- OPPURE -

Nel riquadro di navigazione, scegli I miei siti e nella pagina Gestisci i tuoi WorkDocs siti scegli Crea un WorkDocs sito.

Quello che succede dopo dipende dal fatto che tu abbia o meno una directory.

- Se si dispone di una directory, viene visualizzata la pagina Seleziona una directory che consente di scegliere una directory esistente o creare una directory.
- Se non si dispone di una directory, viene visualizzata la pagina Configura un tipo di directory che consente di creare una directory Simple AD o AD Connector.

I passaggi seguenti spiegano come eseguire entrambe le attività.

Per utilizzare una directory esistente

1. Apri l'elenco delle directory disponibili e scegli la directory che desideri utilizzare.
2. Scegliere Enable directory (Abilita directory).

Per creare una directory

1. Ripeti i passaggi 1 e 2 precedenti.

A questo punto, ciò che fai dipende dal fatto che desideri utilizzare Simple AD o creare un AD Connector.

Per usare Simple AD

- a. Scegli Simple AD, quindi scegli Avanti.

Viene visualizzata la pagina del sito Create Simple AD.

- b. In Punto di accesso, nella casella URL del sito, inserisci l'URL del sito.
- c. In Imposta WorkDocs amministratore, inserisci l'indirizzo e-mail, il nome e il cognome dell'amministratore.
- d. Se necessario, completa le opzioni in Dettagli della directory e configurazione VPC.
- e. Scegli il sito Create Simple AD.

Per creare una directory AD Connector

- a. Scegli AD Connector, quindi scegli Avanti.

Viene visualizzata la pagina del sito Create AD Connector.

- b. Compila tutti i campi in Dettagli della directory.
- c. In Punto di accesso, nella casella URL del sito, inserisci l'URL del sito.
- d. Se lo desideri, completa i campi opzionali in Configurazione VPC.
- e. Scegli Crea sito AD Connector.

Amazon WorkDocs esegue le seguenti operazioni:

- Se hai scelto Configura un VPC per mio conto nel passaggio 4 precedente, Amazon WorkDocs crea un VPC per te. Una directory nel VPC memorizza le informazioni sugli utenti e WorkDocs sul sito Amazon.
- Se hai usato Simple AD, Amazon WorkDocs crea un utente di directory e imposta quell'utente come WorkDocs amministratore Amazon. Se hai creato una directory AD Connector, Amazon WorkDocs imposta l'utente della directory esistente che hai fornito come WorkDocs amministratore.
- Se hai utilizzato una directory esistente, Amazon WorkDocs ti chiede di inserire il nome utente dell'amministratore Amazon WorkDocs . L'utente deve essere un membro della directory.

Note

Amazon WorkDocs non notifica agli utenti il nuovo sito. Devi comunicare loro l'URL e far loro sapere che non hanno bisogno di un accesso separato per utilizzare il sito.

Abilitazione di Single Sign-On

AWS Directory Service consente agli utenti di accedere ad Amazon WorkDocs da un computer inserito nella stessa directory in cui Amazon WorkDocs è registrato, senza inserire le credenziali separatamente. WorkDocs Gli amministratori di Amazon possono abilitare il Single Sign-On utilizzando la console. AWS Directory Service Per ulteriori informazioni, consulta [Single Sign-on nella Guida all'amministrazione. AWS Directory Service](#)

Dopo che l' WorkDocs amministratore Amazon ha abilitato il Single Sign-On, gli utenti WorkDocs del sito Amazon potrebbero anche dover modificare le impostazioni del browser Web per consentire il Single Sign-On. Per ulteriori informazioni, consulta [Single sign-on per IE e Chrome](#) e [Single sign-on per Firefox](#) nella Guida all'amministrazione. AWS Directory Service

Abilitazione dell'autenticazione a più fattori

È possibile utilizzare la AWS Directory Services Console all'[indirizzo https://console.aws.amazon.com/directoryservicev2/](https://console.aws.amazon.com/directoryservicev2/) per abilitare l'autenticazione a più fattori per la directory AD Connector. Per abilitare MFA, è necessario disporre di una soluzione MFA che funge da server Remote Authentication Dial-In User Service (RADIUS) oppure disporre di un plug-in MFA per un server RADIUS già implementato nell'infrastruttura on-premise. La soluzione MFA deve implementare i codici d'accesso monouso (OTP, One Time Passcode) che gli utenti ottengono da un dispositivo hardware o dal software in esecuzione su un dispositivo, ad esempio un telefono cellulare.

RADIUS è un protocollo client/server standard del settore che fornisce l'autenticazione, l'autorizzazione e la gestione contabile per consentire agli utenti di connettersi ai servizi di rete. AWS Managed Microsoft AD include un client RADIUS che si connette al server RADIUS su cui hai implementato la tua soluzione MFA. Il server RADIUS convalida il nome utente e il codice OTP. Se il server RADIUS convalida correttamente l'utente, AWS Managed Microsoft AD autentica l'utente con AD. Una volta completata l'autenticazione AD, gli utenti possono accedere all'applicazione AWS. La comunicazione tra il client AWS Managed Microsoft AD RADIUS e il server RADIUS richiede la configurazione di gruppi di sicurezza AWS che abilitano la comunicazione sulla porta 1812.

Per ulteriori informazioni, consulta [Abilita l'autenticazione a più fattori per AWS Managed Microsoft AD](#) nella AWS Directory Service Administration Guide.

Note

L'autenticazione a più fattori non è disponibile per le directory Simple AD.

Promozione di un utente ad amministratore

Utilizzi la WorkDocs console Amazon per promuovere un utente a amministratore. Segui questi passaggi.

Per promuovere un utente ad amministratore

1. Apri la WorkDocs console Amazon all'[indirizzo https://console.aws.amazon.com/zocalo/](https://console.aws.amazon.com/zocalo/).
2. Nel riquadro di navigazione, scegli I miei siti.

Viene visualizzata la pagina Gestisci WorkDocs i tuoi siti.

3. Seleziona il pulsante accanto al sito desiderato, scegli Azioni, quindi scegli Imposta un amministratore.

Viene visualizzata la finestra di dialogo Imposta WorkDocs amministratore.

4. Nella casella Nome utente, inserisci il nome utente della persona che desideri promuovere, quindi scegli Imposta amministratore.

Puoi anche utilizzare il pannello di controllo di amministrazione del WorkDocs sito Amazon per abbassare il livello di un amministratore. Per ulteriori informazioni, consulta [Modifica di utenti](#).

Gestione di Amazon WorkDocs dalla AWS console

Utilizzi questi strumenti per gestire i tuoi WorkDocs siti Amazon:

- La AWS console all'[indirizzo https://console.aws.amazon.com/zocalo/](https://console.aws.amazon.com/zocalo/).
- Il pannello di controllo dell'amministratore del sito, disponibile per gli amministratori di tutti i WorkDocs siti Amazon.

Ciascuno di questi strumenti fornisce un diverso set di azioni e gli argomenti di questa sezione spiegano le azioni fornite dalla AWS console. Per informazioni sul pannello di controllo di amministrazione del sito, consulta [Gestione di Amazon WorkDocs dal pannello di controllo di amministrazione del sito](#).

Impostazione degli amministratori del sito

Se sei un amministratore, puoi consentire agli utenti di accedere al pannello di controllo del sito e alle azioni che fornisce.

Per impostare un amministratore

1. Apri la WorkDocs console Amazon all'[indirizzo https://console.aws.amazon.com/zocalo/](https://console.aws.amazon.com/zocalo/).
2. Nel riquadro di navigazione, scegli I miei siti.

Viene visualizzata la pagina Gestisci WorkDocs i tuoi siti e mostra un elenco dei tuoi siti.

3. Scegli il pulsante accanto al sito per il quale desideri impostare un amministratore.
4. Apri l'elenco Azioni e scegli Imposta un amministratore.

Viene visualizzata la finestra di dialogo Imposta WorkDocs amministratore.

5. Nella casella Nome utente, inserisci il nome del nuovo amministratore, quindi scegli Imposta amministratore.

Reinvio delle email di invito

Puoi inviare nuovamente un'e-mail di invito in qualsiasi momento.

Per inviare nuovamente l'e-mail di invito

1. Apri la WorkDocs console Amazon all'[indirizzo https://console.aws.amazon.com/zocalo/](https://console.aws.amazon.com/zocalo/).
2. Nel riquadro di navigazione, scegli I miei siti.

Viene visualizzata la pagina Gestisci WorkDocs i tuoi siti e mostra un elenco dei tuoi siti.

3. Scegli il pulsante accanto al sito per il quale desideri inviare nuovamente l'email.
4. Apri l'elenco Azioni e scegli Reinvia l'email di invito.

Nella parte superiore della pagina viene visualizzato un messaggio di successo in un banner verde.

Gestione dell'autenticazione a più fattori

Puoi abilitare l'autenticazione a più fattori dopo aver creato un WorkDocs sito Amazon. Per ulteriori informazioni sull'autenticazione, consulta [Abilitazione dell'autenticazione a più fattori](#).

Impostazione degli URL dei siti

Note

Se hai seguito la procedura di creazione del sito in [Guida introduttiva ad Amazon WorkDocs](#), hai inserito l'URL del sito. Di conseguenza, Amazon WorkDocs rende il comando Set site URL non disponibile, poiché puoi impostare un URL solo una volta. Segui questi passaggi solo se distribuisce Amazon WorkSpaces e lo integri con Amazon WorkDocs. Il processo di WorkSpaces integrazione con Amazon prevede l'immissione di un numero di serie anziché l'URL del sito, quindi è necessario inserire un URL dopo aver completato l'integrazione. Per ulteriori informazioni sull'integrazione di Amazon WorkSpaces e Amazon, WorkDocs consulta [Integrate with WorkDocs](#) nella Amazon WorkSpaces User Guide.

Per impostare l'URL di un sito

1. Apri la WorkDocs console Amazon all'[indirizzo https://console.aws.amazon.com/zocalo/](https://console.aws.amazon.com/zocalo/).
2. Nel riquadro di navigazione, scegli I miei siti.

Viene visualizzata la pagina Gestisci WorkDocs i tuoi siti e mostra un elenco dei tuoi siti.

3. Seleziona il sito che hai integrato con Amazon WorkSpaces. L'URL contiene l'ID di directory della tua WorkSpaces istanza Amazon, ad esempio `https://{directory_id}.awsapps.com`.
4. Scegli il pulsante accanto a quell'URL, apri l'elenco Azioni e scegli Imposta URL del sito.

Viene visualizzata la finestra di dialogo Imposta l'URL del sito.

5. Nella casella URL del sito, inserisci l'URL del sito, quindi scegli Imposta URL del sito.
6. Nella pagina Gestisci i tuoi WorkDocs siti, scegli Aggiorna per vedere il nuovo URL.

Gestione delle notifiche

Note

Per una maggiore sicurezza, crea utenti federati anziché utenti IAM quando possibile.

Le notifiche consentono agli utenti o ai ruoli IAM di chiamare l'[CreateNotificationSubscriptionAPI](#), che puoi utilizzare per impostare il tuo endpoint per l'elaborazione dei messaggi SNS inviati. WorkDocs Per ulteriori informazioni sulle notifiche, consulta [Configurazione delle notifiche per un utente o un ruolo IAM](#) nella Amazon WorkDocs Developer Guide.

Puoi creare ed eliminare notifiche e i passaggi seguenti spiegano come eseguire entrambe le attività.

Note

Per creare una notifica, devi disporre del tuo IAM o del ruolo ARN. Per trovare il tuo IAM ARN, procedi come segue:

1. Aprire la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nella barra di navigazione, seleziona Utenti.
3. Seleziona il tuo nome utente.
4. In Riepilogo, copia il tuo ARN.

Per creare una notifica

1. Apri la WorkDocs console Amazon all'indirizzo <https://console.aws.amazon.com/zocalo/>.
2. Nel riquadro di navigazione, scegli I miei siti.

Viene visualizzata la pagina Gestisci WorkDocs i tuoi siti e mostra un elenco dei tuoi siti.

3. Scegli il pulsante accanto al sito desiderato.
4. Apri l'elenco Azioni e scegli Gestisci notifiche.

Viene visualizzata la pagina Gestisci notifiche.

5. Selezionare Create Notification (Crea notifica).
6. Nella finestra di dialogo Nuova notifica, inserisci il tuo IAM o l'ARN del ruolo, quindi scegli Crea notifiche.

Per eliminare una notifica

1. Apri la WorkDocs console Amazon all'[indirizzo https://console.aws.amazon.com/zocalo/](https://console.aws.amazon.com/zocalo/).
2. Nel riquadro di navigazione, scegli I miei siti.

Viene visualizzata la pagina Gestisci WorkDocs i tuoi siti e mostra un elenco dei tuoi siti.

3. Scegli il pulsante accanto al sito che contiene la notifica che desideri eliminare.
4. Apri l'elenco Azioni e scegli Gestisci notifiche.
5. Nella pagina Gestisci notifiche, scegli il pulsante accanto alla notifica che desideri eliminare, quindi scegli Elimina notifiche.

Eliminazione di un sito

Utilizzi la WorkDocs console Amazon per eliminare un sito.

Warning

Quando elimini un sito, perdi tutti i file. Eliminare un sito solo se si è sicuri che le informazioni non sono più necessarie.

Per eliminare un sito

1. Apri la WorkDocs console Amazon all'[indirizzo https://console.aws.amazon.com/zocalo/](https://console.aws.amazon.com/zocalo/).
2. Nella barra di navigazione, scegli I miei siti.

Viene visualizzata la pagina Gestisci WorkDocs i tuoi siti.

3. Scegli il pulsante accanto al sito che desideri eliminare, quindi scegli Elimina.

Viene visualizzata la finestra di dialogo Elimina l'URL del sito.

4. Facoltativamente, scegli Elimina anche la directory utente.

 Important

Se non fornisci la tua directory per Amazon WorkDocs, ne creiamo una per te. Quando elimini il WorkDocs sito Amazon, ti viene addebitato il costo della directory che creiamo, a meno che tu non elimini quella directory o la usi per un'altra applicazione AWS. Per informazioni sui prezzi, consulta [Prezzi di AWS Directory Service](#).

5. Nella casella URL del sito, inserisci l'URL del sito, quindi scegli Elimina.

Il sito viene eliminato immediatamente e non è più disponibile.

Gestione di Amazon WorkDocs dal pannello di controllo di amministrazione del sito

Utilizzi questi strumenti per gestire i tuoi WorkDocs siti Amazon:

- Il pannello di controllo dell'amministratore del sito, disponibile per gli amministratori di tutti i WorkDocs siti Amazon e descritto nei seguenti argomenti.
- La AWS console all'indirizzo <https://console.aws.amazon.com/zocalo/>.

Ciascuno di questi strumenti fornisce un insieme diverso di azioni. Gli argomenti di questa sezione spiegano le azioni fornite dal pannello di controllo di amministrazione del sito. Per informazioni sulle attività disponibili nella console, consulta [Gestione di Amazon WorkDocs dalla AWS console](#).

Impostazioni lingua preferite

È possibile specificare la lingua per le notifiche e-mail.

Per modificare le impostazioni della lingua

1. In My Account (Account personale) scegliere Open admin control panel (Apri pannello di controllo admin).
2. In Preferred Language Settings (Impostazioni lingua preferita) scegliere la lingua preferita.

Hancom Online Editing e Office Online

Abilita o disabilita le impostazioni Hancom Online Editing e Office Online dal pannello di controllo Admin (Amministratore). Per ulteriori informazioni, consulta [Abilitazione della modifica collaborativa](#).

Storage

È possibile specificare la quantità di storage che i nuovi utenti devono ricevere.

Per modificare le impostazioni di storage

1. In My Account (Account personale) scegliere Open admin control panel (Apri pannello di controllo admin).

2. In Storage scegliere Change (Modifica).
3. Nella finestra di dialogo Storage Limit (Limite di storage) scegliere se offrire storage limitato o illimitato ai nuovi utenti.
4. Seleziona Salva modifiche.

La modifica delle impostazioni di storage interessa solo gli utenti che vengono aggiunti dopo la modifica. La quantità di storage allocata agli utenti esistenti non viene modificata. Per modificare il limite di storage per un utente esistente, vedi [Modifica di utenti](#).

Elenco indirizzi IP consentiti

Gli amministratori dei WorkDocs siti Amazon possono aggiungere impostazioni IP Allow List per limitare l'accesso al sito a un intervallo consentito di indirizzi IP. Puoi aggiungere fino a 500 impostazioni IP Allow List per sito.

Note

L'elenco di indirizzi IP consentiti attualmente funziona solo per gli indirizzi IPv4. L'elenco negato degli indirizzi IP non è attualmente supportato.

Per aggiungere un intervallo di IP all'elenco di IP consentiti

1. In My Account (Account personale) scegliere Open admin control panel (Apri pannello di controllo admin).
2. Per IP Allow List (Elenco di indirizzi IP consentiti) scegli Change (Modifica).
3. Per Inserisci il valore CIDR, inserisci il blocco Classless Inter-Domain Routing (CIDR) per gli intervalli di indirizzi IP e scegli Aggiungi.
 - Per consentire l'accesso da un singolo indirizzo IP, specifica /32 come prefisso CIDR.
4. Seleziona Salva modifiche.
5. L'accesso è consentito agli utenti che si connettono al sito da un indirizzo IP presente nell'elenco degli indirizzi IP consentiti. Gli utenti che tentano di connettersi al sito da indirizzi IP non autorizzati ricevono una risposta di accesso non autorizzato.

⚠ Warning

Se immetti un valore CIDR che ti impedisce di utilizzare l'indirizzo IP corrente per accedere al sito, viene visualizzato un messaggio di avviso. Se scegli di continuare con il valore CIDR corrente, verrà bloccato l'accesso al sito con l'indirizzo IP corrente. Questa operazione può essere annullata solo contattando AWS Support.

Sicurezza: siti semplici ActiveDirectory

Questo argomento spiega le varie impostazioni di sicurezza per i ActiveDirectory siti Simple. Se gestisci siti che utilizzano il ActiveDirectory connettore, consulta la sezione successiva.

Per utilizzare le impostazioni di sicurezza

1. Scegli l'icona del profilo nell'angolo in alto a destra del client WorkDocs



2. In Amministratore, scegli Apri pannello di controllo di amministrazione.
3. Scorri verso il basso fino a Sicurezza e scegli Modifica.

Viene visualizzata la finestra di dialogo Impostazioni dei criteri. La tabella seguente elenca le impostazioni di sicurezza per i ActiveDirectory siti semplici.

Impostazione

Descrizione

In Scegli l'impostazione per i link condivisibili, seleziona una delle seguenti opzioni:

Non consentite link condivisibili a livello di sito o pubblici

Disattiva la condivisione dei link per tutti gli utenti.

Consenti agli utenti di creare link condivisibili a livello di sito, ma non consenti loro di creare link condivisibili pubblici

Limita la condivisione dei link ai soli membri del sito. Gli utenti gestiti possono creare questo tipo di link.

Impostazione

Descrizione

Consenti agli utenti di creare link condivisibili a livello di sito, ma solo gli utenti esperti possono creare link condivisibili pubblici

Gli utenti gestiti possono creare collegamenti a livello di sito, ma solo gli utenti esperti possono creare collegamenti pubblici. I link pubblici consentono l'accesso a chiunque su Internet.

Tutti gli utenti gestiti possono creare link condivisibili pubblici e a livello di sito

Gli utenti gestiti possono creare link pubblici.

In Attivazione automatica, seleziona o deseleziona la casella di controllo.

Consenti l'attivazione automatica di tutti gli utenti della tua directory al primo accesso al tuo WorkDocs sito.

Attiva automaticamente gli utenti al primo accesso al tuo sito.

In Chi dovrebbe essere autorizzato a invitare nuovi utenti WorkDocs sul tuo sito, seleziona una delle seguenti opzioni:

Solo gli amministratori possono invitare nuovi utenti.

Solo gli amministratori possono invitare nuovi utenti.

Gli utenti possono invitare nuovi utenti da qualsiasi luogo condividendo file o cartelle con loro.

Consente agli utenti di invitare nuovi utenti condividendo file o cartelle con tali utenti.

Gli utenti possono invitare nuovi utenti da alcuni domini specifici condividendo file o cartelle con loro.

Gli utenti possono invitare nuovi utenti di domini specifici condividendo con loro file o cartelle.

In Configura il ruolo per i nuovi utenti, seleziona o deseleziona la casella di controllo.

I nuovi utenti della tua directory saranno utenti gestiti (per impostazione predefinita sono utenti ospiti)

Converte automaticamente i nuovi utenti dalla tua directory in utenti gestiti.

4. Al termine, scegli Salva modifiche.

Sicurezza: siti di ActiveDirectory connessione

Questo argomento spiega le varie impostazioni di sicurezza per i siti dei ActiveDirectory connettori. Se gestisci siti che utilizzano Simple ActiveDirectory, consulta la sezione precedente.

Per utilizzare le impostazioni di sicurezza

1. Scegli l'icona del profilo nell'angolo in alto a destra del client. WorkDocs



2. In Amministratore, scegli Apri pannello di controllo di amministrazione.
3. Scorri verso il basso fino a Sicurezza e scegli Modifica.

Viene visualizzata la finestra di dialogo Impostazioni dei criteri. La tabella seguente elenca e descrive le impostazioni di sicurezza per i siti dei ActiveDirectory connettori.

Impostazione	Descrizione
In Scegli l'impostazione per i link condivisibili, seleziona una delle seguenti opzioni:	
Non consentite link condivisibili a livello di sito o pubblici	Se selezionata, disabilita la condivisione dei link per tutti gli utenti.
Consenti agli utenti di creare link condivisibili a livello di sito, ma non consenti loro di creare link condivisibili pubblici	Limita la condivisione dei link ai soli membri del sito. Gli utenti gestiti possono creare questo tipo di link.
Consenti agli utenti di creare link condivisibili a livello di sito, ma solo gli utenti esperti possono creare link condivisibili pubblici	Gli utenti gestiti possono creare collegamenti a livello di sito, ma solo gli utenti esperti possono creare collegamenti pubblici. I link pubblici consentono l'accesso a chiunque su Internet.
Tutti gli utenti gestiti possono creare link condivisibili pubblici e a livello di sito	Gli utenti gestiti possono creare link pubblici.

In Attivazione automatica, seleziona o deseleziona la casella di controllo.

Impostazione

Descrizione

Consenti l'attivazione automatica di tutti gli utenti della tua directory al primo accesso al tuo WorkDocs sito.

Attiva automaticamente gli utenti al primo accesso al tuo sito.

In Chi dovrebbe essere autorizzato ad attivare gli utenti della directory WorkDocs sul tuo sito? , seleziona una delle seguenti opzioni:

Solo gli amministratori possono attivare nuovi utenti dalla tua directory.

Consente solo agli amministratori di attivare nuovi utenti della directory.

Gli utenti possono attivare nuovi utenti dalla directory condividendo file o cartelle con loro.

Consente agli utenti di attivare gli utenti della directory condividendo file o cartelle con gli utenti della directory.

Gli utenti possono attivare nuovi utenti da alcuni domini specifici condividendo file o cartelle con loro.

Gli utenti possono condividere file o cartelle solo da utenti di domini specifici. Quando scegli questa opzione, devi inserire i domini.

In Chi dovrebbe essere autorizzato a invitare nuovi utenti WorkDocs sul tuo sito? , seleziona una delle seguenti opzioni:

Share with external users (Condividi con utenti esterni)

Enables administrators and users to invite new external users to your Amazon WorkDocs site.

Note

Le opzioni seguenti vengono visualizzate solo dopo aver scelto questa impostazione.

Only administrators can invite new external users (Solo gli amministratori possono invitare nuovi utenti esterni)

Solo gli amministratori possono invitare utenti esterni.

Tutti gli utenti gestiti possono invitare nuovi utenti

Consente agli utenti gestiti di invitare utenti esterni.

Impostazione	Descrizione
Solo gli utenti esperti possono invitare nuovi utenti esterni.	Consente solo agli utenti esperti di invitare nuovi utenti esterni.
In Configura il ruolo per i nuovi utenti, seleziona una o entrambe le opzioni.	
I nuovi utenti della tua directory saranno utenti gestiti (per impostazione predefinita sono utenti ospiti)	Converte automaticamente i nuovi utenti dalla tua directory in utenti gestiti.
New external users from your directory will be Managed users (they are Guest users by default) (I nuovi utenti esterni della directory saranno utenti gestiti (utenti guest per impostazione predefinita))	Converte automaticamente i nuovi utenti esterni in utenti gestiti.

4. Al termine, scegli Salva modifiche.

Conservazione del cestino di recupero

Quando un utente elimina un file, Amazon lo WorkDocs archivia nel cestino dell'utente per 30 giorni. Successivamente, Amazon WorkDocs sposta i file in un contenitore di ripristino temporaneo per 60 giorni, quindi li elimina definitivamente. Solo gli amministratori possono visualizzare il contenitore di ripristino temporaneo. Modificando la politica di conservazione dei dati a livello di sito, gli amministratori del sito possono modificare il periodo di conservazione del Recovery Bin da un minimo di zero giorni a un massimo di 365.

Per modificare il periodo di retention del cestino di recupero

1. In My Account (Account personale) scegliere Open admin control panel (Apri pannello di controllo admin).
2. Accanto a Recovery bin retention (Retention cestino di recupero) scegliere Change (Modifica).
3. Inserisci il numero di giorni in cui conservare i file nel cestino di ripristino e scegli Salva.

 Note

Il periodo di retention predefinito è 60 giorni. Puoi utilizzare un periodo compreso tra 0 e 365 giorni.

Gli amministratori possono ripristinare i file degli utenti dal cestino di ripristino prima che Amazon li WorkDocs elimini definitivamente.

Per ripristinare un file utente

1. In My Account (Account personale) scegliere Open admin control panel (Apri pannello di controllo admin).
2. In Manage Users (Gestisci utenti) scegliere l'icona della cartella dell'utente.
3. In Recovery bin (Cestino di recupero), selezionare i file da ripristinare e scegliere l'icona Recover (Recupera).
4. Per Restore file (Ripristina file) scegliere la posizione in cui ripristinare il file, quindi scegliere Restore (Ripristina).

Gestione delle impostazioni utente

È possibile gestire le impostazioni per gli utenti, ad esempio modificare i ruoli utente e invitare, abilitare o disabilitare utenti. Per ulteriori informazioni, consulta [Invitare e gestire WorkDocs gli utenti Amazon](#).

Distribuzione di Amazon WorkDocs Drive su più computer

Se disponi di un parco macchine aggiunto al dominio, puoi utilizzare gli oggetti Criteri di gruppo (GPO) o System Center Configuration Manager (SCCM) per installare il client Amazon WorkDocs Drive. Puoi scaricare il client da <https://amazonworkdocs.com/en/clients>.

Tieni presente che Amazon WorkDocs Drive richiede l'accesso HTTPS sulla porta 443 per tutti gli indirizzi IP AWS. È inoltre necessario confermare che i sistemi di destinazione soddisfano i requisiti di installazione di Amazon WorkDocs Drive. Per ulteriori informazioni, consulta [Installazione di Amazon WorkDocs Drive](#) nella Guida per l'utente di Amazon WorkDocs.

Note

Come best practice quando si utilizza un oggetto Criteri di gruppo o SCCM, installare il client Amazon WorkDocs Drive dopo l'accesso degli utenti.

Il programma di installazione MSI per Amazon WorkDocs Drive supporta i seguenti parametri di installazione opzionali:

- **SITEID** Precompila le informazioni del sito Amazon WorkDocs per gli utenti durante la registrazione. Ad esempio: `SITEID=site-name`.
- **DefaultDriveLetter** Precompila la lettera del drive da utilizzare per il montaggio di Amazon WorkDocs Drive. Ad esempio: `DefaultDriveLetter=W`. Ricorda che ogni utente deve avere una lettera di unità diversa. Inoltre, gli utenti possono modificare il nome dell'unità, ma non la lettera dell'unità, dopo aver avviato Amazon WorkDocs Drive per la prima volta.

L'esempio seguente distribuisce Amazon WorkDocs Drive senza interfacce utente e nessun riavvio. Si noti che utilizza il nome predefinito del file MSI:

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

Invitare e gestire WorkDocs gli utenti Amazon

Per impostazione predefinita, quando alleghi una directory durante la creazione del sito, la funzione di attivazione automatica di Amazon WorkDocs aggiunge tutti gli utenti di quella directory al nuovo sito come utenti gestiti.

In WorkDocs, gli utenti gestiti non devono accedere con credenziali separate. Possono condividere e collaborare sui file e dispongono automaticamente di 1 TB di spazio di archiviazione. Tuttavia, puoi disattivare l'attivazione automatica quando desideri aggiungere solo alcuni utenti in una directory e i passaggi nelle sezioni successive spiegano come farlo.

Inoltre, puoi invitare, abilitare o disabilitare gli utenti e modificare i ruoli e le impostazioni degli utenti. Puoi anche promuovere un utente a amministratore. Per ulteriori informazioni sulla promozione degli utenti, consulta [Promozione di un utente ad amministratore](#).

Esegui queste attività nel pannello di controllo amministrativo del client WorkDocs web Amazon e i passaggi nelle sezioni seguenti spiegano come. Tuttavia, se non conosci Amazon WorkDocs, dedica qualche minuto e scopri i vari ruoli utente prima di immergerti nelle attività amministrative.

Indice

- [Panoramica dei ruoli utente](#)
- [Avvio del pannello di controllo amministrativo](#)
- [Disattivazione dell'attivazione automatica](#)
- [Gestire la condivisione dei link](#)
- [Controllo degli inviti degli utenti con attivazione automatica abilitata](#)
- [Invito di nuovi utenti](#)
- [Modifica di utenti](#)
- [Disabilitazione di utenti](#)
- [Trasferimento della proprietà del documento](#)
- [Scaricamento di elenchi utenti](#)

Panoramica dei ruoli utente

Amazon WorkDocs definisce i seguenti ruoli utente. Puoi modificare i ruoli degli utenti modificando i loro profili utente. Per ulteriori informazioni, consulta [Modifica di utenti](#).

- **Admin (Amministratore):** un utente pagato che dispone di autorizzazioni amministrative per l'intero sito, inclusa la configurazione della gestione degli utenti e delle impostazioni del sito. Per ulteriori informazioni su come promuovere un utente ad amministratore, consulta [Promozione di un utente ad amministratore](#).
- **Power user:** un utente a pagamento che dispone di una serie speciale di autorizzazioni dall'amministratore. Per ulteriori informazioni su come impostare le autorizzazioni per un power user, consulta [Sicurezza: siti semplici ActiveDirectory](#) e [Sicurezza: siti di ActiveDirectory connessione](#).
- **Utente:** un utente a pagamento che può salvare file e collaborare con altri in un WorkDocs sito Amazon.
- **Utente guest:** un utente pagato in grado solo di visualizzare file. È possibile aggiornare gli utenti Guest ai ruoli Utente, Power user o Amministratore.

Note

Quando modifichi il ruolo di un utente ospite, esegui un'azione unica che non puoi annullare.

Amazon definisce WorkDocs anche questi tipi di utenti aggiuntivi.

Utente WS

Un utente con un nome assegnato WorkSpaces Workspace.

- Accesso a tutte le WorkDocs funzionalità di Amazon
- Storage predefinito di 50 GB (può pagare per eseguire l'upgrade a 1 TB)
- Nessun costo mensile

Utente WS aggiornato

Un utente con uno spazio di archiviazione assegnato WorkSpaces Workspace e aggiornato.

- Accesso a tutte le WorkDocs funzionalità di Amazon
- Storage predefinito di 1 TB (spazio di archiviazione aggiuntivo disponibile su pay-as-you-go base)
- Soggetto a costi mensili

WorkDocs Utente Amazon

Un WorkDocs utente Amazon attivo senza un utente assegnato WorkSpaces Workspace.

- Accesso a tutte le WorkDocs funzionalità di Amazon
- Storage predefinito di 1 TB (spazio di archiviazione aggiuntivo disponibile su pay-as-you-go base)
- Soggetto a costi mensili

Avvio del pannello di controllo amministrativo

Utilizzi il pannello di controllo amministrativo nel client WorkDocs web Amazon per attivare e disattivare l'attivazione automatica e modificare i ruoli e le impostazioni degli utenti.

Per aprire il pannello di controllo dell'amministratore

1. Nell'angolo in alto a destra del WorkDocs client, scegli l'icona del profilo.



2. In Amministratore, scegli Apri il pannello di controllo dell'amministratore.

Note

Alcune opzioni del pannello di controllo differiscono tra le directory cloud e le directory connesse.

Disattivazione dell'attivazione automatica

L'attivazione automatica viene disattivata quando non si desidera aggiungere tutti gli utenti di una directory a un nuovo sito e quando si desidera impostare autorizzazioni e ruoli diversi per gli utenti che si invitano a un nuovo sito. Quando disattivi l'attivazione automatica, puoi anche decidere chi ha la possibilità di invitare nuovi utenti sul sito: utenti attuali, utenti esperti o amministratori. In questi passaggi viene descritto come eseguire entrambe le attività.

Disattivazione automatica: Disattivazione automatica

1. Nell'angolo in alto a destra del WorkDocs client, scegli l'icona del profilo.



2. In Amministratore, scegli Apri il pannello di controllo dell'amministratore.
3. Scorri verso il basso fino a Sicurezza e scegli Cambia.

Viene visualizzata la finestra di dialogo Impostazioni policy.

4. In Attivazione automatica, deseleziona la casella di controllo accanto a Consenti a tutti gli utenti della tua directory di essere attivati automaticamente al primo accesso al WorkDocs sito.

Le opzioni cambiano in Chi dovrebbe essere autorizzato ad attivare gli utenti della directory nel tuo WorkDocs sito. Puoi consentire agli utenti attuali di invitare nuovi utenti oppure puoi dare questa possibilità ai power user o ad altri amministratori.

5. Seleziona un'opzione, quindi scegli Salva modifiche.

Ripeti i passaggi 1-4 per riattivare l'attivazione automatica.

Gestire la condivisione dei link

In questo argomento viene descritto come gestire la condivisione dei link. WorkDocs Gli utenti Amazon possono condividere file e cartelle condividendo link ad essi. Possono condividere i link ai file all'interno e all'esterno dell'organizzazione, ma possono condividere solo i link alle cartelle internamente. In qualità di amministratore, sei tu a decidere chi può condividere i link.

Per abilitare la condivisione dei link

1. Nell'angolo in alto a destra del WorkDocs client, scegli l'icona del profilo.



2. In Amministratore, scegli Apri il pannello di controllo dell'amministratore.
3. Scorri verso il basso fino a Sicurezza e scegli Cambia.

Viene visualizzata la finestra di dialogo Impostazioni policy.

4. In Scegli l'impostazione per i link condivisibili, seleziona un'opzione:
 - Non consentire link condivisibili a livello di sito o pubblici: disabilita la condivisione dei link per tutti gli utenti.
 - Consenti agli utenti di creare link condivisibili a livello di sito, ma non consentire loro di creare link condivisibili pubblici: limita la condivisione dei link ai soli membri del sito. Gli utenti gestiti possono creare questo tipo di link.
 - Consenti agli utenti di creare link condivisibili a livello di sito, ma solo i power user possono creare link pubblici condivisibili: gli utenti gestiti possono creare link a livello di sito, ma solo i power user possono creare link pubblici. I link pubblici consentono l'accesso a chiunque su Internet.
 - Tutti gli utenti gestiti possono creare link condivisibili a livello di sito e pubblici: gli utenti gestiti possono creare link pubblici.
5. Seleziona Salva modifiche.

Controllo degli inviti degli utenti con attivazione automatica abilitata

Quando abiliti l'attivazione automatica e ricordi che è attiva per impostazione predefinita, puoi dare agli utenti la possibilità di invitare altri utenti. Puoi concedere l'autorizzazione a uno dei seguenti:

- Tutti gli utenti
- Utenti esperti
- Amministratori.

Puoi anche disabilitare completamente le autorizzazioni e questi passaggi spiegano come.

Per impostare le autorizzazioni degli inviti

1. Nell'angolo in alto a destra del WorkDocs client, scegli l'icona del profilo.



2. In Amministratore, scegli Apri il pannello di controllo dell'amministratore.
3. Scorri verso il basso fino a Sicurezza e scegli Cambia.

Viene visualizzata la finestra di dialogo Impostazioni policy.

4. In Chi dovrebbe essere autorizzato ad attivare gli utenti della directory nel tuo WorkDocs sito, seleziona la casella di controllo Condividi con utenti esterni, seleziona una delle opzioni sotto la casella di controllo, quindi scegli Salva modifiche.

- OPPURE -

Deseleziona la casella di controllo se non desideri che nessuno inviti nuovi utenti, quindi scegli Salva modifiche.

Invito di nuovi utenti

Puoi invitare nuovi utenti a unirsi a una directory. Una volta abilitati, gli utenti esistenti possono anche invitare nuovi utenti. Per ulteriori informazioni, consulta [Sicurezza: siti semplici ActiveDirectory](#) e [Sicurezza: siti di ActiveDirectory connessione](#) in questa guida.

Per invitare nuovi utenti

1. Nell'angolo in alto a destra del WorkDocs client, scegli l'icona del profilo.



2. In Amministratore, scegli Apri il pannello di controllo dell'amministratore.
3. In Manage Users (Gestisci utenti), scegliere Invite Users (Invita utenti).
4. Nella finestra di dialogo Invita utenti, per Chi desideri invitare? , inserisci l'indirizzo email dell'invitato e scegli Invia. Ripetere questa fase per ogni invito.

Amazon WorkDocs invia un'email di invito a ciascun destinatario. L'e-mail contiene un link e le istruzioni su come creare un WorkDocs account Amazon. Il collegamento di invito scade dopo 30 giorni.


Modifica di utenti

È possibile modificare le informazioni e le impostazioni dell'utente.

Per modificare gli utenti

1. Nell'angolo in alto a destra del WorkDocs client, scegli l'icona del profilo.



2. In Amministratore, scegli Apri il pannello di controllo dell'amministratore.
3. In Manage Users (Gestisci utenti), scegliere l'icona a forma di matita  accanto al nome dell'utente.
4. Nella finestra di dialogo Edit User (Modifica utente), puoi modificare le seguenti opzioni:

First Name (Nome) (solo directory del cloud)

Il nome dell'utente.

Last Name (Cognome) (solo directory del cloud)

Il cognome dell'utente.

Stato

Specifica se l'utente è attivo o inattivo. Per ulteriori informazioni, consulta [Disabilitazione di utenti](#).

Ruolo

Specifica se qualcuno è un utente o un amministratore. Puoi anche aggiornare o declassare gli utenti a cui è WorkSpaces Workspace stato assegnato un. Per ulteriori informazioni, consulta [Panoramica dei ruoli utente](#).

Storage

Specifica il limite di storage per un utente esistente.

5. Seleziona Salva modifiche.


Disabilitazione di utenti

Si disabilita l'accesso di un utente modificandone lo stato in Inattivo.

Per cambiare lo stato utente in Inactive (Inattivo)

1. Nell'angolo in alto a destra del WorkDocs client, scegli l'icona del profilo.




2. In Amministratore, scegli Apri il pannello di controllo dell'amministratore.
3. In Manage Users (Gestisci utenti), scegliere l'icona a forma di matita  accanto al nome dell'utente.
4. Scegliere Inactive (Inattivo) e selezionare Save Changes (Salva modifiche).

L'utente inattivato non può accedere al tuo WorkDocs sito Amazon.

Note

La modifica dello stato di un utente allo stato Inattivo non comporta l'eliminazione dei suoi file, cartelle o feedback dal tuo WorkDocs sito Amazon. Tuttavia, puoi trasferire i file e le cartelle di un utente inattivo a un utente attivo. Per ulteriori informazioni, consulta [Trasferimento della proprietà del documento](#).

Eliminazione di utenti in sospeso

È possibile eliminare gli utenti di Simple AD, AWS Managed Microsoft e AD Connector nello stato In sospeso. Per eliminare uno di questi utenti, scegli l'icona del cestino  accanto al nome dell'utente.

Il tuo WorkDocs sito Amazon deve sempre avere almeno un utente attivo che non sia un utente ospite. Se devi eliminare tutti gli utenti, [elimina l'intero sito](#).

Non è consigliabile eliminare utenti registrati. Invece, dovresti cambiare lo stato di un utente da Attivo a Inattivo per impedirgli di accedere al tuo WorkDocs sito Amazon.

Trasferimento della proprietà del documento

Puoi trasferire i file e le cartelle di un utente inattivo a un utente attivo. Per ulteriori informazioni su come disattivazione di un utente, consulta [Disabilitazione di utenti](#).


⚠ Warning

Questa operazione non può essere annullata.

Per trasferire la proprietà del documento

1. Nell'angolo in alto a destra del WorkDocs client, scegli l'icona del profilo.



2. In Amministratore, scegli Apri il pannello di controllo dell'amministratore.
3. In Manage Users (Gestisci utenti), cercare l'utente inattivo.
4. Scegliere l'icona a forma di matita
() accanto al nome dell'utente inattivo.
5. Seleziona Trasferisci la proprietà del documento e inserisci l'indirizzo email del nuovo proprietario.
6. Seleziona Salva modifiche.

Scaricamento di elenchi utenti

Per scaricare un elenco di utenti dal pannello di controllo dell'amministratore, devi installare Amazon WorkDocs Companion. Per installare Amazon WorkDocs Companion, vedi [App e integrazioni per Amazon WorkDocs](#).


Per scaricare un elenco di utenti

1. Nell'angolo in alto a destra del WorkDocs client, scegli l'icona del profilo.



2. In Amministratore, scegli Apri il pannello di controllo dell'amministratore.
3. In Manage Users (Gestisci utenti), scegliere Download Users (Scarica utenti).

4. Per Download user (Scarica utente), scegliere una delle seguenti opzioni per esportare un elenco di utenti come file .json sul desktop:
 - Tutti gli utenti
 - Utente guest
 - Utente WS
 - Utente
 - Utente avanzato
 - Amministratore
5. WorkDocs salva il file in una delle seguenti posizioni:
 - Windows – Downloads/WorkDocsDownloads
 - macOS – *hard drive*/users/*username*/WorkDocsDownloads/folder

 Note

I download potrebbero richiedere del tempo. Inoltre, i file scaricati non arrivano nella/
~users cartella.

Per ulteriori informazioni su questi ruoli utente, consulta [Panoramica dei ruoli utente](#).

Condivisione e collaborazione

I tuoi utenti possono condividere contenuti inviando un link o un invito. Gli utenti possono anche collaborare con utenti esterni se abiliti la condivisione esterna.

Amazon WorkDocs controlla l'accesso a cartelle e file tramite l'uso di autorizzazioni. Il sistema applica le autorizzazioni in base al ruolo dell'utente.

Indice

- [Collegamenti di condivisione](#)
- [Condivisione mediante invito](#)
- [Condivisione esterna](#)
- [Autorizzazioni](#)
- [Abilitazione della modifica collaborativa](#)

Collegamenti di condivisione

Gli utenti possono scegliere Condividi un link per copiare e condividere rapidamente i collegamenti ipertestuali per i WorkDocs contenuti di Amazon con colleghi e utenti esterni sia all'interno che all'esterno dell'organizzazione. Quando gli utenti condividono un collegamento, possono configurarlo per consentire una delle seguenti opzioni di accesso:

- Tutti i membri del WorkDocs sito Amazon possono cercare, visualizzare e commentare il file.
- Chiunque disponga del link, anche le persone che non sono membri del WorkDocs sito Amazon, può visualizzare il file. Questa opzione di collegamento limita le autorizzazioni alla sola visualizzazione.

I destinatari con autorizzazioni di visualizzazione possono solo visualizzare un file. Le autorizzazioni ai commenti consentono agli utenti di commentare ed effettuare operazioni di aggiornamento o eliminazione, come il caricamento di un nuovo file o l'eliminazione di un file esistente.

Per impostazione predefinita, tutti gli utenti gestiti possono creare link pubblici. Per modificare questa impostazione, aggiorna le impostazioni di Security (Sicurezza) dal pannello di controllo admin. Per ulteriori informazioni, consulta [Gestione di Amazon WorkDocs dal pannello di controllo di amministrazione del sito](#).

Condivisione mediante invito

Quando abiliti la condivisione tramite invito, gli utenti del sito possono condividere file o cartelle con singoli utenti e con gruppi inviando e-mail di invito. Gli inviti contengono link ai contenuti condivisi e gli invitati possono aprire i file o le cartelle condivisi. Gli invitati possono anche condividere tali file o cartelle con altri membri del sito e con utenti esterni.

Puoi impostare i livelli di autorizzazione per ogni utente invitato. Puoi anche creare cartelle del team da condividere su invito con i gruppi di directory da te creati.

Note

Gli inviti alla condivisione non includono membri di gruppi annidati. Per includere questi membri, devi aggiungerli all'elenco Condividi tramite invito.

Per ulteriori informazioni, consulta [Gestione di Amazon WorkDocs dal pannello di controllo di amministrazione del sito](#).

Condivisione esterna

La condivisione esterna consente agli utenti gestiti di un WorkDocs sito Amazon di condividere file e cartelle e collaborare con utenti esterni senza incorrere in costi aggiuntivi. Gli utenti del sito possono condividere file e cartelle con utenti esterni senza che i destinatari siano utenti a pagamento del WorkDocs sito Amazon. Quando abiliti la condivisione esterna, gli utenti possono inserire l'indirizzo e-mail dell'utente esterno con cui desiderano condividere e impostare le autorizzazioni di condivisione dei visualizzatori appropriate. Quando vengono aggiunti utenti esterni, le autorizzazioni sono limitate ai soli visualizzatori e le altre autorizzazioni non sono disponibili. Gli utenti esterni riceveranno una notifica e-mail con un link al file o alla cartella condivisa. La scelta del collegamento reindirizza gli utenti esterni al sito, dove inseriscono le proprie credenziali per accedere ad Amazon WorkDocs. Potranno vedere il file o la cartella condivisa nella vista Shared with me (Condivisi con me).

I proprietari del file possono modificare le autorizzazioni di condivisione o revocare l'accesso dell'utente esterno a un file o a una cartella in qualsiasi momento. Perché gli utenti gestiti possano condividere il contenuto con utenti esterni, la condivisione esterna del sito deve essere abilitata dall'amministratore. Perché i Guest users (Utenti guest) possano contribuire o diventare co-proprietari, l'amministratore del sito deve trasferirli al livello User (Utente). Per ulteriori informazioni, consulta [Panoramica dei ruoli utente](#).

Per impostazione predefinita, la condivisione esterna è attivata e tutti gli utenti possono invitare utenti esterni. Per modificare questa impostazione, aggiorna le impostazioni di Security (Sicurezza) dal pannello di controllo admin. Per ulteriori informazioni, consulta [Gestione di Amazon WorkDocs dal pannello di controllo di amministrazione del sito](#).

Autorizzazioni

Amazon WorkDocs utilizza le autorizzazioni per controllare l'accesso a cartelle e file. Le autorizzazioni vengono applicate in base ai ruoli degli utenti.

Indice

- [Ruoli utente](#)
- [Autorizzazioni per le cartelle condivise](#)
- [Autorizzazioni per i file nelle cartelle condivise](#)
- [Autorizzazioni per i file che non si trovano nelle cartelle condivise](#)

Ruoli utente

I ruoli utente controllano le autorizzazioni per cartelle e file. È possibile applicare i seguenti ruoli utente a livello di cartella:

- Proprietario della cartella: il proprietario di una cartella o di un file.
- Comproprietario della cartella: un utente o un gruppo che il proprietario designa come comproprietario di una cartella o di un file.
- Collaboratore di cartelle: qualcuno con accesso illimitato a una cartella.
- Visualizzatore di cartelle: persona con accesso limitato (autorizzazioni di sola lettura) a una cartella.

È possibile applicare i seguenti ruoli utente a livello di singolo file:

- Proprietario: il proprietario di un file.
- Comproprietario: un utente o un gruppo che il proprietario designa come comproprietario del file.
- Collaboratore*: persona autorizzata a fornire feedback sul file.
- Visualizzatore: persona con accesso limitato (autorizzazioni di sola lettura) al file.

- **Visualizzatore anonimo:** un utente non registrato esterno all'organizzazione che può visualizzare un file che è stato condiviso utilizzando un link di visualizzazione esterno. Se non diversamente specificato, un visualizzatore anonimo dispone delle stesse autorizzazioni di un visualizzatore.

* I collaboratori non possono rinominare le versioni dei file esistenti. Tuttavia, possono caricare una nuova versione di un file con un nome diverso.

Autorizzazioni per le cartelle condivise

Le seguenti autorizzazioni si applicano ai ruoli utente per le cartelle condivise:

Note

Le autorizzazioni applicate per una cartella si applicano anche alle sottocartelle e ai file in quella cartella.

- **Visualizza:** visualizza il contenuto di una cartella condivisa.
- **Visualizza sottocartelle:** visualizza una sottocartella.
- **Visualizza condivisioni:** visualizza gli altri utenti con cui è condivisa una cartella.
- **Scarica cartella:** scarica una cartella.
- **Aggiungi sottocartella:** aggiungi una sottocartella.
- **Condividi:** condividi la cartella di primo livello con altri utenti.
- **Revoca condivisione:** revoca la condivisione della cartella di primo livello.
- **Elimina sottocartella:** elimina una sottocartella.
- **Elimina cartella di primo livello:** elimina la cartella condivisa di primo livello.

	Vista	Visualizza sottocartelle	Visualizza le condivisioni	Scarica la cartella	Aggiungi sottocartella	Condivisione	Revoca condivisione	Elimina sottocartella	Elimina la cartella di primo livello
Proprietario della cartella	✓	✓	✓	✓	✓	✓	✓	✓	✓
Comproprietario della cartella	✓	✓	✓	✓	✓	✓	✓	✓	✓
Collaboratore della cartella	✓	✓	✓	✓	✓				
Visualizzatore di cartelle	✓	✓	✓	✓					

Autorizzazioni per i file nelle cartelle condivise

Le seguenti autorizzazioni si applicano ai ruoli utente per i file in una cartella condivisa:

- Annota: aggiungi feedback a un file.
- Elimina: elimina un file in una cartella condivisa.
- Rinomina: rinomina i file.
- Carica: carica nuove versioni di un file.

- **Scarica:** scarica un file. Si tratta dell'autorizzazione predefinita; Puoi utilizzare le proprietà dei file per consentire o negare la possibilità di scaricare file condivisi.
- **Impedisce il download:** impedisce il download di un file.

Note

- Quando si seleziona questa opzione, gli utenti con autorizzazioni di visualizzazione possono comunque scaricare file. Per evitare che ciò accada, apri la cartella condivisa e deseleziona l'impostazione **Consenti download** per ciascuno dei file che non desideri vengano scaricati da tali utenti.
 - Quando il proprietario o il comproprietario di un file MP4 non consente il download di quel file, i collaboratori e i visualizzatori non possono riprodurlo nel client web Amazon WorkDocs
- **Condividi:** condividi un file con altri utenti.
 - **Revoca la condivisione:** revoca la condivisione di un file.
 - **Visualizza:** visualizza un file in una cartella condivisa.
 - **Visualizza condivisioni:** visualizza gli altri utenti con cui è condiviso un file.
 - **Visualizza annotazioni:** visualizza il feedback di altri utenti.
 - **Visualizza attività:** visualizza la cronologia delle attività di un file.
 - **Visualizza versioni:** visualizza le versioni precedenti di un file.
 - **Elimina versioni:** elimina una o più versioni di un file.
 - **Recupera versioni:** recupera una o più versioni eliminate di un file.
 - **Visualizza tutti i commenti privati:** il proprietario/comproprietario può visualizzare tutti i commenti privati relativi a un documento, anche se non si tratta di risposte al commento.

	Annotare	Eliminare	Assegnare di un nuovo nome	Caricare	Scaricare il download	Impedire il download	Condividere	Revocare la condivisione	Vista	Visualizzare le condizioni	Visualizzare le annotazioni	Visualizzare le attività	Visualizzare le azioni	Eliminare le versioni	Recupero le versioni	Visualizzare tutti i commenti privati**
Proprietario del file*	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Proprietario della cartella	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Cometario della cartella*	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Collaboratore della cartella**	✓			✓	✓				✓	✓	✓	✓	✓			
Visualizzatore di cartella					✓				✓	✓						
Visualizzatore anonimo									✓	✓						

* In questo caso, il proprietario del file è la persona che ha caricato la versione originale di un file in una cartella condivisa. Le autorizzazioni per questo ruolo si applicano solo al file di proprietà, non a tutti i file nella cartella condivisa.

** I proprietari e i comproprietari possono vedere tutti i commenti privati. I collaboratori possono vedere solo i commenti privati che sono risposte ai loro commenti.

*** I collaboratori non possono rinominare le versioni dei file esistenti. Tuttavia, possono caricare una nuova versione di un file con un nome diverso.

Autorizzazioni per i file che non si trovano nelle cartelle condivise

Le seguenti autorizzazioni si applicano ai ruoli utente per i file che non si trovano in una cartella condivisa:

- Annota: aggiungi feedback a un file.
- Elimina: elimina un file.
- Rinomina: rinomina i file.
- Carica: carica nuove versioni di un file.
- Scarica: scarica un file. Si tratta dell'autorizzazione predefinita; Puoi utilizzare le proprietà dei file per consentire o negare la possibilità di scaricare file condivisi.
- Impedisce il download: impedisce il download di un file.

Note

Quando il proprietario o il comproprietario di un file MP4 non consente il download di quel file, i collaboratori e i visualizzatori non possono riprodurlo nel client web Amazon WorkDocs

- Condividi: condividi un file con altri utenti.
- Revoca condivisione: revoca la condivisione di un file.
- Visualizza: visualizza un file.
- Visualizza condivisioni: visualizza gli altri utenti con cui viene condiviso un file.
- Visualizza annotazioni: visualizza il feedback di altri utenti.
- Visualizza attività: visualizza la cronologia delle attività di un file.
- Visualizza versioni: visualizza le versioni precedenti di un file.

- Elimina versioni: elimina una o più versioni di un file.
- Recupera versioni: recupera una o più versioni eliminate di un file.

	Annotazione	Eliminazione	Assegnazione di un nuovo nome	Caricamento	Scaricamento	Compendio il download	Condivisione	Revocazione	Vista	Visualizzazione condivisa	Visualizzazione delle attività	Visualizzazione delle versioni	Eliminazione delle versioni	Recupero delle versioni
Proprietario*	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Comproprietario	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Collaboratore*	✓			✓	✓				✓	✓	✓	✓		
Visualizzatore					✓				✓	✓				
Visualizzatore anonimo									✓	✓				

* I proprietari e i comproprietari dei file possono vedere tutti i commenti privati. I collaboratori possono vedere solo i commenti privati che sono risposte ai loro commenti.

** I collaboratori non possono rinominare le versioni dei file esistenti. Tuttavia, possono caricare una nuova versione di un file con un nome diverso.

Abilitazione della modifica collaborativa

Utilizza la sezione Impostazioni di modifica online nel pannello di controllo di amministrazione per abilitare le opzioni di modifica collaborativa.

Indice

- [Attivazione di Hancom ThinkFree](#)
- [Abilitazione di Open with Office Online](#)

Attivazione di Hancom ThinkFree

Puoi abilitare Hancom ThinkFree per il tuo WorkDocs sito Amazon, in modo che gli utenti possano creare e modificare in modo collaborativo file di Microsoft Office dall'applicazione WorkDocs web Amazon. Per ulteriori informazioni, consulta [Editing with Hancom](#). ThinkFree

Hancom ThinkFree è disponibile senza costi aggiuntivi per WorkDocs gli utenti Amazon. Non occorrono licenze o installazioni di software aggiuntive.

Per abilitare Hancom ThinkFree

Abilita la ThinkFree modifica di Hancom dal pannello di controllo di amministrazione.

1. In My account (Account personale), scegliere Open admin control panel (Apri pannello di controllo admin).
2. Per Hancom Online Editing, scegliere Change (Modifica).
3. Selezionare Enable Hancom Online Editing Feature (Abilita funzionalità Hancom Online Editing), esaminare i termini di utilizzo e scegliere Save (Salva).

Per disabilitare Hancom ThinkFree

Disabilita la ThinkFree modifica di Hancom dal pannello di controllo di amministrazione.

1. In My account (Account personale), scegliere Open admin control panel (Apri pannello di controllo admin).
2. Per Hancom Online Editing, scegliere Change (Modifica).
3. Disattivare la casella di controllo Enable Hancom Online Editing Feature (Abilita funzionalità Hancom Online Editing), quindi scegliere Save (Salva).

Abilitazione di Open with Office Online

Abilita Open with Office Online per il tuo WorkDocs sito Amazon, in modo che gli utenti possano modificare in modo collaborativo i file di Microsoft Office dall'applicazione WorkDocs web Amazon.

Open with Office Online è disponibile senza costi aggiuntivi per WorkDocs gli utenti Amazon che dispongono anche di un account Microsoft Office 365 Work or School con una licenza per modificare in Office Online. Per ulteriori dettagli, consulta [Open con Office Online](#).

Per abilitare Open with Office Online

Abilitare Open with Office Online dal pannello di controllo admin.

1. In My account (Account personale), scegliere Open admin control panel (Apri pannello di controllo admin).
2. Per Office Online, scegliere Change (Modifica).
3. Selezionare Enable Office Online (Abilita Office Online), quindi scegliere Save (Salva).

Per disabilitare Open with Office Online

Disabilitare Open with Office Online dal pannello di controllo admin.

1. In My account (Account personale), scegliere Open admin control panel (Apri pannello di controllo admin).
2. Per Office Online, scegliere Change (Modifica).
3. Disattivare la casella di controllo Enable Office Online (Abilita Office Online), quindi scegliere Save (Salva).

Migrazione di file su Amazon WorkDocs

WorkDocs Gli amministratori di Amazon possono utilizzare Amazon WorkDocs Migration Service per eseguire una migrazione su larga scala di più file e cartelle sul proprio sito Amazon WorkDocs . Amazon WorkDocs Migration Service funziona con Amazon Simple Storage Service (Amazon S3). In questo modo puoi migrare le condivisioni di file dipartimentali e le condivisioni di file dell'home drive o degli utenti su Amazon. WorkDocs

Durante questo processo, Amazon WorkDocs fornisce una politica AWS Identity and Access Management (IAM) per te. Utilizza questa politica per creare un nuovo IAM ruolo che consenta l'accesso ad Amazon WorkDocs Migration Service per effettuare le seguenti operazioni:

- Leggi ed elenca il bucket Amazon S3 che hai designato.
- Leggi e scrivi sul WorkDocs sito Amazon che hai indicato.

Completa le seguenti attività per migrare file e cartelle su Amazon WorkDocs. Prima di iniziare, assicurati di disporre delle seguenti autorizzazioni:

- Autorizzazioni di amministratore per il tuo sito Amazon WorkDocs
- Autorizzazioni per creare un ruolo IAM

Se il tuo WorkDocs sito Amazon è configurato nella stessa directory del tuo WorkSpaces parco veicoli, devi rispettare questi requisiti:

- Non utilizzare Admin come nome utente WorkDocs del tuo account Amazon. L'amministratore è un ruolo utente riservato in Amazon WorkDocs.
- Il tuo tipo di utente WorkDocs amministratore Amazon deve essere Utente WS aggiornato. Per ulteriori informazioni, consulta [Panoramica dei ruoli utente](#) e [Modifica di utenti](#).

Note

La struttura delle directory, i nomi e il contenuto dei file vengono conservati durante la migrazione ad Amazon WorkDocs. La titolarità dei file e le autorizzazioni non vengono conservate.

Attività

- [Fase 1: Preparazione dei contenuti per la migrazione](#)
- [Fase 2: Caricamento di file su Amazon S3](#)
- [Fase 3: pianificazione di una migrazione](#)
- [Fase 4: tracciamento di una migrazione](#)
- [Fase 5: pulizia delle risorse](#)

Fase 1: Preparazione dei contenuti per la migrazione

Per preparare i tuoi contenuti per la migrazione

1. Sul tuo WorkDocs sito Amazon, in I miei documenti, crea una cartella in cui vuoi migrare file e cartelle.
2. Conferma quanto segue:
 - La cartella di origine non contiene più di 100.000 file e sottocartelle. Le migrazioni falliscono se si supera tale limite.
 - Nessun singolo file supera i 5 TB.
 - Ogni nome di file contiene al massimo 255 caratteri. Amazon WorkDocs Drive visualizza solo file con un percorso di directory completo di 260 caratteri o meno.

Warning

Il tentativo di migrare file o cartelle con nomi contenenti i seguenti caratteri può causare errori e l'arresto del processo di migrazione. In questo caso, scegli Download report (Scarica report) per scaricare un log che elenca gli errori, i file che non sono stati migrati e quelli che sono stati migrati.

- Spazi finali: ad esempio: uno spazio aggiuntivo alla fine del nome di un file.
- Periodi all'inizio o alla fine, ad esempio: `.file`, `.file.ppt`, `...`, o `file.`
- Tilde all'inizio o alla fine, ad esempio: `file.doc~~file.doc`, o `~$file.doc`
- Nomi di file che terminano con, ad esempio: `.tmp: file.tmp`

- Nomi di file che corrispondono esattamente a questi termini con distinzione tra maiuscole e minuscole: `Microsoft User Data`, `Outlook files`, o `Thumbs.db` `Thumbnails`
- Nomi di file che contengono uno di questi caratteri: * (asterisco), / (barra rovesciata), \ (barra rovesciata), (due punti), : (minore di), < (maggiore di), > (punto interrogativo), ? (barra/barra verticale), | (virgolette doppie) o " (codice carattere 202E). \202E

Fase 2: Caricamento di file su Amazon S3

Per caricare file su Amazon S3

1. Crea un nuovo bucket Amazon Simple Storage Service (Amazon S3) nell' AWS account in cui vuoi caricare file e cartelle. Il bucket Amazon S3 deve trovarsi nello stesso AWS account e nella stessa AWS regione del tuo sito Amazon. WorkDocs Per ulteriori informazioni, consulta la sezione [Guida introduttiva ad Amazon Simple Storage Service](#) nella Guida per l'utente di Amazon Simple Storage Service.
2. Carica i tuoi file nel bucket Amazon S3 creato nel passaggio precedente. Ti consigliamo di AWS DataSync utilizzarlo per caricare file e cartelle nel bucket Amazon S3. DataSync fornisce funzionalità aggiuntive di tracciamento, reportistica e sincronizzazione. Per ulteriori informazioni, consulta [Come AWS DataSync funziona](#) e [Utilizzo delle politiche \(IAMpolitiche\) basate sull'identità DataSync nella Guida per l'utente](#).AWS DataSync

Fase 3: pianificazione di una migrazione

Dopo aver completato i passaggi 1 e 2, utilizza Amazon WorkDocs Migration Service per pianificare la migrazione. Il Servizio di migrazione può impiegare fino a una settimana per elaborare la richiesta di migrazione e inviarti un'e-mail in cui ti informiamo che puoi iniziare la migrazione. Se avvii la migrazione prima di ricevere l'e-mail, la console di gestione visualizza un messaggio che ti dice di aspettare.

Quando pianifichi la migrazione, l'impostazione Storage del tuo account WorkDocs utente Amazon cambia automaticamente in Unlimited.

Note

La migrazione di file che superano il limite WorkDocs di archiviazione di Amazon può comportare costi aggiuntivi. Per ulteriori informazioni, consulta la pagina [WorkDocs dei prezzi di Amazon](#).

Amazon WorkDocs Migration Service fornisce una politica AWS Identity and Access Management (IAM) da utilizzare per la migrazione. Con questa politica, crei un nuovo IAM ruolo che concede ad Amazon WorkDocs Migration Service l'accesso al bucket Amazon S3 e al sito WorkDocs Amazon da te designati. Ti iscrivi anche alle notifiche SNS e-mail di Amazon per ricevere aggiornamenti quando la richiesta di migrazione è pianificata e quando inizia e termina.

Come pianificare una migrazione:

1. Dalla WorkDocs console Amazon, scegli App, Migrazioni.
 - Se è la prima volta che accedi ad Amazon WorkDocs Migration Service, ti verrà richiesto di iscriverti alle notifiche SNS e-mail di Amazon. Iscriverti, eseguire la conferma nel messaggio e-mail che si riceve e scegliere Continue (Continua).
2. Scegliere Create Migration (Crea migrazione).
3. Per Source Type (Tipo di origine), scegliere Amazon S3.
4. Scegli Next (Successivo).
5. Per l'origine e la convalida dei dati, in Sample Policy, copia la politica fornita IAM.
6. Utilizza la IAM politica che hai copiato nel passaggio precedente per creare una nuova IAM politica e un nuovo ruolo, come segue:
 - a. Apri la IAM console all'indirizzo <https://console.aws.amazon.com/iam/>.
 - b. Scegliere Policies (Policy), Create policy (Crea policy).
 - c. Scegli JSON e incolla la IAM politica che hai copiato negli appunti in precedenza.
 - d. Scegli Verifica policy. Immettere il nome e la descrizione di una policy.
 - e. Scegli Create Policy (Crea policy).
 - f. Scegliere Roles (Ruoli), Create role (Crea ruolo).
 - g. Seleziona Altro account. AWS Per Account ID (ID account), immettere uno dei seguenti valori:

- Per la regione Stati Uniti orientali (Virginia settentrionale), inserisci 899282061130
 - Per la regione Stati Uniti occidentali (Oregon), inserisci 814301586344
 - Per la regione Asia Pacifico (Singapore), inserisci 900469912330
 - Per la regione Asia Pacifico (Sydney), inserisci 031131923584
 - Per la regione Asia Pacifico (Tokyo), inserisci 178752524102
 - Per la regione Europa (Irlanda), inserisci 191921258524
- h. Selezionare la policy creata e scegliere Next: Review (Successivo: revisione). Se non si vede la nuova policy, scegliere l'icona di aggiornamento.
 - i. Immettere il nome e la descrizione di un ruolo. Scegliere Crea ruolo.
 - j. Nella pagina Roles (Ruoli), in Role name (Nome ruolo), scegliere il nome del ruolo creato.
 - k. Nella pagina Riepilogo, modifica la durata massima CLI API /sessione su 12 ore.
 - l. Copia il ruolo ARN negli appunti per utilizzarlo nel passaggio successivo.
7. Torna ad Amazon WorkDocs Migration Service. Per Origine e convalida dei dati, in Ruolo ARN, incolla il ruolo ARN dal IAM ruolo che hai copiato nel passaggio precedente.
 8. Per Bucket, seleziona il bucket Amazon S3 da cui migrare i file.
 9. Scegli Next (Successivo).
 10. Per Seleziona una WorkDocs cartella di destinazione, seleziona la cartella di destinazione in Amazon in WorkDocs cui migrare i file.
 11. Scegli Next (Successivo).
 12. In Review (Rivedi), per Title (Titolo), immettere un nome per la migrazione.
 13. Selezionare la data e l'ora della migrazione.
 14. Scegli Invia.

Fase 4: tracciamento di una migrazione

Puoi monitorare la migrazione dalla pagina iniziale di Amazon WorkDocs Migration Service. Per accedere alla pagina di destinazione dal WorkDocs sito Amazon, scegli App, Migrazioni. Scegli la migrazione per visualizzarne i dettagli e monitorarne il progresso. Puoi anche scegliere Cancel Migration (Annulla migrazione) se hai bisogno di annullarla o scegli Update (Aggiorna) per aggiornare la sequenza temporale della migrazione. Al termine della migrazione, puoi scegliere Download report (Scarica report) per scaricare un log dei file migrati con successo e degli errori.

Gli stati possibili della migrazione sono i seguenti:

Pianificati

La migrazione è pianificata ma non è iniziata. Puoi annullare le migrazioni o aggiornare l'ora d'inizio della migrazione fino a cinque minuti prima dell'ora d'inizio pianificata.

Migrating (Migrazione in corso)

La migrazione è in corso.

Riuscito

La migrazione è terminata.

Riuscita parzialmente

La migrazione è riuscita parzialmente. Per ulteriori dettagli, visualizza il riepilogo della migrazione e scarica il report fornito.

Non riuscito

La migrazione non è riuscita. Per ulteriori dettagli, visualizza il riepilogo della migrazione e scarica il report fornito.

Annullato

La migrazione è annullata.

Fase 5: pulizia delle risorse

Una volta completata la migrazione, elimina la politica e il ruolo di migrazione che hai creato dalla IAM console.

Per eliminare la IAM politica e il ruolo

1. Apri la IAM console all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Seleziona Policy.
3. Cercare e selezionare la policy creata.
4. Per Policy actions (Operazioni policy), scegliere Delete (Elimina).
5. Scegli Elimina.
6. Scegli Ruoli.

7. Cercare e selezionare il ruolo creato.
8. Scegliere Delete role (Elimina ruolo), Delete (Elimina).

Quando inizia una migrazione pianificata, l'impostazione di archiviazione del tuo account WorkDocs utente Amazon viene automaticamente modificata in Unlimited. Dopo la migrazione, puoi utilizzare il pannello di controllo di amministrazione per modificare tale impostazione. Per ulteriori informazioni, consulta [Modifica di utenti](#).

Risoluzione dei problemi di Amazon WorkDocsProblemi

Le informazioni seguenti possono essere utili per risolvere i problemi con Amazon WorkDocs.

Problemi

- [Non riesco a configurare il mio Amazon WorkDocs sito in uno specificoAWSRegion](#)
- [Voglio configurare il mio Amazon WorkDocs sito in un Amazon VPC esistente](#)
- [È necessario che gli utenti resettino la propria password](#)
- [Un utente ha condiviso accidentalmente un documento sensibile](#)
- [L'utente ha lasciato l'organizzazione e non ha trasferito la proprietà del documento.](#)
- [Necessità di implementare Amazon WorkDocs Drive o Amazon WorkDocs Compagno per utenti multipli](#)
- [L'editing online non funziona](#)

Non riesco a configurare il mio Amazon WorkDocs sito in uno specificoAWSRegion

Se stai configurando un nuovo Amazon WorkDocs sito, seleziona la regione AWS durante la configurazione. Per ulteriori informazioni, consultare il tutorial relativo al proprio caso d'uso sotto [Guida introduttiva ad Amazon WorkDocs](#).

Voglio configurare il mio Amazon WorkDocs sito in un Amazon VPC esistente

Quando configuri il tuo nuovo Amazon WorkDocs sito, creare una directory utilizzando il cloud privato virtuale (VPC) esistente. Amazon WorkDocs utilizza questa directory per autenticare gli utenti.

È necessario che gli utenti resettino la propria password

Gli utenti possono resettare le loro password scegliendo Forgot password? (Password dimenticata?) nella schermata di accesso.

Un utente ha condiviso accidentalmente un documento sensibile

Per revocare l'accesso a un documento scegliere Share by invite (Condividi per invito) accanto al documento e rimuovere successivamente gli utenti che non devono più avere l'accesso. Se il documento era condiviso tramite un link, scegliere Share a link (Condividi un link) e disabilitare il link.

L'utente ha lasciato l'organizzazione e non ha trasferito la proprietà del documento.

È possibile trasferire la proprietà del documento a un altro utente nel pannello di controllo admin. Per ulteriori informazioni, consulta [Trasferimento della proprietà del documento](#).

Necessità di implementare Amazon WorkDocs Drive o Amazon WorkDocs Compagno per utenti multipli

È possibile distribuire a più utenti in un'enterprise utilizzando la policy del gruppo. Per ulteriori informazioni, consulta [Gestione delle identità e degli accessi per Amazon WorkDocs](#). Per informazioni specifiche sulla distribuzione di Amazon WorkDocs Rivolgiti a più utenti, vedi [Distribuzione di Amazon WorkDocs Drive su più computer](#).

L'editing online non funziona

Verifica di avere Amazon WorkDocs Companion installato. Per installare Amazon WorkDocs Compagno, consulta [App e integrazioni per Amazon WorkDocs](#).

Gestione di Amazon WorkDocs per Amazon Business

Se sei un amministratore per Amazon WorkDocs per Amazon Business, puoi gestire gli utenti accedendo a <https://workdocs.aws/> utilizzando delle credenziali Amazon Business.

Per invitare un nuovo utente su Amazon WorkDocs per Amazon Business

1. Accedere con le proprie credenziali Amazon Business all'indirizzo <https://workdocs.aws/>.
2. Nella home page di Amazon WorkDocs per Amazon Business, aprire il riquadro di navigazione a sinistra.
3. Scegliere Admin Settings (Impostazioni amministratore).
4. Scegliere Add people (Aggiungi persone).
5. In Recipients (Destinatari), inserire gli indirizzi e-mail o i nomi utente degli utenti da invitare.
6. (Facoltativo) Personalizzare il messaggio di invito.
7. Seleziona Done (Fatto).

Per cercare un utente su Amazon WorkDocs per Amazon Business

1. Accedere con le proprie credenziali Amazon Business all'indirizzo <https://workdocs.aws/>.
2. Nella home page di Amazon WorkDocs per Amazon Business, aprire il riquadro di navigazione a sinistra.
3. Scegliere Admin Settings (Impostazioni amministratore).
4. In Search users (Cerca utenti), inserire il nome dell'utente e premere **Enter**.

Per selezionare i ruoli utente su Amazon WorkDocs per Amazon Business

1. Accedere con le proprie credenziali Amazon Business all'indirizzo <https://workdocs.aws/>.
2. Nella home page di Amazon WorkDocs per Amazon Business, aprire il riquadro di navigazione a sinistra.
3. Scegliere Admin Settings (Impostazioni amministratore).
4. In People (Persone), accanto all'utente, selezionare il Role (Ruolo) da assegnare all'utente.

Per eliminare un utente su Amazon WorkDocs per Amazon Business

1. Accedere con le proprie credenziali Amazon Business all'indirizzo <https://workdocs.aws/>.
2. Nella home page di Amazon WorkDocs per Amazon Business, aprire il riquadro di navigazione a sinistra.
3. Scegliere Admin Settings (Impostazioni amministratore).
4. In People (Persone), scegliere i puntini di sospensione (...) accanto all'utente.
5. Scegli Delete (Elimina).
6. Se richiesto, inserire un nuovo utente a cui trasferire i file dell'utente e scegliere Delete (Elimina).

Indirizzo IP e domini da aggiungere all'elenco degli indirizzi consentiti

Se implementi il filtro IP sui dispositivi che accedono ad Amazon WorkDocs, aggiungi i seguenti indirizzi IP e domini all'elenco degli indirizzi consentiti. In questo modo si abilita Amazon WorkDocs e Amazon WorkDocs Unità per connettersi al WorkDocs Servizio.

- 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

Se si desidera utilizzare gli intervalli di indirizzi IP, vedere [AWS Intervalli indirizzi IP](#) nel [AWS Riferimenti generali](#).

Cronologia dei documenti

La tabella seguente descrive le modifiche importanti alla Amazon WorkDocs Administration Guide, a partire da febbraio 2018. Per ricevere notifiche sugli aggiornamenti di questa documentazione, puoi abbonarti a un feed RSS.

Modifica	Descrizione	Data
Nuove autorizzazioni per il proprietario dei file	Gli amministratori possono ora fornire le autorizzazioni Delete Version e Recover Version. Le autorizzazioni fanno parte del rilascio dell'API. DeleteDocumentVersion	29 luglio 2022
WorkDocs Backup su Amazon	È stata rimossa la documentazione di Amazon WorkDocs Backup dalla Amazon WorkDocs Administration Guide perché il componente non è più supportato.	24 giugno 2021
Gestione di Amazon WorkDocs per Amazon Business	Amazon WorkDocs for Amazon Business supporta la gestione degli utenti da parte degli amministratori. Per ulteriori informazioni, consulta Managing Amazon WorkDocs for Amazon Business nella Amazon WorkDocs Administration Guide.	26 marzo 2020
Migrazione di file su Amazon WorkDocs	WorkDocs Gli amministratori di Amazon possono utilizzare Amazon WorkDocs Migration Service per eseguire una migrazione su larga scala di	8 agosto 2019

più file e cartelle sul proprio sito Amazon WorkDocs . Per ulteriori informazioni, consulta la sezione [Migrazione dei file su Amazon WorkDocs nella Amazon WorkDocs Administration Guide](#).

[Impostazioni dell'elenco degli indirizzi IP consentiti](#)

Le impostazioni dell'elenco indirizzi IP consentiti sono disponibili per filtrare l'accesso al tuo WorkDocs sito Amazon in base all'intervallo di indirizzi IP. Per ulteriori informazioni, consulta le [impostazioni dell'elenco degli indirizzi IP consentiti](#) nella Amazon WorkDocs Administration Guide.

22 ottobre 2018

[Hancom ThinkFree](#)

Hancom ThinkFree è disponibile. Gli utenti possono creare e modificare in modo collaborativo file di Microsoft Office dall'applicazione WorkDocs web Amazon. Per ulteriori informazioni, consulta [Enabling Hancom ThinkFree](#) nella Amazon WorkDocs Administration Guide.

21 giugno 2018

[Apri con Office Online](#)

Open with Office Online è disponibile. Gli utenti possono modificare in modo collaborativo i file di Microsoft Office dall'applicazione WorkDocs web Amazon. Per ulteriori informazioni, consulta [Enabling Open with Office Online](#) nella Amazon WorkDocs Administration Guide.

6 giugno 2018

[Risoluzione dei problemi](#)

Aggiunto l'argomento sulla risoluzione dei problemi. Per ulteriori informazioni, consulta [Risoluzione dei WorkDocs problemi di Amazon](#) nella Amazon WorkDocs Administration Guide.

23 maggio 2018

[Modifica il periodo di conservazione del contenitore di ripristino](#)

Il periodo di retention del cestino di recupero può essere modificato. Per ulteriori informazioni, consulta le [impostazioni di conservazione del contenitore di ripristino](#) nella Amazon WorkDocs Administration Guide.

27 febbraio 2018