



Guida per l'utente

Suggerimenti di strategia dell'Hub di migrazione



Suggerimenti di strategia dell'Hub di migrazione: Guida per l'utente

Copyright © 2025 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

Cosa sono i consigli sulla strategia di Migration Hub?	1
Sei un cliente di Strategy Recommendations per la prima volta?	1
Panoramica	2
Servizi correlati	2
Configurazione	4
Registrati per un Account AWS	4
Crea un utente con accesso amministrativo	4
Utenti e ruoli di Strategy Recommendations	6
Nozioni di base	8
Prerequisiti	8
Passaggio 1: scarica il raccogliitore	10
Fase 2: Implementare il raccogliitore	11
Implementa il collector in vCenter	11
Implementa l'AMI del collettore	12
Passaggio 3: accedi al raccogliitore	13
Accedi al collettore distribuito in vCenter	14
Accedi al collector distribuito come istanza Amazon EC2	14
Fase 4: Configurare il raccogliitore	14
Configurazioni AWS	15
Configurazioni vCenter	17
Configurazioni del server remoto	20
Configurazioni di controllo della versione	22
Prepara i server remoti per la raccolta dei dati	23
Verifica la configurazione per la raccolta dei dati	27
Fase 5: Ottieni consigli	29
Raccomandazioni	32
Visualizzazione dei consigli strategici	32
Consigli sui componenti dell'applicazione	33
Utilizzo dei componenti dell'applicazione	33
Analisi del codice sorgente	36
Analisi del database	36
Analisi binaria	38
Consigli sul server	39
Preferenze	40

Origine dati	42
Visualizzazione delle fonti di dati	42
Raccoglitore di dati applicativi	42
Dati raccolti dal raccoglitore	43
Aggiornamento del raccoglitore	46
Importazione dei dati	47
Modello di importazione	48
Rimozione dei dati	53
Sicurezza	54
Protezione dei dati	55
Crittografia dei dati a riposo	56
Crittografia in transito	56
Gestione dell'identità e degli accessi	56
Destinatari	57
Autenticazione con identità	57
Gestione dell'accesso con policy	61
Come funziona Migration Hub Strategy Recommendations con IAM	64
AWS politiche gestite	70
Esempi di policy basate su identità	77
Risoluzione dei problemi	81
Uso di ruoli collegati ai servizi	84
Endpoint VPC (AWS PrivateLink)	87
Convalida della conformità	89
Utilizzo di altri servizi	91
AWS CloudTrail	91
Informazioni sulle raccomandazioni strategiche in CloudTrail	91
Comprensione delle voci dei file di registro di Strategy	93
Quote	95
Note di rilascio	96
17 novembre 2023	96
12 ottobre 2023	96
17 aprile 2023	97
17 marzo 2023	97
07 novembre 2022	97
27 settembre 2022	97
30 giugno 2022	98

18 aprile 2022	98
25 febbraio 2022	98
10 febbraio 2022	98
28 gennaio 2022	99
14 gennaio 2022	99
21 dicembre 2021	99
15 dicembre 2021	99
25 ottobre 2021	100
Cronologia dei documenti	101
.....	ciii

Cosa sono i consigli sulla strategia di Migration Hub?

Suggerimenti di strategia dell'Hub di migrazione offre consigli per pianificare la strategia di migrazione e modernizzazione e delineare percorsi di trasformazione fattibili per le applicazioni.

Strategy Recommendations consente di analizzare l'inventario del server, l'ambiente di runtime e i file binari delle applicazioni per le applicazioni Microsoft IIS e Java Tomcat e Jboss per generare report anti-pattern. Inoltre, è possibile configurare il codice sorgente per consentire a Strategy Recommendations di eseguire l'analisi del codice sorgente e del database di tutte le applicazioni. Strategy Recommendations confronta questa analisi con gli obiettivi aziendali e le preferenze di trasformazione delle applicazioni e dei database che avete fornito per consigliare:

- La strategia di migrazione più efficace per ciascuna delle tue applicazioni.
- Strumenti o servizi di migrazione e modernizzazione che puoi utilizzare.
- Incompatibilità delle applicazioni e anti-pattern da risolvere per un'opzione specifica.

Migration Hub Strategy Recommendations consiglia strategie di migrazione e modernizzazione per il rehosting, il replatforming e il refactoring con destinazioni, strumenti e programmi di implementazione associati. [Per informazioni su rehosting, replatforming e refactoring, consulta Migration terms - 7 Rs nel glossario Prescriptive Guidance.AWS](#)

Strategy Recommendations potrebbe consigliare opzioni semplici, come il rehosting su Amazon Elastic Compute Cloud (Amazon EC2) utilizzando AWS Application Migration Service (MGN).AWS Raccomandazioni più ottimizzate potrebbero includere il replatforming in container utilizzando AWS App2Container o il refactoring verso tecnologie open source come.NET Core e PostgreSQL.

Sei un cliente di Strategy Recommendations per la prima volta?

Se è la prima volta che utilizzi Strategy Recommendations, ti consigliamo di iniziare leggendo le seguenti sezioni:

- [Panoramica dei consigli strategici](#)
- [Impostazione delle raccomandazioni strategiche](#)
- [Guida introduttiva alle raccomandazioni strategiche](#)

Panoramica dei consigli strategici

Puoi iniziare la valutazione del tuo portafoglio di server e applicazioni utilizzando Migration Hub Strategy Recommendations dalla AWS Migration Hub console. La console viene utilizzata per configurare ed eseguire una valutazione. Dopo la valutazione, è possibile utilizzare la console per visualizzare i dati di valutazione per ogni server e applicazione, insieme allo strumento di trasformazione consigliato.

Per ricevere consigli sul refactoring e un elenco di incompatibilità, puoi utilizzare Strategy Recommendations per valutare il codice sorgente e i database dell'applicazione.

Puoi anche scaricare i dati dei consigli in un file Microsoft Excel.

Servizi correlati

- [AWS Migration Hub](#)— Si utilizza la AWS Migration Hub console per accedere alla console Migration Hub Strategy Recommendations. Visualizza anche informazioni sui server da cui vengono raccolti i dati.
- [AWS Application Discovery Service](#)— Utilizzi Application Discovery Service per raccogliere dati sui server e sulle applicazioni nella AWS Migration Hub console prima di utilizzare Strategy Recommendations.
- [AWS Application Migration Service](#): AWS Application Migration Service è il servizio di migrazione principale consigliato per lift-and-shift le migrazioni verso AWS.
- [AWS Database Migration Service](#)— AWS Database Migration Service è un servizio Web che puoi utilizzare per migrare i dati dal tuo database locale, su un'istanza DB di Amazon Relational Database Service (Amazon RDS) o da un database su un'istanza Amazon Elastic Compute Cloud (Amazon EC2) a un database su un servizio AWS.
- [AWS App2Container](#) — AWS App2Container (A2C) è uno strumento a riga di comando per modernizzare le applicazioni .NET e Java in applicazioni containerizzate.
- [Porting Assistant for .NET](#): utilizzato per l'analisi del codice sorgente .NET. Porting Assistant for .NET è uno scanner di compatibilità che riduce lo sforzo manuale richiesto per portare le applicazioni Microsoft .NET Framework su .NET Core. Il Porting Assistant for .NET valuta il codice sorgente dell'applicazione .NET e identifica pacchetti APIs incompatibili e di terze parti.
- [End-of-Support Programma di migrazione per Windows Server](#): il programma di End-of-Support migrazione (EMP) per Windows Server include strumenti per migrare le applicazioni legacy da

Windows Server 2003, 2008 e 2008 R2 a versioni più recenti e supportate, senza alcun refactoring.
AWS

- [AWS Schema Conversion Tool](#): è possibile utilizzare lo AWS Schema Conversion Tool (AWS SCT) per convertire lo schema di database esistente da un motore di database a un altro.
- [Windows Web Application Migration Assistant](#): Windows Web Application Migration Assistant per AWS Elastic Beanstalk è un' PowerShell utilità interattiva che migra le applicazioni ASP.NET e ASP.NET Core dai server Windows IIS locali a Elastic Beanstalk.
- [Babelfish per Aurora PostgreSQL — Babelfish per Aurora PostgreSQL](#) è una nuova funzionalità per l'edizione compatibile con Amazon Aurora PostgreSQL che consente ad Aurora di comprendere i comandi delle applicazioni scritte per il server Microsoft SQL.

Impostazione delle raccomandazioni strategiche

Prima di utilizzare Migration Hub Strategy Recommendations per la prima volta, completa le seguenti attività:

Argomenti

- [Registrati per un Account AWS](#)
- [Crea un utente con accesso amministrativo](#)
- [Utenti e ruoli di Strategy Recommendations](#)

Registrati per un Account AWS

Se non ne hai uno 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 o un messaggio di testo e ti verrà chiesto di inserire un codice di verifica attraverso la tastiera del telefono.

Quando ti iscrivi a un Account AWS, Utente root dell'account AWS viene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS 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 Account AWS, proteggi Utente root dell'account AWS AWS IAM Identity Center, abilita 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 [AWS Management Console](#) come proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.

Per informazioni sull'accesso utilizzando un utente root, consulta la pagina [Signing in as the root user](#) della Guida per l'utente di Accedi ad AWS .

2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

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

Crea un utente con accesso amministrativo

1. Abilita Centro identità IAM.

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

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

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

Accesso come utente amministratore

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

Per informazioni sull'accesso utilizzando un utente IAM Identity Center, consulta [AWS Accedere al portale di accesso](#) nella Guida per l'Accedi ad AWS utente.

Assegna l'accesso a ulteriori utenti

1. In IAM Identity Center, crea un set di autorizzazioni conforme alla best practice dell'applicazione di autorizzazioni con il privilegio minimo.

Segui le istruzioni riportate nella pagina [Creazione di un set di autorizzazioni](#) nella Guida per l'utente di AWS IAM Identity Center .

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

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

Utenti e ruoli di Strategy Recommendations

Ti consigliamo di creare due ruoli per Strategy Recommendations:

- Per accedere alla console, crea un ruolo con le politiche `AWSMigrationHubStrategyConsoleFullAccess` gestite allegate `AWSMigrationHubFullAccess` e quelle gestite.
- Per accedere al raccoglitore di dati dell'applicazione Strategy Recommendations, crea un ruolo con la policy `AWSMigrationHubStrategyCollector` gestita allegata.

Le policy gestite da IAM definiscono il livello di accesso a un servizio da parte degli utenti.

La policy AWS Migration Hub `AWSMigrationHubFullAccess` gestita consente l'accesso alla console Migration Hub. Per ulteriori informazioni, consulta [Ruoli e politiche di Migration Hub](#). Per informazioni sulle politiche `AWSMigrationHubStrategyCollector` gestite `AWSMigrationHubStrategyConsoleFullAccess` e sulle politiche gestite, vedere [AWS politiche gestite per le raccomandazioni strategiche di Migration Hub](#).

Per fornire l'accesso, aggiungi autorizzazioni agli utenti, gruppi o ruoli:

- Utenti e gruppi in AWS IAM Identity Center:

Crea un set di autorizzazioni. Segui le istruzioni riportate nella pagina [Create a permission set](#) (Creazione di un set di autorizzazioni) nella Guida per l'utente di AWS IAM Identity Center .

- Utenti gestiti in IAM tramite un provider di identità:

Crea un ruolo per la federazione delle identità. Segui le istruzioni riportate nella pagina [Create a role for a third-party identity provider \(federation\)](#) della Guida per l'utente IAM.

- Utenti IAM:

• Crea un ruolo che l'utente possa assumere. Segui le istruzioni riportate nella pagina [Create a role for an IAM user](#) della Guida per l'utente IAM.

- (Non consigliato) Collega una policy direttamente a un utente o aggiungi un utente a un gruppo di utenti. Segui le istruzioni riportate nella pagina [Aggiunta di autorizzazioni a un utente \(console\)](#) nella Guida per l'utente IAM.

Guida introduttiva alle raccomandazioni strategiche

Questa sezione descrive come iniziare a usare Migration Hub Strategy Recommendations.

Argomenti

- [Prerequisiti per le raccomandazioni strategiche](#)
- [Passaggio 1: scarica il raccoglitore Strategy Recommendations](#)
- [Fase 2: Implementate il raccoglitore Strategy Recommendations](#)
- [Fase 3: accedete al raccoglitore Strategy Recommendations](#)
- [Fase 4: Configurare il raccoglitore Strategy Recommendations](#)
- [Passaggio 5: utilizza Strategy Recommendations nella console Migration Hub per ottenere consigli](#)

Prerequisiti per le raccomandazioni strategiche

Di seguito sono riportati i prerequisiti per l'utilizzo delle raccomandazioni strategiche di Migration Hub.

- È necessario disporre di uno o più AWS account e gli utenti devono essere configurati per questi account. Per ulteriori informazioni, consulta [Impostazione delle raccomandazioni strategiche](#).
- Il client di raccolta dati dell'applicazione Strategy Recommendations deve essere in grado di raccogliere dati in remoto dai server. Ciò richiede l'utilizzo di un set di credenziali che funzionino per tutti i server Windows e un set di credenziali che funzionino per tutti i server Linux. Le credenziali devono disporre delle autorizzazioni per creare ed eliminare le directory nei server.
- La versione del collector distribuita in vCenter supporta vCenter Server V6.0, VMware V6.5, 6.7 o 7.0.

Puoi anche distribuire il collector in un' EC2 istanza Amazon utilizzando l'AMI collector.

- Verificare che l'ambiente del sistema operativo (OS) sia supportato:
 - Linux
 - Amazon Linux 2012.03, 2015.03
 - Amazon Linux 2 (aggiornamento 25/9/2018 e versioni successive)
 - Ubuntu 12.04, 14.04, 16.04, 18.04, 20.04
 - Red Hat Enterprise Linux 5.11, 6.10, 7.3, 7.7, 8.1
 - CentOS 5.11, 6.9, 7.3

- SUSE 11, 12 SP4 SP5
- Windows
 - Windows Server 2008 R1 SP2, 2008 R2 SP1
 - Windows Server 2012 R1, 2012 R2
 - Windows Server 2016
 - Windows Server 2019
- Per l'analisi del codice sorgente, i repository GitHub dell'utente GitHub e di Enterprise devono disporre di un token di accesso personale con l'ambito del repository che può essere condiviso con il client di raccolta Strategy Recommendations. Per ulteriori informazioni sulla creazione di un token di accesso personale con l'ambito del repository, consulta [Creazione di un token di accesso personale](#) nei Documenti. GitHub

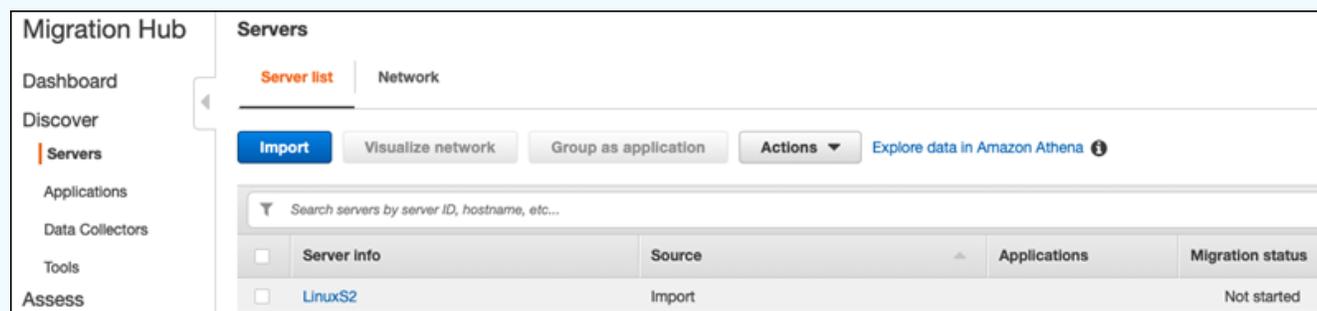
Per analizzare gli archivi .NET per i consigli di Porting Assistant for .NET, è necessario fornire un computer Windows configurato con lo strumento di valutazione del porting Porting Assistant for .NET. Per ulteriori informazioni, vedere [Guida introduttiva a Porting Assistant for .NET nella Guida per l'utente di Porting Assistant for .NET](#).

- Per abilitare Strategy Recommendations per l'analisi del database, è necessario inserire le credenziali in AWS Secrets Manager. Per ulteriori informazioni, consulta [Analisi del database di Strategy Recomm.](#)
- È necessario utilizzare AWS Application Discovery Service per raccogliere dati sui server e sulle applicazioni nella AWS Migration Hub console prima di utilizzare Strategy Recommendations. È possibile utilizzare uno dei seguenti metodi per raccogliere i dati.
 - Importazione da Migration Hub: con Migration Hub import, puoi importare informazioni sui server e sulle applicazioni locali in Migration Hub. Per ulteriori informazioni, vedere [Migration Hub Import](#) nella Guida per l'utente di Application Discovery Service.
 - AWS Application Discovery Service Agentless Collector: Agentless Collector è un' VMware appliance che raccoglie informazioni sulle macchine virtuali (VMware VMs). Per ulteriori informazioni, vedere [Agentless Collector](#) nella Guida per l'utente di Application Discovery Service.
 - AWS Application Discovery Agent: Discovery Agent è un AWS software che si installa sui server locali e consente di acquisire informazioni di sistema e dettagli sulle connessioni di rete tra i sistemi. Per ulteriori informazioni, vedere [AWS Application Discovery Agent](#) nella Application Discovery Service User Guide.

- **Raccogliatore di dati Strategy Recommendations:** se i server sono ospitati in VMware vCenter e l'utente fornisce l'accesso, Strategy Recommendations può recuperare automaticamente l'inventario dei server. La console Strategy Recommendations utilizzerà le informazioni raccolte per facilitare la valutazione.

Note

Per verificare che l'importazione di Migration Hub sia stata completata correttamente, nel pannello di navigazione della console di Migration Hub, in Discover, scegli Server. Tutti i server importati devono essere elencati.



Passaggio 1: scarica il raccogliatore Strategy Recommendations

Il raccogliatore di dati applicativi Migration Hub Strategy Recommendations è un'appliance virtuale che puoi installare nel tuo ambiente locale VMware. Il raccogliatore di dati applicativi Strategy Recommendations è disponibile anche come Amazon Machine Image (AMI). Se desideri utilizzare la versione AMI del raccogliatore per valutare le AWS applicazioni o per qualche altro motivo, non è necessario scaricare il raccogliatore. Puoi saltare questa sezione e andare a [Implementa il raccogliatore Strategy Recommendations in un'istanza Amazon EC2](#)

Questa sezione descrive come scaricare il file Collector Open Virtualization Archive (OVA) utilizzato per distribuire il collector come macchina virtuale (VM) nel proprio ambiente. VMware

Per scaricare il file Collector OVA

1. Utilizzando l'AWS account che hai creato [Impostazione delle raccomandazioni strategiche](#), accedi AWS Management Console e apri la console Migration Hub all'indirizzo <https://console.aws.amazon.com/migrationhub/>.
2. Nel riquadro di navigazione della console Migration Hub, scegli Strategia.

3. Nella pagina Consigli sulla strategia di Migration Hub, scegli Scarica il raccogliore di dati.
4. Facoltativamente, puoi scegliere Scarica il modello di importazione se desideri importare i dati dell'applicazione. Per ulteriori informazioni sull'importazione dei dati, consulta [Importazione di dati in Strategy Recommendations](#)
5. Fai clic sul pulsante Ottieni consigli e scegli Accetto per consentire a Migration Hub di creare un ruolo collegato al servizio (SLR) nel tuo account. Quando configuri Strategy Recommendations per la prima volta, devi creare la SLR. Per ulteriori informazioni, consulta [Utilizzo di ruoli collegati ai servizi per Strategy Recommendations](#).

Fase 2: Implementate il raccogliore Strategy Recommendations

Questa sezione descrive come implementare il raccogliore di dati applicativi Strategy Recommendations. Un application data collector è un raccogliore di dati senza agenti che identifica le applicazioni in esecuzione sui server, esegue l'analisi del codice sorgente e analizza i database.

Esistono due modi per distribuire il raccogliore:

- Implementa come macchina virtuale (VM) nel tuo vCenter Server VMware . Per ulteriori informazioni, consulta [Implementa il raccogliore Strategy Recommendations in vCenter](#).
- Se hai AWS applicazioni da valutare, puoi utilizzare il raccogliore Strategy Recommendations Amazon Machine Image (AMI). Per ulteriori informazioni, consulta [Implementa il raccogliore Strategy Recommendations in un'istanza Amazon EC2](#) .

Implementa il raccogliore Strategy Recommendations in vCenter

Il raccogliore di dati applicativi Migration Hub Strategy Recommendations è un'appliance virtuale che puoi installare nel tuo ambiente locale VMware . Questa sezione descrive come distribuire il file Collector Open Virtualization Archive (OVA) come macchina virtuale (VM) nell'ambiente in uso. VMware

La procedura seguente descrive come implementare il raccogliore Strategy Recommendations nell'ambiente VMware vCenter Server.

Per distribuire il raccogliore in vCenter

1. Accedere a vCenter come amministratore. VMware

2. Distribuisci il file OVA scaricato nel passaggio 1. Il file OVA include il raccogliitore e una CLI che può essere utilizzata per accedere all'API Strategy Recommendations.

Puoi anche scaricare il file OVA dal seguente link:

<https://application-data-collector-release.s3.us-west-2.amazonaws.com/ova/latest/AWSMHubApplicationDataCollector.ova>

Consigliamo le seguenti specifiche per la macchina virtuale.

Strategy Recommendations, specifiche della macchina virtuale da collezione.

- RAM: minimo 8 GB
- CPUs— almeno 4

Note

Per assicurarti di utilizzare la versione più recente del collector con tutte le nuove funzionalità e le correzioni di bug, aggiorna il collector dopo aver distribuito il file Collector OVA. Per istruzioni su come eseguire l'aggiornamento, consulta [Aggiornamento del raccogliitore Strategy Recommendations](#)

Implementa il raccogliitore Strategy Recommendations in un'istanza Amazon EC2

Se hai AWS applicazioni che desideri valutare, puoi utilizzare il raccogliitore di dati applicativi Strategy Recommendations Amazon Machine Image (AMI).

La procedura seguente descrive come avviare un' EC2 istanza Amazon dall'AMI del collettore.

Per distribuire l'istanza Amazon Collector EC2

1. Apri la EC2 console Amazon all'indirizzo <https://console.aws.amazon.com/ec2/>.
2. Nella barra di navigazione nella parte superiore della schermata, viene visualizzata la regione corrente (ad esempio US East [Ohio]). Scegli una regione adatta alle tue esigenze tra le regioni utilizzate da Strategy Recommendations. Per un elenco di queste regioni, consulta [Strategy Recommendations endpoints](#) in. Riferimenti generali di AWS

3. Nel riquadro di navigazione, sotto Immagini, scegli AMIs.
4. Scegli Immagini pubbliche dal menu a discesa di mia proprietà.
5. Scegli la barra di ricerca e seleziona Nome AMI dal menu.
6. Inserisci il nome AWSMHubApplicationDataCollector.
7. Per assicurarti che l'AMI provenga da una fonte sicura, verifica che il proprietario dell'account sia 703163444405.
8. Per avviare un'istanza da questa AMI, selezionala, quindi scegli Avvia. Per ulteriori informazioni sull'avvio di un'istanza tramite la console, consulta [Launching your instance from an AMI](#) nella Amazon EC2 User Guide.

Consigliamo le seguenti specifiche per l' EC2 istanza Amazon.

Strategy Recommendations collector, specifiche delle EC2 istanze Amazon

- RAM: minimo 8 GB
- CPUs— Almeno 4

L'AMI Strategy Recommendations include il raccogliatore e una CLI che può essere utilizzata per accedere all'API Strategy Recommendations.

Note

Per assicurarti di utilizzare la versione più recente del collector con tutte le nuove funzionalità e le correzioni di bug, aggiorna il collector dopo aver distribuito il raccogliatore Strategy Recommendations come istanza Amazon. EC2 Per istruzioni su come effettuare l'upgrade, consulta. [Aggiornamento del raccogliatore Strategy Recommendations](#)

Fase 3: accedete al raccogliatore Strategy Recommendations

Questa sezione descrive come accedere al raccogliatore di dati applicativi Migration Hub Strategy Recommendations distribuito. Il modo in cui accedi al raccogliatore dipende da come lo hai distribuito.

- [Accedi al collettore distribuito nell'ambiente basato su vCenter](#)
- [Accedi al collector distribuito come istanza Amazon EC2](#)

Accedi al collettore distribuito nell'ambiente basato su vCenter

Per accedere al raccogliatore Strategy Recommendations distribuito nell'ambiente basato su vCenter

1. Usa il seguente comando per connetterti al collettore utilizzando un client SSH.

```
ssh ec2-user@CollectorIPAddress
```

2. Quando viene richiesta una password, immettete la password predefinita `aq1@.WSde3`. È necessario modificare la password al primo accesso.

Accedi al collector distribuito come istanza Amazon EC2

Per accedere al raccogliatore Strategy Recommendations distribuito come istanza Amazon EC2

- Usa il seguente comando per connetterti al collettore utilizzando un client SSH.

```
ssh -i "Keyname.pem" ec2-user@CollectorIPAddress
```

`Keyname.pem` è la chiave privata generata quando hai avviato l' EC2 istanza Amazon dall'AMI del collettore.

Fase 4: Configurare il raccogliatore Strategy Recommendations

Questa sezione descrive come utilizzare `collector setup` i comandi della riga di comando per configurare il raccogliatore di dati applicativi Migration Hub Strategy Recommendations. Queste configurazioni vengono archiviate localmente.

Prima di poter utilizzare `collector setup` i comandi, è necessario creare una sessione di shell `bash` nel contenitore Collector Docker utilizzando il seguente comando. `docker exec`

```
docker exec -it application-data-collector bash
```

Il `collector setup` comando esegue tutti i seguenti comandi in successione, ma è possibile eseguirli singolarmente:

- `collector setup --aws-configurations`— Impostare le AWS configurazioni.

- `collector setup --vcenter-configurations`— Configurazione delle configurazioni vCenter.

Note

La configurazione di vCenter è disponibile solo se il collector è ospitato su vCenter. Tuttavia, è possibile forzare la configurazione di vCenter utilizzando il comando `collector setup --vcenter-configurations`

- `collector setup --remote-server-configurations`— Configurare le configurazioni dei server remoti.
- `collector setup --version-control-configurations`— Impostare le configurazioni di controllo della versione.

Per configurare tutte le configurazioni del raccogliitore contemporaneamente

1. Inserire il seguente comando.

```
collector setup
```

2. Immettere le informazioni per le AWS configurazioni come descritto in [Configura le AWS configurazioni](#)
3. Immettere le informazioni per le configurazioni vCenter come descritto in [Configurazione delle configurazioni vCenter](#)
4. Immettere le informazioni per le configurazioni dei server remoti come descritto in [Configurare le configurazioni del server remoto](#)
5. Immettere le informazioni per le configurazioni di controllo della versione come descritto in [Impostare le configurazioni di controllo della versione](#)
6. Prepara i server Windows e Linux per la raccolta dei dati di raccolta seguendo le istruzioni riportate in [Prepara i server Windows e Linux remoti per la raccolta dei dati](#)

Configura le AWS configurazioni

Per impostare AWS le configurazioni, quando si utilizza il `collector setup` comando o il `collector setup --aws-configurations` comando.

1. Digita Y come risposta affermativa alle autorizzazioni Have you setup IAM... domanda. Queste autorizzazioni vengono configurate quando si crea un utente per accedere al raccoglitore utilizzando la politica `AWSMigrationHubStrategyCollector` gestita seguendo i passaggi riportati di seguito. [Utenti e ruoli di Strategy Recommendations](#)
2. Inserisci la chiave di accesso e la chiave segreta dell' AWS account a cui l'utente che hai creato può accedere al raccoglitore seguendo la procedura descritta di seguito. [Utenti e ruoli di Strategy Recommendations](#)
3. Inserisci una regione, ad esempio, `us-west-2`. Scegli una regione adatta alle tue esigenze tra le regioni utilizzate da Strategy Recommendations. Per un elenco di queste regioni, consulta [Strategy Recommendations endpoints](#) in. Riferimenti generali di AWS
4. Digita Y per indicare sì alle metriche relative al collettore Upload to Migration Hub Strategy Service? domanda. Le informazioni sulle metriche aiutano a AWS fornire un supporto adeguato.
5. Digita Y per confermare l'accesso al servizio strategico Upload Collector to Migration Hub? domanda. Le informazioni contenute nei registri aiutano a AWS fornire un supporto adeguato.

L'esempio seguente mostra ciò che viene visualizzato, incluse le voci di esempio per le AWS configurazioni.

```
Have you setup IAM permissions in you AWS account as per the user guide? [Y/N]: Y
Choose one of the following options for providing user credentials:
1. Long term AWS credentials
2. Temporary AWS credentials
Enter your options [1-2]: 2
AWS session token:
AWS access key ID [None]:
AWS secret access Key [None]:
AWS region name [us-west-2]:
AWS configurations are saved successfully
Upload collector related metrics to migration hub strategy service? By default
collector will upload metrics. [Y/N]: Y
Upload collector related logs to migration hub strategy service? By default collector
will upload logs. [Y/N]: Y
Application data collector configurations are saved successfully
Start registering application data collector
Application data collector is registered successfully.
```

Configurazione delle configurazioni vCenter

Per configurare le configurazioni vCenter, quando si utilizza il `collector setup` comando o il comando: `collector setup --vcenter-configurations`

1. Inserisci Y per sì alla domanda Desideri autenticarti utilizzando le credenziali VMware vCenter, se desideri autenticarti utilizzando le credenziali vCenter. VMware

Note

L'autenticazione tramite credenziali VMware vCenter richiede l'installazione di VMware strumenti sui server di destinazione.

Immettere l'URL dell'host, che può essere l'indirizzo IP o l'URL di vCenter. Quindi, inserire il nome utente e la password per VMware vCenter.

2. Inserisci Y per sì alla domanda Hai macchine Windows gestite da VMware vCenter, se desideri configurare i server Windows.

Inserisci il nome utente e la password per Windows.

Note

Se il server remoto Windows appartiene a un dominio Active Directory, è necessario immettere il nome utente come *domain-name\username* quando si utilizza la CLI per fornire configurazioni del server remoto. Ad esempio, se il nome del dominio è `exampledomain` e il nome utente è `Administrator`, il nome utente immesso nella CLI è `exampledomain\ Administrator`.

3. Inserisci Y per sì alla domanda Setup for Linux VMware using vCenter, se desideri configurare i server Linux.

Inserisci il nome utente e la password per Linux.

4. Inserisci Y per sì alle domande Vuoi configurare le credenziali per i server esterni a vCenter usando NTLM per Windows e SSH/Cert based per Linux, se desideri configurare le credenziali del server remoto per server esterni a vCenter.

5. Per la domanda Desideri utilizzare le stesse credenziali di Windows utilizzate durante la configurazione di vCenter, inserisci Y per sì se le credenziali per le macchine Windows gestite all'esterno di vCenter sono le stesse credenziali fornite durante la configurazione delle credenziali per le macchine Windows vCenter. Altrimenti, inserisci N per no.

Se si risponde Y per sì, vengono poste le seguenti domande.

- a. Immettete Y per indicare che accettate che Collector accetti e memorizzi localmente i certificati dei server per vostro conto durante la prima interazione con i server Windows? domanda.
- b. Inserisci 1 per la domanda Inserisci le tue opzioni, se desideri configurare l'autenticazione SSH.

Se scegli di utilizzare l'autenticazione SSH, devi copiare le credenziali della chiave generata sui tuoi server Linux. Per ulteriori informazioni, consulta [Configura l'autenticazione basata su chiavi sui server Linux](#).

L'esempio seguente mostra cosa viene visualizzato, incluse le voci di esempio per le configurazioni VMware vCenter.

```
Your Linux remote server configurations are saved successfully.
collector setup -vcenter-configurations
Start setting up vCenter configurations for remote execution
Note: Authenticating using VMware vCenter credentials requires VMware tools to be
  installed on the target servers
Would you like to authenticate using VMware vCenter credentials? [Y/N]: y

NOTE: Your vSphere user must have Guest Operations privileges enabled.

Host Url for VMware vCenter: domain-name
Username for VMware vCenter: username
Password for VMware vCenter: password
Reenter password for VMware vCenter: password
Successfully stored vCenter credentials...
Do you have Windows machines managed by VMware vCenter? [Y/N]: y

NOTE: For the best experience, we recommend that you create a new Active Directory user
  in the Domain Admins group.

Username for Windows (Domain\User): username
```

```
Password for Windows: password
Reenter password for Windows: password
Successfully stored windows credentials...
You can verify your setup for vCenter windows machines is correct with "collector diag-
check"
Do you have Linux machines managed by VMWare vCenter? [Y/N]: y
Username for Linux: username
Password for Linux: password
Reenter password for Linux: password
Successfully stored linux credentials...
You can verify your setup for vCenter linux machines is correct with "collector diag-
check"
Would you like to setup credentials for servers not managed by vCenter using NTLM for
windows and SSH/Cert based for Linux? [Y/N]: y
Setting up target server for remote execution:
Would you like to setup credentials for servers not managed by vCenter using NLTM for
Windows [Y/N]: y
Would you like to use the same Windows credentials used during vCenter setup? [Y/N]: y
Are you okay with collector accepting and locally storing server certificates on your
behalf during first interaction with windows servers? These certificates will be used
by collector for secure communication with windows servers [Y/N]: y
Successfully stored windows server credentials...
Please note that all windows server certificates are stored in directory /opt/amazon/
application-data-collector/remote-auth/windows/certs

Please note the IP address of the collector and run the script specified in the user
documentation on all the windows servers in your inventory
You can verify your setup for remote windows machines is correct with "collector diag-
check"
Would you like to setup credentials for servers not managed by vCenter using SSH/Cert
based for Linux? [Y/N]: y
Choose one of the following options for remote authentication:
1. SSH based authentication
2. Certificate based authentication
Enter your options [1-2]: 1
Would you like to use the same Linux credentials used during vCenter setup? [Y/N]: y
Generating SSH key on this machine...
Successfully generated SSH key pair

SSH key pair path: /opt/amazon/application-data-collector/remote-auth/linux/keys/
id_rsa_assessment
Please add the public key "id_rsa_assessment.pub" to the "$HOME/.ssh/authorized_keys"
file in your remote machines.
```

```
You can verify your setup for remote linux machines is correct with "collector diag-check
```

Configurare le configurazioni del server remoto

Per configurare le configurazioni del server remoto, quando si utilizza il `collector setup` comando o il `collector setup --remote-server-configurations` comando:

1. Inserisci Y per sì alla domanda Vuoi configurare le credenziali per i server non gestiti da vCenter usando NLTM per Windows, se desideri configurare i server Windows.

Immettere il nome utente e la password per WinRM.

Note

Se il server remoto Windows appartiene a un dominio Active Directory, è necessario immettere il nome utente come `domain-name\username` quando si utilizza la CLI per fornire configurazioni del server remoto. Ad esempio, se il nome del dominio è `exampledomain` e il nome utente è `Administrator`, il nome utente immesso nella CLI è `exampledomain\ Administrator`.

Digita Y per indicare Sì a Are you okay with Collector che accetta e archivia localmente i certificati dei server per tuo conto durante la prima interazione con i server Windows? domanda. I certificati di Windows Server sono archiviati nella `directory/opt/amazon/application-data-collector/remote-auth/windows/certs`.

È necessario copiare le credenziali del server generate sui server Windows. Per ulteriori informazioni, consulta [Configura la configurazione del server remoto sui server Windows](#).

2. Se desideri configurare i server Linux, inserisci Y per rispondere alla domanda Setup for Linux using SSH o Cert.
3. Inserisci 1 per la domanda Inserisci le tue opzioni, se desideri configurare l'autenticazione basata su chiave SSH.

Se scegli di utilizzare l'autenticazione SSH, devi copiare le credenziali della chiave generata sui tuoi server Linux. Per ulteriori informazioni, consulta [Configura l'autenticazione basata su chiavi sui server Linux](#).

- Inserisci 2 per la domanda Inserisci le tue opzioni, se desideri configurare l'autenticazione basata su certificati.

Per informazioni sulla configurazione dell'autenticazione basata su certificati, consulta. [Configura l'autenticazione basata su certificati sui server Linux](#)

L'esempio seguente mostra ciò che è visualizzato, incluse le voci di esempio per le configurazioni del server remoto.

```
Setting up target server for remote execution
Would you like to setup credentials for servers not managed by vCenter using NLTM for
Windows [Y/N]: y

NOTE: For the best experience, we recommend that you create a new Active Directory user
in the Domain Admins group.

Username for WinRM (Domain\User): username
Password for WinRM: password
Reenter password for WinRM: password
Are you okay with collector accepting and locally storing server certificates on your
behalf during first interaction with windows servers? These certificates will be used
by collector for secure communication with windows servers [Y/N]: Y
Successfully stored windows server credentials...
Please note that all windows server certificates are stored in directory /opt/amazon/
application-data-collector/remote-auth/windows/certs

Please note the IP address of the collector and run the script specified in the user
documentation on all the windows servers in your inventory
Would you like to setup credentials for servers not managed by vCenter using SSH/Cert
based for Linux? [Y/N]: Y
Choose one of the following options for remote authentication:
1. SSH based authentication
2. Certificate based authentication
Enter your options [1-2]: 1
User name for remote server: username
Generating SSH key on this machine...
SSH key pair path: /opt/amazon/application-data-collector/remote-auth/linux/keys/
id_rsa_assessment
Please add the public key "id_rsa_assessment.pub" to the "$HOME/.ssh/authorized_keys"
file in your remote machines.
Your Linux remote server configurations are saved successfully.
```

Impostare le configurazioni di controllo della versione

Per impostare le configurazioni di controllo della versione, quando si utilizza il `collector setup` comando o il `collector setup --version-control-configurations` comando:

1. Digitare Y per confermare l'analisi del codice sorgente? domanda.
2. Inserisci 1 per la domanda Inserisci le tue opzioni, se desideri configurare l'endpoint del server Git.

Inserisci github.com per l'endpoint del server GIT:.

3. Inserisci 2 per la domanda Inserisci le tue opzioni, se desideri configurare un Enterprise Server. GitHub

Immettere l'endpoint aziendale senza `https://`, nel modo seguente: endpoint del server GIT: *git-enterprise-endpoint*

4. Inserisci il tuo Git *username* e il tuo accesso personale *token*.
5. Inserisci Y per sì al file Hai dei repository csharp che dovrebbero essere analizzati su un computer Windows? domanda, se vuoi analizzare il codice C#.

Note

Per analizzare i repository.NET per i consigli di Porting Assistant for .NET, è necessario fornire un computer Windows configurato con lo strumento di valutazione del porting Porting Assistant for .NET. Per ulteriori informazioni, vedere [Guida introduttiva a Porting Assistant for .NET nella Guida per l'utente di Porting Assistant for .NET](#).

6. Per la pagina Vuoi riutilizzare le credenziali Windows esistenti su questo computer? domanda. Immettere Y per sì, se la macchina Windows per l'analisi del codice sorgente C# utilizza le stesse credenziali delle credenziali fornite in precedenza come parte della configurazione o. --remote-server-configurations --vcenter-configurations

Inserisci N per no, se desideri inserire nuove credenziali.

7. Per utilizzare le credenziali della macchina Windows VMWare vCenter, immettere 1 per Scegli una delle seguenti opzioni per le credenziali di Windows.
8. Immettere l'indirizzo IP per il computer Windows.

L'esempio seguente mostra ciò che viene visualizzato, incluse le voci di esempio per le configurazioni di controllo della versione.

```
Set up for source code analysis [Y/N]: y
Choose one of the following options for version control type:
1. GIT
2. GIT Enterprise
3. Azure DevOps - Git
Enter your options [1-3]: 3
Your server endpoint: dev.azure.com (http://dev.azure.com/)
Your DevOps Organization name: <Your organization name>
Personal access token [None]:
Your version control credentials are saved successfully.
Do you have any csharp repositories that should be analyzed on a windows machine? [Y/N]: y
Would you like to reuse existing windows credentials on this machine? [Y/N]: y
Choose one of the following options for windows credentials:
1. VMWare vCenter Windows Machine
2. Standard Windows Machine
Enter your options [1-2]:
1
Windows machine IP Address: <Your windows machine IP address>
Using VMWare vCenter Windows Machine credentials
Successfully stored windows server credentials...
```

Prepara i server Windows e Linux remoti per la raccolta dei dati

Note

Questo passaggio non è necessario se si configura il raccogliatore di dati delle applicazioni Strategy Recommendations utilizzando le credenziali vCenter.

Dopo aver configurato le configurazioni del server remoto, se si utilizza il `collector setup --remote-server-configurations` comando `collector setup command o`, è necessario preparare i server remoti in modo che l'agente di raccolta dati delle applicazioni Strategy Recommendations possa raccogliere dati da essi.

Note

È necessario assicurarsi che i server siano raggiungibili utilizzando il loro indirizzo IP privato. Per ulteriori istruzioni su come configurare l'ambiente tramite un cloud privato virtuale (VPC) AWS per l'esecuzione remota, consulta la [Amazon Virtual Private Cloud User Guide](#).

Per preparare i server Linux remoti, consulta [Preparare server Linux remoti](#).

Per preparare i server Windows remoti, consulta [Configura la configurazione del server remoto sui server Windows](#).

Preparare server Linux remoti

Configura l'autenticazione basata su chiavi sui server Linux

Se scegli di configurare l'autenticazione basata su chiave SSH per Linux durante la configurazione delle configurazioni dei server remoti, devi eseguire i seguenti passaggi per configurare l'autenticazione basata su chiave sui tuoi server in modo che i dati possano essere raccolti dal raccogliatore di dati delle applicazioni Strategy Recommendations.

Per configurare l'autenticazione basata su chiavi sui server Linux

1. Copia la chiave pubblica generata con il nome `id_rsa_assessment.pub` dalla seguente cartella nel contenitore:

`/opt/amazon/application-data-collector/remote-auth/linux/keys.`
2. Aggiungi la chiave pubblica copiata nel file per tutte le macchine remote. `$HOME/.ssh/authorized_keys` Se non è disponibile alcun file, crealo utilizzando il comando `touch ovim`.
3. Assicurati che la cartella home sul server remoto abbia un livello di autorizzazione 755 o inferiore. Se lo è 777, non funzionerà. È possibile utilizzare il `chmod` comando per limitare le autorizzazioni.

Configura l'autenticazione basata su certificati sui server Linux

Se si sceglie di configurare l'autenticazione basata su certificati per Linux durante la configurazione delle configurazioni dei server remoti, è necessario eseguire le seguenti operazioni in modo che i dati possano essere raccolti dal raccogliatore di dati dell'applicazione Strategy Recommendations.

Consigliamo questa opzione se disponi già di Certificate Authority (CA) configurata per i server delle applicazioni.

Per configurare l'autenticazione basata su certificati sui server Linux

1. Copia il nome utente che funziona con tutti i tuoi server remoti.
2. Copia la chiave pubblica del raccogliatore nella CA.

La chiave pubblica per il raccogliatore si trova nella seguente posizione:

```
/_rsa_assessment.pub opt/amazon/application-data-collector/remote-auth/linux/keys/id
```

Questa chiave pubblica deve essere aggiunta alla CA per generare il certificato.

3. Copia il certificato generato nel passaggio precedente nella seguente posizione nel raccogliatore:

```
/opt/amazon/application-data-collector/remote-auth/linux/keys
```

Il nome del certificato deve essere `id_rsa_assessment-cert.pub`.

4. Fornisci il nome del file del certificato durante la fase di configurazione.

Configura la configurazione del server remoto sui server Windows

Se si sceglie di configurare Windows durante la configurazione dei server remoti nella configurazione del collector, è necessario eseguire le seguenti operazioni in modo che i dati possano essere raccolti da Strategy Recommendations.

 Per ulteriori informazioni sullo PowerShell script eseguito sul server remoto, leggi questa nota.

Lo script abilita la PowerShell modalità remota e disabilita tutti i metodi di autenticazione diversi da Negotiate. Viene utilizzato per Windows NT LAN Manager (NTLM) e imposta il WSMAN protocollo "AllowUnencrypted" su false per garantire che il listener appena creato accetti solo traffico crittografato. Utilizzando lo script fornito da `MicrosoftNew-SelfSignedCertificateEx.ps1`, crea un certificato autofirmato.

Qualsiasi WSMAN istanza con un listener HTTP viene rimossa insieme ai listener HTTPS esistenti. Quindi, crea un nuovo listener HTTPS. Crea inoltre una regola firewall in entrata per la porta TCP 5986. Nel passaggio finale, il servizio WinRM viene riavviato.

Per configurare la raccolta dei dati tramite una connessione remota sui server Windows 2008

1. Usa il seguente comando per verificare la versione PowerShell installata sul tuo server.

```
$PSVersionTable
```

2. Se la PowerShell versione non è 5.1, scarica e installa WMF 5.1 seguendo le istruzioni riportate in [Installazione e configurazione di WMF 5.1 nella documentazione Microsoft](#).
3. Utilizzate il seguente comando in una nuova PowerShell finestra per assicurarvi che PowerShell la versione 5.1 sia installata.

```
$PSVersionTable
```

4. Segui la prossima serie di passaggi, che descrive come configurare la raccolta dei dati tramite una connessione remota in Windows 2012 e versioni successive.

Per configurare la raccolta dei dati tramite una connessione remota su server Windows 2012 e versioni successive

1. Scarica lo script di installazione dal seguente URL:

<https://application-data-collector-release.s3.us-west-2.amazonaws.com/scripts/RMSetupWin.ps1>

2. Scaricate il file `New-SelfSignedCertificateEx.ps1` dal seguente URL e incollate lo script nella stessa cartella in cui avete scaricato: `WinRMSetup.ps1`

<https://github.com/Azure/azure-libraries-for-net/blob/master/Samples/Asset/New-SelfSignedCertificateEx.ps1>

3. Per completare la configurazione, esegui PowerShell lo script scaricato su tutti i server delle applicazioni.

```
.\WinRMSetup.ps1
```

Note

Se Windows Remote Management (WinRM) non è configurato correttamente su Windows Remote Server, il tentativo di raccogliere dati da quel server avrà esito negativo. In tal caso,

è necessario eliminare il certificato corrispondente a quel server dalla seguente posizione nel contenitore:

`opt/amazon/application-data-collector/remote-auth/windows/certs/ads-server-id.cer`

Dopo aver eliminato il certificato, attendi che venga ripetuto il processo di raccolta dei dati.

Verifica che il raccogliatore e i server siano configurati per la raccolta dei dati

Verifica che il raccogliatore e i server siano configurati correttamente per la raccolta dei dati utilizzando il comando seguente.

```
collector diag-check
```

Questo comando esegue una serie di controlli diagnostici sulle configurazioni del server e fornisce input in caso di controlli non riusciti.

Quando si utilizza il comando in `-a` modalità, si ottiene l'output in un `DiagnosticCheckResultfile.txt` al termine dei controlli.

```
collector diag-check -a
```

È possibile eseguire un controllo diagnostico sulle configurazioni del server di un singolo server con l'indirizzo IP di quel server.

Gli esempi seguenti mostrano il risultato di una configurazione corretta.

Server Linux

```
Provide your test server IP address: IP address
-----
Start checking connectivity & credentials...
Connectivity and Credential Checks succeeded
-----
Start checking permissions...
Permission Check succeeded
-----
Start checking OS version...
OS version check succeeded
```

```
-----  
Start checking Linux Bash installation...  
Linux Bash installation check succeeded  
-----  
All diagnostic checks complete successfully.  
This server is correctly set up and ready for data collection.
```

Server Windows

```
Windows PowerShell Version Check succeeded  
Provide your test server IP address: IP address  
-----  
Start checking connectivity & credentials...  
Connectivity and Credential Checks succeeded  
-----  
Start checking permissions...  
Permission Check succeeded  
-----  
Start checking OS version...  
OS version check succeeded  
-----  
Start checking Windows architecture type...  
Windows Architecture Type Check succeeded  
-----  
All diagnostic checks complete successfully.  
This server is correctly set up and ready for data collection.
```

L'esempio seguente mostra un messaggio di errore che viene visualizzato quando le credenziali del server remoto non sono corrette.

```
Unable to authenticate the server credentials with IP address ${IPAddress}.  
Ensure that your credentials are accurate and the server is configured correctly.  
Use the following command to reset incorrect credentials.  
collector setup --remote-server-configurations
```

Passaggio 5: utilizza Strategy Recommendations nella console Migration Hub per ottenere consigli

Questa sezione descrive come utilizzare Strategy Recommendations nella console Migration Hub per ottenere consigli sulla migrazione per la prima volta.

Per ottenere le raccomandazioni

1. Utilizzando l' AWS account che hai creato [Impostazione delle raccomandazioni strategiche](#), accedi AWS Management Console e apri la console Migration Hub all'indirizzo <https://console.aws.amazon.com/migrationhub/>.
2. Nel riquadro di navigazione della console Migration Hub, scegli Strategia.
3. Nella pagina Consigli sulla strategia di Migration Hub, scegli Ottieni consigli.
4. Scegli Accetto se accetti di consentire a Migration Hub di creare un ruolo collegato al servizio (SLR) nel tuo account. Per ulteriori informazioni sulla reflex, consulta. [Utilizzo di ruoli collegati ai servizi per Strategy Recommendations](#)
5. Configurare le fonti di dati
 - a. Nella pagina Configura le fonti di dati, devi scegliere l'origine dei tuoi server da analizzare tra le seguenti opzioni:
 - i. Raccoglitore di dati applicativi Strategy Recommendations: è possibile utilizzare il raccoglitore Strategy Recommendations per recuperare automaticamente le informazioni sull'hosting VMs in VMware vCenter. Utilizzando questa opzione, non è necessario eseguire configurazioni aggiuntive.
 - ii. Importazione manuale: se desideri importare i dati relativi ai server e alle applicazioni in modo indipendente, puoi utilizzare il modello di importazione di Strategy Recommendations. Il modello di importazione è un file JSON in cui puoi inserire le informazioni disponibili per il tuo VMs.
 - iii. Application Discovery Service: è possibile utilizzare Application Discovery Service per raccogliere informazioni sulle applicazioni e sui server locali. Nella console Migration Hub, nella sezione Strumenti, puoi scegliere tra diverse opzioni in Discovery tools. Ad esempio, puoi scegliere Application Discovery Service Agentless Collector, AWS Discovery Agent o Import (per i file CSV).
 - b. La tabella Server elenca tutti i server disponibili in base alla selezione effettuata nella sezione Origine dati.

- c. In Raccoglitori di dati applicativi registrati, sono elencati i raccoglitori di dati delle applicazioni che hai configurato. Se non hai configurato alcun raccoglitore di dati, puoi scaricare il raccoglitore di dati e quindi distribuirlo. Per ulteriori informazioni, consulta [Passaggio 1: scarica il raccoglitore Strategy Recommendations](#) e [Fase 2: Implementate il raccoglitore Strategy Recommendations](#).

 Note

Per ottenere consigli strategici, è necessario configurare almeno un raccoglitore di dati applicativi o eseguire un'importazione dei dati delle applicazioni. Se desideri aggiungere i dati a livello di applicazione senza configurare un raccoglitore, puoi utilizzare il modello di importazione dei dati dell'applicazione. Puoi aggiungere altre fonti di dati in un secondo momento.

- d. Se hai selezionato Importazione manuale, in Dettagli di importazione, scegli Aggiungi nuova importazione.
- e. In Importa nome, inserisci un nome per l'importazione.
- f. Per l'URI del bucket S3, inserisci l'URI del bucket S3 in cui caricare il file JSON di importazione.

 Important

Il nome del bucket S3 deve iniziare con un prefisso di **migrationhub-strategy**

- g. Scegli Next (Successivo).
6. Specificare le preferenze
 - a. Nella pagina Specificare le preferenze, imposta gli obiettivi aziendali e le preferenze di migrazione. Strategy Recommendations consiglia la strategia ottimale per la migrazione e la modernizzazione delle applicazioni e dei database in base alle preferenze specificate. È possibile modificare queste preferenze in un secondo momento.
 - b. Scegli Next (Successivo).
 7. Rivedi e invia.
 - a. Rivedi le fonti di dati configurate e le preferenze di migrazione.

- b. Se tutto sembra corretto, scegli **Avvia analisi dei dati**. Questo eseguirà un'analisi dell'inventario del server e dell'ambiente di runtime e dei file binari dell'applicazione per le applicazioni Microsoft IIS e Java.

 **Note**

Lo stato dell'analisi binaria non viene visualizzato nella console. Al termine dell'analisi, verrà visualizzato un collegamento al rapporto anti-pattern o un messaggio che indica che l'analisi non ha avuto esito positivo.

Strategia, raccomandazioni, raccomandazioni

Questa sezione descrive come visualizzare i consigli di migrazione e modernizzazione di Strategy Recommendations per server e applicazioni nel tuo portafoglio di migrazione.

Argomenti

- [Visualizzazione dei consigli strategici in Strategy Recommendations](#)
- [Strategy Recommendations: consigli sui componenti](#)
- [Strategy Recommendations: consigli](#)
- [Preferenze relative ai consigli strategici](#)

Visualizzazione dei consigli strategici in Strategy Recommendations

Questa sezione descrive come utilizzare Strategy Recommendations nella AWS Migration Hub console per visualizzare i consigli sulla strategia di migrazione.

Per visualizzare i consigli strategici

1. Utilizzando l' AWS account che hai creato [Impostazione delle raccomandazioni strategiche](#), accedi AWS Management Console e apri la console Migration Hub all'indirizzo <https://console.aws.amazon.com/migrationhub/>.
2. Nel riquadro di navigazione della console Migration Hub, scegli Strategia, quindi scegli Consigli.
3. Nella pagina Consigli, puoi visualizzare ed esportare consigli riassuntivi del tuo portafoglio e consigli dettagliati sulla strategia di migrazione «R». È inoltre possibile visualizzare gli strumenti e le destinazioni di migrazione e modernizzazione e gli anti-pattern per i server e i componenti delle applicazioni.

Gli anti-pattern sono un elenco di problemi noti riscontrati nel vostro portafoglio, classificati in base alla gravità. Gli anti-pattern ad alta gravità rappresentano incompatibilità che devono essere risolte, gli anti-pattern di media gravità rappresentano avvisi e gli anti-pattern a bassa gravità rappresentano problemi informativi. Per informazioni sulla strategia «R», vedere [Termini di migrazione - 7 R](#) nel glossario AWS Prescriptive Guidance.

- Se si verifica una modifica nel data center o se si aggiornano le preferenze, si consiglia di rianalizzare i dati. Per rianalizzare i dati e ottenere nuovi consigli, scegli [Rianalizza i dati](#).

Fino al completamento del processo di rianalisi, i risultati dei dati di raccomandazione possono essere una combinazione di dati precedenti e nuovi dati.

Per scaricare un file di report con i consigli, scegli [Esporta consigli](#).

4. Nella scheda Componenti dell'applicazione, puoi visualizzare i consigli per i componenti delle applicazioni nel tuo portafoglio di migrazione. Per ulteriori informazioni, consulta [Strategy Recommendations: consigli sui componenti](#).
5. Nella scheda Server, puoi visualizzare i consigli per i server del tuo portafoglio di migrazione. Per ulteriori informazioni, consulta [Strategy Recommendations: consigli](#).
6. Nella scheda Preferenze, puoi modificare le preferenze specificate in [Fase 5: Ottieni consigli](#). Per informazioni sulla modifica delle preferenze, consulta [Preferenze relative ai consigli strategici](#).

Strategy Recommendations: consigli sui componenti

Questa sezione descrive come utilizzare Strategy Recommendations nella console Migration Hub per visualizzare e analizzare i consigli sulla strategia di migrazione per i componenti dell'applicazione.

Argomenti

- [Utilizzo dei componenti dell'applicazione in Strategy Recommendations](#)
- [Strategy Recommendations, analisi del codice](#)
- [Analisi del database di Strategy Recomm](#)
- [Strategy Recommendations \(analisi](#)

Utilizzo dei componenti dell'applicazione in Strategy Recommendations

Questa sezione descrive come utilizzare Migration Hub Strategy Recommendations nella console Migration Hub per visualizzare e configurare i consigli sulle strategie di migrazione e modernizzazione.

Argomenti

- [Visualizzazione dei consigli sui componenti dell'applicazione](#)

- [Configurare l'analisi del codice sorgente per un componente dell'applicazione](#)
- [Configurare l'analisi del database per un componente dell'applicazione](#)

Visualizzazione dei consigli sui componenti dell'applicazione

Questa sezione descrive come utilizzare Strategy Recommendations nella console Migration Hub per visualizzare le raccomandazioni sulla strategia di migrazione per i componenti dell'applicazione.

Per visualizzare i dettagli dei consigli per i componenti dell'applicazione

1. Utilizzando l' AWS account che hai creato [Impostazione delle raccomandazioni strategiche](#), accedi AWS Management Console e apri la console Migration Hub all'indirizzo <https://console.aws.amazon.com/migrationhub/>.
2. Nel riquadro di navigazione della console Migration Hub, scegli Strategia, quindi scegli Consigli.
3. Nella pagina Consigli, scegli la scheda Componenti dell'applicazione.
 - a. In Riepilogo dei componenti dell'applicazione, è disponibile una panoramica dei vari tipi di componenti applicativi in esecuzione nel portafoglio di server.
 - b. In Componenti dell'applicazione, puoi visualizzare il nome del componente, il tipo di componente e i consigli sulla strategia di migrazione «R». È inoltre possibile visualizzare la destinazione della migrazione e gli strumenti di migrazione e modernizzazione da utilizzare per i vari componenti applicativi in esecuzione nel portafoglio di server. Per informazioni sulla strategia «R», vedere [Termini di migrazione - 7 R](#) nel glossario AWS Prescriptive Guidance.
4. Per visualizzare i dettagli di un componente dell'applicazione, selezionate un componente dell'applicazione, quindi scegliete Visualizza dettagli.
5. Nella pagina dei dettagli del componente dell'applicazione (la pagina con il nome del componente come titolo) in Riepilogo dei consigli, puoi visualizzare i consigli per il componente dell'applicazione. È inoltre possibile visualizzare i modelli Anti identificati. Gli anti-pattern sono un elenco di problemi noti riscontrati nel vostro portafoglio, classificati in base alla gravità.
6. Scegliete la scheda Opzioni di strategia per visualizzare i consigli di migrazione per il componente dell'applicazione. È possibile ignorare la strategia consigliata selezionando una strategia diversa e quindi scegliendo Imposta preferita.
7. A seconda del tipo di componente dell'applicazione che state visualizzando, è disponibile una configurazione di origine o una scheda di configurazione del database. Per informazioni sulla configurazione del codice sorgente, vedere [Configurare l'analisi del codice sorgente](#)

[per un componente dell'applicazione](#). Per informazioni sulla configurazione del database, vedere [Configurare l'analisi del database per un componente dell'applicazione](#).

Configurare l'analisi del codice sorgente per un componente dell'applicazione

Questa sezione descrive come utilizzare Strategy Recommendations nella console Migration Hub per configurare l'analisi del codice sorgente per un componente dell'applicazione.

Per configurare l'analisi del codice sorgente per un componente dell'applicazione

1. Nel riquadro di navigazione della console Migration Hub, scegli Strategia, quindi scegli Consigli.
2. Nella pagina Consigli, scegli la scheda Componenti dell'applicazione.
3. Dall'elenco dei componenti in Componenti dell'applicazione, selezionate un componente dell'applicazione con un tipo di componente java, dotnetframework o IIS, quindi scegliete Visualizza dettagli.
4. Nella pagina dei dettagli del componente dell'applicazione (la pagina con il nome del componente come intestazione), scegli la scheda Configurazione del codice sorgente.
5. In Dettagli di configurazione del codice sorgente, scegli Analizza il codice sorgente.
6. Nella pagina Analizza codice sorgente, fornisci il nome del repository, il nome del ramo e il nome del progetto (se applicabile) in cui è archiviato il codice sorgente per il componente dell'applicazione. Seleziona il tipo di controllo della versione del codice GitHub sorgente che desideri utilizzare, quindi scegli Analizza.

Una volta completata l'analisi, è possibile visualizzare i consigli aggiornati nella pagina dei dettagli dei componenti dell'applicazione.

Per ulteriori informazioni sull'analisi del codice sorgente, vedere [Strategy Recommendations, analisi del codice](#).

Configurare l'analisi del database per un componente dell'applicazione

Questa sezione descrive come utilizzare Strategy Recommendations nella console Migration Hub per configurare l'analisi del database per un componente dell'applicazione.

Per configurare l'analisi del database per un componente dell'applicazione

1. Nel riquadro di navigazione della console Migration Hub, scegli Strategia, quindi scegli Consigli.

2. Nella pagina Consigli, scegli la scheda Componenti dell'applicazione.
3. Dall'elenco dei componenti in Componenti dell'applicazione, selezionate un componente dell'applicazione con il tipo di SQLServercomponente, quindi scegliete Visualizza dettagli.
4. Nella pagina dei dettagli del componente dell'applicazione (la pagina con il nome del componente come intestazione), scegli la scheda Configurazione del database.
5. In Dettagli di configurazione del database, scegli Analizza i dettagli del database.
6. Scegliete un nome segreto dal menu a discesa creato in AWS Secrets Manager da utilizzare per le credenziali del database, quindi scegliete Analizza.

Una volta completata l'analisi, è possibile visualizzare i consigli aggiornati nella pagina dei dettagli dei componenti dell'applicazione.

Per ulteriori informazioni sull'analisi del database e sull'impostazione di un nome segreto, vedere [Analisi del database di Strategy Recomm.](#)

Strategy Recommendations, analisi del codice

Migration Hub Strategy Recommendations identifica automaticamente le applicazioni del tuo portafoglio e crea componenti applicativi per esse. Ad esempio, se nel portafoglio è presente un'applicazione Java, questa viene identificata come componente dell'applicazione con un tipo di componente java.

Strategy Recommendations analizza il codice sorgente dei componenti dell'applicazione se lo configurate a tale scopo. Per informazioni sulla configurazione di un componente dell'applicazione per l'analisi del codice sorgente, vedere. [Configurare l'analisi del codice sorgente per un componente dell'applicazione](#)

Strategy Recommendations esegue l'analisi del codice sorgente per i linguaggi di programmazione Java e C#.

Per informazioni sui prerequisiti per l'utilizzo dell'analisi del codice sorgente di Strategy Recommendations, vedere. [Prerequisiti per le raccomandazioni strategiche](#)

Analisi del database di Strategy Recomm

Strategy Recommendations identifica automaticamente i server di database del tuo portafoglio e crea i relativi componenti applicativi. Ad esempio, se nel portafoglio è presente un database SQL Server, questo viene identificato come componente dell'applicazione sqlservr.exe.

Strategy Recommendations analizza i singoli database nel componente dell'applicazione SQL Server identificato, sqlservr.exe, utilizzando lo AWS Schema Conversion Tool. Strategy Recommendations identifica anche le incompatibilità nella migrazione dei database verso database AWS come Amazon Aurora MySQL Compatible Edition, Amazon Aurora PostgreSQL Compatible Edition, Amazon RDS for MySQL e Amazon RDS for PostgreSQL.

Attualmente, l'analisi del database Strategy Recommendations è disponibile solo per SQL Server.

Per configurare Strategy Recommendations per analizzare i database, è necessario fornire le credenziali per il raccoglitore di dati dell'applicazione Strategy Recommendations per connettersi ai database. Per fare ciò, crea un segreto in AWS Secrets Manager nel tuo AWS account.

Per informazioni sulle autorizzazioni e i privilegi delle credenziali fornite, consulta. [Privilegi necessari per le credenziali AWS dello Schema Conversion Tool](#) Per informazioni sulla creazione di un segreto con le credenziali, vedere. [Creazione di un segreto in Secrets Manager per le credenziali del database](#)

Dopo aver impostato le credenziali e il segreto, è possibile configurare l'analisi AWS dello Schema Conversion Tool sul server del database. Per ulteriori informazioni, consulta [Configurare l'analisi del database per un componente dell'applicazione](#).

Dopo aver configurato l'analisi del database per il componente dell'applicazione, viene pianificata un'attività di inventario AWS dello Schema Conversion Tool. Al termine di questa attività, vedrete i nuovi componenti dell'applicazione creati per ogni singolo database su quel server di database. Ad esempio, se SQL Server dispone di due database (exampledb1 ed exampledb2), viene creato un componente applicativo per ciascuno dei database con i nomi exampledb1 ed exampledb2.

Se desideri vedere degli anti-pattern nella migrazione di ogni database identificato ai database, configura l'analisi per ogni database seguendo i passaggi riportati di seguito. AWS [Configurare l'analisi del database per un componente dell'applicazione](#)

Privilegi necessari per le credenziali AWS dello Schema Conversion Tool

Le credenziali di accesso fornite a AWS Secrets Manager sono solo esigenze VIEW SERVER STATE e VIEW ANY DEFINITION privilegi.

È possibile fornire il nome e la password di accesso desiderati durante la creazione dell'accesso a SQL Server.

Creazione di un segreto in Secrets Manager per le credenziali del database

Dopo che le credenziali sono pronte per consentire al raccoglitore di dati dell'applicazione Strategy Recommendations di connettersi a un database, crea un segreto in AWS Secrets Manager nel tuo AWS account come descritto nella procedura seguente.

Per creare un segreto con AWS Secrets Manager nel tuo AWS account

1. Utilizzando l' AWS account che hai creato [Impostazione delle raccomandazioni strategiche](#), accedi AWS Management Console e apri la console AWS Secrets Manager all'indirizzo <https://console.aws.amazon.com/secretsmanager/>.
2. Scegli Archivia un nuovo segreto.
3. Seleziona il tipo di segreto come Altro tipo di segreti.
4. In Coppie chiave/valore, inserisci le seguenti informazioni.

nome utente - *your-username*

Quindi scegli + Aggiungi riga e inserisci le seguenti informazioni.

password - *your-password*

5. Scegli Next (Successivo).
6. Inserisci il nome segreto come qualsiasi stringa con il prefisso migrationhub-strategy -. Ad esempio, migrationhub-strategy-one.

Note

Conserva il tuo nome segreto in un posto sicuro per un uso successivo.

7. Scegli Avanti, quindi scegli nuovamente Avanti.
8. Scegli Store.

È possibile utilizzare il segreto creato per le credenziali del database durante l'impostazione dell'analisi del database in Strategy Recommendations.

Strategy Recommendations (analisi)

Migration Hub Strategy Recommendations identifica automaticamente le applicazioni del portafoglio e i componenti applicativi che vi appartengono. Ad esempio, se nel portafoglio è presente

un'applicazione Java, Strategy Recommendations la identifica come un componente dell'applicazione con un componente di tipo java. Senza dover configurare l'accesso al codice sorgente, Strategy Recommendations può eseguire analisi binarie esaminando l'applicazione IIS DLLs su Windows o i file JAR dell'applicazione su Linux e fornendo report anti-pattern o report di incompatibilità. Un rapporto anti-pattern è un elenco di problemi noti che Strategy Recommendations rileva nel tuo portafoglio, classificati in base alla gravità. Un rapporto di incompatibilità contiene un sottoinsieme degli anti-pattern, che sono compatibilità API, Nuget Package e Porting Action.

Strategy Recommendations esegue analisi per le applicazioni Windows IIS e Java Tomcat e Jboss. Se si dispone di un'applicazione IIS, Strategy Recommendations genera un rapporto di incompatibilità per impostazione predefinita; è necessario configurare l'accesso al codice sorgente per ricevere il rapporto anti-pattern completo. Se disponi di un'applicazione Java, Strategy Recommendations genera il rapporto anti-pattern completo per impostazione predefinita.

Il report incompatibile o contrario allo schema viene visualizzato al termine dell'analisi. Se l'analisi non ha esito positivo, è possibile provare a eseguire un'analisi del codice sorgente fornendo l'accesso al codice sorgente come descritto in [Impostare le configurazioni di controllo della versione](#)

Strategy Recommendations: consigli

Questa sezione descrive come utilizzare Migration Hub Strategy Recommendations nella console Migration Hub per visualizzare i consigli sulla strategia di migrazione per i server del portafoglio di migrazione.

Per visualizzare i consigli per i server

1. Utilizzando l' AWS account che hai creato [Impostazione delle raccomandazioni strategiche](#), accedi AWS Management Console e apri la console Migration Hub all'indirizzo <https://console.aws.amazon.com/migrationhub/>.
2. Nel riquadro di navigazione della console Migration Hub, scegli Strategia, quindi scegli Consigli.
3. Nella pagina Consigli, scegli la scheda Server.
 - a. In Riepilogo dei server, puoi visualizzare una panoramica dei vari tipi di server che utilizzi nel tuo portafoglio.
 - b. In Server, puoi visualizzare i dettagli del server e del sistema operativo e i consigli sulla strategia di migrazione «R». È inoltre possibile visualizzare la destinazione della migrazione e il numero di anti-pattern identificati sui server, in base ai consigli. Per informazioni sulla strategia «R», vedere [Termini di migrazione - 7 R](#) nel glossario AWS Prescriptive Guidance.

4. Per visualizzare dettagli dettagliati sui consigli per un server, seleziona il server dall'elenco, quindi scegli Visualizza dettagli. È possibile visualizzare i metadati raccolti per il server, insieme ad analisi approfondite e consigli relativi, basati sui componenti dell'applicazione trovati in esecuzione sul server.
5. Nella pagina dei dettagli del server (la pagina con il nome del server come intestazione), in Riepilogo dei consigli, è possibile visualizzare una panoramica dei consigli strategici per il server. È inoltre possibile visualizzare i modelli Anti identificati. Gli anti-pattern sono un elenco di problemi noti riscontrati nel vostro portafoglio, classificati in base alla gravità.
6. Scegli la scheda Opzioni di strategia per visualizzare i consigli di migrazione per il server. Puoi ignorare la strategia consigliata selezionando una strategia diversa e quindi scegliendo Imposta preferita.
7. Scegliete la scheda Componenti dell'applicazione per visualizzare l'elenco dei componenti dell'applicazione associati al server.
8. Per visualizzare i dettagli sul componente dell'applicazione, selezionate il componente dall'elenco, quindi scegliete Visualizza dettagli. Per ulteriori informazioni sui componenti dell'applicazione, vedere [Utilizzo dei componenti dell'applicazione](#).

Preferenze relative ai consigli strategici

Questa sezione descrive come visualizzare e modificare le preferenze di Migration Hub Strategy Recommendations nella console Migration Hub.

Scegli le tue preferenze di raccomandazione quando configuri per la prima volta Strategy Recommendations come descritto in [Fase 5: Ottieni consigli](#). È possibile modificare queste preferenze.

Per modificare le preferenze relative ai consigli

1. Utilizzando l' AWS account che hai creato [Impostazione delle raccomandazioni strategiche](#), accedi AWS Management Console e apri la console Migration Hub all'indirizzo <https://console.aws.amazon.com/migrationhub/>.
2. Nel riquadro di navigazione della console Migration Hub, scegli Strategia, quindi scegli Consigli.
3. Nella pagina Consigli, scegli la scheda Preferenze.
4. In Obiettivi aziendali prioritari, puoi trascinare e rilasciare gli obiettivi aziendali per riorganizzarli.
5. Scegli le preferenze dell'applicazione e le preferenze del database che desideri, quindi scegli Salva modifiche.

Se modificate le preferenze, viene visualizzato un banner per ricordarvi di scegliere Rianalizza i dati.

Fonti di dati sulle raccomandazioni strategiche

Questa sezione descrive le fonti di dati utilizzate da Strategy Recommendations.

Argomenti

- [Visualizzazione delle fonti di dati di Strategy Recomm](#)
- [Strategy Recommendations, raccolta di dati applicativi](#)
- [Importazione di dati in Strategy Recommendations](#)
- [Rimuovere i dati da Strategy Recommendations](#)

Visualizzazione delle fonti di dati di Strategy Recomm

Questa sezione descrive come visualizzare le fonti di dati Strategy Recommendations in AWS Management Console.

Per visualizzare le fonti di dati

1. Utilizzando l' AWS account che hai creato [Impostazione delle raccomandazioni strategiche](#), accedi AWS Management Console e apri la console Migration Hub all'indirizzo <https://console.aws.amazon.com/migrationhub/>.
2. Nel riquadro di navigazione della console Migration Hub, scegli Strategia, quindi scegli Origini dati.
3. Nella scheda Raccoglitori, puoi visualizzare i raccoglitori di dati dell'applicazione Strategy Recommendations che hai configurato. Per ulteriori informazioni sul raccoglitore, consulta [Strategy Recommendations, raccolta di dati applicativi](#)
4. Nella scheda Importazioni, puoi importare dati e visualizzare le importazioni di dati. Per ulteriori informazioni, consulta [Importazione di dati in Strategy Recommendations](#).
5. Nella scheda Strumenti, puoi scaricare il modello di dati di importazione del raccoglitore e dell'applicazione.

Strategy Recommendations, raccolta di dati applicativi

Questa sezione descrive come utilizzare il raccoglitore di dati dell'applicazione Strategy Recommendations.

Per informazioni sul download e la configurazione di un raccoglitore di dati di un'applicazione, vedere.

[Passaggio 1: scarica il raccoglitore Strategy Recommendations](#)

Argomenti

- [Dati raccolti dal raccoglitore Strategy Recommendations](#)
- [Aggiornamento del raccoglitore Strategy Recommendations](#)

Dati raccolti dal raccoglitore Strategy Recommendations

Questa sezione descrive il tipo di dati raccolti dal raccoglitore di dati dell'applicazione Migration Hub Strategy Recommendations. Un raccoglitore di dati applicativi è un raccoglitore di dati senza agenti che identifica le applicazioni in esecuzione sui server, esegue l'analisi del codice sorgente e analizza i database.

Campo dati	Descrizione
Tipo di sistema operativo	Windows o Linux
Versione SO	La versione specifica del sistema operativo. Ad esempio, Windows Server 2003, RHEL 5.2.
Architettura del sistema operativo	Sistema operativo a 32 o 64 bit
È una macchina virtuale del server	Il server è una macchina virtuale o una macchina fisica.
Software di virtualizzazione	Ad esempio, vCenter, Hyper-V.
Ubicazione	Ad esempio, la console Amazon Elastic Compute Cloud (Amazon EC2) o in locale.
È DualBoot	Consente l'avvio in più OSs
Tipo di firmware	BIOS, UEFI
Boot loader	GRUB, GRUB 2
Tipo di tabella delle partizioni	MBR, GPT

Campo dati	Descrizione
Velocità della CPU	Velocità della CPU in GHz. Ad esempio, 2.4 GHz.
Windows OS data	
Edizione Windows	Standard, Data Center, Enterprise
Versione.NET Framework	La versione del framework.NET installata.
Versione.NET Core	La versione di.NET Core installata.
Linux data	
Distribuzione del sistema operativo Linux	RHEL, CentOS, SUSE e così via.
Versione del kernel	output <code>uname -r</code> , ad esempio <code>4.9.217-0.1.ac.205.84.332.meta11.x86_64</code>
For each disk volume	
Tipo di file system	FAT32, NTFS, ReFS, ext4, jfs e così via.
Dimensioni del volume del disco	Dimensione totale del disco
Spazio libero nel volume del disco	Spazio libero su disco
Formato dell'immagine del disco virtuale	vmdk, vhd, vhdx
Tipo di disco (Windows)	Di base, dinamico
Application level data	
Nome applicazione	Il nome del processo in esecuzione. Ad esempio, <code>SQLServr.exe</code> , <code>MSdtsservr.exe</code> e così via.
Tipo di applicazione	IIS JBoss, Tomcat e così via.
Linguaggio e versione di programmazione	C#, Java

Campo dati	Descrizione
Versione JDK	La versione del JDK installata.
Il codice sorgente è disponibile	Se fornite un archivio di codice sorgente, ciò indica che il codice sorgente è disponibile.
Dimensione in bit dell'applicazione	16 bit, 32 bit, 64 bit
Windows	
Versione.NET framework utilizzata dall'app	La versione della DLL di.NET framework caricata in fase di esecuzione per l'applicazione.
Versione.NET Core	La versione.NET Core DLL caricata in fase di esecuzione dell'applicazione.
Utilizza il framework WPF?	Determina se l'applicazione basata su .NET è un tipo di app WPF o meno.
Utilizza il framework WCF?	Determina se l'applicazione basata su .NET è un tipo di app WCF o meno.
Versione ASP.NET	La versione di ASP.NET.
Versione IIS	La versione del server IIS installata sul computer Windows.
Dimensione in bit dei driver del sistema operativo dell'applicazione	32 bit, 64 bit
Utilizzo del registro di Windows	Interroga le chiavi di registro del computer per trovare informazioni come la versione del database, la versione Java, la versione.NET e così via.
Tutte DLLs utilizzate dall'applicazione	Recupera l'elenco di tutti i DLLs file caricati in fase di esecuzione da un processo di Windows.

Campo dati	Descrizione
PowerShell versione	Verifica la PowerShell versione installata sul computer, che dovrebbe essere 5.1 o successiva.
Linux	
Tipo di framework applicativo	Tomcat, Spring Boot, JBoss, WebLogic WebSphere
Versione del framework applicativo	La versione del framework applicativo.
Database	
Tipo di database	MS SQL, Oracle, MySQL e così via.
Versione del database	La versione del database.

Rimuovi i tuoi dati da Strategy Recommendations

Per far rimuovere tutti i tuoi dati da Strategy Recommendations, contatta [Supporto AWS](#) e richiedi l'eliminazione completa dei dati.

Aggiornamento del raccogliatore Strategy Recommendations

Il raccogliatore di dati dell'applicazione Migration Hub Strategy Recommendations si aggiorna automaticamente. È possibile utilizzare la seguente procedura per aggiornare manualmente il raccogliatore, se necessario.

Per aggiornare il raccogliatore Strategy Recommendations

1. Usa il seguente comando per connetterti alla macchina virtuale del collettore utilizzando un client SSH.

```
ssh ec2-user@CollectorIPAddress
```

2. Passate alla directory di aggiornamento nella VM del collettore, come mostrato nell'esempio seguente.

```
cd /home/ec2-user/collector/upgrades
```

3. Utilizzare il comando seguente per eseguire lo script di aggiornamento.

```
sudo bash application-data-collector-upgrade
```

Importazione di dati in Strategy Recommendations

In alternativa all'utilizzo dell'Application Data Collector, puoi importare informazioni sulle applicazioni e sui server per i quali desideri consigli di migrazione e modernizzazione.

Quando si importano dati, i consigli non sono così approfonditi come lo sono quando si utilizza il raccogliitore di dati. Ad esempio, non è possibile utilizzare l'analisi del codice sorgente sui dati importati.

Questa sezione descrive come utilizzare il modello di importazione dell'applicazione per importare i dati in Strategy Recommendations nella console Migration Hub.

Per importare dati

1. Utilizzando l' AWS account che hai creato [Impostazione delle raccomandazioni strategiche](#), accedi AWS Management Console e apri la console Migration Hub all'indirizzo <https://console.aws.amazon.com/migrationhub/>.
2. Nel riquadro di navigazione della console Migration Hub, scegli Strategia, quindi scegli Origini dati.
3. Scegli la scheda Importazioni.
4. Scegliete Scarica modello di importazione per scaricare il modello di importazione dell'applicazione.
5. Compila il modello e caricalo in un bucket Amazon S3. Assicurati che il nome del bucket inizi con il prefisso. migrationhub-strategy
6. Torna alla scheda Importazioni e scegliete Importa.
7. Inserisci un nome per l'importazione, inserisci l'URI dell'oggetto Amazon S3 per il modello di dati compilato, quindi scegli Avvia importazione.

Il modello di importazione Strategy Recommendations

Il modello di importazione scaricato è un .json file, come illustrato nell'esempio seguente.

```
{
  "ImportFormatVersion": 1,
  "Resources": [
    {
      "ResourceType": "SERVER",
      "ResourceName": "",
      "ResourceId": "",
      "IpAddress": "",
      "OSDistribution": "",
      "OSType": "",
      "HostName": "",
      "OSVersion": "",
      "CPUArchitecture": ""
    },
    {
      "ResourceType": "PROCESS",
      "ResourceName": "",
      "ResourceId": "",
      "ApplicationType": "",
      "DotNetFrameworkVersion": "",
      "ApplicationVersion": "",
      "DotNetCoreVersion": "",
      "JdkVersion": "",
      "ProgrammingLanguage": "",
      "DatabaseType": "",
      "DatabaseVersion": "",
      "DatabaseEdition": "",
      "AssociatedServerIds": []
    }
  ]
}
```

Per facilitare la compilazione del modello di importazione, i valori validi per i campi dati sono elencati nelle tabelle seguenti.

I campi obbligatori per i server sono elencati nella tabella seguente.

Nome	Descrizione	Tipo	Richiesto	Valori validi
ResourceId	Un ID univoco per la risorsa	Stringa	Si	Qualsiasi stringa univoca
ResourceName	Il nome della risorsa	Stringa	Si	Qualsiasi stringa
ResourceType	Il tipo di risorsa da importare	Stringa	Si	«Server», «Processo»
OSDistribution	Windows, Windows Server, Ubuntu	Stringa	Si	Windows: «PC Windows», «Windows Server» Linux: «Ubuntu», «RHEL», «Amazon Linux», «DEBIAN», «SLES», «CENT_OS», «ORACLE_LINUX», «FEDORA», «KALI»
OSType	Il tipo di sistema operativo	Stringa	Si	«Windows», «Linux»
OSVersion	La versione del kernel	Stringa	Si	Vedi la versione HTML della documentazione.
CPUArchitecture	L'architettura della CPU	Stringa	No	«32 bit», «64 bit»
IpAddress	L'indirizzo IP del server	Array	No	Nel formato xxx.xxx.xxx.xxx
MacAddresses	Gli indirizzi Mac associati al server	Array	No	Nel formato xx:xx:xx:xx:xx:xx

Nome	Descrizione	Tipo	Richiesto	Valori validi
Hostname (Nome host)	Il nome dell'host	Stringa	No	Qualsiasi stringa

I campi obbligatori per i processi sono elencati nella tabella seguente.

Nome	Descrizione	Tipo	Richiesto	Valori validi
ResourceId	Un ID univoco per la risorsa	Stringa	Sì	Qualsiasi stringa univoca
ResourceName	Il nome della risorsa	Stringa	Sì	Qualsiasi stringa
ResourceType	Il tipo di risorsa da importare	Stringa	Sì	«Server», «Processo»
AssociatedServerIds	Un elenco di server IDs su cui è in esecuzione il processo.	Stringa	Sì	ResourceId Dal "Resource Type": «SERVER» che hai definito.
ApplicationType	Il tipo di applicazione	Stringa	Sì	«Tomcat», JBoss «Spring», «IIS», «Mongo DB», «Maria DB», DB2 «MySQL», «Oracle», «Sybase», «Postger», SQLServer «Cassandra», «IBM WebSphere», «SQLServerOracle», «Java Generic» WebLogic

Nome	Descrizione	Tipo	Richiesto	Valori validi
ApplicationVersion	La versione dell'applicazione	Stringa	Sì	«IIS 1.0», «IIS 2.0», «IIS 3.0», «IIS 4.0», «IIS 5.1», «IIS 6.0», «IIS 7.0», «IIS 7.5», «IIS 8.0», «IIS 8.0», «IIS 8.5», «IIS 10.0»
ProgrammingLanguage	Il linguaggio di programmazione per l'applicazione	Stringa	No	«Java», «CSharp»

Nome	Descrizione	Tipo	Richiesto	Valori validi
DotNetCoreVersion	La versione di .NET Core se l'applicazione è basata su .NET Core	Stringa	No	«.NET Core 1.0», «.NET Core 1.1», «.NET Core 2.0», «.NET Core 2.1», «.NET Core 2.2», «.NET Core 3.0», «.NET Core 3.1»
JdkVersion	La versione del JDK, se l'applicazione utilizza il JDK	Stringa	No	"JDK1.0", ".0", ".0", "...", "JDK2 .0" JDK3 JDK11
DatabaseType	Il tipo di database	Stringa	No	«», SQLServer «Oracle», «Sybase», «Mongo DB», «Maria DB», «Apache Cassandra», «MySQL», «IBM», «Postgre» DB2 SQLServer
DatabaseEdition	L'edizione del database	Stringa	No	
DatabaseVersion	La versione del database	Stringa	No	Vedi la versione HTML della documentazione.

Rimuovere i dati da Strategy Recommendations

Per far rimuovere tutti i tuoi dati dai consigli strategici di Migration Hub, contatta [Supporto AWS](#).

Raccomandazioni sulla strategia sulla sicurezza in Migration Hub

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

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

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi in Cloud AWS. AWS fornisce inoltre servizi che è possibile utilizzare in modo sicuro. I revisori esterni testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei [AWS Programmi di AWS conformità dei Programmi di conformità](#) dei di . Per ulteriori informazioni sui programmi di conformità che si applicano alle raccomandazioni della strategia di Migration Hub, vedere [AWS Servizi nell'ambito del programma di conformitàAWS](#) .
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

Questa documentazione aiuta a capire come applicare il modello di responsabilità condivisa quando si utilizza Strategy Recommendations. I seguenti argomenti mostrano come configurare Strategy Recommendations per soddisfare gli obiettivi di sicurezza e conformità. Imparerai anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le tue risorse Strategy Recommendations.

Argomenti

- [La protezione dei dati nelle raccomandazioni strategiche di Migration Hub](#)
- [Gestione delle identità e degli accessi per le raccomandazioni strategiche di Migration Hub](#)
- [Convalida della conformità per le raccomandazioni strategiche di Migration Hub](#)

La protezione dei dati nelle raccomandazioni strategiche di Migration Hub

Il modello di [responsabilità AWS condivisa modello](#) di di si applica alla protezione dei dati nelle raccomandazioni strategiche di Migration Hub. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per ulteriori informazioni sulla privacy dei dati, vedi le [Domande frequenti sulla privacy dei dati](#). Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al [Modello di responsabilità condivisa AWS e GDPR](#) nel Blog sulla sicurezza AWS .

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Usa SSL/TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail Per informazioni sull'utilizzo dei CloudTrail percorsi per acquisire AWS le attività, consulta [Lavorare con i CloudTrail percorsi](#) nella Guida per l'AWS CloudTrail utente.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-3 per accedere AWS tramite un'interfaccia a riga di comando o un'API, usa un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il [Federal Information Processing Standard \(FIPS\) 140-3](#).

Ti consigliamo di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando si lavora con Strategy Recommendations o altro Servizi AWS utilizzando la console, l'API o. AWS CLI AWS SDKs I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando fornisci un URL a un

server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

Crittografia dei dati a riposo

Tutti i dati archiviati nel database di Strategy Recommendations sono crittografati.

Crittografia in transito

Strategy Recommendations Le comunicazioni internetwork supportano la crittografia TLS 1.2 tra tutti i componenti e i client.

Gestione delle identità e degli accessi per le raccomandazioni strategiche di Migration Hub

AWS Identity and Access Management (IAM) è uno strumento Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse di Strategy Recommendations. IAM è uno Servizio AWS strumento che puoi utilizzare senza costi aggiuntivi.

Argomenti

- [Destinatari](#)
- [Autenticazione con identità](#)
- [Gestione dell'accesso con policy](#)
- [Come funziona Migration Hub Strategy Recommendations con IAM](#)
- [AWS politiche gestite per le raccomandazioni strategiche di Migration Hub](#)
- [Esempi di policy basate sull'identità per le raccomandazioni strategiche di Migration Hub](#)
- [Risoluzione dei problemi relativi a Migration Hub Strategy Recommendations: identità e accesso](#)
- [Utilizzo di ruoli collegati ai servizi per Strategy Recommendations](#)
- [Raccomandazioni sulla strategia di Migration Hub e endpoint VPC di interfaccia \(\)AWS PrivateLink](#)

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia a seconda del lavoro svolto in Strategy Recommendations.

Utente del servizio: se utilizzi il servizio Strategy Recommendations per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più funzionalità di Strategy Recommendations 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 Strategy Recommendations, consulta [Risoluzione dei problemi relativi a Migration Hub Strategy Recommendations: identità e accesso](#).

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

Amministratore IAM: se sei un amministratore IAM, potresti voler conoscere i dettagli su come scrivere policy per gestire l'accesso a Strategy Recommendations. Per visualizzare esempi di policy basate sull'identità di Strategy Recommendations che puoi utilizzare in IAM, consulta [Esempi di policy basate sull'identità per le raccomandazioni strategiche di Migration Hub](#)

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi essere autenticato (aver effettuato l'accesso root dell'account AWS) come utente IAM o assumendo un ruolo IAM.

Puoi accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center (precedentemente AWS Single Sign-On), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Quando accedi AWS utilizzando la federazione, assumi 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 (CLI) per firmare crittograficamente le tue richieste utilizzando le tue credenziali. Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sul metodo consigliato per la firma delle richieste, consulta [Signature Version 4 AWS per le richieste API](#) nella Guida per l'utente IAM.

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'utente di AWS IAM Identity Center e [Utilizzo dell'autenticazione a più fattori \(MFA\)AWS in IAM](#) nella Guida per l'utente IAM.

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzale per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione [Attività che richiedono le credenziali dell'utente root](#) nella Guida per l'utente IAM.

Identità federata

Come procedura consigliata, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente dell'elenco utenti aziendale, di un provider di identità Web AWS Directory Service, della directory Identity Center o di qualsiasi utente che accede utilizzando le Servizi AWS credenziali fornite tramite un'origine di identità. Quando le identità federate accedono Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di

utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per ulteriori informazioni su IAM Identity Center, consulta [Cos'è IAM Identity Center?](#) nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un [utente IAM](#) è un'identità interna Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, se si hanno casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina [Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine](#) nella Guida per l'utente IAM.

Un [gruppo IAM](#) 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 amministrare le risorse IAM.

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 utenti IAM](#) nella Guida per l'utente IAM.

Ruoli IAM

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

I ruoli IAM 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 ulteriori informazioni sulla federazione dei ruoli, consulta [Create a role for a third-party identity provider \(federation\)](#) nella Guida per l'utente IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per informazioni sui set di autorizzazioni, consulta [Set di autorizzazioni](#) nella Guida per l'utente di AWS IAM Identity Center.

- **Autorizzazioni utente IAM temporanee:** un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- **Accesso multi-account:** è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'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 informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta [Accesso a risorse multi-account in IAM](#) nella Guida per l'utente IAM.
- **Accesso a più servizi:** alcuni Servizi AWS utilizzano le funzionalità di 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 inoltrato (FAS):** quando utilizzi un utente o un ruolo IAM 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, combinate con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS 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 delle policy relative alle richieste FAS, consulta [Forward access sessions](#).
- **Ruolo di servizio:** un ruolo di servizio è un [ruolo IAM](#) che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione [Create a role to delegate permissions to an Servizio AWS](#) nella Guida per l'utente IAM.
- **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 amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un' EC2 istanza e che AWS CLI effettuano richieste AWS API. 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 ruolo IAM per concedere le autorizzazioni alle applicazioni in esecuzione su EC2 istanze Amazon](#) nella IAM User Guide.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e collegandole 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 documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta [Panoramica delle policy JSON](#) nella Guida per l'utente IAM.

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire operazioni 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 operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Le policy IAM definiscono le autorizzazioni relative a un'operazione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dall' AWS Management Console AWS CLI, dall' AWS API.

Policy basate sull'identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che utenti e

ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta [Definizione di autorizzazioni personalizzate IAM con policy 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 nel tuo Account AWS. Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta [Scelta fra policy gestite e policy inline](#) nella Guida per l'utente IAM.

Policy basate sulle risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Esempi di policy basate sulle risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket 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 operazioni 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 puoi utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Liste di controllo degli accessi () ACLs

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 della lista di controllo degli accessi \(ACL\)](#) 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 delle autorizzazioni è una funzionalità avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a

un'entità IAM (utente o ruolo 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 IAM](#) nella Guida per l'utente IAM.

- Politiche di controllo del servizio (SCPs): SCPs sono politiche JSON 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 di proprietà dell' Account AWS 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. L'SCP limita le autorizzazioni per le entità presenti negli account dei membri, inclusa ciascuna di esse. 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.
- Politiche di controllo delle risorse (RCPs): RCPs sono politiche JSON che puoi utilizzare per impostare le autorizzazioni massime disponibili per le risorse nei tuoi account senza aggiornare le politiche IAM allegate a ciascuna risorsa di tua proprietà. L'RCP limita le autorizzazioni per le risorse negli account dei membri e può influire sulle autorizzazioni effettive per le identità, incluse le Utente root dell'account AWS, indipendentemente dal fatto che appartengano o meno all'organizzazione. Per ulteriori informazioni su Organizations e RCPs, incluso un elenco di Servizi AWS tale supporto RCPs, vedere [Resource control policies \(RCPs\)](#) nella Guida per l'AWS Organizations 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 [Policy di sessione](#) nella Guida per l'utente IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire o meno una richiesta quando sono coinvolti più tipi di policy, consulta la [logica di valutazione delle policy](#) nella IAM User Guide.

Come funziona Migration Hub Strategy Recommendations con IAM

Prima di utilizzare IAM per gestire l'accesso a Strategy Recommendations, scopri quali funzionalità IAM sono disponibili per l'uso con Strategy Recommendations.

Funzionalità IAM che puoi utilizzare con Migration Hub Strategy Recommendations

Funzionalità IAM	Supporto per consigli strategici
Policy basate su identità	Sì
Policy basate su risorse	No
Azioni di policy	Sì
Risorse relative alle policy	No
Chiavi di condizione delle policy	No
ACLs	No
ABAC (tag nelle policy)	No
Credenziali temporanee	Sì
Autorizzazioni del principale	Sì
Ruoli di servizio	No
Ruoli collegati al servizio	Sì

Per avere una visione di alto livello di come Strategy Recommendations e altri AWS servizi funzionano con la maggior parte delle funzionalità IAM, consulta [AWS i servizi che funzionano con IAM nella IAM](#) User Guide.

Politiche basate sull'identità per le raccomandazioni strategiche

Supporta le policy basate su identità: sì

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta [Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente](#) nella Guida per l'utente IAM.

Con le policy basate su identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta [Guida di riferimento agli elementi delle policy JSON IAM](#) nella Guida per l'utente di IAM.

Esempi di politiche basate sull'identità per raccomandazioni strategiche

Per visualizzare esempi di politiche basate sull'identità di Strategy Recommendations, vedere. [Esempi di policy basate sull'identità per le raccomandazioni strategiche di Migration Hub](#)

Politiche basate sulle risorse all'interno di Strategy Recommendations

Supporta le policy basate su risorse: no

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Esempi di policy basate sulle risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket 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 operazioni 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

Per consentire l'accesso multi-account, puoi specificare un intero account o entità IAM in un altro account come principale in una policy basata sulle risorse. L'aggiunta di un principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il principale e la risorsa sono diversi Account AWS, un amministratore IAM dell'account affidabile deve inoltre concedere all'entità principale (utente o ruolo) l'autorizzazione ad accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta [Accesso a risorse multi-account in IAM](#) nella Guida per l'utente IAM.

Azioni politiche per raccomandazioni strategiche

Supporta le operazioni di policy: si

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

L'elemento `Actions` di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Le azioni politiche in genere hanno lo stesso nome dell'operazione AWS API associata. Ci sono alcune eccezioni, ad esempio le operazioni di sola autorizzazione che non hanno un'operazione API corrispondente. 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.

Per visualizzare un elenco delle azioni Strategy Recommendations, consulta [Actions Defined by Migration Hub Strategy Recommendations](#) nel Service Authorization Reference.

Le azioni politiche in Strategy Recommendations utilizzano il seguente prefisso prima dell'azione:

```
migrationhub-strategy
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

```
"Action": [  
  "migrationhub-strategy:action1",  
  "migrationhub-strategy:action2"  
]
```

Per visualizzare esempi di politiche basate sull'identità di Strategy Recommendations, vedere [Esempi di policy basate sull'identità per le raccomandazioni strategiche di Migration Hub](#)

Risorse politiche per le raccomandazioni strategiche

Supporta risorse politiche: No

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

L'elemento `Resource` della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Le istruzioni devono includere un elemento `Resource` o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo [nome della risorsa Amazon \(ARN\)](#). È possibile eseguire questa operazione per operazioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*" 
```

Per visualizzare un elenco dei tipi di risorse Strategy Recommendations e relativi ARNs, consulta [Resources Defined by Migration Hub Strategy Recommendations](#) nel Service Authorization Reference. Per sapere con quali azioni è possibile specificare l'ARN di ogni risorsa, consulta [Azioni definite dai consigli strategici di Migration Hub](#).

Per visualizzare esempi di politiche basate sull'identità di Strategy Recommendations, vedi [Esempi di policy basate sull'identità per le raccomandazioni strategiche di Migration Hub](#)

Chiavi relative alle condizioni politiche per le raccomandazioni strategiche

Supporta le chiavi delle condizioni delle politiche specifiche del servizio: No

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

L'elemento `Condition` (o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition` è facoltativo. È possibile compilare espressioni condizionali che utilizzano [operatori di condizione](#), ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition` in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione AND logica. Se si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione logica. OR Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

È possibile anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, è possibile autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo

nome utente IAM. Per ulteriori informazioni, consulta [Elementi delle policy IAM: variabili e tag](#) nella Guida per l'utente di IAM.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di [contesto delle condizioni AWS globali nella Guida](#) per l'utente IAM.

Per visualizzare un elenco delle chiavi di condizione di Strategy Recommendations, consulta [Condition Keys for Migration Hub Strategy Recommendations](#) nel Service Authorization Reference. Per sapere con quali azioni e risorse è possibile utilizzare una chiave di condizione, consulta [Azioni definite dai consigli strategici di Migration Hub](#).

Per visualizzare esempi di politiche basate sull'identità di Strategy Recommendations, vedi. [Esempi di policy basate sull'identità per le raccomandazioni strategiche di Migration Hub](#)

Accedi agli elenchi di controllo (ACLs) in Strategy Recommendations

Supporti ACLs: No

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.

Controllo degli accessi basato sugli attributi (ABAC) con raccomandazioni strategiche

Supporta ABAC (tag nelle politiche): No

Il controllo dell'accesso basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. Puoi allegare tag a entità IAM (utenti o ruoli) e a molte AWS risorse. L'assegnazione di tag alle entità e alle risorse è il primo passaggio di ABAC. In seguito, vengono progettate policy ABAC per consentire operazioni quando il tag dell'entità principale corrisponde al tag sulla risorsa a cui si sta provando ad accedere.

La strategia ABAC è utile in ambienti soggetti a una rapida crescita e aiuta in situazioni in cui la gestione delle policy diventa impegnativa.

Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'[elemento condizione](#) di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Yes (Sì). Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per ulteriori informazioni su ABAC, consulta [Definizione delle autorizzazioni con autorizzazione ABAC](#) nella Guida per l'utente IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta [Utilizzo del controllo degli accessi basato su attributi \(ABAC\)](#) nella Guida per l'utente di IAM.

Utilizzo di credenziali temporanee con consigli strategici

Supporta le credenziali temporanee: sì

Alcune Servizi AWS non funzionano quando si accede utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che Servizi AWS funzionano con credenziali temporanee, consulta la sezione relativa alla [Servizi AWS compatibilità con IAM nella IAM User Guide](#).

Stai utilizzando credenziali temporanee se accedi AWS Management Console utilizzando qualsiasi metodo tranne nome utente e password. Ad esempio, quando accedi AWS utilizzando il link Single Sign-On (SSO) della tua azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sullo scambio dei ruoli, consulta [Passaggio da un ruolo utente a un ruolo IAM \(console\)](#) nella Guida per l'utente IAM.

È possibile creare manualmente credenziali temporanee utilizzando l'API or. AWS CLI AWS È quindi possibile utilizzare tali credenziali temporanee per accedere. AWS AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta [Credenziali di sicurezza provvisorie in IAM](#).

Autorizzazioni principali per diversi servizi per Strategy Recommendations

Supporta l'inoltro delle sessioni di accesso (FAS): sì

Quando utilizzi un utente o un ruolo IAM 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 Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS 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 delle policy relative alle richieste FAS, consulta [Forward access sessions](#).

Ruoli di servizio per le raccomandazioni strategiche

Supporta i ruoli di servizio: no

Un ruolo di servizio è un [ruolo IAM](#) che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione [Create a role to delegate permissions to an Servizio AWS](#) nella Guida per l'utente IAM.

Warning

La modifica delle autorizzazioni per un ruolo di servizio potrebbe interrompere la funzionalità di Strategy Recommendations. Modifica i ruoli di servizio solo quando Strategy Recommendations fornisce indicazioni in tal senso.

Ruoli collegati ai servizi per Strategy Recommendations

Supporta ruoli collegati ai servizi: Sì

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 amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

Per informazioni dettagliate sulla creazione o la gestione dei ruoli collegati ai servizi di Strategy Recommendations, consulta [Utilizzo di ruoli collegati ai servizi per Strategy Recommendations](#)

AWS politiche gestite per le raccomandazioni strategiche di Migration Hub

Per aggiungere autorizzazioni a utenti, gruppi e ruoli, è più facile utilizzare le policy AWS gestite che scriverle da soli. Creare [policy gestite dal cliente IAM](#) per fornire al tuo team solo le autorizzazioni di cui ha bisogno richiede tempo e competenza. Per iniziare rapidamente, puoi utilizzare le nostre politiche AWS gestite. Queste policy coprono i casi d'uso comuni e sono disponibili nel tuo Account AWS. Per ulteriori informazioni sulle policy AWS gestite, consulta le [policy AWS gestite](#) nella IAM User Guide.

AWS i servizi mantengono e aggiornano le politiche AWS gestite. Non è possibile modificare le autorizzazioni nelle politiche AWS gestite. I servizi aggiungono occasionalmente autorizzazioni aggiuntive a una policy AWS gestita per supportare nuove funzionalità. Questo tipo di aggiornamento interessa tutte le identità (utenti, gruppi e ruoli) a cui è collegata la policy. È più probabile che i servizi aggiornino una politica AWS gestita quando viene lanciata una nuova funzionalità o quando diventano disponibili nuove operazioni. I servizi non rimuovono le autorizzazioni da una policy AWS gestita, quindi gli aggiornamenti delle policy non comprometteranno le autorizzazioni esistenti.

Inoltre, AWS supporta politiche gestite per le funzioni lavorative che si estendono su più servizi. Ad esempio, la policy `ReadOnlyAccess` AWS gestita fornisce l'accesso in sola lettura a tutti i AWS servizi e le risorse. Quando un servizio lancia una nuova funzionalità, AWS aggiunge autorizzazioni di sola lettura per nuove operazioni e risorse. Per l'elenco e la descrizione delle policy di funzione dei processi, consulta la sezione [Policy gestite da AWS per funzioni di processi](#) nella Guida per l'utente di IAM.

AWS politica gestita: `AWSMigrationHubStrategyConsoleFullAccess`

È possibile allegare la policy `AWSMigrationHubStrategyConsoleFullAccess` alle identità IAM.

La `AWSMigrationHubStrategyConsoleFullAccess` politica garantisce a un utente l'accesso completo al servizio Strategy Recommendations tramite AWS Management Console.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `discovery`— Concede all'utente l'accesso per ottenere il riepilogo delle scoperte in Application Discovery Service.
- `iam`— Consente la creazione di un ruolo collegato al servizio per l'utente, requisito necessario per l'utilizzo di Strategy Recommendations.
- `migrationhub-strategy`— Garantisce all'utente l'accesso completo a Strategy Recommendations.
- `s3`— Consente all'utente di creare e leggere dai bucket S3 utilizzati da Strategy Recommendations.
- `secretsmanager`— Consente all'utente di elencare gli accessi segreti nel Secrets Manager.

Per visualizzare le autorizzazioni relative a questa politica, vedere [AWSMigrationHubStrategyConsoleFullAccess](#) nella AWS Managed Policy Reference Guide.

AWS politica gestita: AWSMigration HubStrategyCollector

È possibile allegare la policy `AWSMigrationHubStrategyCollector` alle identità IAM.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `application-transformation`— Concede le autorizzazioni per caricare dati di log e metrici per le operazioni di trasformazione delle applicazioni e collabora con valutazioni e raccomandazioni sulla compatibilità del porting.
- `execute-api`— Consente all'utente di accedere ad Amazon API Gateway su cui caricare log e metriche. AWS
- `migrationhub-strategy`— Concede all'utente l'accesso per registrare messaggi, inviare messaggi, caricare dati di registro e caricare dati metrici su Strategy Recommendations.
- `s3`— Garantisce all'utente l'accesso ai bucket degli elenchi e alle relative posizioni. Agli utenti viene inoltre concesso l'accesso alla scrittura, al recupero di oggetti, all'aggiunta di oggetti, alla restituzione dell'elenco di controllo degli accessi (ACL) di, alla creazione, all'accesso, alla configurazione della crittografia, alla modifica della `PublicAccessBlock` configurazione, all'impostazione dello stato di controllo delle versioni e alla creazione o sostituzione di una configurazione del ciclo di vita per i bucket S3 utilizzati da Strategy Recommendations.
- `secretsmanager`— Consente all'utente di accedere ai segreti nel Secrets Manager utilizzati da Strategy Recommendations.

Per visualizzare le autorizzazioni relative a questa politica, vedere [AWSMigrationHubStrategyCollector](#) nella AWS Managed Policy Reference Guide.

Strategy Recommendations: aggiornamenti alle policy AWS gestite

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite per Strategy Recommendations da quando questo servizio ha iniziato a tenere traccia di queste modifiche. Per ricevere avvisi

automatici sulle modifiche a questa pagina, iscriviti al feed RSS nella pagina di cronologia del documento Strategy Recommendations.

Modifica	Descrizione	Data
<p>AWSMigrationHubStrategyCollector: aggiornamento a una policy esistente</p>	<p>Questa policy viene aggiornata per includere PutLogData , StartPort ingCompatibilityAssessment GetPortin gCompatibilityAssessment , StartPort ingRecommendationAssessment e le azioni di trasformazione delle GetPortingRecommendationAssessment applicazioni per consentire al servizio di trasformazione delle applicazioni di inviare log e metriche al servizio. I ListBucket e GetBucketLocation sono stati aggiunti per Amazon Simple Storage Service (Amazon S3) per supportare carichi di log e metriche. PutMetricData Sono stati inoltre aggiunti per consentire al raccoglitore Strategy Recommendations di inviare log e metriche all'endpoint del servizio. PutLogData</p>	<p>1 aprile 2024</p>
<p>AWSMigrationHubStrategyCollector: aggiornamento a una policy esistente</p>	<p>Questa politica viene aggiornata con le PutLogDat</p>	<p>5 febbraio 2024</p>

Modifica	Descrizione	Data
	<p>azioni <code>PutMetricData</code> e. Queste azioni garantiscono il caricamento di dati di log e metrici per le operazioni di trasformazione delle applicazioni. Questo aggiornamento aggiunge anche condizioni per garantire che l'autorizzazione all'uso del servizio e delle azioni Amazon Simple <code>aws:PrincipalAccountStorage</code> inclusi <code>aws:ResourceAccount</code> sia uguale all'autorizzazione all'uso del servizio e AWS Secrets Manager delle azioni Amazon Simple Storage inclusi.</p>	
<p>AWSMigrationHubStrategyCollector: aggiornamento a una policy esistente</p>	<p>Questa politica viene aggiornata con i seguenti Amazon S3 APIs <code>:CreateBucket</code>, <code>PutEncryptionConfiguration</code>, <code>PutBucketPublicAccessBlock</code>, <code>PutBucketPolicy</code>, <code>PutBucketVersioning</code>, e <code>PutLifecycleConfiguration</code>.</p>	<p>15 settembre 2023</p>
<p>AWSMigrationHubStrategyCollector: aggiornamento a una policy esistente</p>	<p>Questo aggiornamento delle policy concede autorizzazioni che consentono l'analisi del codice sorgente.</p>	<p>8 marzo 2023</p>

Modifica	Descrizione	Data
<p>AWSMigrationHubStrategyConsoleFullAccess: aggiornamento a una policy esistente</p>	<p>Questa politica viene aggiornata con tre AWS Application Discovery Service APIs : DescribeConfigurations DescribeTags , e. ListConfigurations</p>	<p>10 novembre 2022</p>
<p>AWSMigrationHubStrategyCollector: aggiornamento a una policy esistente</p>	<p>Questa politica viene aggiornata con l'UpdateCollectorConfiguration azione. Questa azione memorizza la configurazione del raccoglitore per un facile recupero.</p>	<p>07 settembre 2022</p>
<p>AWSMigrationHubStrategyConsoleFullAccess— Nuova politica resa disponibile al momento del lancio</p>	<p>AWSMigrationHubStrategyConsoleFullAccess garantisce a un utente l'accesso completo al servizio Strategy Recommendations tramite. AWS Management Console</p>	<p>25 ottobre 2021</p>

Modifica	Descrizione	Data
<p>AWSMigrationHubStrategyCollector— Nuova politica resa disponibile al momento del lancio</p>	<p>AWSMigrationHubStrategyCollector concede a un utente l'accesso al servizio Strategy Recommendations e l'accesso in lettura/scrittura ai bucket S3 correlati al servizio. Garantisce inoltre l'accesso ad Amazon API Gateway per caricare log e metriche e l'accesso a AWS Secrets Manager per recuperare le credenziali.</p>	<p>25 ottobre 2021</p>
<p>AWSMigrationHubStrategyServiceRolePolicy— Nuova policy resa disponibile al momento del lancio</p>	<p>La politica relativa AWSMigrationHubStrategyServiceRolePolicy ai ruoli collegati ai servizi fornisce l'accesso a AWS Migration Hub e AWS Application Discovery Service. Questa politica concede anche le autorizzazioni per l'archiviazione dei report in Amazon Simple Storage Service (Amazon S3).</p>	<p>25 ottobre 2021</p>
<p>Strategy Recommendations ha iniziato a tracciare</p>	<p>Strategy Recommendations ha iniziato a tenere traccia delle modifiche alle politiche AWS gestite.</p>	<p>25 ottobre 2021</p>

Esempi di policy basate sull'identità per le raccomandazioni strategiche di Migration Hub

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare risorse Strategy Recommendations. Inoltre, non possono eseguire attività utilizzando AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS l'API. Per concedere agli utenti l'autorizzazione a eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta [Creazione di policy IAM \(console\)](#) nella Guida per l'utente IAM.

Per i dettagli sulle azioni e sui tipi di risorse definiti da Strategy Recommendations, incluso il formato di ARNs per ogni tipo di risorsa, vedere [Actions, Resources and Condition Keys for Migration Hub Strategy Recommendations](#) nel Service Authorization Reference.

Argomenti

- [Best practice per le policy](#)
- [Utilizzo della console Strategy Recommendations](#)
- [Consentire agli utenti di visualizzare le loro autorizzazioni](#)
- [Accesso a un bucket Amazon S3](#)

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare le risorse di Strategy Recommendations 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 [Policy gestite da AWS](#) o [Policy gestite da AWS per le funzioni dei processi](#) nella Guida per l'utente IAM.

- Applica le autorizzazioni con privilegio minimo: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. È possibile 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 di IAM per applicare le autorizzazioni, consulta [Policy e autorizzazioni in IAM](#) nella Guida per l'utente IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse è possibile aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione [Elementi delle policy JSON di IAM: condizione](#) nella Guida per l'utente IAM.
- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta [Convalida delle policy per il Sistema di analisi degli accessi IAM](#) nella Guida per l'utente IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta [Protezione dell'accesso API con MFA](#) nella Guida per l'utente IAM.

Per maggiori informazioni sulle best practice in IAM, consulta [Best practice di sicurezza in IAM](#) nella Guida per l'utente di IAM.

Utilizzo della console Strategy Recommendations

Per accedere alla console Migration Hub Strategy Recommendations, è necessario disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle risorse Strategy Recommendations presenti nel tuo Account AWS. Se crei una policy basata sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Non è necessario consentire autorizzazioni minime per la console agli utenti che effettuano chiamate solo verso AWS CLI o l' AWS API. Al contrario, concedi l'accesso solo alle operazioni che corrispondono all'operazione API che stanno cercando di eseguire.

Per garantire che gli utenti e i ruoli possano ancora utilizzare la console Strategy Recommendations, collega anche la Strategy Recommendations ConsoleAccess o la policy ReadOnly AWS gestita alle entità. Per ulteriori informazioni, consulta [Aggiunta di autorizzazioni a un utente](#) nella Guida per l'utente IAM.

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono collegate alla relativa identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando l'API o a livello di codice. AWS CLI AWS

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

```
]
}
```

Accesso a un bucket Amazon S3

In questo esempio, vuoi concedere a un utente IAM l' Account AWS accesso a uno dei tuoi bucket Amazon S3, `amzn-s3-demo-bucket`. Si vuole anche consentire all'utente di aggiungere, aggiornare ed eliminare oggetti.

Oltre ad assegnare le autorizzazioni `s3:PutObject`, `s3:GetObject` e `s3:DeleteObject` all'utente, la policy assegna anche le autorizzazioni `s3:ListAllMyBuckets`, `s3:GetBucketLocation` e `s3:ListBucket`. Queste sono le autorizzazioni aggiuntive richieste dalla console. Inoltre, le operazioni `s3:PutObjectAcl` e `s3:GetObjectAcl` sono necessarie per essere in grado di copiare, tagliare e incollare gli oggetti nella console. Per un esempio di procedura dettagliata che concede le autorizzazioni agli utenti e li verifica utilizzando la console, consulta [Un esempio di procedura dettagliata: Using user policy to control access to your bucket.](#)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListBucketsInConsole",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets"
      ],
      "Resource": "arn:aws:s3::*:*"
    },
    {
      "Sid": "ViewSpecificBucketInfo",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
    },
    {
      "Sid": "ManageBucketContents",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
```

```
        "s3:PutObjectAcl",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:DeleteObject"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
}
]
```

Risoluzione dei problemi relativi a Migration Hub Strategy

Recommendations: identità e accesso

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi comuni che potresti riscontrare quando lavori con Strategy Recommendations e IAM.

Argomenti

- [Non sono autorizzato a eseguire un'azione in Strategy Recommendations](#)
- [Non sono autorizzato a eseguire iam: PassRole](#)
- [Desidero visualizzare le mie chiavi di accesso](#)
- [Sono un amministratore e desidero consentire ad altri di accedere a Strategy Recommendations](#)
- [Voglio consentire a persone esterne a me di accedere Account AWS alle mie risorse Strategy Recommendations](#)

Non sono autorizzato a eseguire un'azione in Strategy Recommendations

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.

L'errore di esempio seguente si verifica quando l'utente mateojackson IAM prova a utilizzare la console per visualizzare i dettagli relativi a una risorsa *my-example-widget* fittizia ma non dispone di autorizzazioni migrationhub-strategy:*GetWidget* fittizie.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
migrationhub-strategy:GetWidget on resource: my-example-widget
```

In questo caso, Mateo richiede al suo amministratore di aggiornare le policy per poter accedere alla risorsa *my-example-widget* utilizzando l'azione `migrationhub-strategy:GetWidget`.

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 assegnare un ruolo a Strategy Recommendations.

Alcuni Servizi AWS consentono di trasferire un ruolo esistente a quel servizio anziché 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.

L'errore di esempio seguente si verifica quando un utente IAM denominato `marymajor` tenta di utilizzare la console per eseguire un'azione in Strategy Recommendations. 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 colui che ti ha fornito le credenziali di accesso.

Desidero visualizzare le mie chiavi di accesso

Dopo aver creato le chiavi di accesso utente IAM, è possibile visualizzare il proprio ID chiave di accesso in qualsiasi momento. Tuttavia, non è possibile visualizzare nuovamente la chiave di accesso segreta. Se perdi la chiave segreta, dovrai creare una nuova coppia di chiavi di accesso.

Le chiavi di accesso sono composte da due parti: un ID chiave di accesso (ad esempio `AKIAIOSFODNN7EXAMPLE`) e una chiave di accesso segreta (ad esempio, `wJa1rXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY`). Come un nome utente e una password, è necessario utilizzare sia l'ID chiave di accesso sia la chiave di accesso segreta insieme per autenticare le richieste dell'utente. Gestisci le tue chiavi di accesso in modo sicuro mentre crei il nome utente e la password.

⚠ Important

Non fornire le chiavi di accesso a terze parti, neppure per aiutare a [trovare l'ID utente canonico](#). In questo modo, potresti concedere a qualcuno l'accesso permanente al tuo Account AWS.

Quando crei una coppia di chiavi di accesso, ti viene chiesto di salvare l'ID chiave di accesso e la chiave di accesso segreta in una posizione sicura. La chiave di accesso segreta è disponibile solo al momento della creazione. Se si perde la chiave di accesso segreta, è necessario aggiungere nuove chiavi di accesso all'utente IAM. È possibile avere massimo due chiavi di accesso. Se se ne hanno già due, è necessario eliminare una coppia di chiavi prima di crearne una nuova. Per visualizzare le istruzioni, consulta [Gestione delle chiavi di accesso](#) nella Guida per l'utente di IAM.

Sono un amministratore e desidero consentire ad altri di accedere a Strategy Recommendations

Per consentire ad altri di accedere a Strategy Recommendations, devi concedere l'autorizzazione alle persone o alle applicazioni che devono accedervi. Se si utilizza AWS IAM Identity Center per gestire persone e applicazioni, si assegnano set di autorizzazioni a utenti o gruppi per definirne il livello di accesso. I set di autorizzazioni creano e assegnano automaticamente le policy IAM ai ruoli IAM associati alla persona o all'applicazione. Per ulteriori informazioni, consulta [Set di autorizzazioni](#) nella Guida per l'AWS IAM Identity Center utente.

Se non utilizzi IAM Identity Center, devi creare entità IAM (utenti o ruoli) per le persone o le applicazioni che necessitano di accesso. È quindi necessario allegare una policy all'entità che concede loro le autorizzazioni corrette in Strategy Recommendations. Dopo aver concesso le autorizzazioni, fornisci le credenziali all'utente o allo sviluppatore dell'applicazione. Utilizzeranno tali credenziali per accedere. AWS Per ulteriori informazioni sulla creazione di utenti, gruppi, policy e autorizzazioni IAM, consulta [IAM Identities](#) and [Policies and permissions in IAM nella IAM User Guide](#).

Voglio consentire a persone esterne a me di accedere Account AWS alle mie risorse Strategy Recommendations

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 concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se Strategy Recommendations supporta queste funzionalità, consulta [Come funziona Migration Hub Strategy Recommendations con IAM](#)
- Per scoprire come fornire l'accesso alle tue risorse attraverso Account AWS le risorse di tua proprietà, consulta [Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà](#) nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta [Fornire l'accesso a soggetti Account AWS di proprietà di terze parti](#) nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta [Fornire l'accesso a utenti autenticati esternamente \(Federazione delle identità\)](#) nella Guida per l'utente IAM.
- Per informazioni sulle differenze di utilizzo tra ruoli e policy basate su risorse per l'accesso multi-account, consulta [Accesso a risorse multi-account in IAM](#) nella Guida per l'utente IAM.

Utilizzo di ruoli collegati ai servizi per Strategy Recommendations

Migration Hub Strategy Recommendations utilizza ruoli [collegati ai servizi AWS Identity and Access Management](#) (IAM). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM collegato direttamente a Strategy Recommendations. I ruoli collegati ai servizi sono predefiniti da Strategy Recommendations e includono tutte le autorizzazioni richieste dal servizio per chiamare altri servizi per tuo conto. AWS

Un ruolo collegato al servizio semplifica la configurazione di Strategy Recommendations perché non è necessario aggiungere manualmente le autorizzazioni necessarie. Strategy Recommendations definisce le autorizzazioni dei ruoli collegati ai servizi e, se non diversamente definito, solo Strategy Recommendations può assumerne i ruoli. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere collegata a nessun'altra entità IAM.

Per informazioni su altri servizi che supportano i ruoli collegati ai servizi, consulta [AWS Servizi che funzionano con IAM e cerca i servizi con](#) Sì nella colonna Service-Linked Role. Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Autorizzazioni di ruolo collegate ai servizi per Strategy Recommendations

Strategy Recommendations utilizza il ruolo collegato al servizio denominato

`AWSServiceRoleForMigrationHubStrategy` lo associa alla policy

`AWSMigrationHubStrategyServiceRolePolicyIAM`: fornisce l'accesso a e. AWS Migration Hub AWS Application Discovery Service Questa politica concede anche le autorizzazioni per l'archiviazione dei report in Amazon Simple Storage Service (Amazon S3).

Ai fini dell'assunzione del ruolo, il ruolo collegato ai servizi `AWSServiceRoleForMigrationHubStrategy` considera attendibili i seguenti servizi:

- `migrationhub-strategy.amazonaws.com`

La politica di autorizzazione dei ruoli consente a Strategy Recommendations di completare le seguenti azioni.

AWS Application Discovery Service azioni

`discovery:ListConfigurations`

`discovery:DescribeConfigurations`

AWS Migration Hub azioni

`mgh:GetHomeRegion`

Operazioni di Amazon S3

`s3:GetBucketAcl`

`s3:GetBucketLocation`

`s3:GetObject`

`s3:ListAllMyBuckets`

`s3:ListBucket`

`s3:PutObject`

`s3:PutObjectAcl`

Per visualizzare le autorizzazioni relative a questa politica, vedere [AWSMigrationHubStrategyServiceRolePolicy](#) nella AWS Managed Policy Reference Guide.

Per visualizzare la cronologia degli aggiornamenti di questa politica, vedere [Strategy Recommendations: aggiornamenti alle policy AWS gestite](#).

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta [Autorizzazioni del ruolo collegato ai servizi](#) nella Guida per l'utente di IAM.

Creazione di un ruolo collegato al servizio per Strategy Recommendations

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando accetti di consentire a Migration Hub di creare un ruolo collegato al servizio (SLR) nel tuo account in AWS Management Console, Strategy Recommendations crea il ruolo collegato al servizio per te.

Se elimini questo ruolo collegato ai servizi, è possibile ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando accetti di consentire a Migration Hub di creare un ruolo collegato al servizio (SLR) nel tuo account, Strategy Recommendations crea nuovamente il ruolo collegato al servizio per te.

Modifica di un ruolo collegato al servizio per Strategy Recommendations

Strategy Recommendations non consente di modificare il ruolo collegato al `AWSServiceRoleForMigrationHubStrategy` servizio. Dopo aver creato un ruolo collegato al servizio, non potrai modificarne il nome perché varie entità potrebbero farvi riferimento. Tuttavia, puoi modificare la descrizione del ruolo utilizzando la console Strategy Recommendations, la CLI o l'API.

Eliminazione di un ruolo collegato al servizio per Strategy Recommendations

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Utilizza la console IAM AWS CLI, l'AWS API per eliminare il ruolo collegato al `AWSServiceRoleForMigrationHubStrategy` servizio. Per ulteriori informazioni, consulta [Eliminazione del ruolo collegato ai servizi](#) nella Guida per l'utente di IAM.

Quando si eliminano le risorse Strategy Recommendations utilizzate dalla `AWSServiceRoleForMigrationHubStrategySLR`, non è possibile eseguire alcuna valutazione (attività per la generazione di consigli). Inoltre, non è possibile eseguire alcuna valutazione di base.

Se le valutazioni sono in esecuzione, l'eliminazione della SLR non riesce nella console IAM. Se l'eliminazione della SLR fallisce, puoi riprovare l'eliminazione dopo che tutte le attività in background sono state completate. Non è necessario pulire le risorse create prima di eliminare la reflex.

Regioni supportate per i ruoli collegati al servizio Strategy Recommendations

Strategy Recommendations supporta l'utilizzo di ruoli collegati ai servizi in tutte le regioni in cui il servizio è disponibile. Per ulteriori informazioni, consulta [Regioni ed endpoint di AWS](#).

Raccomandazioni sulla strategia di Migration Hub e endpoint VPC di interfaccia ()AWS PrivateLink

Puoi stabilire una connessione privata tra il tuo VPC e Migration Hub Strategy Recommendations creando un endpoint VPC di interfaccia. Endpoint di interfaccia con tecnologia AWS PrivateLink. Con AWS PrivateLink, puoi accedere in modo privato alle operazioni dell'API Strategy Recommendations senza un gateway Internet, un dispositivo NAT, una connessione VPN o una connessione. AWS Direct Connect Le istanze nel tuo VPC non necessitano di indirizzi IP pubblici per comunicare con le operazioni dell'API Strategy Recommendations. Il traffico tra il tuo VPC e Strategy Recommendations rimane all'interno della rete Amazon.

Ogni endpoint dell'interfaccia è rappresentato da una o più [interfacce di rete elastiche](#) nelle sottoreti.

Per ulteriori informazioni, consultare [Endpoint VPC di interfaccia \(AWS PrivateLink\)](#) nella Guida per l'utente di Amazon VPC.

Considerazioni sulle raccomandazioni strategiche (endpoint VPC)

[Prima di configurare un endpoint VPC di interfaccia per Strategy Recommendations, assicurati di esaminare le proprietà, le limitazioni e AWS PrivateLink le quote degli endpoint dell'interfaccia nella Amazon VPC User Guide.](#)

Strategy Recommendations supporta le chiamate a tutte le sue azioni API dal tuo VPC. Per utilizzare tutti gli Strategy Recommendations, devi creare un endpoint VPC.

Creazione di un endpoint VPC di interfaccia per consigli strategici

Puoi creare un endpoint VPC per Strategy Recommendations utilizzando la console Amazon VPC o il (). AWS Command Line Interface AWS CLI Per ulteriori informazioni, consulta [Creazione di un endpoint dell'interfaccia](#) nella Guida per l'utente di Amazon VPC.

Crea un endpoint VPC per Strategy Recommendations utilizzando il seguente nome di servizio:

- `com.amazonaws.region.migrationhub-strategy`

Se utilizzi un DNS privato per l'endpoint, puoi effettuare richieste API a Strategy Recommendations utilizzando il nome DNS predefinito per la regione. Ad esempio, puoi usare il nome `migrationhub-strategy.us-east-1.amazonaws.com`

Per ulteriori informazioni, consulta [Accesso a un servizio tramite un endpoint dell'interfaccia](#) in Guida per l'utente di Amazon VPC.

Creazione di una policy sugli endpoint VPC per consigli strategici

Puoi allegare una policy per gli endpoint all'endpoint VPC che controlla l'accesso a Strategy Recommendations. La policy specifica le informazioni riportate di seguito:

- Il principale che può eseguire operazioni.
- Le azioni che possono essere eseguite.
- Le risorse su cui è possibile eseguire queste azioni.

Per ulteriori informazioni, consulta [Controllo degli accessi ai servizi con endpoint VPC](#) nella Guida per l'utente di Amazon VPC.

Esempio: policy degli endpoint VPC per le azioni Strategy Recommendations

Di seguito è riportato un esempio di politica degli endpoint per Strategy Recommendations. Se associata a un endpoint, questa policy consente l'accesso alle azioni elencate in formato Strategy Recommendations a tutti i responsabili su tutte le risorse.

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "migrationhub-strategy:ListContacts",
      ],
      "Resource": "*"
    }
  ]
}
```

```
]
}
```

Convalida della conformità per le raccomandazioni strategiche di Migration Hub

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:

- [Governance e conformità per la sicurezza](#): queste guide all'implementazione di soluzioni illustrano considerazioni relative all'architettura e i passaggi per implementare le funzionalità di sicurezza e conformità.
- [Riferimenti sui servizi conformi ai requisiti HIPAA](#): elenca i servizi HIPAA idonei. Non tutti Servizi AWS sono idonei alla normativa HIPAA.
- [AWS Risorse per la conformità](#): questa raccolta di cartelle di lavoro e guide potrebbe essere valida per 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)).
- [Valutazione delle risorse con regole](#) nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida e alle normative del settore.
- [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, come lo standard 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 l'AWS utilizzo per semplificare la gestione del rischio e la conformità alle normative e agli standard di settore.

Utilizzo di altri servizi

Questa sezione descrive altri AWS servizi che interagiscono con i consigli strategici di Migration Hub.

Argomenti

- [Registrazione delle chiamate API Strategy Recommendations con AWS CloudTrail](#)

Registrazione delle chiamate API Strategy Recommendations con AWS CloudTrail

Migration Hub Strategy Recommendations è integrato con AWS CloudTrail un servizio che fornisce un registro delle azioni intraprese da un utente, ruolo o AWS servizio in Strategy Recommendations. CloudTrail acquisisce le chiamate API per Strategy Recommendations come eventi. Le chiamate acquisite includono chiamate dalla console Strategy Recommendations e chiamate in codice alle operazioni dell'API Strategy Recommendations.

Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per Strategy Recommendations. Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni raccolte da CloudTrail, è possibile determinare la richiesta effettuata a Strategy Recommendations, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e ulteriori dettagli.

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

Informazioni sulle raccomandazioni strategiche in CloudTrail

CloudTrail è abilitato sul tuo Account AWS quando crei l'account. Quando si verifica un'attività in Strategy Recommendations, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi di AWS servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare gli eventi recenti in Account AWS. Per ulteriori informazioni, vedere [Visualizzazione degli eventi con la cronologia degli CloudTrail eventi](#).

Per una registrazione continua degli eventi del tuo Account AWS, compresi gli eventi per Strategy Recommendations, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un percorso nella console, questo sarà

valido in tutte le Regioni AWS. Il trail registra gli eventi di 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, consulta gli argomenti seguenti:

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

Strategy Recommendations supporta la registrazione delle seguenti azioni come eventi nei file di CloudTrail registro:

- [GetApplicationComponentStrategies](#)
- [GetApplicationComponentDetails](#)
- [GetAssesment](#)
- [GetImportFileTask](#)
- [GetPortfolioPreferences](#)
- [GetPortfolioSummary](#)
- [GetServerDetails](#)
- [GetServerStrategies](#)
- [ListApplicationComponents](#)
- [ListCollectors](#)
- [ListImportFileTask](#)
- [ListServers](#)
- [PutPortfolioPreferences](#)
- [StartAssessment](#)
- [StartImportFileTask](#)
- [StopAssessment](#)
- [UpdateApplicationComponetConfig](#)
- [UpdateServerConfig](#)

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 utente root o AWS Identity and Access Management (IAM)
- 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, consulta [Elemento CloudTrail userIdentity](#).

Comprensione delle voci dei file di registro di Strategy

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 chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'[GetServerDetails](#)azione.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "777777777777",
    "arn": "arn:aws:sts::111122223333:assumed-role/myUserName/...",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "777777777777",
        "arn": "arn:aws:iam::111122223333:role/myUserName",
        "accountId": "111122223333",
        "userName": "myUserName"
      },
      "webIdFederationData": {},
      "attributes": {
```

```
        "creationDate": "2021-09-20T01:07:16Z",
        "mfaAuthenticated": "false"
    }
},
"eventTime": "2021-09-20T01:07:43Z",
"eventSource": "migrationhub-strategy.amazonaws.com",
"eventName": "GetServerDetails",
"awsRegion": "us-west-2",
"sourceIPAddress": "",
"userAgent": "",
"requestParameters": {
    "serverId": "ads-server-006"
},
"responseElements": null,
"requestID": "07D681279BD94AED",
"eventID": "cdc4b7ed-e171-4cef-975a-ad829d4123e8",
"readOnly": true,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "111122223333",
"eventCategory": "Management"
}
```

Raccomandazioni sulla strategia Quotas for Migration Hub

Il tuo AWS account ha delle quote predefinite, precedentemente denominate limiti, per ogni servizio. AWS Salvo diversa indicazione, ogni quota si applica a una regione specifica. Se per alcune quote è possibile richiedere aumenti, altre quote non possono essere modificate.

Per visualizzare un elenco delle quote per i consigli strategici di Migration Hub, vedi [Quote del servizio Strategy Recommendations](#).

Puoi anche visualizzare le quote per Strategy Recommendations aprendo la console [Service Quotas](#). Nel riquadro di navigazione, scegli AWS servizi e seleziona Migration Hub Strategy Recommendations.

Per richiedere un aumento delle quote, consultare [Richiesta di aumento delle quote](#) nella Guida per l'utente di Service Quotas. Se la quota non è ancora disponibile in Service Quotas, utilizza il [modulo di incremento dei limiti](#).

Note di rilascio

Argomenti

- [17 novembre 2023](#)
- [12 ottobre 2023](#)
- [17 aprile 2023](#)
- [17 marzo 2023](#)
- [07 novembre 2022](#)
- [27 settembre 2022](#)
- [30 giugno 2022](#)
- [18 aprile 2022](#)
- [25 febbraio 2022](#)
- [10 febbraio 2022](#)
- [28 gennaio 2022](#)
- [14 gennaio 2022](#)
- [21 dicembre 2021](#)
- [15 dicembre 2021](#)
- [25 ottobre 2021](#)

17 novembre 2023

Nuove funzionalità

- Collezionista v1.1.47
- Support per applicazioni.NET 8.

12 ottobre 2023

Nuove funzionalità

- Collector v1.1.45
- Support per più fonti di dati.

17 aprile 2023

Nuove funzionalità

- Collector v1.1.22
- Miglioramenti degli script di aggiornamento. Ciò richiede la versione più recente di Collector.

17 marzo 2023

Nuova caratteristica

È stata aggiunta l'analisi binaria, che fornisce il rilevamento di anti-pattern e incompatibilità senza codice sorgente.

07 novembre 2022

Nuova caratteristica

- Filtraggio delle applicazioni per le applicazioni
- Filtraggio dei server per tag AWS Application Discovery Service

27 settembre 2022

Nuova caratteristica

- Collector v1.1.12
 - SCT versione 667
 - EMPAnalyzer 2.2.0.368
- Aggiunti `diag check` comandi per Server Insights.
- È stato aggiunto il supporto per i potenziali consigli.
- Interfaccia utente migliorata per verificare lo stato della configurazione e della valutazione.

Correzioni di bug

- Porting Assistant Translator e altre correzioni.

30 giugno 2022

Nuova caratteristica

- Collector v1.1.11
 - Aggiunto il supporto API. VMware
 - A2C ha richiesto modifiche per aggiungere l'intestazione utente durante il download del file binario.
 - Sono stati aggiunti il percorso home di Linux, la shell predefinita e la terminazione remota di tutte le shell.
- Binario pubblico A2C v1.17
 - È stato aggiunto il supporto per Azure DevOps come obiettivo di distribuzione della pipeline.

18 aprile 2022

Nuova caratteristica

- Collector v1.1.7
- È stata aggiunta la possibilità di scaricare dinamicamente il binario A2C dall'URL pubblico.

Correzioni di bug

- A2C v1.1.5

25 febbraio 2022

Correzioni di bug

- SCT v5.6.9
- A2C v1.1.2
- Collettore v1.1.4

10 febbraio 2022

Correzioni di bug

- SCT v5.6.8
- A2C versione 1.1.1
 - Aggiunto un controllo per il comando su Linux. tar
 - È stato risolto il problema del controllo delle immagini delle applicazioni in Amazon ECR.
 - È stato risolto il problema che richiedeva la rimozione del contenitore per la preconvalida.
- Collector v1.1.3
 - Risolto l'errore 4xx per un computer remoto a 32 bit.
 - Aggiornati i codici di errore A2C.
 - Ha convalidato l'indirizzo IP C# per l'analisi del codice sorgente del computer remoto.

28 gennaio 2022

Nuova caratteristica

- Collector v1.1.2
- È stato aggiunto il supporto del DevOps repository Azure Git per l'analisi del codice sorgente.

14 gennaio 2022

Nuova caratteristica

- Collector v1.1.1
- Aggiunti consigli Babelfish per i database SQL.

21 dicembre 2021

Problema risolto

- Collector v1.1.0
- L'analisi del database è stata ripristinata.

15 dicembre 2021

Problema noto

- Collector v1.0.4
- L'analisi del database non è attualmente supportata (CVE-2021-44228).

25 ottobre 2021

Nuova caratteristica

- Collector v1.0.0
- Versione iniziale della Guida per l'utente di Migration Hub Strategy Recommendations.

Cronologia dei documenti e delle versioni

La tabella seguente descrive le versioni della documentazione per Strategy Recommendations. Per ulteriori informazioni, consulta [Note di rilascio](#).

Modifica	Descrizione	Data
AWS aggiornamenti delle politiche gestiti: aggiornamento a AWSMigrationHubStrategyCollector	La AWSMigrationHubStrategyCollector politica è stata aggiornata per includere nuove s3 migration hub-strategy azioni e. application-transformation	1 aprile 2024
AWS aggiornamenti delle politiche gestiti: aggiornamento a AWSMigrationHubStrategyCollector	È stata aggiornata la AWSMigrationHubStrategyCollector politica per includere nuove application-transformation azioni. Questo aggiornamento aggiunge anche condizioni per limitare varie azioni che aws:ResourceAccount devono essere uguali aaws:PrincipalAccount .	5 febbraio 2024
Nuova caratteristica	Il client di raccolta dati delle applicazioni Strategy Recommendations v1.1.47 è disponibile con supporto per le applicazioni.NET 8.	17 novembre 2023
Nuova caratteristica	Il client di raccolta dati applicativo Strategy Recommendations v1.1.45 è	12 ottobre 2023

	disponibile con supporto per più fonti di dati.	
AWS aggiornamenti delle politiche gestiti: aggiornamento a AWSMigrationHubStrategyCollector	La AWSMigrationHubStrategyCollector policy è stata aggiornata per includere il nuovo Amazon S3 APIs.	15 settembre 2023
AWS aggiornamenti delle politiche gestiti: aggiornamento a AWSMigrationHubStrategyCollector	È stata aggiornata la AWSMigrationHubStrategyCollector politica per includere nuovi analizzatori per il codice sorgente.	8 marzo 2023
Aggiornamenti delle best practice di IAM	Per ulteriori informazioni, consulta Best practice per la sicurezza in IAM.	25 febbraio 2023
AWS aggiornamenti gestiti delle politiche: aggiornamento a una politica esistente	Migration Hub Strategy Recommendations ne AWS Application Discovery Service APIs ha aggiunti tre a una policy esistente.	10 novembre 2022
Aggiornamenti di sicurezza	Stabilisci una connessione privata con l'interfaccia VPC endpoint.	07 marzo 2022
Nuova caratteristica	È stato aggiunto il supporto del DevOps repository Azure Git per l'analisi del codice sorgente.	28 gennaio 2022
Nuova caratteristica	Aggiunti consigli Babelfish per i database SQL.	14 gennaio 2022
Rilascio iniziale	Versione iniziale della Guida per l'utente di Migration Hub Strategy Recommendations.	25 ottobre 2021

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.