



Guida per l'utente

AWS Servizio Application Discovery



AWS Servizio Application Discovery: Guida per l'utente

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

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

Table of Contents

Cos'è AWS Application Discovery Service?	1
Individuazione VMware	2
Individuazione del database	3
Confronta Agentless Collector e Discovery Agent	3
Presupposti	4
Configurazione	6
Iscriviti ad Amazon Web Services	6
Crea utenti IAM	6
Creazione di un utente amministrativo IAM	7
Creazione di un utente IAM non amministrativo	7
Accedi a Migration Hub e scegli una regione d'origine	8
Agente Discovery	9
Prerequisiti	10
Installazione del su Linux	12
Requisiti per le piattaforme Linux precedenti	15
Gestisci il processo di Discovery Agent su Linux	16
Disinstallare un agente	17
Risoluzione dei problemi di Linux Discovery Agent	18
Installazione di su Windows	19
Firma dei pacchetti e aggiornamenti automatici	23
Gestisci il processo di Discovery Agent in Windows	23
Risoluzione dei problemi in Windows	25
Dati raccolti	26
Avvia o interrompi la raccolta dei dati	29
Agentless Collector	31
Nozioni di base	32
Prerequisiti	32
Fase 1: Creare un utente IAM	34
Passaggio 2: scarica il raccogliatore	37
Fase 3: Implementare il raccogliatore	37
Fase 4: Accedere alla console Collector	39
Fase 5: Configurare il raccogliatore	39
Fase 6: Configurare i moduli di raccolta dati	46
Fase 7: Visualizzazione dei dati raccolti	61

Dati raccolti	61
Dati raccolti dal modulo VMware	62
Dati raccolti dal database e dal modulo di analisi	66
Utilizzo della console	67
Prestazioni della raccolta	68
Modifica le impostazioni del raccoglitore	70
Modifica delle credenziali vCenter	71
Aggiornamenti	72
Risoluzione dei problemi	73
Fixing Agentless Collector non AWS riesce a raggiungerlo durante la configurazione	74
Risoluzione dei problemi di certificazione autofirmata durante la connessione all'host proxy	75
Trovare collezionisti malsani	76
Risoluzione dei problemi relativi all'indirizzo IP	77
Risoluzione dei problemi relativi alle credenziali vCenter	78
Risoluzione dei problemi di inoltro dei dati	78
Risoluzione dei problemi di connessione	79
Supporto per host ESX autonomi	81
Contattare AWS Support	81
Importa	82
Campi di file di importazione supportati	82
Impostazione delle autorizzazioni di importazione	88
Caricamento del file di importazione in Amazon S3	91
Importazione di dati	92
Tracciamento delle richieste di importazione dell'Migration Hub	94
Visualizza, esporta ed esplora i dati	97
Visualizzazione dati di log	97
Logica di log	98
Esportazione dei dati raccolti	99
Esplorazione dei dati in Athena	101
Abilitare l'esplorazione dei dati in Amazon Athena	102
Lavorare con l'esplorazione dei dati in Amazon Athena	103
Procedure guidate console	114
Pannello di controllo principale	114
Pannello di controllo principale	114
Strumenti di raccolta dei dati	115

Avvio e arresto dei raccoglitori di dati	115
Visualizzazione e ordinamento dei raccoglitori di dati	116
Visualizza, esporta ed esplora i dati	119
Visualizzazione e ordinamento dei server	120
Server di tagging	121
Esportazione dei dati del server	122
L'esplorazione dei dati in Athena	124
Applicazioni	124
Utilizzo dell'API per interrogare gli elementi scoperti	126
Utilizzo dell'DescribeConfigurationsazione	126
Utilizzo dell'azione ListConfigurations	130
Consistenza finale	146
Sicurezza	147
Identity and Access Management	148
Destinatari	148
Autenticazione con identità	149
Gestione dell'accesso tramite policy	152
Come AWS Application Discovery Service funziona con IAM	155
AWS politiche gestite	157
Esempi di policy basate su identità	162
Comprendere e utilizzare i ruoli collegati ai servizi	170
Risoluzione dei problemi relativi a IAM	177
Registrazione e monitoraggio in AWS Application Discovery Service	178
Registrazione delle chiamate API di Application Discovery Service conAWS CloudTrail	178
Quote	182
Risoluzione dei problemi	183
Interrompi la raccolta dei dati mediante l'esplorazione dei dati	183
Rimuovi i dati raccolti dall'esplorazione dei dati	184
Risolvi i problemi più comuni relativi all'esplorazione dei dati in Amazon Athena	186
L'esplorazione dei dati in Amazon Athena non viene avviata perché non è possibile creare ruoli collegati ai servizi e risorse richieste AWS	186
I dati dei nuovi agenti non vengono visualizzati in Amazon Athena	186
Non disponi di autorizzazioni sufficienti per accedere ad Amazon S3, Amazon Data Firehose o AWS Glue	188
Risoluzione dei record di importazione non riusciti	188
Cronologia dei documenti	191

Glossario per AWS	195
Appendice	196
.....	196
Appendice: Discovery Connector	196
Dati raccolti da Discovery Connector	197
Raccolta di dati sui connettori	201
Risoluzione dei problemi del Discovery Connector	203
.....	ccviii

Cos'è AWS Application Discovery Service?

AWS Application Discovery Service aiuta a pianificare la migrazione al AWS cloud raccogliendo dati di utilizzo e configurazione relativi ai server e database locali. Application Discovery Service è integrato con AWS Migration Hub, AWS Database Migration Service e Fleet Advisor. Migration Hub semplifica il monitoraggio della migrazione in quanto aggrega le informazioni sullo stato della migrazione in un'unica console. Puoi visualizzare i server rilevati, raggrupparli in applicazioni e quindi tenere traccia dello stato della migrazione di ciascuna applicazione dalla console Migration Hub nella tua regione di residenza. È possibile utilizzare DMS Fleet Advisor per valutare le opzioni di migrazione per i carichi di lavoro del database.

Tutti i dati rilevati vengono archiviati nella tua regione di AWS Migration Hub residenza. Pertanto, è necessario impostare la propria regione di residenza nella console di Migration Hub o con i comandi CLI prima di eseguire qualsiasi attività di rilevamento e migrazione. I tuoi dati possono essere esportati per l'analisi in Microsoft Excel o in strumenti di AWS analisi come Amazon Athena e Amazon QuickSight.

Utilizzando le API Application Discovery Service, è possibile esportare i dati sulle prestazioni e sull'utilizzo del sistema per i server rilevati. Inserisci questi dati nel tuo modello di costo per calcolare il costo di gestione di quei server AWS. Inoltre, puoi esportare i dati sulle connessioni di rete esistenti tra i server. Queste informazioni ti consentono di determinare le dipendenze di rete tra i server e raggrupparle in applicazioni per la pianificazione della migrazione.

Note

La tua regione di residenza deve essere impostata AWS Migration Hub prima di iniziare il processo di scoperta, perché i tuoi dati verranno archiviati nella tua regione di origine. Per ulteriori informazioni su come lavorare con una regione di residenza, vedi [Regione d'origine](#).

Application Discovery Service offre due modi per eseguire l'individuazione e la raccolta di dati sui server locali:

- Il rilevamento senza agenti può essere eseguito implementando Application Discovery Service Agentless Collector (Agentless Collector) (file OVA) tramite VMware vCenter. Una volta configurato, Agentless Collector identifica le macchine virtuali (VM) e gli host associati a vCenter. Agentless Collector raccoglie i seguenti dati di configurazione statici: nomi host del server, indirizzi

IP, indirizzi MAC, allocazioni di risorse del disco, versioni del motore di database e schemi di database. Inoltre, raccoglie i dati di utilizzo per ogni VM e database fornendo l'utilizzo medio e massimo per metriche come CPU, RAM e I/O del disco.

- L'individuazione basata su agenti può essere eseguita implementando l'AWSApplication Discovery Agent su ciascuna delle macchine virtuali e dei server fisici. Il programma di installazione dell'agente è disponibile per i sistemi operativi Windows e Linux. Vengono raccolti dati di configurazione statici, informazioni dettagliate sulle prestazioni di sistema delle serie temporali, connessioni di rete in entrata e in uscita e processi in esecuzione.

Application Discovery Service si integra con le soluzioni di scoperta delle applicazioni deiAWS partner Partner Network (APN). Queste soluzioni di terze parti possono aiutarti a importare dettagli sul tuo ambiente locale direttamente in Migration Hub, senza utilizzare alcun raccogliatore o agente di rilevamento senza agenti. Gli strumenti di individuazione delle applicazioni di terze parti possono interrogareAWS Application Discovery Service e possono scrivere nel database di Application Discovery Service utilizzando l'API pubblica. In questo modo, è possibile importare i dati in Migration Hub e visualizzarli, in modo da poter associare le applicazioni ai server e monitorare le migrazioni.

Individuazione VMware

Se si dispone di macchine virtuali (VM) in esecuzione nell'ambiente VMware vCenter, è possibile utilizzare Agentless Collector per raccogliere informazioni di sistema senza dover installare un agente su ciascuna macchina virtuale. Al contrario, puoi caricare questa appliance locale in vCenter e lasciare che rilevi tutti gli host e le macchine virtuali.

Agentless Collector acquisisce informazioni sulle prestazioni del sistema e sull'utilizzo delle risorse per ogni VM in esecuzione nel vCenter, indipendentemente dal sistema operativo in uso. Poiché, tuttavia, non può "scrutare" all'interno di ogni singola macchina virtuale, non è in grado di capire quali processi sono in esecuzione su ogni macchina virtuale né quali sono le connessioni di rete esistenti. Pertanto, se hai bisogno di questo livello di dettaglio e desideri esaminare più da vicino alcune delle tue VM esistenti per aiutarti a pianificare la migrazione, puoi installare Discovery Agent in base alle necessità.

Inoltre, per le macchine virtuali ospitate su VMware, è possibile utilizzare sia Agentless Collector che Discovery Agent per eseguire il rilevamento contemporaneamente. Per informazioni dettagliate sui tipi di dati esatti che verranno raccolti da ogni strumento di rilevamento, consulta [Dati raccolti da Agentless Collector](#) e [Dati raccolti da Discovery Agent](#).

Individuazione del database

Se disponi di server di database e analisi nel tuo ambiente locale, puoi utilizzare Agentless Collector per individuare e inventariare questi server. È quindi possibile raccogliere le metriche delle prestazioni per ogni server di database senza la necessità di installare Agentless Collector su ogni computer del proprio ambiente.

Il modulo di raccolta dati di analisi e database Agentless Collector acquisisce metadati e metriche prestazionali che forniscono informazioni sull'infrastruttura dei dati. Il modulo di raccolta dei dati di database e analisi utilizza LDAP in Microsoft Active Directory per raccogliere informazioni sul sistema operativo, sul database e sui server di analisi della rete. Quindi, il modulo di raccolta dati esegue periodicamente interrogazioni per raccogliere le metriche di utilizzo effettivo della CPU, della memoria e della capacità del disco per i database e i server di analisi. Per i dettagli relativi alle metriche raccolte, consulta [Dati raccolti dal database e dal modulo di analisi](#).

Dopo che Agentless Collector ha completato la raccolta dei dati dal tuo ambiente, puoi utilizzare laAWS DMS console per ulteriori analisi e pianificare la migrazione. Ad esempio, per scegliere un obiettivo di migrazione ottimale inCloud AWS, è possibile generare consigli sugli obiettivi per i database di origine. Per ulteriori informazioni, consulta [Modulo di raccolta dati di analisi e database](#).

Confronta Agentless Collector e Discovery Agent

La tabella seguente fornisce un rapido confronto tra gli strumenti di raccolta dati di Application Discovery Service.

	Agentless	Discovery
Supported server types		
Macchina virtuale VMware	Si	Si
Server fisico	No	Si
Deployment		
Per server	No	Si
Per vCenter	Si	No

	Agentless	Discovery
Collected data		
Dati statici di configurazione del server	Yes	Yes
Dati di configurazione del database	Yes	No
Parametri di utilizzo macchina virtuale	Yes	No
Metriche di utilizzo del database	Yes	No
Informazioni sulle prestazioni delle serie temporali	No	Yes (Export only)
Connessioni di rete in entrata/in uscita	No	Yes (Export only)
Processi in esecuzione	No	Yes (Export only)
Sistema operativo supportato	Any OS running in VMware vCenter V5.5+	Per l'elenco dei sistemi operativi Linux e Windows supportati, vedere Prerequisiti per Discovery Agent .
Database supportati	Oracle, SQL Server, MySQL, and PostgreSQL	Nessuno

Presupposti

Per utilizzare Application Discovery Service, si presuppone quanto segue:

- Ti sei registrato a AWS. Per ulteriori informazioni, consulta [Configurazione di Application Discovery Service](#).

- Hai selezionato una regione di origine Migration Hub. Per ulteriori informazioni, consulta [la documentazione relativa alle regioni di residenza](#).

Ecco cosa aspettarsi:

- La regione principale di Migration Hub è l'unica regione in cui Application Discovery Service archivia i dati di scoperta e pianificazione.
- Gli agenti, i connettori e le importazioni di Discovery possono essere utilizzati solo nella regione di origine di Migration Hub selezionata.
- Per un elenco delleAWS regioni in cui è possibile utilizzare Application Discovery Service, vedere il [Riferimenti generali di Amazon Web Services](#).

Configurazione di Application Discovery Service

Prima di utilizzarlo AWS Application Discovery Service per la prima volta, completate le seguenti attività:

[Iscriviti ad Amazon Web Services](#)

[Crea utenti IAM](#)

[Accedi alla console Migration Hub e scegli una regione d'origine](#)

Iscriviti ad Amazon Web Services

Se non ne possiedi uno Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti a un Account AWS

1. Apri la pagina all'indirizzo <https://portal.aws.amazon.com/billing/signup>.
2. Segui le istruzioni online.

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

Quando ti iscrivi a un Account AWS, 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 procedura consigliata in materia di sicurezza, assegna l'accesso amministrativo a un utente e utilizza solo l'utente root per eseguire [attività che richiedono l'accesso da parte dell'utente root](#).

Crea utenti IAM

Quando crei un AWS account, ottieni un'identità di accesso singolo con accesso completo a tutti i AWS servizi e le risorse dell'account. Questa identità è denominata utente root dell' AWS account. L'accesso AWS Management Console utilizzando l'indirizzo e-mail e la password utilizzati per creare l'account consente l'accesso completo a tutte le AWS risorse dell'account.

Ti consigliamo vivamente di non utilizzare l'utente root per le attività quotidiane, nemmeno quelle amministrative. Segui invece le best practice di sicurezza [Create Individual IAM Users](#) e crea un utente amministratore AWS Identity and Access Management (IAM). Quindi conservare al sicuro le

credenziali dell'utente root e utilizzarle per eseguire solo alcune attività di gestione dell'account e del servizio.

Oltre a creare un utente amministrativo, dovrai creare anche utenti IAM non amministrativi. I seguenti argomenti spiegano come creare entrambi i tipi di utenti IAM.

Argomenti

- [Creazione di un utente amministrativo IAM](#)
- [Creazione di un utente IAM non amministrativo](#)

Creazione di un utente amministrativo IAM

Per impostazione predefinita, un account amministratore eredita tutte le policy necessarie per accedere ad Application Discovery Service.

Per creare utente amministratore

- Crea un utente amministratore nel tuo AWS account. Per istruzioni, consulta [Creating Your First IAM User and Administrators Group](#) (Creazione del primo utente e del primo gruppo di amministratori IAM) nella IAM User Guide (Guida per l'utente di IAM).

Creazione di un utente IAM non amministrativo

Quando crei utenti IAM non amministrativi, segui le best practice di sicurezza Grant Least [Privilege, che concede agli utenti autorizzazioni minime](#).

Utilizza le policy gestite da IAM per definire il livello di accesso ad Application Discovery Service da parte degli utenti IAM non amministrativi. Per informazioni sulle policy gestite di Application Discovery Service, vedere [AWS politiche gestite per AWS Application Discovery Service](#).

Per creare un utente IAM non amministratore

1. In AWS Management Console, accedi alla console IAM.
2. Crea un utente IAM non amministratore seguendo le istruzioni per creare un utente con la console, come descritto nella sezione [Creazione di un utente IAM nel tuo AWS account](#) nella Guida per l'utente IAM.

Seguendo le istruzioni contenute nella Guida per l'utente IAM:

- Nella fase di selezione del tipo di accesso, seleziona Accesso programmatico. Nota, sebbene non sia consigliato, seleziona l'accesso alla console di AWS gestione solo se prevedi di utilizzare le stesse credenziali utente IAM per accedere alla AWS console.
- Nella fase relativa alla pagina Imposta autorizzazione, scegli l'opzione Allega le politiche esistenti direttamente all'utente. Quindi seleziona una policy IAM gestita per Application Discovery Service dall'elenco delle policy. Per informazioni sulle policy gestite di Application Discovery Service, vedere [AWS politiche gestite per AWS Application Discovery Service](#).
- Durante la fase di visualizzazione delle chiavi di accesso dell'utente (ID delle chiavi di accesso e chiavi di accesso segrete), segui le indicazioni contenute nella Nota importante sul salvataggio del nuovo ID della chiave di accesso e della chiave di accesso segreta dell'utente in un luogo sicuro e protetto.

Accedi alla console Migration Hub e scegli una regione d'origine

Devi scegliere una regione AWS Migration Hub d'origine nell' AWS account che stai utilizzando per AWS Application Discovery Service.

Per scegliere la regione d'origine

1. Utilizzando il tuo AWS account, accedi AWS Management Console e apri la console Migration Hub all'[indirizzo https://console.aws.amazon.com/migrationhub/](https://console.aws.amazon.com/migrationhub/).
2. Nel pannello di navigazione della console Migration Hub, scegli Impostazioni, quindi scegli una regione di origine.

I dati del Migration Hub vengono archiviati nella regione di origine per scopi di individuazione, pianificazione e monitoraggio della migrazione. Per ulteriori informazioni, consulta [The Migration Hub Home Region](#).

AWS Agente di individuazione delle applicazioni

AWS Application Discovery Agent (Discovery Agent) è un software che si installa su server e macchine virtuali locali destinati al rilevamento e alla migrazione. Gli agenti acquisiscono la configurazione di sistema, le prestazioni di sistema, i processi in esecuzione e i dettagli delle connessioni di rete tra i sistemi. Gli agenti supportano la maggior parte dei sistemi operativi Linux e Windows e puoi distribuirli su server fisici locali, istanze Amazon EC2 e macchine virtuali.

Note

Prima di distribuire Discovery Agent, è necessario scegliere una [regione principale di Migration Hub](#). È necessario registrare l'agente nella regione di origine.

Discovery Agent viene eseguito nell'ambiente locale e richiede i privilegi di root. Quando si avvia, Discovery Agent si connette in modo sicuro alla propria area geografica e si registra con Application Discovery Service.

- Ad esempio, se `eu-central-1` è la tua regione di residenza, si registra `arsenal-discovery.eu-central-1.amazonaws.com` con Application Discovery Service.
- Oppure sostituisci la tua regione in base alle esigenze con tutte le altre regioni tranne `us-west-2`.
- Se `us-west-2` è la tua regione di residenza, si registra `arsenal.us-west-2.amazonaws.com` con Application Discovery Service.

Come funziona

Dopo la registrazione, l'agente inizia a raccogliere dati per l'host o la macchina virtuale in cui risiede. L'agente esegue il ping dell'Application Discovery Service a intervalli di 15 minuti per ottenere informazioni di configurazione.

I dati raccolti includono le specifiche di sistema, i dati di utilizzo o di prestazioni delle serie temporali, le connessioni di rete e i dati di elaborazione. Puoi utilizzare queste informazioni per mappare i tuoi asset IT e le relative dipendenze di rete. Tutti questi punti dati possono aiutarti a determinare il costo di esecuzione di questi server AWS e anche a pianificare la migrazione.

I dati vengono trasmessi in modo sicuro dai Discovery Agents ad Application Discovery Service utilizzando la crittografia Transport Layer Security (TLS). Se sono disponibili nuove versioni, gli agenti

sono configurati per l'aggiornamento automatico. Se necessario, puoi modificare questa impostazione di configurazione.

Tip

Prima di scaricare e iniziare l'installazione di Discovery Agent, assicurati di leggere tutti i prerequisiti richiesti in [Prerequisiti per Discovery Agent](#)

Argomenti

- [Prerequisiti per Discovery Agent](#)
- [Installa Discovery Agent su Linux](#)
- [Installazione di su Windows](#)
- [Dati raccolti da Discovery Agent](#)
- [Avvia o interrompi la raccolta dei dati di Discovery Agent](#)

Prerequisiti per Discovery Agent

Di seguito sono riportati i prerequisiti e le attività da eseguire prima di poter installare correttamente AWS Application Discovery Agent (Discovery Agent).

- È necessario impostare una [regione AWS Migration Hub principale](#) prima di iniziare l'installazione di Discovery Agent.
- Se si dispone di una versione 1.x dell'agente installato, è necessario rimuoverla prima di installare la versione più recente.
- Se l'host su cui viene installato l'agente esegue Linux, verifica che l'host supporti almeno l'architettura CPU Intel i686 (nota anche come microarchitettura P6).
- 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

USA 11 SP4, 12 SP5

Windows

Windows Server 2003 R2 SP2

Windows Server 2008 R1 SP2, 2008 R2 SP1

Windows Server 2012 R1, 2012 R2

Windows Server 2016

Windows Server 2019

Windows Server 2022

- Se le connessioni in uscita dalla rete sono limitate, occorre aggiornare le impostazioni del firewall. Gli agenti devono accedere a `arsenal` sulla porta TCP 443. Non richiedono l'apertura di alcuna porta in entrata.

Ad esempio, se la regione di origine è `eu-central-1`, dovresti usare `https://arsenal-discovery.eu-central-1.amazonaws.com:443`

- L'accesso ad Amazon S3 nella tua regione d'origine è necessario per il funzionamento dell'upgrade automatico.
- Crea un utente AWS Identity and Access Management (IAM) nella console e collega la `AWSApplicationDiscoveryAgentAccess` policy gestita IAM esistente. Questa policy consente di eseguire le operazioni dell'agente necessarie per conto dell'utente. Per ulteriori informazioni sulle policy gestite, consulta [AWS politiche gestite per AWS Application Discovery Service](#).
- Verifica la differenza di orario dal tuo server NTP (Network Time Protocol) e correggi se necessario. La sincronizzazione non corretta dell'ora impedisce la riuscita della chiamata di registrazione agente.

Note

Discovery Agent dispone di un agente eseguibile a 32 bit, che funziona su sistemi operativi a 32 e 64 bit. Disporre di un singolo eseguibile riduce il numero di pacchetti di installazione necessari per la distribuzione. Questo agente eseguibile funziona per Linux e per il sistema operativo Windows. Viene descritto nelle rispettive sezioni di installazione indicate di seguito.

Installa Discovery Agent su Linux

Completare la procedura seguente su Linux. Assicurati che la tua [regione di origine di Migration Hub](#) sia stata impostata prima di iniziare questa procedura.

Note

Se utilizzi una versione non corrente di Linux, consulta [Requisiti per le piattaforme Linux precedenti](#).

Per installare AWS Application Discovery Agent nel tuo data center

1. Accedi al tuo server o macchina virtuale basato su Linux e crea una nuova directory per contenere i componenti dell'agente.
2. Passare alla nuova directory e scaricare lo script di installazione dalla riga di comando o dalla console.
 - a. Per eseguire il download dalla riga di comando, eseguire il seguente comando.

```
curl -o ./aws-discovery-agent.tar.gz https://s3-us-west-2.amazonaws.com/aws-discovery-agent.us-west-2/linux/latest/aws-discovery-agent.tar.gz
```

- b. Per effettuare il download dalla console Migration Hub, procedi come segue:
 - i. Aprire la console e accedere alla pagina [Discovery Tools \(Strumenti di rilevamento\)](#).
 - ii. Nella casella Discovery Agent (Agente di rilevamento), scegliere Download agent (Scarica agente), quindi selezionare Linux nella casella di riepilogo risultante. Il download inizia immediatamente.
3. Verificare la firma crittografica del pacchetto di installazione con i seguenti tre comandi:

```
curl -o ./agent.sig https://s3.us-west-2.amazonaws.com/aws-discovery-agent.us-west-2/linux/latest/aws-discovery-agent.tar.gz.sig
```

```
curl -o ./discovery.gpg https://s3.us-west-2.amazonaws.com/aws-discovery-agent.us-west-2/linux/latest/discovery.gpg
```

```
gpg --no-default-keyring --keyring ./discovery.gpg --verify agent.sig aws-  
discovery-agent.tar.gz
```

L'impronta della chiave pubblica dell'agente (`discovery.gpg`) è 7638 F24C 6717 F97C 4F1B 3BC0 5133 255E 4DF4 2DA2.

4. Estrarre dal tarball come mostrato di seguito.

```
tar -xzf aws-discovery-agent.tar.gz
```

5. Per installare l'agente, scegli uno dei seguenti metodi di installazione.

A...	Esegui questa operazione...
Installa Discovery Agent	<p>Per installare l'agente, esegui il comando <code>agent install</code> come illustrato nell'esempio seguente. Nell'esempio, sostituiscilo <i>your-home-region</i> con il nome della tua regione di residenza, <i>aws-access-key-id</i> con l'ID della tua chiave di accesso e <i>aws-secret-access-key</i> con la tua chiave di accesso segreta.</p> <pre>sudo bash install -r your-home- region -k aws-access-key-id -s aws- secret-access-key</pre> <p>Per impostazione predefinita, gli agenti scaricano e applicano automaticamente gli aggiornamenti non appena sono disponibili.</p> <p>Ti consigliamo di usare questa configurazione predefinita.</p> <p>Tuttavia, se non desideri che gli agenti scarichino e applichino gli aggiornamenti automaticamente, includi il <code>-u false</code></p>

A...	Esegui questa operazione...
(Facoltativo) Installa Discovery Agent e configura un proxy non trasparente	<p>parametro quando esegui il comando <code>agent install</code>.</p> <p>Per configurare un proxy non trasparente, aggiungi i seguenti parametri al comando <code>agent install</code>:</p> <ul style="list-style-type: none"> • -e La password del proxy. • -f Il numero di porta del proxy. • -g Lo schema proxy. • -i Il nome utente del proxy. <p>Di seguito è riportato un esempio del comando <code>agent install</code> che utilizza i parametri proxy non trasparenti.</p> <pre>sudo bash install -r <i>your-home-region</i> -k <i>aws-access-key-id</i> -s <i>aws-secret-access-key</i> -d <i>myproxy.mycompany.com</i> -e <i>mypassword</i> -f <i>proxy-port-number</i> -g https -i <i>myusername</i></pre> <p>Se il proxy non richiede l'autenticazione, tralascia i -i parametri -e and.</p> <p>Il comando <code>install</code> di esempio utilizza <code>https</code>, se il proxy utilizza HTTP, specificare <code>http</code> il valore del -g parametro.</p>

6. Se le connessioni in uscita dalla rete sono limitate, occorre aggiornare le impostazioni del firewall. Gli agenti devono accedere a `arsenal` sulla porta TCP 443. Non richiedono l'apertura di alcuna porta in entrata.

Ad esempio, se la regione di origine è `eu-central-1`, dovresti usare `https://arsenal-discovery.eu-central-1.amazonaws.com:443`

Argomenti

- [Requisiti per le piattaforme Linux precedenti](#)
- [Gestisci il processo di Discovery Agent su Linux](#)
- [Disinstallare Discovery Agent su Linux](#)
- [Risoluzione dei problemi di Linux Discovery Agent](#)

Requisiti per le piattaforme Linux precedenti

Alcune piattaforme Linux precedenti come SUSE 10, CentOS 5 e RHEL 5 sono alla fine del loro ciclo di vita oppure solo minimamente supportate. Queste piattaforme possono essere soggette a suite di out-of-date crittografia che impediscono allo script di aggiornamento dell'agente di scaricare i pacchetti di installazione.

Curl

L'agente Application Discovery richiede `curl` comunicazioni sicure con il AWS server. Alcune vecchie versioni di `curl` non sono in grado di comunicare in modo sicuro con un servizio Web moderno.

Per utilizzare la versione di `curl` inclusa nell'agente Application Discovery per tutti gli operatori, esegui lo script di installazione con il parametro `-c true`.

Bundle dell'autorità di certificazione

I sistemi Linux meno recenti potrebbero disporre di un pacchetto out-of-date Certificate Authority (CA), fondamentale per proteggere le comunicazioni Internet.

Per utilizzare il bundle CA incluso nell'agente Application Discovery per tutte le operazioni, esegui lo script di installazione con il parametro `-b true`.

Queste opzioni dello script di installazione possono essere utilizzate insieme. Nel seguente comando di esempio, entrambi i parametri dello script vengono passati allo script di installazione:

```
sudo bash install -r your-home_region -k aws-access-key-id -s aws-secret-access-key -c true -b true
```

Gestisci il processo di Discovery Agent su Linux

È possibile gestire il comportamento di Discovery Agent a livello di sistema utilizzando gli System V `init` strumenti `systemd` `Upstart`, o. Le seguenti schede delineare i comandi per le attività supportate in ciascuno dei rispettivi strumenti.

systemd

Comandi di gestione per Application Discovery Agent

Attività	Comando
Verificare che un agente sia in esecuzione	<code>sudo systemctl status aws-discovery-daemon.service</code>
Avviare un agente	<code>sudo systemctl start aws-discovery-daemon.service</code>
Arrestare un agente	<code>sudo systemctl stop aws-discovery-daemon.service</code>
Riavviare un agente	<code>sudo systemctl restart aws-discovery-daemon.service</code>

Upstart

Comandi di gestione per Application Discovery Agent

Attività	Comando
Verificare che un agente sia in esecuzione	<code>sudo initctl status aws-discovery-daemon</code>
Avviare un agente	<code>sudo initctl start aws-discovery-daemon</code>
Arrestare un agente	<code>sudo initctl stop aws-discovery-daemon</code>
Riavviare un agente	<code>sudo initctl restart aws-discovery-daemon</code>

System V init

Comandi di gestione per Application Discovery Agent

Attività	Comando
Verificare che un agente sia in esecuzione	<code>sudo /etc/init.d/aws-discovery-daemon status</code>
Avviare un agente	<code>sudo /etc/init.d/aws-discovery-daemon start</code>
Arrestare un agente	<code>sudo /etc/init.d/aws-discovery-daemon stop</code>
Riavviare un agente	<code>sudo /etc/init.d/aws-discovery-daemon restart</code>

Disinstallare Discovery Agent su Linux

Questa sezione descrive come disinstallare Discovery Agent su Linux.

Per disinstallare un agente se si utilizza il gestore di pacchetti yum

- Usa il seguente comando per disinstallare un agente se usi yum.

```
rpm -e --nodeps aws-discovery-agent
```

Per disinstallare un agente se si utilizza il gestore di pacchetti apt-get

- Usa il seguente comando per disinstallare un agente se usi apt-get.

```
apt-get remove aws-discovery-agent:i386
```

Per disinstallare un agente se stai usando il gestore di pacchetti zypper

- Usa il seguente comando per disinstallare un agente se usi zypper.

```
zypper remove aws-discovery-agent
```

Risoluzione dei problemi di Linux Discovery Agent

In caso di problemi durante l'installazione o l'utilizzo di Discovery Agent su Linux, consulta la seguente guida sulla registrazione e la configurazione. Quando aiuta a risolvere potenziali problemi con l'agente o la sua connessione all'Application Discovery Service, AWS Support richiede spesso questi file.

- File di log

I file di registro per Discovery Agent si trovano nella seguente directory.

```
/var/log/aws/discovery/
```

I file di registro sono denominati per indicare se sono generati dal demone principale, dall'aggiornamento automatico o dal programma di installazione.

- File di configurazione

I file di configurazione per la versione 2.0.1617.0 o successiva di Discovery Agent si trovano nella seguente directory.

```
/etc/opt/aws/discovery/
```

I file di configurazione per le versioni di Discovery Agent precedenti alla 2.0.1617.0 si trovano nella directory seguente.

```
/var/opt/aws/discovery/
```

- Per istruzioni su come rimuovere le versioni precedenti di Discovery Agent, vedere. [Prerequisiti per Discovery Agent](#)

Installazione di su Windows

Per installare un agente in Windows, completare la procedura seguente. Assicurati che la tua [regione di origine di Migration Hub](#) sia stata impostata prima di iniziare questa procedura.

Per installare AWS Application Discovery Agent nel tuo data center

1. Scaricate il programma di [installazione di Windows Agent](#) ma non fate doppio clic per eseguirlo in Windows.

Important

Non fate doppio clic per eseguire il programma di installazione in Windows, poiché l'installazione non riuscirà. L'installazione dell'agente funziona solo dal prompt dei comandi. Se si è già fatto doppio clic sul programma di installazione, è necessario passare a Installazione applicazioni e disinstallare l'agente prima di continuare con le restanti fasi dell'installazione.

Se il programma di installazione dell'agente di Windows non rileva alcuna versione del runtime x86 di Visual C++ sull'host, installa automaticamente il runtime di Visual C++ x86 2015—2019 prima di installare il software dell'agente.

2. Apri un prompt dei comandi come amministratore e naviga fino alla posizione in cui hai salvato il pacchetto di installazione.
3. Per installare l'agente, scegli uno dei seguenti metodi di installazione.

A...	Esegui questa operazione...
Installa Discovery Agent	<p>Per installare l'agente, esegui il comando <code>agent install</code> come illustrato nell'esempio seguente. Nell'esempio, sostituiscilo <i>your-home-region</i> con il nome della tua regione di residenza, <i>aws-access-key-id</i> con l'ID della tua chiave di accesso e <i>aws-secret-access-key</i> con la tua chiave di accesso segreta.</p> <p>Facoltativamente, è possibile impostare la posizione di installazione dell'agente</p>

A...

Esegui questa operazione...

specificando il percorso della cartella **C:** `\install-location` per il parametro INSTALLLOCATION. Ad esempio, `INSTALLLOCATION=" C:\install-location "`. La gerarchia di cartelle risultante sarà `[INSTALLLOCATION path]\Discovery.AWS` Per impostazione predefinita, il percorso di installazione è la cartella Program Files


Facoltativamente, è possibile utilizzare `LOGANDCONFIGLOCATION` per sovrascrivere la directory predefinita (ProgramData) per la cartella dei registri degli agenti e il file di configurazione. La gerarchia di cartelle risultante è `[LOGANDCONFIGLOCATION path]\AWS Discovery`

```
.\AWSDiscoveryAgentInstall.exe REGION=" your-home-region "
KEY_ID="aws-access-key-id "
KEY_SECRET=" aws-secret-access-key " /quiet
```

Per impostazione predefinita, gli agenti scaricano e applicano automaticamente gli aggiornamenti non appena sono disponibili.

Ti consigliamo di usare questa configurazione predefinita.

Tuttavia, se non desideri che gli agenti scarichino e applichino gli aggiornamenti automaticamente, includi il seguente parametro quando esegui il comando `agent install: AUTO_UPDATE=false`

A...	Esegui questa operazione...
	<p> Warning</p> <p>La disabilitazione degli aggiornamenti automatici impedirà l'installazione delle patch di sicurezza più recenti.</p>

A...	Esegui questa operazione...
<p>(Facoltativo) Installa Discovery Agent e configura un proxy non trasparente</p>	<p>Per configurare un proxy non trasparente, aggiungi le seguenti proprietà pubbliche al comando <code>agent install</code>:</p> <ul style="list-style-type: none">• <code>PROXY_HOST</code> — Il nome dell'host proxy• <code>PROXY_SCHEME</code> — Lo schema proxy• <code>PROXY_PORT</code> — Il numero di porta del proxy• <code>PROXY_USER</code> — Il nome utente del proxy• <code>PROXY_PASSWORD</code> — La password dell'utente proxy <p>Di seguito è riportato un esempio del comando di installazione dell'agente che utilizza le proprietà proxy non trasparenti.</p> <pre data-bbox="862 1003 1507 1402">.\AWSDiscoveryAgentInstall.exe REGION=" <i>your-home-region</i> " KEY_ID="<i>aws-access-key-id</i> " KEY_SECRET="<i>aws-secret-access-key</i> " PROXY_HOST="<i>myproxy.mycompany.com</i> " PROXY_SCHEME="https" PROXY_PORT="<i>proxy-port-number</i> " PROXY_USER="<i>myusername</i> " PROXY_PASSWORD="<i>mypassword</i> " /quiet</pre> <p>Se il proxy non richiede l'autenticazione, ometti le proprietà <code>PROXY_USER</code> and <code>PROXY_PASSWORD</code> . L'esempio utilizzato o <code>https</code> dal comando <code>install</code>. Se il tuo proxy utilizza HTTP, specifica <code>http</code> il <code>PROXY_SCHEME</code> valore.</p>

4. Se le connessioni in uscita dalla rete sono limitate, è necessario aggiornare le impostazioni del firewall. Gli agenti devono accedere a `arsenal` sulla porta TCP 443. Non richiedono l'apertura di alcuna porta in entrata.

Ad esempio, se la tua regione di residenza è `eu-central-1`, utilizzerai quanto segue:
`https://arsenal-discovery.eu-central-1.amazonaws.com:443`

Firma dei pacchetti e aggiornamenti automatici

Per Windows Server 2008 e versioni successive, Amazon firma crittograficamente il pacchetto di installazione dell'agente Application Discovery Service con un certificato SHA256. Per gli aggiornamenti automatici con firma SHA2 su Windows Server 2008 SP2, assicurati che sugli host sia installato un hotfix per supportare l'autenticazione con firma SHA2. L'ultimo [hotfix](#) di supporto di Microsoft aiuta a supportare l'autenticazione SHA2 su Windows Server 2008 SP2.

Note

Gli aggiornamenti rapidi per il supporto SHA256 per Windows 2003 non sono più disponibili pubblicamente presso Microsoft. Se queste correzioni non sono già installate nell'host Windows 2003, sono necessari aggiornamenti manuali.

Per eseguire gli aggiornamenti manualmente

1. Scarica [Windows Agent Updater](#).
2. Apri il prompt dei comandi come amministratore.
3. Vai alla posizione in cui è stato salvato il programma di aggiornamento.
4. Esegui il comando seguente.

```
AWSDiscoveryAgentUpdater.exe /Q
```

Gestisci il processo di Discovery Agent in Windows

È possibile gestire il comportamento di Discovery Agent a livello di sistema tramite la console di Windows Server Manager Services. Nella seguente tabella viene descritto come fare.

Attività	Nome del servizio	Stato servizio/Azione
Verificare che un agente sia in esecuzione	AWS Discovery Agent AWS Discovery Updater	Avviato
Avviare un agente	AWS Agente Discovery AWS Discovery Updater	Scegli Start (Avvia)
Arrestare un agente	AWS Agente Discovery AWS Discovery Updater	Scegli Stop (Arresta)
Riavviare un agente	AWS Agente Discovery AWS Discovery Updater	Scegli Restart (Riavvia)

Per disinstallare Discovery Agent su Windows

1. Apri il Pannello di controllo in Windows.
2. Scegliere Programmi.
3. Scegliere Programmi e funzionalità.
4. Seleziona AWS Discovery Agent.
5. Scegliere Uninstall (Disinstalla).

Note

Se scegli di reinstallare l'agente dopo averlo disinstallato, esegui il comando seguente con le opzioni `/repair and/norestart`.

```
.\AWSDiscoveryAgentInstaller.exe REGION="your-home-region" KEY_ID="aws-access-key-id" KEY_SECRET="aws-secret-access-key" /quiet /repair /norestart
```

Per disinstallare un discovery agent su Windows utilizzando la riga di comando

1. Fate clic con il pulsante destro
2. Scegli Command Prompt.
3. Usa il seguente comando per disinstallare un discovery agent su Windows.

```
wmic product where name='AWS Discovery Agent' call uninstall
```

Risoluzione dei problemi di Discovery Agent in Windows

In caso di problemi durante l'installazione o l'utilizzo di AWS Application Discovery Agent su Windows, consultate le seguenti indicazioni sulla registrazione e la configurazione. AWS Support spesso richiede questi file quando aiuta a risolvere potenziali problemi con l'agente o la sua connessione all'Application Discovery Service.

- File di registro installazione

In alcuni casi, il comando `agent install` sembra non riuscire. Ad esempio, può comparire un guasto in cui Windows Services Manager mostra che i servizi di rilevamento non vengono creati. In questo caso, aggiungi `/log install.log` al comando per generare un log di installazione dettagliato.

- Registrazione operativa

In Windows Server 2008 e versioni successive, i file di log degli agenti sono disponibili nella seguente directory.

```
C:\ProgramData\AWS\AWS Discovery\Logs
```

In Windows Server 2003, i file di log degli agenti sono disponibili nella seguente directory.

```
C:\Documents and Settings\All Users\Application Data\AWS\AWS Discovery\Logs
```

I file di registro sono denominati per indicare se sono generati dal servizio principale, dagli aggiornamenti automatici o dal programma di installazione.

- File di configurazione

In Windows Server 2008 e versioni successive, il file di configurazione dell'agente è disponibile nella posizione seguente.

```
C:\ProgramData\AWS\AWS Discovery\config
```

In Windows Server 2003, il file di configurazione dell'agente è disponibile nella posizione seguente.

```
C:\Documents and Settings\All Users\Application Data\AWS\AWS Discovery\config
```

- Per istruzioni su come rimuovere le versioni precedenti di Discovery Agent, vedere. [Prerequisiti per Discovery Agent](#)

Dati raccolti da Discovery Agent

AWS Application Discovery Agent (Discovery Agent) è un software che si installa su server e macchine virtuali locali. Discovery Agent raccoglie dati sulla configurazione del sistema, sull'utilizzo delle serie temporali o sulle prestazioni, i dati di processo e le connessioni di rete TCP (Transmission Control Protocol). Questa sezione descrive i dati raccolti.

Legenda della tabella per i dati raccolti da Discovery Agent:

- Il termine host si riferisce a un server fisico o a una macchina virtuale.
- I dati raccolti sono misurati in kilobyte (KB) salvo diversamente specificato.
- I dati equivalenti nella console Migration Hub sono riportati in megabyte (MB).
- Il periodo di votazione è a intervalli di circa 15 secondi e viene inviato ogni 15 minuti. AWS
- I campi dati contrassegnati da un asterisco (*) sono disponibili solo nei .csv file prodotti dalla funzione di esportazione API dell'agente.

Campo dati	Descrizione
agentAssignedProcess ^{Id (*)}	ID processo dei processi rilevati dall'agente
agentId	ID univoco dell'agente
agentProvidedTime ^{Timbro *}	Data e ora dell'osservazione agente (mm/gg/aa aa hh.mm.ss AM/PM)

Campo dati	Descrizione
cmdLine *	Processo inserito dalla riga di comando
cpuType	Tipo di CPU (unità di elaborazione centrale) utilizzato nell'host
destinationIp *	Indirizzo IP del dispositivo cui viene inviato il pacchetto
destinationPort *	Numero di porta cui vengono inviati i dati/ricieste
family *	Famiglia di protocollo di instradamento
freeRAM (MB)	La RAM libera e la RAM nella cache, misurate in MB, che possono essere rese immediatamente disponibili per le applicazioni.
gateway *	Indirizzo nodo di rete
hostName	Nome dell'host su cui sono stati raccolti i dati
hypervisor	Tipo di hypervisor
ipAddress	Indirizzo IP dell'host
ipVersion *	Numero versione IP
isSystem *	Attributo booleano per indicare se un processo è di proprietà del sistema operativo
macAddress	Indirizzo MAC dell'host
name *	Nome dell'host, della rete, dei parametri e così via per cui vengono raccolti i dati
netMask *	Prefisso indirizzo IP cui appartiene l'host di rete
osName	Nome del sistema operativo su host

Campo dati	Descrizione
osVersion	Versione del sistema operativo su host
path	Percorso del comando originato dalla riga di comando
sourceIp [*]	Indirizzo IP del dispositivo che invia il pacchetto IP
sourcePort [*]	Numero di porta da cui originano dati/richieste
timestamp [*]	Data e ora dell'attributo segnalato registrato da agente
totalCpuUsagePct	Percentuale di utilizzo della CPU su host durante il periodo di polling
totalDiskBytesReadPerSecond (Kbps)	Kilobit totali letti al secondo su tutti i dischi
totalDiskBytesWrittenPerSecond (Kbps)	Kilobit totali scritti al secondo su tutti i dischi
totalDiskFreeDimensioni (GB)	Spazio libero su disco espresso in GB
totalDiskReadOpsPerSecond	Numero totale di operazioni di I/O di lettura al secondo
totalDiskSize (GB)	Capacità totale del disco espressa in GB
totalDiskWriteOpsPerSecond	Numero totale di operazioni di I/O di scrittura al secondo
totalNetworkBytesReadPerSecond (Kbps)	Quantità totale di throughput di byte letti al secondo
totalNetworkBytesWrittenPerSecond (Kbps)	Quantità totale di throughput di byte scritti al secondo
totalNumCores	Numero totale di unità di elaborazione indipendenti all'interno della CPU

Campo dati	Descrizione
totalNumCpus	Numero totale di unità di elaborazione centrali
totalNumDisks	Il numero di dischi rigidi fisici in un host
totalNumLogical ^{Processori *}	Numero totale di core fisici moltiplicato per il numero di thread che possono essere eseguiti su ciascun core
totalNumNetworkCarte	Conteggio totale delle schede di rete su server
totalRAM (MB)	Quantità totale di RAM disponibile su host
transportProtocol [*]	Tipo di protocollo di trasporto utilizzato

Avvia o interrompi la raccolta dei dati di Discovery Agent

Dopo aver distribuito e configurato Discovery Agent, se la raccolta dei dati si interrompe, puoi riavviarlo. È possibile avviare o interrompere la raccolta dei dati tramite la console o effettuando chiamate API tramite AWS CLI. Entrambi questi metodi sono descritti nelle procedure seguenti.

Using the Migration Hub console

La procedura seguente mostra come avviare o interrompere il processo di raccolta dati di Discovery Agent, nella pagina Data Collectors della console Migration Hub.

Per avviare o interrompere la raccolta dei dati

1. Nel riquadro di navigazione, selezionare Data Collectors (Agenti di raccolta dati).
2. Selezionare la scheda Agents (Agenti).
3. Seleziona la casella di controllo dell'agente che desideri avviare o interrompere.

Tip

Se hai installato più agenti ma desideri avviare o interrompere la raccolta dei dati solo su determinati host, la colonna Hostname nella riga dell'agente identifica l'host su cui è installato l'agente.

4. Selezionare Start data collection (Avvia raccolta dei dati) o Stop data collection (Arresta raccolta dei dati).

Using the AWS CLI

Per avviare o interrompere il processo di raccolta dati di Discovery Agent da AWS CLI, è necessario prima installarlo AWS CLI nel proprio ambiente, quindi è necessario impostare la CLI per utilizzare la regione [principale di Migration Hub](#) selezionata.

Per installare AWS CLI e avviare o interrompere la raccolta dei dati

1. Se non l'hai ancora fatto, installa quello AWS CLI appropriato per il tuo tipo di sistema operativo (Windows o Mac/Linux). Consulta la [Guida per AWS Command Line Interface l'utente per le istruzioni](#).
2. Aprire il prompt dei comandi (Windows) o Terminal (Mac/Linux).
 - a. Digitare `aws configure` e premere Invio.
 - b. Inserisci AWS l'ID della chiave di accesso e la chiave di accesso AWS segreta.
 - c. Immettere la propria regione di origine, ad esempio `us-west-2`, per il nome della regione predefinito. In questo esempio supponiamo che `us-west-2` sia la regione d'origine.
 - d. Immettere `text` per Default Output Format (Formato di output predefinito).
3. Per trovare l'ID dell'agente per cui desideri interrompere o avviare la raccolta dei dati, digita il comando seguente:

```
aws discovery describe-agents
```

4. Per avviare la raccolta dei dati da parte dell'agente, digita il seguente comando:

```
aws discovery start-data-collection-by-agent-ids --agent-ids <agent ID>
```

Per interrompere la raccolta dei dati da parte dell'agente, digitare il comando seguente:

```
aws discovery stop-data-collection-by-agent-ids --agent-ids <agent ID>
```

Application Discovery Service Agentless Collector

Application Discovery Service Agentless Collector (Agentless Collector) è un'applicazione locale che raccoglie informazioni tramite metodi agentless sull'ambiente locale, incluse informazioni sul profilo del server (ad esempio, sistema operativo, numero di CPU, quantità di RAM), metadati del database e metriche di utilizzo. Agentless Collector si installa come macchina virtuale (VM) nell'ambiente VMware vCenter Server utilizzando un file Open Virtualization Archive (OVA).

Agentless Collector ha un'architettura modulare che consente l'uso di più metodi di raccolta senza agenti. Agentless Collector attualmente supporta moduli per la raccolta di dati da macchine virtuali VMware e da server di database e analisi. I moduli futuri supporteranno la raccolta delle connessioni di rete, la raccolta da piattaforme di virtualizzazione aggiuntive e la raccolta a livello di sistema operativo.

Agentless Collector supporta la raccolta di dati per AWS Application Discovery Service (Application Discovery Service), che consente di pianificare la migrazione verso il Cloud AWS raccogliendo dati di utilizzo e configurazione sui server e i database locali.

Application Discovery Service è integrato con AWS Migration Hub, il che semplifica il monitoraggio della migrazione in quanto aggrega le informazioni sullo stato della migrazione in un'unica console. Puoi visualizzare i server rilevati, ottenere consigli su Amazon EC2, visualizzare le connessioni di rete, raggruppare i server in applicazioni e quindi monitorare lo stato della migrazione di ciascuna applicazione dalla console Migration Hub nella tua regione di origine.

Il database Agentless Collector e il modulo di raccolta dei dati di analisi sono integrati con (). AWS Database Migration Service AWS DMS Questa integrazione aiuta a pianificare la migrazione verso. Cloud AWS Puoi utilizzare il modulo di raccolta dei dati di database e analisi per individuare i server di database e analisi presenti nel tuo ambiente e creare un inventario dei server su cui desideri migrare Cloud AWS. Questo modulo di raccolta dati raccoglie i metadati del database e le metriche di utilizzo effettivo di CPU, memoria e capacità del disco. Dopo aver raccolto queste metriche, puoi utilizzare la AWS DMS console per generare consigli sugli obiettivi per i tuoi database di origine.

Argomenti

- [Guida introduttiva a Agentless Collector](#)
- [Dati raccolti da Agentless Collector](#)
- [Utilizzo della console Agentless Collector](#)

- [Aggiornamento manuale di Agentless Collector](#)
- [Risoluzione dei problemi di Agentless Collector](#)

Guida introduttiva a Agentless Collector

Questa sezione descrive come iniziare a utilizzare Application Discovery Service Agentless Collector (Agentless Collector).

Argomenti

- [Prerequisiti per Agentless Collector](#)
- [Fase 1: Creare un utente IAM per Agentless Collector](#)
- [Passaggio 2: scarica Agentless Collector](#)
- [Fase 3: Implementazione di Agentless Collector](#)
- [Fase 4: Accedere alla console Agentless Collector](#)
- [Fase 5: Configurare Agentless Collector](#)
- [Fase 6: Configurare i moduli di raccolta dati Agentless Collector](#)
- [Fase 7: Visualizzazione dei dati raccolti](#)

Prerequisiti per Agentless Collector

Di seguito sono riportati i prerequisiti per l'utilizzo di Application Discovery Service Agentless Collector (Agentless Collector):

- Uno o più account. AWS
- Un AWS account con la regione di AWS Migration Hub origine impostata, vedi [Accedi alla console Migration Hub e scegli una regione d'origine](#). I dati del Migration Hub vengono archiviati nella regione di origine per scopi di individuazione, pianificazione e monitoraggio della migrazione.
- Un utente IAM dell'AWSaccount configurato per utilizzare la policy AWS gestita `AWSApplicationDiscoveryAgentlessCollectorAccess`. Per utilizzare il database e il modulo di raccolta dei dati di analisi, questo utente IAM deve utilizzare anche due policy IAM gestite dal cliente `DMSCollectorPolicy` e `FleetAdvisorS3Policy`. Per ulteriori informazioni, consulta [Fase 1: Creare un utente IAM per Agentless Collector](#). L'utente IAM deve essere creato in un AWS account con Migration Hub home Region impostata.

- VMware vCenter Server V5.5, V6, V6.5, 6.7 o 7.0.

Note

Agentless Collector supporta tutte queste versioni di VMware, ma attualmente eseguiamo test con le versioni 6.7 e 7.0.

- Per la configurazione di VMware vCenter Server, assicurati di poter fornire le credenziali vCenter con le autorizzazioni di lettura e visualizzazione impostate per il gruppo System.
- Agentless Collector richiede l'accesso in uscita tramite la porta TCP 443 a diversi domini. AWS Per un elenco di questi domini, consulta [Configura il firewall per l'accesso in uscita ai domini AWS](#)
- Per utilizzare il modulo di raccolta dei dati di database e analisi, crea un bucket Amazon S3 nella regione Regione AWS che hai impostato come regione principale di Migration Hub. I moduli di raccolta dei dati di database e analisi archiviano i metadati dell'inventario in questo bucket Amazon S3. Per ulteriori informazioni, consulta [Creare un bucket nella Guida](#) per l'utente di Amazon S3.

Configura il firewall per l'accesso in uscita ai domini AWS

Se le connessioni in uscita dalla rete sono limitate, è necessario aggiornare le impostazioni del firewall per consentire l'accesso in uscita ai AWS domini richiesti da Agentless Collector. AWSI domini che richiedono l'accesso in uscita dipendono dal fatto che la regione di origine di Migration Hub sia Stati Uniti occidentali (Oregon), us-west-2 o un'altra regione.

I seguenti domini richiedono l'accesso in uscita se la regione di origine dell'account è us-west-2: AWS

- `arsenal-discovery.us-west-2.amazonaws.com`— Il raccogliatore utilizza questo dominio per verificare che sia configurato con le credenziali utente IAM richieste. Il raccogliatore lo utilizza anche per inviare e archiviare i dati raccolti poiché la regione di origine è us-west-2.
- `migrationhub-config.us-west-2.amazonaws.com`— Il raccogliatore utilizza questo dominio per determinare a quale regione di origine il raccogliatore invia i dati in base alle credenziali utente IAM fornite.
- `api.ecr-public.us-east-1.amazonaws.com`— Il raccogliatore utilizza questo dominio per scoprire gli aggiornamenti disponibili.
- `public.ecr.aws`— Il raccogliatore utilizza questo dominio per scaricare gli aggiornamenti.
- `dms.your-migrationhub-home-region.amazonaws.com`— Il raccogliatore utilizza questo dominio per connettersi al raccogliatore di AWS DMS dati.

- `s3.amazonaws.com`— Il raccoglitore utilizza questo dominio per caricare i dati raccolti dal database e dal modulo di raccolta dei dati di analisi nel tuo bucket Amazon S3.

I seguenti domini richiedono l'accesso in uscita se la regione di origine del tuo AWS account non è: **us-west-2**

- `arsenal-discovery.us-west-2.amazonaws.com`— Il raccoglitore utilizza questo dominio per verificare che sia configurato con le credenziali utente IAM richieste.
- `arsenal-discovery.your-migrationhub-home-region.amazonaws.com`— Il raccoglitore utilizza questo dominio per inviare e archiviare i dati raccolti.
- `migrationhub-config.us-west-2.amazonaws.com`— Il raccoglitore utilizza questo dominio per determinare a quale regione di origine il raccoglitore deve inviare i dati in base alle credenziali utente IAM fornite.
- `api.ecr-public.us-east-1.amazonaws.com`— Il raccoglitore utilizza questo dominio per scoprire gli aggiornamenti disponibili.
- `public.ecr.aws`— Il raccoglitore utilizza questo dominio per scaricare gli aggiornamenti.
- `dms.your-migrationhub-home-region.amazonaws.com`— Il raccoglitore utilizza questo dominio per connettersi al raccoglitore di AWS DMS dati.
- `s3.amazonaws.com`— Il raccoglitore utilizza questo dominio per caricare i dati raccolti dal database e dal modulo di raccolta dei dati di analisi nel tuo bucket Amazon S3.

Durante la configurazione di Agentless Collector, potresti ricevere errori del tipo Configurazione non riuscita: controlla le tue credenziali e riprova. In caso contrario, l'operazione non è raggiungibile. AWS Verifica le impostazioni di rete. Questi errori possono essere causati da un tentativo fallito da parte di Agentless Collector di stabilire una connessione HTTPS a uno dei AWS domini a cui deve accedere in uscita.

Se non è possibile stabilire una connessione a, Agentless Collector AWS non può raccogliere dati dall'ambiente locale. Per informazioni su come correggere la connessione a, vedere. [AWS Fixing Agentless Collector non AWS riesce a raggiungerlo durante la configurazione](#)

Fase 1: Creare un utente IAM per Agentless Collector

Per utilizzare Agentless Collector, nell'AWSaccount in cui è stato utilizzato [Accedi alla console Migration Hub e scegli una regione d'origine](#), è necessario creare un utente (IAM). AWS Identity and

Access Management Quindi, configura questo utente IAM per utilizzare la seguente AWS politica gestita. [AWSApplicationDiscoveryAgentlessCollectorAccess](#) Allega questa policy IAM quando crei l'utente IAM.

Per utilizzare il database e il modulo di raccolta dei dati di analisi, crea due policy IAM gestite dal cliente. Queste policy forniscono l'accesso al bucket Amazon S3 e all'API. AWS DMS Per ulteriori informazioni, consulta [Creare una policy gestita dai clienti nella Guida](#) per l'utente IAM.

- Utilizza il seguente codice JSON per creare la **DMSCollectorPolicy** policy.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "dms:DescribeFleetAdvisorCollectors",
      "dms:ModifyFleetAdvisorCollectorStatuses",
      "dms:UploadFileMetadataList"
    ],
    "Resource": "*"
  }]
}
```

- Utilizza il seguente codice JSON per creare la **FleetAdvisorS3Policy** policy.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject*",
        "s3:GetBucket*",
        "s3:List*",
        "s3:DeleteObject*",
        "s3:PutObject*"
      ],
      "Resource": [
        "arn:aws:s3:::bucket_name",
        "arn:aws:s3:::bucket_name/*"
      ]
    }
  ]
}
```

```
}
```

Nell'esempio precedente, sostituiscilo *bucket_name* con il nome del bucket Amazon S3 creato nella fase dei prerequisiti.

Ti consigliamo di creare un utente IAM non amministrativo da utilizzare con Agentless Collector. Quando crei utenti IAM non amministrativi, segui le best practice di sicurezza Grant Least [Privilege, che concede agli utenti autorizzazioni minime](#).

Per creare un utente IAM non amministratore da utilizzare con Agentless Collector

1. In AWS Management Console, accedi alla console IAM, utilizzando l'AWS account che hai usato per impostare la home region. [Accedi alla console Migration Hub e scegli una regione d'origine](#)
2. Crea un utente IAM non amministratore seguendo le istruzioni per creare un utente con la console, come descritto nella sezione [Creazione di un utente IAM nel tuo AWS account](#) nella Guida per l'utente IAM.

Seguendo le istruzioni contenute nella Guida per l'utente IAM:

- Nella fase di selezione del tipo di accesso, seleziona Accesso programmatico. Nota, sebbene non sia consigliato, seleziona l'accesso alla console di AWS gestione solo se prevedi di utilizzare le stesse credenziali utente IAM per accedere alla AWS console.
- Nella fase relativa alla pagina Imposta autorizzazione, scegli l'opzione Allega le politiche esistenti direttamente all'utente. Quindi seleziona la politica `AWSApplicationDiscoveryAgentlessCollectorAccess` AWS gestita dall'elenco delle politiche.

Quindi, seleziona le politiche IAM gestite `FleetAdvisorS3Policy` dal cliente `DMSCollectorPolicy` e quelle gestite dal cliente.

- Durante la fase di visualizzazione delle chiavi di accesso dell'utente (ID delle chiavi di accesso e chiavi di accesso segrete), segui le indicazioni contenute nella Nota importante sul salvataggio del nuovo ID della chiave di accesso e della chiave di accesso segreta dell'utente in un luogo sicuro e protetto. Avrai bisogno di queste chiavi di accesso [Fase 5: Configurare Agentless Collector](#).

La rotazione delle chiavi di accesso è una best practice di AWS sicurezza. Per informazioni sulla rotazione delle chiavi, consulta [Ruotare regolarmente le chiavi di accesso per i casi d'uso che richiedono credenziali a lungo termine nella IAM User Guide](#).

Passaggio 2: scarica Agentless Collector

Per configurare Application Discovery Service Agentless Collector (Agentless Collector), è necessario scaricare e distribuire il file Agentless Collector Open Virtualization Archive (OVA). Agentless Collector è un'appliance virtuale che si installa nell'ambiente VMware locale. Questo passaggio descrive come scaricare il file OVA del collettore e il passaggio successivo descrive come distribuirlo.

Per scaricare il file Collector OVA e verificarne il checksum

1. Accedi a vCenter come amministratore di VMware e passa alla directory in cui desideri scaricare il file OVA di Agentless Collector.
2. Scarica il file OVA dal seguente URL:

[Collettore senza agente \(OVA\)](#)

3. A seconda dell'algoritmo di hashing in uso nell'ambiente di sistema, scaricare [MD5](#) o [SHA256](#) per ottenere il file contenente il valore checksum. Utilizza il valore scaricato per verificare il `ApplicationDiscoveryServiceAgentlessCollector` file scaricato nel passaggio precedente.
4. A seconda della variante di Linux, eseguire il comando MD5 appropriato versione o il comando SHA256 per verificare che la firma crittografica del file `ApplicationDiscoveryServiceAgentlessCollector.oVA` corrisponda al valore nel rispettivo file MD5/SHA256 scaricato.

```
$ md5sum ApplicationDiscoveryServiceAgentlessCollector.oVA
```

```
$ sha256sum ApplicationDiscoveryServiceAgentlessCollector.oVA
```

Fase 3: Implementazione di Agentless Collector

Application Discovery Service Agentless Collector (Agentless Collector) è un'appliance virtuale che si installa nell'ambiente VMware locale. Questa sezione descrive come distribuire il file Open Virtualization Archive (OVA) scaricato nel passaggio precedente, nell'ambiente VMware.

Specifiche della macchina virtuale Agentless Collector

- Sistema operativo: Amazon Linux 2
- RAM: 16 GB

- CPU: 4 core

La procedura seguente illustra la distribuzione del file OVA Agentless Collector nell'ambiente VMware.

Per distribuire Agentless Collector

1. Accedi a vCenter come amministratore VMware.
2. Utilizzate uno dei seguenti metodi per installare il file OVA:
 - Usa l'interfaccia utente: scegli File, scegli Deploy OVF Template, seleziona il file Collector OVA scaricato nella sezione precedente, quindi completa la procedura guidata.
 - Usa la riga di comando: per installare il file Collector OVA dalla riga di comando, scarica e utilizza VMware Open Virtualization Format Tool (ovftool). [Per scaricare ovftool, seleziona una versione dalla pagina della documentazione dello strumento OVF.](#)

Di seguito è riportato un esempio di utilizzo dello strumento da riga di comando ovftool per installare il file OVA del collettore.

```
ovftool --acceptAllEulas --name=AgentlessCollector --datastore=datastore1  
-dm=thin ApplicationDiscoveryServiceAgentlessCollector.ova  
'vi://username:password@vcenterurl/Datacenter/host/esxi/'
```

Di seguito vengono descritti i valori **sostituibili** nell'esempio

- Il nome è il nome che desideri utilizzare per la tua macchina virtuale Agentless Collector.
 - Il datastore è il nome del datastore nel tuo vCenter.
 - Il nome del file OVA è il nome del file Collector OVA scaricato.
 - Il nome utente/password sono le tue credenziali vCenter.
 - Il vcenterurl è l'URL del tuo vCenter.
 - Il percorso vi è il percorso verso l'host VMware ESXi.
3. Individua l'Agentless Collector distribuito nel tuo vCenter. Fai clic con il pulsante destro del mouse sulla macchina virtuale, quindi scegli Power, Power On.
 4. Dopo alcuni minuti, l'indirizzo IP del raccoglitore viene visualizzato in vCenter. Questo indirizzo IP viene utilizzato per connettersi al raccoglitore.

Fase 4: Accedere alla console Agentless Collector

La procedura seguente descrive come accedere alla console Application Discovery Service Agentless Collector (Agentless Collector).

Per accedere alla console Agentless Collector

1. Apri un browser Web, quindi digita il seguente URL nella barra degli indirizzi: **https://** /<ip_address>, da dove <ip_address> proviene l'indirizzo IP del raccoglitore. [Fase 3: Implementazione di Agentless Collector](#)
2. Scegli Inizia la prima volta che accedi ad Agentless Collector. Successivamente, ti verrà chiesto di accedere.

Se accedi alla console Agentless Collector per la prima volta, la prossima volta lo farai. [Fase 5: Configurare Agentless Collector](#) Altrimenti, vedrete dopo. [La dashboard di Agentless Collector](#)

Fase 5: Configurare Agentless Collector

Application Discovery Service Agentless Collector (Agentless Collector) è una macchina virtuale (VM) basata su Amazon Linux 2. La sezione seguente descrive come configurare una macchina virtuale di raccolta nella pagina Configure Agentless Collector della console Agentless Collector.

Per configurare una macchina virtuale di raccolta nella pagina Configure Agentless Collector

1. Per il nome del collezionista, inserisci un nome per il raccoglitore per identificarlo. Il nome può contenere spazi ma non può contenere caratteri speciali.
2. In Sincronizzazione dei dati, inserisci la chiave di AWS accesso e la chiave segreta per l'AWSaccount che l'utente IAM deve specificare come account di destinazione per ricevere i dati scoperti dal raccoglitore. Per informazioni sui requisiti per l'utente IAM, consulta. [Fase 1: Creare un utente IAM per Agentless Collector](#)
 - a. Per la AWSchiave di accesso, inserisci la chiave di accesso dell'utente IAM dell'AWSaccount che stai specificando come account di destinazione.
 - b. Per la AWSchiave segreta, inserisci la chiave segreta dell'AWSaccount utente IAM che stai specificando come account di destinazione.
 - c. (Facoltativo) Se la tua rete richiede l'uso di un proxy per accedereAWS, inserisci l'host proxy, la porta proxy e, facoltativamente, le credenziali necessarie per l'autenticazione con il tuo server proxy esistente.

3. In Password Agentless Collector, impostate una password da utilizzare per autenticare l'accesso ad Agentless Collector.
 - Le password fanno distinzione tra maiuscole e minuscole
 - Le password devono avere una lunghezza compresa tra 8 e 64 caratteri
 - Le password devono contenere almeno un carattere per ognuna delle quattro categorie seguenti:
 - Lettere minuscole (a-z)
 - Lettere maiuscole (A-Z)
 - Numeri (0-9)
 - Caratteri non alfanumerici (@\$! #%*? &)
 - Le password non possono contenere caratteri speciali diversi dai seguenti: @\$! #%*? &
 - a. Per la password di Agentless Collector, inserisci una password da utilizzare per autenticare l'accesso al raccoglitore.
 - b. Per reinserire la password di Agentless Collector, per la verifica, inserisci nuovamente la password.
4. In Altre impostazioni, leggi il Contratto di licenza. Se accetti di accettarlo, seleziona la casella di controllo.
5. Per abilitare gli aggiornamenti automatici per Agentless Collector, in Altre impostazioni, seleziona Agentless Collector automaticamente. Se non selezioni questa casella di controllo, dovrai aggiornare manualmente Agentless Collector come descritto in [Aggiornamento manuale di Agentless Collector](#)
6. Scegli Salva configurazioni.

I seguenti argomenti descrivono le attività opzionali di configurazione del collettore.

Attività di configurazione opzionali

- [\(Facoltativo\) Configurare un indirizzo IP statico per la macchina virtuale Agentless Collector](#)
- [\(Facoltativo\) Reimposta la macchina virtuale Agentless Collector all'utilizzo di DHCP](#)
- [\(Facoltativo\) Configurare il protocollo di autenticazione Kerberos](#)

(Facoltativo) Configurare un indirizzo IP statico per la macchina virtuale Agentless Collector

I passaggi seguenti descrivono come configurare un indirizzo IP statico per la macchina virtuale Application Discovery Service Agentless Collector (Agentless Collector). Quando viene installata per la prima volta, la macchina virtuale di raccolta è configurata per utilizzare il Dynamic Host Configuration Protocol (DHCP).

Note

L'Agentless Collector supporta IPv4. Non supporta IPv6.

Per configurare un indirizzo IP statico per la macchina virtuale del collettore

1. Raccogli le seguenti informazioni di rete da VMware vCenter:
 - Indirizzo IP statico: un indirizzo IP non firmato nella sottorete. Ad esempio, 192.168.1.138.
 - Maschera di rete: è possibile ottenerla controllando l'impostazione dell'indirizzo IP dell'host VMware vCenter che ospita la macchina virtuale del collettore. Ad esempio, 255.255.255.0.
 - Gateway predefinito: è possibile ottenerlo controllando l'impostazione dell'indirizzo IP dell'host VMware vCenter che ospita la macchina virtuale del collettore. Ad esempio, 192.168.1.1.
 - DNS primario: è possibile ottenerlo controllando l'impostazione dell'indirizzo IP dell'host VMware vCenter che ospita la macchina virtuale del collettore. Ad esempio, 192.168.1.1.
 - (Facoltativo) DNS secondario
 - (Facoltativo) Nome di dominio locale: consente al raccogliatore di raggiungere l'URL dell'host vCenter senza il nome di dominio.
2. Apri la console VM del raccogliatore e accedi **ec2-user** utilizzando la password, **collector** come mostrato nell'esempio seguente.

```
username: ec2-user  
password: collector
```

3. Disabilita l'interfaccia di rete, inserendo il seguente comando nel terminale remoto.

```
sudo /sbin/ifdown eth0
```

4. Aggiorna la configurazione eth0 dell'interfaccia usando i seguenti passaggi.

a. Aprire ifcfg-eth0 nell'editor vi usando il seguente comando.

```
sudo vi /etc/sysconfig/network-scripts/ifcfg-eth0
```

b. Aggiornate i valori dell'interfaccia, come mostrato nell'esempio seguente, con le informazioni raccolte nel passaggio Raccogli informazioni di rete.

```
DEVICE=eth0
BOOTPROTO=static
ONBOOT=yes
IPADDR=static-ip-value
NETMASK=netmask-value
GATEWAY=gateway-value
TYPE=Ethernet
USERCTL=yes
PEERDNS=no
RES_OPTIONS="timeout:2 attempts:5"
```

5. Aggiorna il Domain Name System (DNS) utilizzando i seguenti passaggi.

a. Aprire il resolv.conf file in vi utilizzando il seguente comando.

```
sudo vi /etc/resolv.conf
```

b. Aggiornate il resolv.conf file in vi utilizzando il seguente comando.

```
search localdomain-name
options timeout:2 attempts:5
nameserver dnsserver-value
```

L'esempio seguente mostra un resolv.conf file modificato.

```
search vsphere.local
options timeout:2 attempts:5
nameserver 192.168.1.1
```

6. Abilita l'interfaccia di rete, inserendo il seguente comando.


```
sudo /sbin/ifup eth0
```

7. Riavviare la macchina virtuale come illustrato nell'esempio seguente.

```
sudo reboot
```

8. Verifica le impostazioni di rete utilizzando i seguenti passaggi.

- a. Verifica se l'indirizzo IP è configurato correttamente, inserendo i seguenti comandi.

```
ifconfig  
  
ip addr show
```

- b. Verifica che il gateway sia stato aggiunto correttamente, inserendo il seguente comando.

```
route -n
```

L'output dovrebbe essere simile all'esempio seguente.

```
Kernel IP routing table  
Destination      Gateway          Genmask         Flags Metric Ref    Use Iface  
0.0.0.0          192.168.1.1    0.0.0.0        UG    0      0      0 eth0  
172.17.0.0       0.0.0.0        255.255.0.0    U    0      0      0 docker0  
192.168.1.0      0.0.0.0        255.255.255.0  U    0      0      0
```

- c. Verifica di poter eseguire il ping di un URL pubblico immettendo il seguente comando.

```
ping www.google.com
```

- d. Verificare di poter eseguire il ping dell'indirizzo IP o del nome host di vCenter come mostrato nell'esempio seguente.

```
ping vcenter-host-url
```

(Facoltativo) Reimposta la macchina virtuale Agentless Collector all'utilizzo di DHCP

I passaggi seguenti descrivono come riconfigurare la macchina virtuale Agentless Collector per utilizzare DHCP.

Per configurare la VM collector per l'utilizzo di DHCP

1. Disabilita l'interfaccia di rete, inserendo il seguente comando nel terminale remoto.

```
sudo /sbin/ifdown eth0
```

2. Aggiorna la configurazione di rete utilizzando i seguenti passaggi.

- a. Aprire il `ifcfg-eth0` file nell'editor vi utilizzando il seguente comando.

```
sudo /sbin/ifdown eth0
```

- b. Aggiornate i valori nel `ifcfg-eth0` file come illustrato nell'esempio seguente.

```
DEVICE=eth0
BOOTPROTO=dhcp
ONBOOT=yes
TYPE=Ethernet
USERCTL=yes
PEERDNS=yes
DHCPV6C=yes
DHCPV6C_OPTIONS=-nw
PERSISTENT_DHCLIENT=yes
RES_OPTIONS="timeout:2 attempts:5"
```

3. Reimposta l'impostazione DNS, inserendo il seguente comando.

```
echo "" | sudo tee /etc/resolv.conf
```

4. Abilita l'interfaccia di rete, inserendo il seguente comando.

```
sudo /sbin/ifup eth0
```

5. Riavviare la macchina virtuale del collettore come illustrato nell'esempio seguente.

```
sudo reboot
```

(Facoltativo) Configurare il protocollo di autenticazione Kerberos

Se il server del sistema operativo supporta il protocollo di autenticazione Kerberos, è possibile utilizzare questo protocollo per connettersi al server. A tale scopo, è necessario configurare la macchina virtuale Application Discovery Service Agentless Collector.

I passaggi seguenti descrivono come configurare il protocollo di autenticazione Kerberos sulla macchina virtuale Application Discovery Service Agentless Collector.

Per configurare il protocollo di autenticazione Kerberos sulla tua macchina virtuale collector

1. Apri la console VM del raccogliatore e accedi **ec2-user** utilizzando la password, come mostrato nell'**collectore** esempio seguente.

```
username: ec2-user
password: collector
```

2. Apri il file `krb5.conf` di configurazione nella cartella `/etc`. A tale scopo, è possibile utilizzare il seguente esempio di codice.

```
cd /etc
sudo nano krb5.conf
```

3. Aggiornate il file di `krb5.conf` configurazione con le seguenti informazioni.

```
[libdefaults]
    forwardable = true
    dns_lookup_realm = true
    dns_lookup_kdc = true
    ticket_lifetime = 24h
    renew_lifetime = 7d
    default_realm = default_Kerberos_realm

[realms]
    default_Kerberos_realm = {
        kdc = KDC_hostname
        server_name = server_hostname
        default_domain = domain_to_expand_hostnames
    }

[domain_realm]
    .domain_name = default_Kerberos_realm
```

```
domain_name = default_Kerberos_realm
```

Salvare il file e uscire dall'editor di testo.

4. Riavviare la macchina virtuale del collettore come illustrato nell'esempio seguente.

```
sudo reboot
```

Fase 6: Configurare i moduli di raccolta dati Agentless Collector

Nella pagina dashboard della console di Application Discovery Service Agentless Collector (Agentless Collector) in Raccolta dati puoi configurare il modulo di raccolta dati per raccogliere dati di inventario, profilo e utilizzo dai tuoi server.

Agentless Collector attualmente supporta la raccolta di dati da macchine virtuali VMware e da server di database e analisi. I moduli futuri supporteranno la raccolta da piattaforme di virtualizzazione aggiuntive e la raccolta a livello di sistema operativo.

Argomenti

- [Modulo di raccolta dati VMware vCenter Agentless Collector](#)
- [Modulo di raccolta dati di analisi e database](#)

Modulo di raccolta dati VMware vCenter Agentless Collector

Questa sezione descrive il modulo di raccolta dati VMware vCenter di Application Discovery Service Agentless Collector (Agentless Collector), utilizzato per raccogliere i dati di inventario, profilo e utilizzo dei server dalle macchine virtuali VMware.

Argomenti

- [Come configurare il modulo di raccolta dati Agentless Collector per VMware vCenter](#)
- [Dettagli della raccolta dei dati VMware](#)
- [Controlla l'ambito della raccolta dei dati vCenter](#)

Come configurare il modulo di raccolta dati Agentless Collector per VMware vCenter

Questa sezione descrive come configurare il modulo di raccolta dati Agentless Collector VMware vCenter per raccogliere i dati di inventario, profilo e utilizzo dei server dalle macchine virtuali VMware.

Note

Prima di iniziare la configurazione di vCenter, assicurati di poter fornire le credenziali di vCenter con le autorizzazioni di lettura e visualizzazione impostate per il gruppo System.

Per configurare il modulo di raccolta dati VMware vCenter

1. Nella pagina della dashboard di Agentless Collector, in Raccolta dati, scegli Configurazione nella sezione VMware vCenter.
2. Nella pagina Configura la raccolta dati di VMware vCenter, esegui le seguenti operazioni:
 - a. Sotto le credenziali vCenter:
 - i. Per vCenter URL/IP, immettere l'indirizzo IP dell'host VMware vCenter Server.
 - ii. Per nome utente vCenter, inserisci il nome di un utente locale o di dominio che il raccoglitore utilizza per comunicare con vCenter. Per gli utenti del dominio, usa il modulo dominio\nome utente o nome utente@dominio.
 - iii. Per vCenter Password (Password vCenter), digita la password dell'utente locale o del dominio.
 - b. In Preferenze di raccolta dati:
 - Per avviare automaticamente la raccolta dei dati subito dopo una corretta configurazione, selezionare Avvia raccolta dati automaticamente.
 - c. Scegliere Set up (Configura).

Successivamente, verrà visualizzata la pagina dei dettagli della raccolta dati VMware, descritta nel prossimo argomento.

Dettagli della raccolta dei dati VMware

La pagina dei dettagli della raccolta dati VMware mostra i dettagli sul vCenter in cui è stato configurato [Come configurare il modulo di raccolta dati Agentless Collector per VMware vCenter](#).

In Server vCenter scoperti, il vCenter configurato è elencato con le seguenti informazioni sul vCenter:

- L'indirizzo vCenter.
- Il numero di server nel vCenter.

- Lo stato dei dati.
- Quanto tempo è passato dall'ultimo aggiornamento.

Scegliere Rimuovi server vCenter per rimuovere il server vCenter visualizzato e tornare alla pagina Configura la raccolta dati di VMware vCenter.

Se non hai scelto di avviare la raccolta dati automaticamente, puoi iniziare la raccolta dei dati utilizzando il pulsante Avvia raccolta dati in questa pagina. Dopo l'avvio della raccolta dei dati, il pulsante di avvio cambia in Interrompi raccolta dati.

Se la colonna Stato della raccolta mostra Raccolta, la raccolta dei dati è iniziata.

I dati raccolti vengono visualizzati nella AWS Migration Hub console. Se stai raccogliendo dati per un inventario di server VMware vCenter, puoi accedere ai dati che appaiono nella console circa 15 minuti dopo l'attivazione della raccolta dei dati.

Puoi scegliere Visualizza server in Migration Hub in questa pagina per aprire la console di Migration Hub, se l'accesso a Internet non è bloccato. Che tu scelga o meno questo pulsante, per informazioni su come accedere alla console di Migration Hub, consulta [Fase 7: Visualizzazione dei dati raccolti](#).

Di seguito sono riportate le linee guida per la durata consigliata della raccolta dei dati in base alle attività di pianificazione della migrazione:

- TCO (costo totale di proprietà): da 2 a 4 settimane
- Pianificazione della migrazione: da 2 a 6 settimane

Controlla l'ambito della raccolta dei dati vCenter

L'utente vCenter richiede autorizzazioni di sola lettura su ogni host o macchina virtuale ESX per l'inventario utilizzando Application Discovery Service. Utilizzando le impostazioni di autorizzazione, puoi controllare quali host e VM sono inclusi nella raccolta dati. È possibile consentire l'inventario di tutti gli host e le VM del vCenter corrente o concedere autorizzazioni su caso-by-case base regolare.

Note

Come best practice di sicurezza, consigliamo di non concedere autorizzazioni aggiuntive e non necessarie all'utente vCenter di Application Discovery Service.

Nelle procedure seguenti sono descritti gli scenari di configurazione ordinati a partire dal meno granulare al più granulare. Queste procedure sono per vSphere Client v6.7.0.2. Le procedure per le altre versioni del client potrebbero essere diverse, a seconda della versione del client vSphere in uso.

Per individuare i dati relativi a tutti gli host e le VM ESX nel vCenter corrente

1. Nel tuo client VMware vSphere, seleziona vCenter, quindi seleziona Hosts and Clusters o VMs and Templates.
2. Scegli una risorsa del datacenter, quindi scegli Autorizzazioni.
3. Scegli l'utente vCenter e quindi scegli il simbolo per aggiungere, modificare o rimuovere un ruolo utente.
4. Scegliete Sola lettura dal menu Ruolo.
5. Scegliete Propaga ai bambini, quindi scegliete OK.

Per individuare i dati relativi a un host ESX specifico e tutti i suoi oggetti figli

1. Nel tuo client VMware vSphere, seleziona vCenter, quindi seleziona Hosts and Clusters o VMs and Templates.
2. Scegli Related Objects, Hosts.
3. Facendo clic con il pulsante destro del mouse, apri il menu contestuale del nome host e scegli All vCenter Actions, Add Permission.
4. Sotto Add Permission, aggiungi l'utente vCenter all'host. Per Assigned Role, scegli Read-only.
5. Seleziona Propagate to children, OK.

Per scoprire i dati relativi a un host ESX specifico o a una macchina virtuale secondaria

1. Nel tuo client VMware vSphere, seleziona vCenter, quindi seleziona Hosts and Clusters o VMs and Templates.
2. Scegli Related Objects.
3. Seleziona Hosts (che mostra un elenco di host ESX noti a vCenter) o Virtual Machines (che mostra un elenco di VM in tutti gli host ESX).
4. Facendo clic con il pulsante destro del mouse, apri il menu contestuale del nome host o VM e scegli All vCenter Actions, Add Permission.
5. Sotto Add Permission, aggiungi l'utente vCenter all'host o alla VM. Per Assigned Role, scegli Read-only.

6. Scegli OK.

Note

Se si sceglie Propaga ai figli, è comunque possibile rimuovere l'autorizzazione di sola lettura dagli host e dalle VM ESX su caso-by-case base regolare. Quest'opzione non ha effetto sulle autorizzazioni ereditate applicabili ad altri host ESX e VM.

Modulo di raccolta dati di analisi e database

In questa sezione viene descritto come impostare, configurare e utilizzare un modulo di raccolta dati di database e analisi. Puoi utilizzare questo modulo di raccolta dati per connetterti al tuo ambiente di dati e raccogliere metadati e metriche delle prestazioni dai database e dai server di analisi locali. Per informazioni sulle metriche che è possibile raccogliere con questo modulo, consulta [Dati raccolti dal database Agentless Collector e dal modulo di raccolta dati di analisi](#).

Ad alto livello, quando si utilizza il modulo di raccolta dei dati di database e analisi, si eseguono i seguenti passaggi.

1. Completa i passaggi prerequisiti, configura il tuo utente IAM e crea il raccogliitore di AWS DMS dati.
2. Configura l'inoltro dei dati per assicurarti che il tuo modulo di raccolta dati possa inviare i metadati raccolti e le metriche delle prestazioni a AWS.
3. Aggiungi i tuoi server LDAP e usali per scoprire i server del sistema operativo nel tuo ambiente di dati. In alternativa, aggiungi i server del tuo sistema operativo manualmente o usa il [Modulo di raccolta dei dati VMware](#).
4. Configura le credenziali di connessione ai server del tuo sistema operativo e poi usale per scoprire i server del database.
5. Configura le credenziali di connessione al database e ai server di analisi, quindi esegui la raccolta dei dati. Per ulteriori informazioni, consulta [Raccolta di dati di analisi e database](#).
6. Visualizza i dati raccolti nella AWS DMS console e utilizzali per generare consigli mirati per una migrazione verso il Cloud AWS. Per ulteriori informazioni, consulta [Raccolta di dati di analisi e database](#).

Argomenti

- [Sistema operativo, database e server di analisi supportati](#)

- [Crea il raccogliatore diAWS DMS dati](#)
- [Configurazione dell'inoltro dei dati](#)
- [Aggiungi i tuoi server LDAP e OS](#)
- [Scopri i tuoi server di database](#)

Sistema operativo, database e server di analisi supportati

Il modulo di raccolta dati di database e analisi in Agentless Collector supporta i server LDAP di Microsoft Active Directory.

Questo modulo di raccolta dati supporta i seguenti server OS.

- Amazon Linux 2
- CentOS Linux versione 6 e successive
- Debian versione 10 e successive
- Red Hat Enterprise Linux versione 7 e successive
- SUSE Linux Enterprise Server versione 12 e successive
- Ubuntu versione 16.01 e successive
- Windows Server 2012 e successive
- Windows XP e versioni successive

Inoltre, il modulo di raccolta dati di database e analisi supporta i seguenti server di database.

- Microsoft SQL Server versione 2012 e successive al 2019
- MySQL versione 5.6 e successive alla 8
- Oracle versione 11g Release 2 e fino a 12c, 19c e 21c
- PostgreSQL versione 9.6 e successive alla 13

Crea il raccogliatore diAWS DMS dati

Il modulo di raccolta dei dati di database e analisi utilizza un raccogliatore diAWS DMS dati per interagire con laAWS DMS console. È possibile visualizzare i dati raccolti nellaAWS DMS console o utilizzarli per determinare il motore diAWS destinazione delle dimensioni corrette. Per ulteriori informazioni, vedere [Utilizzo della funzione Target Recommendations diAWS DMS Fleet Advisor](#).

Prima di creare un raccogliitore di AWS DMS dati, crea un ruolo IAM che il tuo raccogliitore di AWS DMS dati utilizzi per accedere al tuo bucket Amazon S3. Hai creato questo bucket Amazon S3 quando hai completato i prerequisiti in [Prerequisiti per Agentless Collector](#).

Per creare un ruolo IAM affinché il tuo raccogliitore AWS DMS dati possa accedere a Amazon S3

1. Accedi alla AWS Management Console e apri la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel riquadro di navigazione, scegli Ruoli, quindi scegli Crea ruolo.
3. Nella pagina Seleziona entità attendibile, per Tipo di entità attendibile, scegli AWS Servizio. Per Casi d'uso per altri AWS servizi, scegli DMS.
4. Seleziona la casella di controllo DMS e scegli Avanti.
5. Nella pagina Aggiungi autorizzazioni, scegli FleetAdvisorS3Policy che hai creato in precedenza. Seleziona Successivo.
6. Nella pagina Nome, revisione e creazione, inserisci **FleetAdvisorS3Role** il nome del ruolo, quindi scegli Crea ruolo.
7. Apri il ruolo che hai creato e scegli la scheda Relazioni di fiducia. Seleziona Edit trust policy (Modifica policy di attendibilità).
8. Nella pagina Modifica politica di fiducia, incolla il seguente JSON nell'editor, sostituendo il codice esistente.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "",
    "Effect": "Allow",
    "Principal": {
      "Service": [
        "dms.amazonaws.com",
        "dms-fleet-advisor.amazonaws.com"
      ]
    },
    "Action": "sts:AssumeRole"
  }]
}
```

9. Scegli Update policy (Aggiorna policy).

Ora, crea un raccoglitore di dati nellaAWS DMS console.

Per creare un raccoglitore diAWS DMS dati

1. Accedere aAWS Management Console e aprire laAWS DMS console all'[indirizzo https://console.aws.amazon.com/dms/v2/](https://console.aws.amazon.com/dms/v2/).
2. Scegli quellaRegione AWS che hai impostato come regione di origine del tuo Migration Hub. Per ulteriori informazioni, consulta [Accedi a Migration Hub e scegli una regione d'origine](#).
3. Nel riquadro di navigazione, seleziona Raccoglitori dati in Discover. Si apre la pagina Raccoglitori di dati.
4. Scegli Crea raccoglitore di dati. Viene visualizzata la pagina Crea raccoglitore di dati.
5. In Nome nella sezione Configurazione generale, inserisci il nome del tuo raccoglitore di dati.
6. Nella sezione Connettività, scegli Browse S3. Scegli il bucket Amazon S3 creato in precedenza dall'elenco.
7. Per il ruolo IAM, scegliFleetAdvisorS3Role quello che hai creato prima.
8. Scegli Crea raccoglitore di dati.

Configurazione dell'inoltro dei dati

Dopo aver creato leAWS risorse necessarie, configura l'inoltro dei dati dal database e dal modulo di raccolta dei dati di analisi al tuoAWS DMS raccoglitore.

Per configurare l'inoltro dei dati

1. Apri la console Agentless Collector. Per ulteriori informazioni, consulta [Fase 4: Accedere alla console Collector](#).
2. Scegli Visualizza database e raccoglitore di analisi.
3. Nella pagina Dashboard, scegli Configura l'inoltro dei dati nella sezione Inoltro dei dati.
4. Per Regione AWS l'ID della chiave di accesso IAM e la chiave di accesso segreta IAM, Agentless Collector utilizza i valori configurati in precedenza. Per ulteriori informazioni, consultare [Accedi a Migration Hub e scegli una regione d'origine](#) e [Fase 1: Creare un utente IAM](#).
5. Per Connected DMS data collector, scegli il raccoglitore di dati che hai creato nellaAWS DMS console.
6. Seleziona Salva.

Dopo aver configurato l'inoltro dei dati, controlla la sezione Inoltro dei dati nella pagina Dashboard. Assicurati che il modulo di raccolta dei dati di database e analisi mostri



for Access to DMS e Access to S3.

Aggiungi i tuoi server LDAP e OS

Il modulo di raccolta dei dati di database e analisi utilizza LDAP in Microsoft Active Directory per raccogliere informazioni sul sistema operativo, sul database e sui server di analisi della rete. Lightweight Directory Access Protocol (LDAP) è un protocollo applicativo standard aperto. È possibile utilizzare questo protocollo per accedere e gestire i servizi di informazione sulle directory distribuiti sulla rete IP.

Puoi aggiungere un server LDAP esistente al tuo database e al modulo di raccolta dei dati di analisi per scoprire automaticamente i server del sistema operativo nella tua rete. Se non si utilizza LDAP, è possibile aggiungere i server del sistema operativo manualmente.

Per aggiungere un server LDAP al modulo di raccolta dei dati di database e analisi

1. Apri la console Agentless Collector. Per ulteriori informazioni, consulta [Fase 4: Accedere alla console Collector](#).
2. Scegli Visualizza database e collettore di analisi, quindi scegli Server LDAP in Discovery nel riquadro di navigazione.
3. Scegli Aggiungi server LDAP. Viene visualizzata la pagina Aggiungi server LDAP.
4. In Hostname, inserisci il nome host del tuo server LDAP.
5. In Porta, immettere il numero di porta utilizzato per le richieste LDAP.
6. In Nome utente, immettere il nome utente utilizzato per connettersi al server LDAP.
7. In Password, immettere la password utilizzata per la connessione al server LDAP.
8. (Facoltativo) Scegli Verifica connessione per assicurarti di aver aggiunto correttamente le credenziali del server LDAP. In alternativa, puoi verificare le credenziali di connessione al server LDAP in un secondo momento, dall'elenco nella pagina dei server LDAP.
9. Scegli Aggiungi server LDAP.
10. Nella pagina dei server LDAP, seleziona il tuo server LDAP dall'elenco e scegli Discover OS servers.

⚠ Important

Per l'individuazione del sistema operativo, il modulo di raccolta dati necessita di credenziali affinché il server di dominio esegua le richieste utilizzando il protocollo LDAP.

Il modulo di raccolta dei dati di database e analisi si connette al server LDAP e rileva i server del sistema operativo. Dopo che il modulo di raccolta dati ha completato l'individuazione dei server del sistema operativo, è possibile visualizzare l'elenco dei server del sistema operativo rilevati scegliendo **Visualizza server del sistema operativo**.

In alternativa, è possibile aggiungere i server del sistema operativo manualmente o CSV) con valori separati dalla virgola. Inoltre, puoi utilizzare il modulo di raccolta dati VMware vCenter Agentless Collector per scoprire i server del tuo sistema operativo. Per ulteriori informazioni, consulta [Modulo di raccolta dei dati VMware](#).

Per aggiungere un server del sistema operativo al database e al modulo di raccolta dei dati di analisi

1. Nella pagina del raccoglitore di database e analisi, scegli **Server del sistema operativo in Discovery** nel riquadro di navigazione.
2. Scegli **Aggiungi server OS**. Viene visualizzata la pagina **Aggiungi server OS**.
3. Fornisci le credenziali del server del sistema operativo.
 - a. Per il tipo di sistema operativo, scegli il sistema operativo del tuo server.
 - b. In **Hostname/IP**, inserisci il nome host o l'indirizzo IP del server del tuo sistema operativo.
 - c. In **Porta**, immettere il numero di porta utilizzato per le query remote.
 - d. Per **Tipo di autenticazione**, scegli il tipo di autenticazione utilizzato dal server del sistema operativo.
 - e. In **Nome utente**, immettere il nome utente utilizzato per connettersi al server del sistema operativo.
 - f. In **Password**, immettere la password utilizzata per connettersi al server del sistema operativo.
 - g. Scegli **Verifica** per assicurarti di aver aggiunto correttamente le credenziali del server del sistema operativo.
4. (Facoltativo) **Aggiungi più server del sistema operativo da un file CSV**.
 - a. Scegli **Importa server OS in blocco da CSV**.

- b. Scegli Scarica modello per salvare un file CSV che include un modello che puoi personalizzare.
- c. Inserisci le credenziali di connessione per i server del tuo sistema operativo nel file in base al modello. L'esempio seguente mostra come fornire le credenziali di connessione al server del sistema operativo in un file CSV.

```
OS type,Hostname/IP,Port,Authentication type,Username,Password
Linux,192.0.2.0,22,Key-based authentication,USER-EXAMPLE,ANPAJ2UCCR6DPCEXAMPLE
Windows,203.0.113.0,,NTLM,USER2-EXAMPLE,AKIAIOSFODNN7EXAMPLE
```

Salva il file CSV dopo aver aggiunto le credenziali per tutti i server del sistema operativo.

- d. Scegli Sfoglia, quindi scegli il tuo file CSV.
5. Scegli Aggiungi server OS.
 6. Dopo aver aggiunto le credenziali per tutti i server del sistema operativo, seleziona i server del sistema operativo e scegli Discover database servers.

Scopri i tuoi server di database

Per l'individuazione dei database, crea utenti per i database di origine con le autorizzazioni minime richieste per il modulo di raccolta dati. Per ulteriori informazioni, vedere [Creazione di utenti del database per AWS DMS Fleet Advisor](#) nella Guida per l'AWS DMS utente.

Per scoprire i database in esecuzione sui server OS aggiunti in precedenza, il modulo di raccolta dati richiede l'accesso al sistema operativo e ai server del database. Assicurati che il database sia accessibile dalla porta specificata nelle impostazioni di connessione. Quindi, attiva l'autenticazione remota sul server del database. Inoltre, fornisci al tuo modulo di raccolta dati le seguenti autorizzazioni.

Per scoprire i server di database in Windows

1. Fornisci credenziali con sovvenzioni per eseguire interrogazioni su Windows Management Instrumentation (WMI) e WMI Query Language (WQL) e leggere il registro.
2. Aggiungi l'utente Windows specificato nelle credenziali di connessione del server del sistema operativo ai seguenti gruppi: utenti COM distribuiti, utenti del registro delle prestazioni, utenti del monitoraggio delle prestazioni e lettori del registro degli eventi. A tale scopo, utilizza il seguente esempio di codice.

```
net localgroup "Distributed COM Users" username /ADD
net localgroup "Performance Log Users" username /ADD
net localgroup "Performance Monitor Users" username /ADD
net localgroup "Event Log Readers" username /ADD
```

Nell'esempio precedente, sostituire *username* con il nome dell'utente Windows specificato nelle credenziali di connessione al server del sistema operativo.

3. Concedi le autorizzazioni necessarie per l'utente Windows specificato nelle credenziali di connessione al server del sistema operativo.
 - Per le proprietà di gestione e strumentazione di Windows, scegli Avvio locale e Attivazione remota.
 - Per WMI Control, scegli le autorizzazioni Execute Methods, Abilita account, Remote Enable e Read Security per iWMI namespaceCIMV2DEFAULTStandartCimv2,, e.
 - Per il plug-in WMI, `winrm configsdcl default` esegui e scegli Leggi ed esegui.
4. Configura il tuo host Windows utilizzando il seguente esempio di codice.

```
netsh advfirewall firewall add rule name="Open Ports for WinRM incoming traffic"
  dir=in action=allow protocol=TCP localport=5985, 5986 # Opens ports for WinRM
netsh advfirewall firewall add rule name="All ICMP V4" protocol=icmpv4:any,any
  dir=in action=allow # Allows ICMP traffic

Enable-PSRemoting -Force # Enables WinRM
Set-Service WinRM -StartMode Automatic # Allows WinRM service to run on host
  startup
Set-Item WSMan:\localhost\Client\TrustedHosts -Value {IP} -Force # Sets the
  specific IP from which the access to WinRM is allowed

winrm set winrm/config/service '{@Negotiation="true"}' # Allow Negotiate auth usage
winrm set winrm/config/service '{@AllowUnencrypted="true"}' # Allow unencrypted
  connection
```

Per scoprire i server di database in Linux

1. Fornisci l'accesso sudo `ainetstat` comandiss and.

Il seguente esempio di codice concede a sudo l'accesso `ainetstat` comandiss and.

```
sudo bash -c "cat << EOF >> /etc/sudoers.d/username
username ALL=(ALL) NOPASSWD: /usr/bin/ss
username ALL=(ALL) NOPASSWD: /usr/bin/netstat
EOF"
```

Nell'esempio precedente, sostituire *username* con il nome dell'utente Linux specificato nelle credenziali di connessione al server del sistema operativo.

L'esempio precedente utilizza il `/usr/bin/` percorso de `netstat` comand `ss` and. Questo percorso potrebbe essere diverso nel tuo ambiente. Per determinare il percorso de `netstat` comand `ss` and, esegui `which netstat` i comandi `which ss` and.

2. Configura i tuoi server Linux per consentire l'esecuzione di script SSH remoti e consentire il traffico ICMP (Internet Control Message Protocol).

Per iniziare la scoperta dei server del tuo database

1. Nella pagina del raccogliitore di database e analisi, scegli Server del sistema operativo in Discovery nel riquadro di navigazione.
2. Seleziona i server del sistema operativo che includono il database e i server di analisi, quindi scegli Verifica connessione nel menu Azioni.
3. Per i server con lo stato Connettività non riuscita, modificare le credenziali di connessione.
 - a. Seleziona uno o più server quando hanno credenziali identiche, quindi scegli Modifica dal menu Azioni. Viene visualizzata la pagina Modifica server OS.
 - b. In Porta, immettere il numero di porta utilizzato per le query remote.
 - c. Per Tipo di autenticazione, scegli il tipo di autenticazione utilizzato dal server del sistema operativo.
 - d. In Nome utente, immettere il nome utente utilizzato per connettersi al server del sistema operativo.
 - e. In Password, immettere la password utilizzata per connettersi al server del sistema operativo.
 - f. Scegli Verifica connessione per assicurarti di aver aggiornato correttamente le credenziali del server del sistema operativo. Quindi, scegli Salva.
4. Dopo aver aggiornato le credenziali per tutti i server del sistema operativo, seleziona i server del sistema operativo e scegli Discover database servers.

Il modulo di raccolta dei dati di database e analisi si connette ai server del sistema operativo e rileva i server di database e analisi supportati. Dopo che il modulo di raccolta dati ha completato l'individuazione, è possibile visualizzare l'elenco dei database e dei server di analisi rilevati scegliendo **Visualizza server di database**.

In alternativa, puoi aggiungere il database e i server di analisi all'inventario manualmente. Inoltre, puoi importare l'elenco dei server da un file CSV. Se hai già aggiunto tutti i database e i server di analisi all'inventario.

Per aggiungere manualmente un database o un server di analisi

1. Nella pagina del raccoglitore di database e analisi, scegli **Raccolta dati** nel riquadro di navigazione.
2. Scegli **Aggiungi server di database**. Viene visualizzata la pagina **Aggiungi server di database**.
3. Fornisci le credenziali del server del database.
 - a. Per **Motore di database**, scegli il motore di database del tuo server. Per ulteriori informazioni, consulta [Sistema operativo, database e server di analisi supportati](#).
 - b. In **Hostname/IP**, inserisci il nome host o l'indirizzo IP del tuo database o del server di analisi.
 - c. In **Porta**, inserisci la porta in cui viene eseguito il server.
 - d. Per **Tipo di autenticazione**, scegli il tipo di autenticazione utilizzato dal database o dal server di analisi.
 - e. In **Nome utente**, immettere il nome utente utilizzato per connettersi al server.
 - f. In **Password**, immettere la password utilizzata per la connessione al server.
 - g. Scegli **Verifica** per assicurarti di aver aggiunto correttamente le credenziali del database o del server di analisi.
4. (Facoltativo) **Aggiungi più server da un file CSV**.
 - a. Scegli **Server di database di importazione in blocco da CSV**.
 - b. Scegli **Scarica modello** per salvare un file CSV che include un modello che puoi personalizzare.
 - c. Inserisci le credenziali di connessione per il tuo database e i server di analisi nel file in base al modello. L'esempio seguente mostra come fornire credenziali di connessione al database o CSV.

```
Database engine,Hostname/IP,Port,Authentication type,Username,Password,Oracle
service name,Database,Allow public key retrieval,Use SSL,Trust server
certificate
Oracle,192.0.2.1,1521,Login/Password authentication,USER-
EXAMPLE,AKIAI44QH8DHBEXAMPLE,orcl,,,,
PostgreSQL,198.51.100.1,1533,Login/Password authentication,USER2-
EXAMPLE,bPxRfiCYEXAMPLE,,postgre,,TRUE,
MSSQL,203.0.113.1,1433,Login/Password authentication,USER3-
EXAMPLE,h3yCo8nvnBEXAMPLE,,,,,TRUE
MySQL,2001:db8:4006:812:ffff:200e,8080,Login/Password authentication,USER4-
EXAMPLE,APKAEIVFHP46CEXAMPLE,,mysql,TRUE,TRUE,
```

Salva il file CSV dopo aver aggiunto le credenziali per tutti i database e i server di analisi.

- d. Scegli Sfoglia, quindi scegli il tuo file CSV.
5. Scegli Aggiungi server di database.
6. Dopo aver aggiunto le credenziali per tutti i server del sistema operativo, seleziona i server del sistema operativo e scegli Discover database servers.

Dopo aver aggiunto tutti i database e i server di analisi nel modulo di raccolta dati, aggiungili all'inventario. Il modulo di raccolta dei dati di database e analisi può connettersi ai server dall'inventario e raccogliere metadati e metriche delle prestazioni.

Per aggiungere il database e i server di analisi all'inventario

1. Nella pagina del raccogliitore di database e analisi, scegli Server di database in Discovery nel riquadro di navigazione.
2. Seleziona il database e i server di analisi per i quali desideri raccogliere metadati e metriche delle prestazioni.
3. Scegli Aggiungi all'inventario.

Dopo aver aggiunto tutti i server di database e analisi al tuo inventario, puoi iniziare a raccogliere metadati e metriche delle prestazioni. Per ulteriori informazioni, consulta [Raccolta di dati di analisi e database](#).

Fase 7: Visualizzazione dei dati raccolti

È possibile visualizzare i dati raccolti dall'Application Discovery Service Agentless Collector (Agentless Collector) nella console Migration Hub. È possibile visualizzare le metriche raccolte per i server di database e analisi nella console. AWS DMS

Per visualizzare i dati rilevati dal modulo di raccolta dati VMware vCenter Agentless Collector

1. Accedere AWS Management Console e aprire la console Migration Hub all'[indirizzo https://console.aws.amazon.com/migrationhub/](https://console.aws.amazon.com/migrationhub/). Per questa attività, ti consigliamo di utilizzare un account utente IAM diverso da quello dell'utente IAM che hai creato per configurare e accedere ad Agentless Collector.
2. Nel pannello di navigazione della console Migration Hub, in Discover, scegli Server.
3. Per visualizzare i dettagli su un server, scegli il nome host del server dalla colonna Informazioni sul server. La pagina dei dettagli del server mostra informazioni sul server, come nome host, indirizzo IP, metriche delle prestazioni e così via.

Per visualizzare i dati rilevati dal database e dal modulo di raccolta dei dati di analisi

1. Accedi AWS Management Console e apri la AWS DMS console all'[indirizzo https://console.aws.amazon.com/dms/v2/](https://console.aws.amazon.com/dms/v2/).
2. Scegli Inventario in Scopri. Si apre la pagina Inventario.
3. Scegli Analizza gli inventari per determinare le proprietà dello schema del database, come la somiglianza e la complessità.
4. Scegli la scheda Schemi per visualizzare i risultati dell'analisi.

È possibile utilizzare la AWS DMS console per identificare schemi duplicati, determinare la complessità della migrazione ed esportare le informazioni di inventario per le analisi future. Per ulteriori informazioni, vedere [Utilizzo degli inventari per l'analisi in AWS DMS Fleet Advisor](#).

Dati raccolti da Agentless Collector

È necessario configurare il modulo di raccolta dati Application Discovery Service Agentless Collector (Agentless Collector) per raccogliere dati di inventario, profilo e utilizzo dai server.

Agentless Collector attualmente supporta la raccolta di dati da macchine virtuali VMware e da server di database e analisi. I moduli futuri supporteranno la raccolta da piattaforme di virtualizzazione

aggiuntive e la raccolta a livello di sistema operativo. Per informazioni sulla configurazione della raccolta dei dati, vedere [Fase 6: Configurare i moduli di raccolta dati Agentless Collector](#).

I seguenti argomenti descrivono i dati raccolti dai moduli di raccolta dati di Application Discovery Service Agentless Collector (Agentless Collector).

Argomenti

- [Dati raccolti dal modulo di raccolta dati Agentless Collector VMware vCenter](#)
- [Dati raccolti dal database Agentless Collector e dal modulo di raccolta dati di analisi](#)

Dati raccolti dal modulo di raccolta dati Agentless Collector VMware vCenter

Le seguenti informazioni descrivono i dati raccolti dal modulo di raccolta dati VMware vCenter di Application Discovery Service Agentless Collector (Agentless Collector). Per informazioni sulla configurazione della raccolta dei dati, vedere. [Come configurare il modulo di raccolta dati Agentless Collector per VMware vCenter](#)

Legenda della tabella per i dati raccolti da Agentless Collector VMware vCenter:

- I dati raccolti sono misurati in kilobyte (KB) salvo diversamente specificato.
- I dati equivalenti nella console Migration Hub sono riportati in megabyte (MB).
- I campi dati contrassegnati da un asterisco (*) sono disponibili solo nei file.csv prodotti dalla funzione di esportazione dell'API Application Discovery Service.

Agentless Collector supporta l'esportazione dei dati tramite la CLI. AWS Per esportare i dati raccolti utilizzando la AWS CLI, segui le istruzioni descritte in Esportazione dei dati sulle prestazioni del sistema per tutti i server nella pagina [Esportazione dei dati raccolti](#) nella guida per l'utente di Application Discovery Service.

- Il periodo di polling è in intervalli di circa 60 minuti.
- Attualmente, i campi dati identificati con un asterisco (**) restituiscono un valore null.

Campo dati	Descrizione
applicationConfigurationId*	ID dell'applicazione di migrazione in cui è raggruppata la macchina virtuale.

Campo dati	Descrizione
avgCpuUsagePct	Percentuale media di utilizzo della CPU durante il periodo di polling.
avgDiskBytesReadPerSecond	Numero medio di byte letti dal disco durante il periodo di polling.
avgDiskBytesWrittenPerSecond	Numero medio di byte scritti su disco durante il periodo di polling.
avgDiskReadOpsPerSecond**	Numero medio di operazioni di I/O in lettura al secondo nullo.
avgDiskWriteOpsPerSecond**	Numero medio di operazioni di I/O di scrittura al secondo.
avgFreeRAM	RAM libera media espressa in MB.
avgNetworkBytesReadPerSecond	Quantità media di velocità effettiva di byte letti al secondo.
avgNetworkBytesWrittenPerSecond	Quantità media di velocità effettiva di byte scritti al secondo.
Produttore di computer	Fornitore segnalato dall'host ESXi.
Modello di computer	Modello di computer riportato dall'host ESXi.
configId	ID assegnato da Application Discovery Service alla macchina virtuale rilevata.
configType	Tipo di risorsa scoperta.
connectorId	ID dell'appliance virtuale.
cpuType	vCPU per una macchina virtuale, modello effettivo per un host.
datacenterId	ID del vCenter.

Campo dati	Descrizione
hostId*	ID dell'host VM.
hostName	Nome dell'host che esegue il software di virtualizzazione.
hypervisor	Tipo di hypervisor.
id	ID del server.
lastModifiedTime ^{Timbro *}	Data e ora più recenti della raccolta dei dati prima dell'esportazione dei dati.
macAddress	Indirizzo MAC della macchina virtuale.
manufacturer	Creatore del software di virtualizzazione.
maxCpuUsagePct	Percentuale massima di utilizzo della CPU durante il periodo di polling.
maxDiskBytesReadPerSecond	Numero massimo di byte letti dal disco durante il periodo di polling.
maxDiskBytesWrittenPerSecond	Numero massimo di byte scritti su disco durante il periodo di polling.
maxDiskReadOpsPerSecond**	Numero massimo di operazioni di I/O di lettura al secondo.
maxDiskWriteOpsPerSecond**	Numero massimo di operazioni di I/O di scrittura al secondo.
maxNetworkBytesReadPerSecond	Quantità massima di velocità effettiva di byte letti al secondo.
maxNetworkBytesWrittenPerSecond	Quantità massima di velocità effettiva di byte scritti al secondo.

Campo dati	Descrizione
memoryReservation [*]	Limite per evitare un sovraccarico di memoria sulla VM.
moRefId	ID di riferimento vCenter Managed Object univoco.
name [*]	Nome della macchina virtuale o della rete (specificato dall'utente).
numCores	Numero di core CPU assegnati alla VM.
numCpus	Numero di socket CPU sull'host ESXi.
numDisks ^{**}	Numero di dischi sulla macchina virtuale.
numNetworkCards ^{**}	Numero di schede di rete sulla VM.
osName	Nome del sistema operativo sulla VM.
osVersion	Versione del sistema operativo su VM.
portGroupId [*]	ID del gruppo di porte membri della VLAN.
portGroupName [*]	Nome del gruppo di porte membri della VLAN.
powerState [*]	Stato dell'alimentazione.
serverId	ID assegnato da Application Discovery Service alla macchina virtuale rilevata.
smBiosId [*]	ID/versione del BIOS di gestione del sistema.
state [*]	Stato dell'appliance virtuale.
toolsStatus	Stato operativo degli strumenti VMware
totalDiskFreeDimensioni	Spazio libero su disco espresso in MB. Disponibile per vCenter Server 7.0 e versioni successive.

Campo dati	Descrizione
totalDiskSize	Capacità totale del disco espressa in MB.
totalRAM	Quantità totale di RAM disponibile sulla macchina virtuale in MB.
type (tipo)	Tipo di host.
vCenterId	Numero ID univoco di una macchina virtuale.
vCenterName *	Nome dell'host vCenter.
virtualSwitchName *	Nome dello switch virtuale.
vmFolderPath	Percorso della directory dei file della macchina virtuale.
vmName	Nome della macchina virtuale.

Dati raccolti dal database Agentless Collector e dal modulo di raccolta dati di analisi

Il modulo di raccolta dei dati di analisi e database di Application Discovery Service Agentless Collector (Agentless Collector) raccoglie le seguenti metriche dal tuo ambiente di dati. Per informazioni su come impostare la raccolta di dati, consulta [Modulo di raccolta dati di analisi e database](#).

Quando si utilizza il modulo di raccolta dei dati di database e analisi per raccogliere metadati e capacità del database, vengono acquisite le seguenti metriche.

- Memoria disponibile sui server del sistema operativo
- Spazio di archiviazione disponibile sui server del sistema operativo
- Versione ed edizione del database
- Numero di CPU sui server del sistema operativo
- Numero di schemi
- Numero di procedure archiviate

- Numero di tabelle
- Numero di righe INSTEAD OF
- Numero di viste
- Struttura dello schema

Dopo aver avviato l'analisi dello schema nellaAWS DMS console, il modulo di raccolta dati analizza e visualizza le seguenti metriche.

- Date di supporto del database
- Numero di righe di codice
- Complessità dello schema
- Somiglianza degli schemi

Quando si utilizza il modulo di raccolta dei dati di database e analisi per raccogliere metadati, capacità del database e utilizzo delle risorse, vengono acquisite le seguenti metriche.

- Velocità di I/O sui server del database
- Il numero di operazioni di input/output al secondo (IOPS) sui server di database
- Numero di CPU utilizzate dai server del sistema operativo
- Utilizzo della memoria sui server del sistema operativo
- Utilizzo dello spazio di archiviazione sui server del sistema operativo

È possibile utilizzare il modulo di raccolta dei dati di database e analisi per raccogliere metadati, capacità e metriche di utilizzo dai database Oracle e SQL Server. Allo stesso tempo, per i database PostgreSQL e MySQL, il modulo di raccolta dati può raccogliere solo metadati.

Utilizzo della console Agentless Collector

Questa sezione spiega come utilizzare la console di Application Discovery Service Agentless Collector (Agentless Collector).

Argomenti

- [La dashboard di Agentless Collector](#)
- [Modifica delle impostazioni di Agentless Collector](#)

- [Modifica delle credenziali VMware vCenter](#)

La dashboard di Agentless Collector

Nella pagina del dashboard di Application Discovery Service Agentless Collector (Agentless Collector) è possibile visualizzare lo stato del raccogliitore e scegliere un metodo di raccolta dei dati come descritto negli argomenti seguenti.

Argomenti

- [Status del collezionista](#)
- [Raccolta dei dati](#)

Status del collezionista

Lo stato del raccogliitore fornisce informazioni sullo stato del raccogliitore. Il nome del raccogliitore, lo stato della connessione del raccogliitore ad AWS, la regione di origine del Migration Hub e la versione.

In caso di problemi di AWS connessione, potresti dover modificare le impostazioni di configurazione di Agentless Collector.

Per modificare le impostazioni di configurazione del raccogliitore, scegli Modifica impostazioni del raccogliitore e segui le istruzioni descritte in [Modifica delle impostazioni di Agentless Collector](#).

Raccolta dei dati

In Raccolta dati puoi scegliere un metodo di raccolta dati. Application Discovery Service Agentless Collector (Agentless Collector) attualmente supporta la raccolta di dati da macchine virtuali VMware e da server di database e analisi. I moduli futuri supporteranno la raccolta da piattaforme di virtualizzazione aggiuntive e la raccolta a livello di sistema operativo.

Argomenti

- [Prestazioni della raccolta dati VMware vCenter](#)
- [Raccolta di dati di analisi e database](#)

Prestazioni della raccolta dati VMware vCenter

Per raccogliere i dati di inventario, profilo e utilizzo dei server dalle macchine virtuali VMware, configura le connessioni ai server vCenter. Per configurare le connessioni, scegli Configurazione nella sezione VMware vCenter e segui le istruzioni descritte in [Fase 6: Configurare i moduli di raccolta dati Agentless Collector](#).

Dopo aver impostato la raccolta dei dati di vCenter, dalla dashboard è possibile eseguire le seguenti operazioni:

- Visualizza lo stato della raccolta dati
- Avviare la raccolta dati
- Interrompere la raccolta dei dati

Note

Nella pagina del dashboard, dopo aver impostato la raccolta dati di vCenter, il pulsante Configurazione nella sezione VMware vCenter viene sostituito con informazioni sullo stato della raccolta dati, un pulsante Interrompi raccolta dati e un pulsante Visualizza e modifica.

Raccolta di dati di analisi e database

È possibile eseguire il modulo di raccolta dei dati di database e analisi nelle due modalità seguenti.

Metadati e capacità del database

Il modulo di raccolta dati raccoglie informazioni quali schemi, versioni, edizioni, CPU, memoria e capacità del disco dal database e dai server di analisi. È possibile utilizzare queste informazioni raccolte per calcolare i consigli sugli obiettivi nellaAWS DMS console. Se il database di origine è sovrafornito o sottofornito, anche i consigli di destinazione verranno forniti in eccesso o in quantità insufficiente.

Questa è la modalità predefinita.

Metadati, capacità del database e utilizzo delle risorse

Oltre ai metadati e alle informazioni sulla capacità del database, il modulo di raccolta dati raccoglie le metriche di utilizzo effettivo della CPU, della memoria e della capacità del disco per i database e i server di analisi. Questa modalità fornisce consigli sugli obiettivi più accurati rispetto

alla modalità predefinita perché si basano sui carichi di lavoro effettivi del database. In questa modalità, il modulo di raccolta dati raccoglie le metriche delle prestazioni ogni minuto.

Per iniziare a raccogliere metadati e metriche delle prestazioni dal database e dai server di analisi

1. Nella pagina del raccogliitore di database e analisi, scegli Raccolta dati nel riquadro di navigazione.
2. Dall'elenco dell'inventario del database, seleziona il database e i server di analisi per i quali desideri raccogliere metadati e metriche delle prestazioni.
3. Scegli Esegui raccolta dati. Viene visualizzata la finestra di dialogo Tipo di raccolta dati.
4. Scegli come raccogliere i dati per l'analisi.

Se scegli l'opzione Metadati, capacità del database e utilizzo delle risorse, imposta il periodo di raccolta dei dati. Puoi raccogliere dati durante i prossimi 7 giorni o impostare l'intervallo personalizzato da 1 a 60 giorni.

5. Scegli Esegui raccolta dati. Si apre la pagina Raccolta dati.
6. Scegli la scheda Stato della raccolta per vedere lo stato della raccolta dei dati.

Dopo aver completato la raccolta dei dati, il modulo di raccolta dati carica i dati raccolti nel bucket Amazon S3. Quindi, puoi visualizzare questi dati raccolti come descritto in [Fase 7: Visualizzazione dei dati raccolti](#).

Modifica delle impostazioni di Agentless Collector

Hai configurato il raccogliitore quando hai impostato per la prima volta Application Discovery Service Agentless Collector (Agentless Collector) come descritto in [Fase 5: Configurare Agentless Collector](#). La procedura seguente viene descritto come modificare le impostazioni di configurazione di Agentless Collector.

Per modificare le impostazioni di configurazione del raccogliitore

- Scegli il pulsante Modifica impostazioni del raccogliitore nella dashboard di Agentless Collector.

Nella pagina Modifica impostazioni del raccogliitore, effettuate le seguenti operazioni:

- a. Per Nome del Prestazioni della raccolta, immettere un nome per identificare il Prestazioni della raccolta. Il nome può contenere spazi ma non può contenere caratteri speciali.

- b. In AWSAccount di destinazione per i dati di rilevamento, inserisci la chiave diAWS accesso e la chiave segretaAWS dell'account da specificare come account di destinazione per ricevere i dati scoperti dal raccogliitore. Per informazioni sui requisiti per l'utente IAM, consulta[Fase 1: Creare un utente IAM per Agentless Collector](#).
 - i. Per la AWSchiave di accesso, inserisci la chiave di accesso dell'AWSaccount utente IAM che stai specificando come account di destinazione.
 - ii. Per la AWSchiave segreta, inserisci la chiave segreta dell'AWSaccount utente IAM che stai specificando come account di destinazione.
- c. Nella sezione Password Agentless Collector, modifica la password da utilizzare per autenticare l'accesso a Agentless Collector.
 - i. Per la password Agentless Collector, inserisci una password da utilizzare per autenticare l'accesso a Agentless Collector.
 - ii. Per reinserire la password di Agentless Collector, per la verifica, inserisci nuovamente la password.
- d. Scegli Salva configurazioni.

Successivamente, vedrai[La dashboard di Agentless Collector](#).

Modifica delle credenziali VMware vCenter

Per raccogliere i dati di inventario, profilo e utilizzo dei server dalle macchine virtuali VMware, configura le connessioni ai server vCenter. Per informazioni sulla configurazione delle connessioni VMware vCenter, consulta[Fase 6: Configurare i moduli di raccolta dati Agentless Collector](#).

Questa sezione spiega come modificare le credenziali vCenter.

Note

Prima di modificare le credenziali vCenter, assicurati di poter fornire le credenziali vCenter con le autorizzazioni di lettura e visualizzazione impostate per il gruppo System.

Per modificare le credenziali di VMware vCenter

Nella[Dettagli della raccolta dei dati VMware](#) pagina, scegli Modifica server vCenter.

- Nella pagina Edit vCenter, effettuate le seguenti operazioni:
 - a. Sotto le credenziali vCenter:
 - i. Per vCenter URL/IP, immettere l'indirizzo IP dell'host VMware vCenter Server.
 - ii. Per vCenter Username (Nome utente vCenter), digita il nome di un utente locale o di dominio che il connettore usa per comunicare con vCenter. Per gli utenti del dominio, usa il modulo dominio\nome utente o nome utente@dominio.
 - iii. Per vCenter Password (Password vCenter), digita la password dell'utente locale o del dominio.
 - b. Seleziona Salva.

Aggiornamento manuale di Agentless Collector

Quando si configura Application Discovery Service Agentless Collector (Agentless Collector), è possibile scegliere di abilitare gli aggiornamenti automatici come descritto in [Fase 5: Configurare Agentless Collector](#). Se non abiliti gli aggiornamenti automatici, dovrai aggiornare manualmente Agentless Collector.

La procedura seguente descrive come aggiornare manualmente Agentless Collector.

Per aggiornare manualmente Agentless Collector

1. Ottieni il file Agentless Collector Open Virtualization Archive (OVA) più recente.
2. (Facoltativo) Ti consigliamo di eliminare il precedente file OVA di Agentless Collector, prima di distribuire quello più recente.
3. Nella [Guida introduttiva a Agentless Collector](#) sezione, segui i passaggi descritti. [Fase 3: Implementazione di Agentless Collector](#) [Fase 6: Configurare i moduli di raccolta dati Agentless Collector](#)

La procedura precedente aggiorna solo Agentless Collector. È responsabilità dell'utente mantenere aggiornato il sistema operativo.

Per aggiornare la tua istanza Amazon EC2

1. Ottieni l'indirizzo IP di Agentless Collector da VMware vCenter.

2. Apri la console VM del raccoglitore e accedi **ec2-user** utilizzando la password, come mostrato nell'esempio seguente. **collector**

```
username: ec2-user
password: collector
```

3. Segui le istruzioni in [Update instance software sulla tua istanza AL2](#) nella Amazon Linux 2 User Guide.

Applicazione di patch Kernel Live su Amazon Linux 2

La macchina virtuale Agentless Collector utilizza Amazon Linux 2 come descritto in. [Fase 3: Implementazione di Agentless Collector](#)

Per abilitare e utilizzare il live patching per Amazon Linux 2, consulta [Kernel Live Patching on Amazon Linux 2 nella Amazon EC2 User Guide](#).

Risoluzione dei problemi di Agentless Collector

Questa sezione contiene argomenti che possono aiutarti a risolvere i problemi noti con Application Discovery Service Agentless Collector (Agentless Collector).

Argomenti

- [Fixing Agentless Collector non AWS riesce a raggiungerlo durante la configurazione](#)
- [Risoluzione dei problemi di certificazione autofirmata durante la connessione all'host proxy](#)
- [Trovare collezionisti malsani](#)
- [Risoluzione dei problemi relativi all'indirizzo IP](#)
- [Risoluzione dei problemi relativi alle credenziali vCenter](#)
- [Risoluzione dei problemi di inoltro dei dati nel database e nel modulo di raccolta dei dati di analisi](#)
- [Risoluzione dei problemi di connessione nel database e nel modulo di raccolta dei dati di analisi](#)
- [Supporto per host ESX autonomi](#)
- [Contattare l' AWS assistenza per problemi relativi a Agentless Collector](#)

Fixing Agentless Collector non AWS riesce a raggiungerlo durante la configurazione

Agentless Collector richiede l'accesso in uscita tramite la porta TCP 443 a diversi domini. AWS Quando si configura Agentless Collector nella console, è possibile che venga visualizzato il seguente messaggio di errore.

Impossibile raggiungerlo AWS

AWS non può essere raggiunto. Verifica le impostazioni di rete.

Questo errore si verifica a causa di un tentativo fallito di Agentless Collector di stabilire una connessione HTTPS a un AWS dominio con cui il raccoglitore deve comunicare durante il processo di configurazione. La configurazione di Agentless Collector fallisce se non è possibile stabilire una connessione.

Per correggere la connessione a AWS

1. Rivolgeti all'amministratore IT per verificare se il firewall aziendale sta bloccando il traffico in uscita sulla porta 443 verso uno dei AWS domini che richiedono l'accesso in uscita. AWS I domini che richiedono l'accesso in uscita dipendono dal fatto che la tua regione di origine sia la regione degli Stati Uniti occidentali (Oregon), us-west-2 o un'altra regione.

I seguenti domini richiedono l'accesso in uscita se la regione di residenza del tuo AWS account è us-west-2:

- `arsenal-discovery.us-west-2.amazonaws.com`
- `migrationhub-config.us-west-2.amazonaws.com`
- `api.ecr-public.us-east-1.amazonaws.com`
- `public.ecr.aws`

I seguenti domini richiedono l'accesso in uscita se la regione di residenza dell'account AWS non è: **us-west-2**

- `arsenal-discovery.us-west-2.amazonaws.com`
- `arsenal-discovery.your-home-region.amazonaws.com`

- `migrationhub-config.us-west-2.amazonaws.com`
- `api.ecr-public.us-east-1.amazonaws.com`
- `public.ecr.aws`

Se il firewall blocca l'accesso in uscita ai AWS domini con cui Agentless Collector deve comunicare, configura un host proxy nella sezione Sincronizzazione dei dati in Configurazione Collector.

2. Se l'aggiornamento del firewall non risolve il problema di connessione, utilizza i seguenti passaggi per assicurarti che la macchina virtuale Collector disponga della connettività di rete in uscita ai domini elencati nel passaggio precedente.
 - a. Ottieni l'indirizzo IP di Agentless Collector da VMware vCenter.
 - b. Apri la console VM del raccogliitore e accedi **ec2-user** utilizzando la password, come mostrato nell'esempio seguente. **collector**

```
username: ec2-user
password: collector
```

- c. Verifica la connessione ai domini elencati eseguendo telnet sulle porte 443, come mostrato nell'esempio seguente.

```
telnet migrationhub-config.us-west-2.amazonaws.com 443
```

3. Se telnet non è in grado di risolvere il dominio, prova a configurare un server DNS statico utilizzando le istruzioni [per Amazon Linux 2](#).
4. Se l'errore persiste, per ulteriore assistenza, consulta. [Contattare l' AWS assistenza per problemi relativi a Agentless Collector](#)

Risoluzione dei problemi di certificazione autofirmata durante la connessione all'host proxy

Se la comunicazione con il proxy fornito opzionalmente avviene tramite HTTPS e il proxy dispone di un certificato autofirmato, potrebbe essere necessario fornire un certificato.

1. Ottieni l'indirizzo IP di Agentless Collector da VMware vCenter.

2. Apri la console VM del raccoglitore e accedi `ec2-user` con la password, come mostrato nell'esempio seguente. `collector`

```
username: ec2-user
password: collector
```

3. Incolla il corpo del certificato associato al proxy sicuro, inclusi entrambi `-----BEGIN CERTIFICATE-----` e `-----END CERTIFICATE-----`, nel seguente file:

```
/etc/pki/ca-trust/source/anchors/https-proxy-ca.pem
```

4. Per installare il nuovo certificato, esegui i seguenti comandi:

```
sudo update-ca-trust
```

5. Riavvia Agentless Collector eseguendo il seguente comando:

```
sudo shutdown -r now
```

Trovare collezionisti malsani

Le informazioni sullo stato di ogni raccoglitore si trovano nella pagina [Data collectors](#) della console AWS Migration Hub (Migration Hub). È possibile identificare i raccoglitori con problemi individuando i raccoglitori con lo stato di Richiede attenzione.

La procedura seguente descrive come accedere alla console Agentless Collector per identificare problemi di salute.

Per accedere alla console Agentless Collector

1. Utilizzando il tuo AWS account, accedi AWS Management Console e apri la console Migration Hub all'[indirizzo https://console.aws.amazon.com/migrationhub/](https://console.aws.amazon.com/migrationhub/).
2. Nel pannello di navigazione della console Migration Hub sotto Discover, scegli Raccoglitori di dati.
3. Nella scheda Agentless collectors, prendi nota dell'indirizzo IP di ogni connettore con lo stato Richiede attenzione.

4. Per aprire la console Agentless Collector, apri un browser web. Quindi digita il seguente URL nella barra degli indirizzi: **https://** /<ip_address>, dove ip_address è l'indirizzo IP di un raccoglitore non funzionante.
5. Scegli Accedi, quindi inserisci la password di Agentless Collector, che è stata impostata al momento della configurazione del raccoglitore. [Fase 5: Configurare Agentless Collector](#)
6. Nella pagina dashboard di Agentless Collector, in Raccolta dati, scegli Visualizza e modifica nella sezione VMware vCenter.
7. Segui le istruzioni riportate per correggere l'URL e le [Modifica delle credenziali VMware vCenter](#) credenziali.

Dopo aver corretto i problemi di integrità, il raccoglitore ristabilirà la connettività con il server vCenter e lo stato del raccoglitore passerà allo stato Collecting. Se i problemi persistono, consulta. [Contattare l' AWS assistenza per problemi relativi a Agentless Collector](#)

Le cause più comuni dei raccoglitori non integri sono i problemi relativi all'indirizzo IP e alle credenziali. [Risoluzione dei problemi relativi all'indirizzo IP](#) e [Risoluzione dei problemi relativi alle credenziali vCenter](#) può aiutarti a risolvere questi problemi e riportare un raccoglitore in uno stato integro.

Risoluzione dei problemi relativi all'indirizzo IP

Un collector può andare in uno stato non integro se l'endpoint vCenter fornito durante la configurazione del collector è malformato, non valido o se il server vCenter è attualmente inattivo e non raggiungibile. In questo caso, riceverai un messaggio di errore di connessione.

La procedura seguente consente di risolvere i problemi relativi all'indirizzo IP.

Per risolvere i problemi relativi all'indirizzo IP del raccoglitore

1. Ottieni l'indirizzo IP di Agentless Collector da VMware vCenter.
2. Apri la console Agentless Collector aprendo un browser Web, quindi digita il seguente URL nella barra degli indirizzi: **https://** /<ip_address>, dove ip_address è l'indirizzo IP del raccoglitore. [Fase 3: Implementazione di Agentless Collector](#)
3. Scegli Accedi, quindi inserisci la password di Agentless Collector, che è stata impostata al momento della configurazione del raccoglitore. [Fase 5: Configurare Agentless Collector](#)
4. Nella pagina dashboard di Agentless Collector, in Raccolta dati, scegli Visualizza e modifica nella sezione VMware vCenter.

5. Nella pagina dei dettagli della raccolta dati VMware, in Server vCenter scoperti, annota l'indirizzo IP nella colonna vCenter.
6. Utilizzando uno strumento a riga di comando separato come `ping` o `tracert`, verifica che il server vCenter associato sia attivo e che l'IP sia raggiungibile dalla macchina virtuale del collettore.
 - Se l'indirizzo IP non è corretto e il servizio vCenter è attivo, aggiorna l'indirizzo IP nella console di raccolta e scegli Avanti.
 - Se l'indirizzo IP è corretto ma il server vCenter non è attivo, attivarlo.
 - Se l'indirizzo IP è corretto e il server vCenter è attivo, verificare se blocca le connessioni di rete in ingresso a causa di problemi di firewall. In caso affermativo, aggiorna le impostazioni del firewall per consentire le connessioni in entrata dalla macchina virtuale del collettore.

Risoluzione dei problemi relativi alle credenziali vCenter

I raccoglitori possono andare in uno stato non integro se le credenziali utente vCenter fornite durante la configurazione di un raccoglitore non sono valide o non dispongono dei privilegi dell'account vCenter Read and View.

Se riscontri problemi relativi alle credenziali vCenter, assicurati di avere i permessi di lettura e visualizzazione di vCenter impostati per il gruppo System.

Per informazioni sulla modifica delle credenziali vCenter, vedere [Modifica delle credenziali VMware vCenter](#)

Risoluzione dei problemi di inoltro dei dati nel database e nel modulo di raccolta dei dati di analisi

La home page del database e del modulo di raccolta dei dati di analisi di Agentless Collector mostra lo stato della connessione per Access to DMS e Access to S3. Se vedi No access for Access to DMS e Access to S3, configura l'inoltro dei dati. Per ulteriori informazioni, consulta [Configurazione dell'inoltro dei dati](#).

Se riscontri questo problema dopo aver configurato l'inoltro dei dati, assicurati che il modulo di raccolta dati possa accedere a Internet. Quindi, assicurati di aver aggiunto le policy DMS CollectorPolicy e FleetAdvisorS3Policy al tuo utente IAM. Per ulteriori informazioni, consulta [Fase 1: Creare un utente IAM per Agentless Collector](#).

Se il modulo di raccolta dati non riesce a connettersi AWS, fornisci l'accesso in uscita ai seguenti domini.

- `dms.your-home-region.amazonaws.com`
- `s3.amazonaws.com`

Risoluzione dei problemi di connessione nel database e nel modulo di raccolta dei dati di analisi

Il modulo di raccolta dei dati di database e analisi di Agentless Collector si connette ai server LDAP per individuare i server del sistema operativo nel tuo ambiente di dati. Quindi, il modulo di raccolta dati si collega ai server del sistema operativo per scoprire i server di database e analisi. Da questi server di database, il modulo di raccolta dati raccoglie metriche di capacità e prestazioni. Se il modulo di raccolta dati non è in grado di connettersi a questi server, verifica di poterti connettere ai server.

Negli esempi seguenti, sostituisci i valori *sostituibili* con i tuoi valori.

- Per verificare di poterti connettere al tuo server LDAP, installa il `ldap-util` pacchetto. Per farlo, esegui il comando seguente.

```
sudo apt-get install ldap-util
```

Quindi, eseguire il comando riportato di seguito.

```
ldapsearch -x -D "CN=user,CN=Users,DC=example,DC=com" -w "password" -b "dc=example,dc=com" -h
```

- Per verificare che sia possibile connettersi a un server del sistema operativo Linux, utilizzare i seguenti comandi.

```
ssh -i C:\Users\user\private_key.pem -p 22 username@my-linux-host.domain.com
```

Eseguite l'esempio precedente come amministratore in Windows.

```
ssh username@my-linux-host.domain.com
```

Esegui l'esempio precedente in Linux.

- Per verificare che sia possibile connettersi a un server del sistema operativo Windows, utilizzare i seguenti comandi.

```
winrs -r:[hostname or ip] -u:username -p:password cmd
```

Esegui l'esempio precedente come amministratore in Windows.

```
sudo apt install -y winrm  
winrm --user=username --password=password [http or https]://[hostname or ip]:[port]  
"[cmd.exe or any other CLI command]"
```

Esegui l'esempio precedente in Linux.

- Per verificare che sia possibile connettersi a un database di SQL Server, utilizzare i seguenti comandi.

```
sqlcmd -S [hostname or IP] -U username -P 'password'  
SELECT GETDATE() AS sysdate
```

- Per verificare che sia possibile connettersi a un database MySQL, utilizzare i seguenti comandi.

```
mysql -u username -p 'password' -h [hostname or IP] -P [port]  
SELECT NOW() FROM DUAL
```

- Per verificare che sia possibile connettersi a un database Oracle, utilizzare i seguenti comandi.

```
sqlplus username/password@[hostname or IP]:port/servicename  
SELECT SYSDATE FROM DUAL
```

- Per verificare che sia possibile connettersi a un database PostgreSQL, utilizzare i seguenti comandi.

```
psql -U username -h [hostname or IP] -p port -d database  
SELECT CURRENT_TIMESTAMP AS sysdate
```

Se non riesci a connetterti al database e ai server di analisi, assicurati di fornire le autorizzazioni richieste. Per ulteriori informazioni, consulta [Scopri i tuoi server di database](#).

Supporto per host ESX autonomi

Agentless Collector non supporta un host ESX autonomo. L'host ESX deve essere parte dell'istanza di vCenter Server.

Contattare l' AWS assistenza per problemi relativi a Agentless Collector

Se riscontri problemi con Application Discovery Service Agentless Collector (Agentless Collector) e hai bisogno di aiuto, contatta l'[AWS assistenza](#). Verrai contattato e ti potrebbe essere chiesto di inviare i log del raccoglitore.

Per ottenere i log di Agentless Collector

1. Ottieni l'indirizzo IP di Agentless Collector da VMware vCenter.
2. Apri la console VM del raccoglitore e accedi **ec2-user** utilizzando la password, come mostrato nell'esempio seguente. **collector**

```
username: ec2-user
password: collector
```

3. Usa il seguente comando per accedere alla cartella di registro.

```
cd /var/log/aws/collector
```

4. Comprimi i file di registro utilizzando i seguenti comandi.

```
sudo cp /local/agentless_collector/compose.log .
docker inspect $(docker ps --format {{.Names}}) | sudo tee docker_inspect.log >/dev/null
sudo tar czf logs_$(date '+%d-%m-%Y_%H.%M.%S').tar.gz * --exclude='db.mv*'
```

5. Copia il file di registro dalla macchina virtuale Agentless Collector.

```
scp logs*.tar.gz targetuser@targetaddress
```

6. Consegnare il tar .gz file a AWS Enterprise Support.

Importance

AWS Migration Hub L'importazione (Migration Hub) consente di importare i dettagli dell'ambiente locale direttamente in Migration Hub senza utilizzare Application Discovery Service Agentless Collector (Agentless Collector) o AWS Application Discovery Agent (Discovery Agent), in modo da poter eseguire la valutazione e la pianificazione della migrazione direttamente dai dati importati. È anche possibile raggruppare i dispositivi come applicazioni e monitorarne lo stato di migrazione.

Per avviare una richiesta di importazione

- Scaricare il modello di importazione CSV (valori separati da virgole) appositamente formattato.
- Compilarlo con i dati esistenti del server locale.
- Caricarlo su Migration Hub utilizzando la console Migration Hub AWS CLI o uno dei AWS SDK.

È possibile inviare più richieste di importazione. Ogni richiesta viene elaborata in sequenza. È possibile verificare lo stato delle richieste di importazione in qualsiasi momento, tramite la console o le API di importazione.

Una volta completata la richiesta di importazione, è possibile visualizzare i dettagli dei singoli record importati. Visualizza i dati di utilizzo, i tag e le mappature delle applicazioni direttamente dalla console di Migration Hub. In caso di errori durante l'importazione, è possibile esaminare il conteggio dei record corretti e non riusciti e i dettagli dell'errore per ogni record non riuscito.

Gestire gli errori: Viene fornito un collegamento per scaricare i file di log degli errori e dei record con esito negativo come file CSV in un archivio compresso. Utilizza questi file per inviare nuovamente la richiesta di importazione dopo aver corretto gli errori.


Vengono applicati dei limiti relativi al numero di record importati, server importati e record eliminati. Per ulteriori informazioni, consulta la pagina [Quote di AWS Application Discovery Service](#).

Campi di file di importazione supportati

Migration Hub consente di importare dati da qualsiasi origine. I dati forniti devono essere nel formato supportato per un file CSV e i dati devono contenere solo i campi supportati con i relativi intervalli supportati per tali campi.

Un asterisco accanto al nome di un campo di importazione nella tabella riportata di seguito indica che è un campo obbligatorio. Ogni record del file di importazione deve avere almeno uno o più di questi

campi obbligatori compilati per identificare in modo univoco un server o un'applicazione. Altrimenti, un record senza nessun campo obbligatorio non verrà importato.

 Note


Se usi uno VMware.MoRefId o VMware.VCenterId, per identificare un record, è necessario avere entrambi i campi nello stesso record.

Nome del campo di importazione	Descrizione	Examples (Esempi)
ExternalId*	Un identificatore personalizzato che consente di contrassegnare ciascun record come univoco. Ad esempio, ExternalId può essere l'ID inventario del server nel data center.	Inventory Id 1 Server 2 CMBD Id 3
SMBiosId	ID del BIOS di gestione del sistema (SMBIOS).	
IPAddress*	Un elenco separato da virgole di indirizzi IP del server, tra virgolette.	192.0.0.2 "10.12.31.233, 10.12.32.11"
MACAddress*	Un elenco separato da virgole di indirizzi MAC del server, tra virgolette.	00:1B:44:11:3A:B7 "00-15-E9-2B-99-3C, 00-14-22-01-23-45"
HostName*	Il nome host del server. Consigliamo di usare il nome di dominio completo (FQDN) per questo valore.	ip-1-2-3-4 localhost.domain

Nome del campo di importazione	Descrizione	Examples (Esempi)
VMware.MoRefId*	L'ID di riferimento dell'oggetto gestito. Deve essere fornito con un VMware.v.CenterId.	
VMware.v.CenterId*	Identificatore univoco della macchina virtuale. Deve essere fornito con un VMware.MoRefId.	
CPU.NumberOfProcessors	Il numero di CPU.	4
CPU.NumberOfCores	Il numero totale di core fisici.	8
CPU.NumberOfLogicalCores	Il numero totale di thread che possono essere eseguiti simultaneamente su tutte le CPU di un server. Alcune CPU supportano l'esecuzione simultanea di più thread su un singolo core di CPU. In questi casi, questo numero sarà superiore al numero di core (fisico o virtuale).	16
OS.Name	Il nome del sistema operativo.	Linux Windows.Hat
OS.Version	La versione del sistema operativo.	16.04.3 NT 6.2.8
VMware.VMName	Il nome della macchina virtuale.	Corp1

Nome del campo di importazione	Descrizione	Examples (Esempi)
RAM.TotalSizeInMB	La RAM totale disponibile sul server in MB.	64 128
RAM.UsedSizeInMb.avg	La quantità media di RAM utilizzata sul server, in MB.	64 128
RAM.UsedSizeInMB.max	La quantità massima di RAM utilizzata disponibile sul server, in MB.	64 128
CPU.UsagePct.Media Vg	L'utilizzo medio della CPU quando lo strumento di rilevamento raccoglieva i dati.	45 23.9
CPU.UsagePct.max	L'utilizzo massimo della CPU quando lo strumento di rilevamento raccoglieva i dati.	55.34 24
DiskReadsPerSecondInKb.avg	Il numero medio di letture del disco al secondo, in KB.	1159 84506
DiskWritesPerSecondInKb.avg	Il numero medio di scritture del disco al secondo, in KB.	199 6197
DiskReadsPerSecondInKb.max	Il numero massimo di letture del disco al secondo, in KB.	37892 869962
DiskWritesPerSecondInKb.max	Il numero massimo di scritture del disco al secondo, in KB.	18436 1808

Nome del campo di importazione	Descrizione	Examples (Esempi)
DiskReadsOpsPerSecond.Media Vg	Il numero medio di operazioni di lettura del disco al secondo.	45 28
DiskWritesOpsPerSecond.Media Vg	Il numero medio di operazioni di scrittura su disco al secondo.	8 3
DiskReadsOpsPerSecond.max	Il numero massimo di operazioni di lettura del disco al secondo.	1083 176
DiskWritesOpsPerSecond.max	Il numero massimo di operazioni di scrittura su disco al secondo.	535 71
NetworkReadsPerSecond.InKb.avg	Il numero medio di operazioni di lettura sulla rete al secondo, in KB.	45 28
NetworkWritesPerSecond.InKb.avg	Il numero medio di operazioni di scrittura sulla rete al secondo, in KB.	8 3
NetworkReadsPerSecond.InKb.max	Il numero massimo di operazioni di lettura sulla rete al secondo, in KB.	1083 176
NetworkWritesPerSecond.InKb.max	Il numero massimo di operazioni di scrittura sulla rete al secondo, in KB.	535 71

Nome del campo di importazione	Descrizione	Examples (Esempi)
Applicazioni	Un elenco separato da virgole di applicazioni che includono questo server, tra virgolette. Questo valore può includere le applicazioni esistenti e/ o nuove applicazioni che vengono create durante l'importazione.	Application1 "Application2, Application3"
Tag	Un elenco separato da virgole di tag formattati come nome:valore. <div data-bbox="591 863 1029 1178" style="border: 1px solid #f08080; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Important</p> <p>Non memorizzare informazioni sensibili (come i dati personali) nei tag.</p> </div>	"zone:1, critical:yes" "zone:3, critical:no, zone:1"

È possibile importare i dati anche se non tutti i campi definiti nel modello di importazione sono compilati a condizione che ogni record contenga almeno uno dei campi obbligatori. I duplicati vengono gestiti su più richieste di importazione utilizzando una chiave corrispondente esterna o interna. Se si compila la propria chiave corrispondente, `External ID`, questo campo viene utilizzato per identificare in modo univoco e importare i record. Se non viene specificata alcuna chiave corrispondente, l'importazione utilizza una chiave corrispondente generata internamente derivata da alcune delle colonne del modello di importazione. Per ulteriori informazioni su questa corrispondenza, consulta [Logica corrispondente per i server e le applicazioni rilevati](#).

Note

L'importazione di Migration Hub non supporta altri campi oltre a quelli definiti nel modello di importazione. Eventuali campi personalizzati forniti verranno ignorati e non saranno importati.

Impostazione delle autorizzazioni di importazione

Prima di importare i dati, accertarsi che l'utente IAM abbia le autorizzazioni Amazon S3 necessarie per caricare (`s3:PutObject`) il file di importazione in Amazon S3 e per leggere l'oggetto (`s3:GetObject`). È inoltre necessario stabilire l'accesso programmatico (per laAWS CLI) o l'accesso alla console, creando una policy IAM e collegandola all'utente IAM che esegue le importazioni nell'AWSconto.

Console Permissions

Utilizza la procedura seguente per modificare la policy di autorizzazioni per l'utente IAM che effettuerà le richieste di importazione nell'AWSaccount mediante la console.

Per modificare le policy gestite collegate a un utente

1. Accedi alla AWS Management Console e apri la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel pannello di navigazione, seleziona Users (Utenti).
3. Selezionare il nome dell'utente per cui modificare la policy di autorizzazione.
4. Seleziona la scheda Permissions (Autorizzazioni) e scegli Add permissions (Aggiungi autorizzazioni).
5. Scegli Attach existing policies directly (Collega direttamente le policy esistenti), quindi seleziona Create policy (Crea policy).
 - a. Nella pagina Create policy (Crea policy) che si apre, scegli JSON e copia la policy seguente. Ricorda di sostituire il nome del bucket con il nome effettivo del bucket in cui l'utente IAM caricherà i file di importazione.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource": "*"
    }
  ],
}
```

```

    {
      "Effect": "Allow",
      "Action": ["s3:ListBucket"],
      "Resource": ["arn:aws:s3:::importBucket"]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource": ["arn:aws:s3:::importBucket/*"]
    }
  ]
}

```

- b. Scegli Review policy (Esamina policy).
 - c. Assegna alla policy un nuovo Nome e una descrizione facoltativa prima di esaminare il riepilogo della policy.
 - d. Scegli Create Policy (Crea policy).
6. Torna alla su. Connessione di autorizzazioni Pagina della console IAM per l'utente che effettuerà le richieste di importazione nella AWS S3.
 7. Aggiorna la tabella di policy e cerca il nome della policy appena creata.
 8. Seleziona Successivo: Verifica.
 9. Scegli Add Permissions (Aggiungi autorizzazioni).

Ora che hai aggiunto la policy all'utente IAM, sei pronto per iniziare il processo di importazione.

AWS CLI Permissions

Utilizzare la seguente procedura per creare i criteri gestiti necessari per concedere a un utente IAM le autorizzazioni per effettuare richieste di dati di importazione utilizzando il AWS CLI.

Creazione e collegamento di policy gestite

1. Utilizzo dell'`aws iam create-policy` AWS CLI comando per creare una policy IAM con le seguenti autorizzazioni. Ricorda di sostituire il nome del bucket con il nome effettivo del bucket in cui l'utente IAM caricherà i file di importazione.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["s3:ListBucket"],
      "Resource": ["arn:aws:s3:::importBucket"]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource": ["arn:aws:s3:::importBucket/*"]
    }
  ]
}
```

Per ulteriori informazioni sull'utilizzo di questo comando, consulta la sezione [create-policy](#) nella AWS CLI Riferimento ai comandi.

- Utilizzo dell'`aws iam create-policy` AWS CLI per creare una policy IAM aggiuntiva con le seguenti autorizzazioni.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "discovery:ListConfigurations",
        "discovery:CreateApplication",
        "discovery:UpdateApplication",
        "discovery:AssociateConfigurationItemsToApplication",
        "discovery:DisassociateConfigurationItemsFromApplication",
        "discovery:GetDiscoverySummary",
        "discovery:StartImportTask",
        "discovery:DescribeImportTasks",
        "discovery:BatchDeleteImportData"
      ]
    }
  ]
}
```



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

3. Utilizzo dell'`aws iam attach-user-policy` AWS CLI per collegare le policy create nei due passaggi precedenti all'utente IAM che effettuerà le richieste di importazione nella AWS account utilizzando il AWS CLI. Per ulteriori informazioni sull'utilizzo di questo comando, consulta la sezione [attach-user-policy](#) nella AWS CLI Riferimento ai comandi.

Ora che hai aggiunto le policy all'utente IAM, sei pronto per iniziare il processo di importazione.

Ricorda che quando l'utente IAM carica gli oggetti nel bucket Amazon S3 specificato, deve lasciare le autorizzazioni predefinite per gli oggetti impostati in modo che l'utente possa leggere l'oggetto.

Caricamento del file di importazione in Amazon S3

A questo punto, è necessario caricare i file di importazione in formato CSV in Amazon S3 in modo che possa essere importato. Prima di iniziare, è necessario disporre di un bucket Amazon S3 che conterrà il file di importazione creato e/o scelto in anticipo.

Console S3 Upload

Per caricare il file di importazione in Amazon S3

1. Accedi alla AWS Management Console e apri la console di Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nell'elenco Bucket name (Nome bucket) selezionare il nome del bucket in cui si desidera caricare l'oggetto.
3. Scegliere Upload (Carica).
4. Nella finestra di dialogo Upload (Carica) selezionare Add files (Aggiungi file) per scegliere il file da caricare.
5. Seleziona un file da caricare, quindi scegli Apri.
6. Scegliere Upload (Carica).
7. Una volta che il file è stato caricato, scegli il nome dell'oggetto file di dati dal pannello di controllo del bucket.

8. Dalla scheda Overview (Panoramica) della pagina dei dettagli dell'oggetto, copia l'Object URL (URL oggetto). Sarà necessario durante la creazione della richiesta di importazione.
9. Passare alla su.Importanella console di Migration Hub come descritto in [Importazione di dati](#). Quindi, incollare l'URL dell'oggetto nella casellaURL dell'oggetto Amazon S3.

AWS CLI S3 Upload

Per caricare il file di importazione in Amazon S3

1. Apri una finestra del terminale e accedi alla directory in cui è stato salvato il file di importazione.
2. Immetti il comando seguente:

```
aws s3 cp ImportFile.csv s3://BucketName/ImportFile.csv
```

3. Restituisce i seguenti risultati:

```
upload: .\ImportFile.csv to s3://BucketName/ImportFile.csv
```

4. Copia il percorso completo di un oggetto Amazon S3 che viene restituito. Sarà necessario al momento della creazione della richiesta di importazione.

Importazione di dati

Dopo aver scaricato il modello di importazione dalla console di Migration Hub e averlo compilato con i dati del server locale esistente, è possibile avviare l'importazione dei dati in Migration Hub. Le seguenti istruzioni descrivono due modi per eseguire questa operazione: utilizzando la console o effettuando chiamate API tramite laAWS CLI.

Console Import

Avvia l'importazione di dati inStrumentipagina della console di Migration Hub.

Per avviare l'importazione di dati

1. Nel riquadro di navigazione, in Discover (Rileva), scegli Tools (Strumenti).
2. Se non si dispone già di un modello di importazione compilato, è possibile scaricare il modello scegliendo import template (modello di importazione) nella casella Import (Importa). Apri

il modello scaricato e compilalo con i dati del server locale esistente. È inoltre possibile scaricare il modello di importazione dai nostri bucket Amazon S3 all'indirizzo https://s3.us-west-2.amazonaws.com/templates-7cfff56-bd96-4b1c-b45b-a5b42f282e46/import_template.csv

3. Per aprire la pagina di importazione, scegliere **Importa** nella pagina **Importa** (Creare snapshot finale?).
4. Under **Nome** processo di importazione, specificare un nome per l'importazione.
5. Compila il modulo di URL dell'oggetto Amazon S3. Per eseguire questa operazione, è necessario caricare i file di dati di importazione in Amazon S3. Per ulteriori informazioni, consulta la pagina [Caricamento del file di importazione in Amazon S3](#).
6. Scegli **Import** (**Importa**) nell'area in basso a destra. Verrà aperta la pagina **Imports** (**Importazioni**), in cui è possibile visualizzare l'importazione e il relativo stato elencato nella tabella.

Dopo aver seguito la procedura precedente per avviare l'importazione di dati, la pagina **Imports** (**Importazioni**) visualizzerà i dettagli di ciascuna richiesta di importazione, compreso lo stato di avanzamento, il tempo di completamento e il numero di record con esito positivo o negativo con la possibilità di scaricare questi record. Da questa schermata, è anche possibile passare alla pagina **Servers** (**Server**) sotto **Discover** (**Rileva**) per visualizzare i dati effettivamente importati.

Nella pagina **Servers** (**Server**), è possibile consultare un elenco di tutti i server (dispositivi) rilevati con il nome di importazione. Quando si naviga dalla pagina **Importazioni** (cronologia delle importazioni) selezionando il nome dell'importazione elencato nella colonna **Nome**, verrà visualizzata la pagina **Server** in cui viene applicato un filtro in base al set di dati dell'importazione selezionato. Quindi, vengono visualizzati solo i dati appartenenti a quella particolare importazione.

L'archivio è in formato .zip e contiene due file: `errors-file` e `failed-entries-file`. Il file di errori contiene un elenco di messaggi di errore associati a ogni riga con esito negativo e il nome di colonna associato dal file di dati per cui l'importazione non è riuscita. È possibile usare questo file per identificare rapidamente dove si sono verificati i problemi. Il file `failed-entries` include ogni riga e tutte le colonne fornite con esito negativo. È possibile eseguire le modifiche indicate nel file di errori in questo file e tentare di importare nuovamente il file con le informazioni corrette.

AWS CLI Import

Per avviare il processo di importazione dei dati dalla AWS CLI, è necessario innanzitutto installarla nel proprio ambiente. Per ulteriori informazioni, consulta [Installazione di AWS CLI](#) nella [AWS Command Line Interface Guida per l'utente](#).

Note

Se non si dispone già di un modello di importazione compilato, è possibile scaricare il modello di importazione dai nostri bucket Amazon S3 qui: https://s3.us-west-2.amazonaws.com/templates-7cfcf56-bd96-4b1c-b45b-a5b42f282e46/import_template.csv

Per avviare l'importazione di dati

1. Apri una finestra del terminale e digita il comando seguente:

```
aws discovery start-import-task --import-url s3://BucketName/ImportFile.csv --  
name ImportName
```

2. In questo modo si crea l'attività di importazione e vengono restituite le seguenti informazioni sullo stato:

```
{  
  "task": {  
    "status": "IMPORT_IN_PROGRESS",  
    "applicationImportSuccess": 0,  
    "serverImportFailure": 0,  
    "serverImportSuccess": 0,  
    "name": "ImportName",  
    "importRequestTime": 1547682819.801,  
    "applicationImportFailure": 0,  
    "clientRequestToken": "EXAMPLE1-abcd-1234-abcd-EXAMPLE1234",  
    "importUrl": "s3://BucketName/ImportFile.csv",  
    "importTaskId": "import-task-EXAMPLE1229949eabfEXAMPLE03862c0"  
  }  
}
```

Tracciamento delle richieste di importazione dell'Migration Hub

Puoi tenere traccia dello stato delle richieste di importazione di Migration Hub utilizzando la console, AWS CLI, o uno dei AWS SDK.

Console Tracking

Da almportazioninella console di Migration Hub, potrai trovare i seguenti elementi.

- NomeIl nome della richiesta di importazione.
- ID di importazione— L'ID univoco della richiesta di importazione.
- Ora di importazioneLa data e l'ora di creazione della richiesta di importazione.
- Stato dell'importazioneLo stato della richiesta di importazione. Può essere uno dei seguenti valori:
 - Importazione di— Questo file di dati è in fase di importazione.
 - Importa— L'intero file di dati è stato correttamente importato.
 - Importato con errori— Uno o più record del file di dati non sono stati importati. Per risolvere i record con esito negativo, scegli Download failed records (Scarica record con errori) per l'attività di importazione, risolvi gli errori nel file failed-entries.csv ed effettua nuovamente l'importazione.
 - Importance— Nessuno dei record del file di dati è stato importato. Per risolvere i record con esito negativo, scegli Download failed records (Scarica record con errori) per l'attività di importazione, risolvi gli errori nel file failed-entries.csv ed effettua nuovamente l'importazione.
- Record importati— Il numero di record in uno specifico file di dati che sono stati correttamente importati.
- Record falliti— Il numero di record in uno specifico file di dati che non sono stati importati.

CLI Tracking

Puoi monitorare lo stato delle attività di importazione con il comando `aws discovery describe-import-tasks` della AWS CLI.

1. Apri una finestra del terminale e digita il comando seguente:

```
aws discovery describe-import-tasks
```

2. Questo restituirà un elenco di tutte le attività di importazione in formato JSON, completo dello stato e altre informazioni rilevanti. Eventualmente, è possibile filtrare i risultati per ottenere un sottoinsieme delle attività di importazione.

Monitorando le attività di importazione, è possibile che il valore `serverImportFailure` restituito sia superiore a zero. Quando ciò si verifica, il file di importazione aveva una o più voci che non è stato possibile importare. Questo può essere risolto scaricando l'archivio dei record con errori, esaminando i file all'interno ed effettuando un'altra richiesta di importazione con il file `failed-entries.csv` modificato.

Dopo aver creato l'attività di importazione, è possibile eseguire operazioni aggiuntive per facilitare la gestione e il monitoraggio della migrazione dei dati. Ad esempio, è possibile scaricare un archivio di record con errori per una richiesta specifica. Per informazioni sull'utilizzo dell'archivio di record con errori per risolvere problemi di importazione, consulta [Risoluzione dei record di importazione non riusciti](#).

Visualizza, esporta ed esplora i dati scoperti

Application Discovery Service Agentless Collector (Agentless Collector) e AWS Discovery Agent (Discovery Agent) fornisce dati sulle prestazioni del sistema in base all'utilizzo medio e massimo. È possibile utilizzare i dati sulle prestazioni del sistema raccolti per ottenere un costo totale di proprietà (TCO) di alto livello. I Discovery Agent raccolgono dati più dettagliati, inclusi i dati delle serie temporali per informazioni sulle prestazioni del sistema, le connessioni di rete in entrata e in uscita e i processi in esecuzione sul server. Puoi utilizzare questi dati per comprendere le dipendenze di rete tra i server e raggruppare i server correlati come applicazioni per la pianificazione della migrazione.

In questa sezione sono disponibili le istruzioni su come visualizzare e utilizzare i dati scoperti da Agentless Collector e Discovery Agent sia dalla console che dall'AWS CLI.

Argomenti

- [Visualizza i dati raccolti utilizzando la console Migration Hub](#)
- [Esportazione dei dati raccolti](#)
- [Esplorazione dei dati in Amazon Athena](#)

Visualizza i dati raccolti utilizzando la console Migration Hub

Sia per Application Discovery Service Agentless Collector (Agentless Collector) che per AWS Discovery Agent (Discovery Agent), dopo l'avvio del processo di raccolta dei dati, è possibile utilizzare la console per visualizzare i dati raccolti su server e VM. I dati vengono visualizzati nella console circa 15 minuti dopo l'inizio della raccolta dei dati. Puoi anche visualizzare questi dati in formato CSV esportando i dati raccolti effettuando chiamate API utilizzando l'AWS CLI. L'esportazione dei dati raccolti è descritta nella sezione successiva [Esportazione dei dati raccolti](#).

Per visualizzare i dati raccolti relativi ai server rilevati

1. Nel riquadro di navigazione della console, selezionare Servers (Server). I server rilevati vengono visualizzati nell'elenco dei server.
2. Per informazioni dettagliate comprensive dei dati raccolti, selezionare il collegamento nome server nella colonna Server info (Informazioni sul server). In questo modo viene visualizzata una schermata contenente informazioni dettagliate, ad esempio informazioni di sistema, parametri di prestazioni e molto altro.

Per ulteriori informazioni sull'utilizzo della console per visualizzare, ordinare e etichettare i server scoperti dai tuoi Agentless Collectors o Discovery Agents, consulta [AWS Application Discovery Service Procedure guidate console](#).

Il modulo di raccolta dei dati di analisi e database Agentless Collector carica i dati raccolti nel bucket Amazon S3. È possibile visualizzare i dati di questo bucket nella console AWS DMS.

Per visualizzare i dati raccolti sui database e sui server di analisi rilevati

1. Accedi AWS Management Console e apri la console AWS DMS all'[indirizzo https://console.aws.amazon.com/dms/v2/](https://console.aws.amazon.com/dms/v2/).
2. Scegli Inventario in Scopri. La pagina Inventario si apre e mostra un elenco di database e server di analisi rilevati.

Logica corrispondente per i server e le applicazioni rilevati

AWS Application Discovery Service (Application Discovery Service) dispone di una logica di corrispondenza integrata che identifica quando i server che rileva corrispondono alle voci esistenti. Quando questa logica trova una corrispondenza, aggiorna le informazioni per il server rilevato già esistente con i nuovi valori.

Questa logica di abbinamento gestisce server duplicati da più fonti, tra cui l'importazione AWS Migration Hub (Migration Hub), Application Discovery Service Agentless Collector (Agentless Collector), AWS Application Discovery Agent (Discovery Agent) e altri strumenti di migrazione. Per ulteriori informazioni sull'importazione di Migration Hub, consulta [Migration Hub Import](#).

Quando viene effettuato il rilevamento di server, ogni voce viene controllata con i record importati in precedenza per verificare che il server importato non esista già. Se non viene trovata alcuna corrispondenza, viene creato un nuovo record e viene assegnato un nuovo identificatore univoco al server. Se viene trovata una corrispondenza, viene comunque creata una nuova voce ma viene assegnato lo stesso identificatore univoco del server esistente. Quando visualizzi questo server nella console Migration Hub, trovi solo una voce univoca per il server.

Gli attributi del server associati a questa voce vengono uniti per visualizzare i valori degli attributi da un record disponibile in precedenza insieme al record appena importato. Se per un determinato attributo di server da diverse origini è presente più di un valore, ad esempio due valori diversi all'interno per Total RAM associati a un determinato server rilevato utilizzando l'importazione e anche dal Discovery Agent, nel record corrispondente al server viene mostrato il valore che è stato rilevato più recentemente.

Campi corrispondenti

I seguenti campi vengono utilizzati per abbinare i server quando vengono usati gli strumenti di rilevamento.

- **ExternalId**— Questo è il campo principale utilizzato per abbinare i server. Se il valore in questo campo è identico a un altro `ExternalId` in un'altra voce, Application Discovery Service confronta le due voci, indipendentemente dal fatto che gli altri campi corrispondano o meno.
- **IPAddress**
- **HostName**
- **MacAddress**
- **VMware. MoRefId** e **VMware. vCenterId**— Entrambi questi valori devono essere identici ai rispettivi campi di un'altra voce affinché Application Discovery Service possa eseguire una corrispondenza.

Esportazione dei dati raccolti

Sia per Application Discovery Service Agentless Collector (Agentless Collector) che per AWS Application Discovery Agent (Discovery Agent), dopo l'avvio del processo di raccolta dei dati, è possibile esportare i dati raccolti sui server e sulle VM. Questi dati possono essere esportati interagendo con la console o effettuando chiamate API tramite il AWS CLI, a seconda dello strumento di rilevamento utilizzato per raccogliere i dati.

Di seguito vengono fornite le istruzioni per entrambi i modi espandendo il metodo di scelta.

Esporta i dati raccolti per tutti i server utilizzando il AWS CLI

I dati raccolti da tutti i raccoglitori senza agenti e gli agenti di rilevamento in esecuzione sugli host e sulle macchine virtuali possono essere esportati in blocco utilizzando AWS Command Line Interface (AWS CLI). AWS CLI è necessario installarlo nell'ambiente prima di esportare i dati.

Per installare AWS CLI ed esportare i dati raccolti

1. Se non è già stato fatto, installare il AWS CLI appropriato per il tipo di sistema operativo (Windows o Mac/Linux). Per le istruzioni di installazione, consulta la [Guida per AWS Command Line Interface l'utente](#).
2. Aprire il prompt dei comandi (Windows) o Terminal (Mac/Linux).
 - a. Digitare `aws configure` e premere Invio.

- b. Inserisci AWS l'ID della chiave di accesso e la chiave di accesso AWS segreta.
 - c. Immettere `us-west-2` per Default Region Name (Nome della regione predefinito).
 - d. Immettere `text` per Default Output Format (Formato di output predefinito).
3. Digitare il comando seguente per generare un ID esportazione:

```
aws discovery start-export-task
```

4. Utilizzando l'ID di esportazione generato nella fase precedente, digitare il comando seguente per generare un URL S3 come un valore per il parametro "configurationsDownloadUrl":

```
aws discovery describe-export-tasks --export-ids <export ID>
```

5. Copiare l'URL generato nella fase precedente e incollarlo in un browser per scaricare il file ZIP con i dati raccolti dei server rilevati.

L'agente di esportazione ha raccolto i dati utilizzando la console

L'esportazione dei dati raccolti dall'agente dalla console è limitata a un agente, quando ci si trova nella pagina dei dettagli di un server specifico. Nella pagina dei dettagli, puoi trovare i lavori di esportazione del server elencati nella parte inferiore dello schermo, sotto Esportazioni. Se non è stata creata alcuna pagina, la pagina è vuota. È possibile eseguire fino a cinque esportazioni di dati del server alla volta.

Per esportare i dati raccolti relativi a un server rilevato

1. Nel riquadro di navigazione, selezionare Servers (Server).
2. Nella colonna Server info (Informazioni sul server), selezionare il collegamento per il server per cui si desidera esportare dati.
3. Nella sezione Exports (Esportazioni) nella parte inferiore della schermata, selezionare Export server details (Esporta dettagli server).
4. Per Export server details (Esporta dettagli server), compila i campi Start date (Data di inizio) e Time (Ora).

Note

L'ora di inizio non può essere più di 72 ore precedente all'ora corrente.

5. Scegli Export (Esporta) per avviare il processo. Lo stato iniziale è In-progress (In corso); per aggiornare lo stato, fare clic sull'icona di aggiornamento per la sezione Exports (Esportazioni).
6. Una volta completato il processo di esportazione, selezionare Download (Scarica) e salvare il file ZIP.
7. Decomprimi il file salvato. Un set di file.csv contiene i dati di esportazione.

Puoi aprire i file CSV in Microsoft Excel e rivedere i dati server esportati.

Tra i file, puoi trovare un file JSON contenente dati sull'attività di esportazione e i relativi risultati.

Note

Per informazioni sulla generazione ed esportazione dei consigli sulle istanze di Amazon Elastic Compute Cloud (Amazon EC2) nellaAWS Migration Hub console, consulta i consigli [sulle istanze di Amazon EC2](#) nella Guida per l'AWS Migration Hubutente.

Esplorazione dei dati in Amazon Athena

L'esplorazione dei dati in Amazon Athena consente di analizzare i dati raccolti da tutti i server locali scoperti da Discovery Agents in un'unica posizione. Una volta abilitata l'esplorazione dei dati in Amazon Athena dalla console di Migration Hub (o utilizzando il StartContinuousExport API) e la raccolta dei dati per gli agenti è attivata, i dati raccolti dagli agenti vengono automaticamente archiviati nel bucket S3 a intervalli regolari.

Puoi quindi visitare Amazon Athena per eseguire query predefinite per analizzare le prestazioni del sistema delle serie temporali per ogni server, il tipo di processi in esecuzione su ogni server e le dipendenze di rete tra server diversi. Inoltre, puoi scrivere le tue query personalizzate utilizzando Amazon Athena, caricare fonti di dati esistenti aggiuntive come le esportazioni del database di gestione della configurazione (CMDB) e associare i server scoperti alle applicazioni aziendali effettive. Puoi anche integrare il database Athena con Amazon QuickSight per visualizzare i risultati delle interrogazioni ed eseguire analisi aggiuntive

Fasi

1. [Abilitare l'esplorazione dei dati in Amazon Athena](#)
2. [Lavorare con l'esplorazione dei dati in Amazon Athena](#)

Abilitare l'esplorazione dei dati in Amazon Athena

L'esplorazione dei dati in Amazon Athena è abilitata attivando l'esportazione continua utilizzando la console Migration Hub o una chiamata API da AWS CLI. Devi attivare l'esplorazione dei dati prima di poter vedere e iniziare a esplorare i dati scoperti in Amazon Athena.

Quando attivi l'esegui l'esportazione continua, il ruolo collegato al servizio `AWS::ServiceRoleForApplicationDiscoveryServiceContinuousExport` viene utilizzato automaticamente dal tuo account. Per ulteriori informazioni sul ruolo collegato a questo servizio, consulta [Autorizzazioni del ruolo collegato ai servizi per Application Discovery Service](#).

Le seguenti istruzioni mostrano come abilitare l'esplorazione dei dati in Amazon Athena utilizzando la console e l'AWS CLI.

Enable with the console

L'esplorazione dei dati in Amazon Athena è abilitata dall'attivazione implicita dell'esportazione continua quando scegli «Avvia raccolta dati» o fai clic sull'interruttore denominato «Esplorazione dati in Amazon Athena» sul pannello di controllo della console Migration Hub.

Per abilitare l'esplorazione dei dati in Amazon Athena dalla console

1. Nel riquadro di navigazione, selezionare Data Collectors (Agenti di raccolta dati).
2. Selezionare la scheda Agents (Agenti).
3. Scegli Avvia raccolta dei dati oppure, se hai già attivato la raccolta dei dati, fai clic su Esplorazione dei dati in Amazon Athena attiva/disattiva.
4. Nella finestra di dialogo generata dal passaggio precedente, fare clic sulla casella di controllo dando il consenso ai costi associati e scegliere Continue (Continua) o Enable (Abilita).

Note

I tuoi agenti sono ora in esecuzione in modalità «esportazione continua» che ti consentirà di visualizzare e lavorare con i dati scoperti in Amazon Athena. La prima volta che viene abilitata, potrebbero essere necessari fino a 30 minuti prima che i tuoi dati vengano visualizzati in Amazon Athena.

Enable with the AWS CLI

L'esplorazione dei dati in Amazon Athena è abilitata dall'esportazione continua attivata esplicitamente tramite una chiamata API da AWS CLI. Per eseguire questa operazione, AWS CLI deve prima essere installata nel tuo ambiente.

Per installare AWS CLI e abilita l'esplorazione dei dati in Amazon Athena

1. Installare AWS CLI per il sistema operativo in uso (Linux, macOS o Windows). Consulta il [AWS Command Line Interface Guida per l'utente di](#) per istruzioni.
2. Aprire il prompt dei comandi (Windows) o Terminal (Linux o macOS).
 - a. Digitare `aws configure` e premere Invio.
 - b. Inserisci il tuo AWS ID chiave di accesso e AWS Chiave di accesso segreta.
 - c. Immettere `us-west-2` per Default Region Name (Nome della regione predefinito).
 - d. Immettere `text` per Default Output Format (Formato di output predefinito).
3. Digita il seguente comando:

```
aws discovery start-continuous-export
```

Note

I tuoi agenti sono ora in esecuzione in modalità «esportazione continua» che ti consentirà di visualizzare e lavorare con i dati scoperti in Amazon Athena. La prima volta che viene abilitata, potrebbero essere necessari fino a 30 minuti prima che i tuoi dati vengano visualizzati in Amazon Athena.

Lavorare con l'esplorazione dei dati in Amazon Athena

Dopo aver abilitato l'esplorazione dei dati in Amazon Athena, puoi iniziare a esplorare e lavorare con dati correnti dettagliati scoperti dai tuoi agenti interrogando i dati direttamente in Athena. È possibile utilizzare i dati per generare fogli di calcolo, eseguire un'analisi dei costi, trasferire la query su un programma di visualizzazione per una rappresentazione grafica delle dipendenze di rete e altro ancora.

Gli argomenti di questa sezione descrivono i modi in cui è possibile utilizzare i dati in Athena per valutare e pianificare la migrazione dell'ambiente locale verso AWS.

Argomenti

- [Esplorazione di dati direttamente in Amazon Athena](#)
- [Visualizzazione di dati di Amazon Athena](#)
- [Interrogazioni predefinite da utilizzare in Athena](#)

Esplorazione di dati direttamente in Amazon Athena

Le seguenti istruzioni illustrano come esplorare i dati dell'agente direttamente nella console Athena. Se non disponi di dati in Athena o non hai abilitato l'esplorazione dei dati in Amazon Athena, ti verrà richiesto di abilitare l'esplorazione dei dati in Amazon Athena, come spiegato in [Abilitare l'esplorazione dei dati in Amazon Athena](#).

Per esplorare i dati scoperti dagli agenti direttamente in Athena

1. Aprire la console AWS Migration Hub e scegliere Servers (Server) nel riquadro di navigazione.
2. Per aprire la console Amazon Athena, scegli Esplora i dati in Amazon Athena.
3. Nella pagina Editor di query, nel riquadro di navigazione in Database, assicurarsi che sia selezionato `application_discovery_service_database`.

Note

In Tabelle le tabelle seguenti rappresentano i set di dati raggruppati in base agli agenti.

- `os_info_agent`
- `network_interface_agent`
- `sys_performance_agent`
- `processes_agent`
- `inbound_connection_agent`
- `outbound_connection_agent`
- `id_mapping_agent`

4. Interroga i dati nella console Amazon Athena scrivendo ed eseguendo interrogazioni SQL nell'Athena Query Editor. Ad esempio, è possibile utilizzare la seguente query per visualizzare tutti gli indirizzi IP del server rilevati.

```
SELECT * FROM network_interface_agent;
```

Per ulteriori query di esempio, consulta [Interrogazioni predefinite da utilizzare in Athena](#).

Visualizzazione di dati di Amazon Athena

Per visualizzare i dati, è possibile trasferire una query su un programma di visualizzazione come Amazon QuickSight o altri strumenti di visualizzazione open source come Cytoscape, yEd o Gelphi. Utilizza questi strumenti per eseguire il rendering di diagrammi di rete, grafici di riepilogo e altre rappresentazione grafiche. Quando si utilizza questo metodo, ci si connette ad Athena tramite il programma di visualizzazione in modo che possa accedere ai dati raccolti come fonte per produrre la visualizzazione.

Per visualizzare i dati di Amazon Athena utilizzando Amazon QuickSight

1. Accesso [Amazon QuickSight](#).
2. Seleziona Connect to another data source or upload a file (Connessione a un'altra origine dati o caricamento di un file).
3. Scegli Athena. In Nuova origine dati Athena viene visualizzata una finestra di dialogo.
4. Immetti un nome nel campo Data source name (Nome origine dati).
5. Seleziona Create data source (Crea origine dati).
6. Select UNgents-servers-ostabella in Scegli il tuo tavolo finestra di dialogo e scegli Select.
7. Nella finestra di dialogo Termina la creazione del set di dati, seleziona Importa su SPICE per analisi più rapide e scegli Visualizza.

La visualizzazione viene renderizzata.

Interrogazioni predefinite da utilizzare in Athena

Questa sezione contiene un insieme di query predefinite che eseguono casi d'uso tipici, ad esempio l'analisi TCO e la visualizzazione di rete. È possibile utilizzare queste query così come sono o modificarle in base alle esigenze.

Per utilizzare una query predefinita

1. Aprire la console AWS Migration Hub e scegliere Servers (Server) nel riquadro di navigazione.
2. Per aprire la console Amazon Athena, scegliEsplora i dati in Amazon Athena.
3. Nella pagina Editor di query, nel riquadro di navigazione in Database, assicurarsi che sia selezionato `application_discovery_service_database`.
4. Scegliere il segno più (+) nell'editor delle query per creare una scheda per una nuova query.
5. Copiare una delle query da [Query predefinite](#).
6. Incollare la query nel riquadro delle query della nuova scheda di query appena creata.
7. Scegliere Run Query (Esegui query).

Query predefinite

Scegliere un titolo per visualizzare le informazioni sulla query.

Ottieni indirizzi IP e nomi host per i server

Questa funzione helper di visualizzazione consente di recuperare gli indirizzi IP e i nomi host per un determinato server. È possibile utilizzare questa visualizzazione in altre query. Per informazioni su come creare una visualizzazione, consulta [CREARE UNA VISUALIZZAZIONE](#) nel Guida per l'utente di Amazon Athena.

```
CREATE OR REPLACE VIEW hostname_ip_helper AS
SELECT DISTINCT
  "os"."host_name"
, "nic"."agent_id"
, "nic"."ip_address"
FROM
  os_info_agent os
, network_interface_agent nic
WHERE ("os"."agent_id" = "nic"."agent_id");
```

Identifica i server con o senza agenti

Questa query consente di eseguire la convalida dei dati. Se hai distribuito agenti su una serie di server nella rete, puoi usare questa query per capire se ci sono altri server nella rete su cui non sono stati distribuiti agenti. In questa query, viene esaminato il traffico di rete in entrata e in uscita e viene

filtrato solo il traffico per gli indirizzi IP privati. Si tratta quindi degli indirizzi IP che iniziano con 192, 10 o 172.

```

SELECT DISTINCT "destination_ip" "IP Address" ,
    (CASE
    WHEN (
    (SELECT "count"(*)
    FROM network_interface_agent
    WHERE ("ip_address" = "destination_ip") ) = 0) THEN
        'no'
    WHEN (
    (SELECT "count"(*)
    FROM network_interface_agent
    WHERE ("ip_address" = "destination_ip") ) > 0) THEN
        'yes' END) "agent_running"
    FROM outbound_connection_agent
WHERE (((("destination_ip" LIKE '192.%')
    OR ("destination_ip" LIKE '10.%'))
    OR ("destination_ip" LIKE '172.%'))
UNION
SELECT DISTINCT "source_ip" "IP ADDRESS" ,
    (CASE
    WHEN (
    (SELECT "count"(*)
    FROM network_interface_agent
    WHERE ("ip_address" = "source_ip") ) = 0) THEN
        'no'
    WHEN (
    (SELECT "count"(*)
    FROM network_interface_agent
    WHERE ("ip_address" = "source_ip") ) > 0) THEN
        'yes' END) "agent_running"
    FROM inbound_connection_agent
WHERE (((("source_ip" LIKE '192.%')
    OR ("source_ip" LIKE '10.%'))
    OR ("source_ip" LIKE '172.%')));

```

Analizza i dati relativi alle prestazioni del sistema per i server

È possibile usare questa query per analizzare i dati delle prestazioni del sistema e dei modelli di utilizzo per i server locali su cui sono installati agenti. La query combina la tabella `system_performance_agent` con la tabella `os_info_agent` per identificare il nome host per

ogni server. Questa query restituisce i dati di utilizzo delle serie temporali (in intervalli di 15 minuti) per tutti i server su cui sono eseguiti agenti.

```
SELECT "OS"."os_name" "OS Name" ,
       "OS"."os_version" "OS Version" ,
       "OS"."host_name" "Host Name" ,
       "SP"."agent_id" ,
       "SP"."total_num_cores" "Number of Cores" ,
       "SP"."total_num_cpus" "Number of CPU" ,
       "SP"."total_cpu_usage_pct" "CPU Percentage" ,
       "SP"."total_disk_size_in_gb" "Total Storage (GB)" ,
       "SP"."total_disk_free_size_in_gb" "Free Storage (GB)" ,
       ("SP"."total_disk_size_in_gb" - "SP"."total_disk_free_size_in_gb") "Used
Storage" ,
       "SP"."total_ram_in_mb" "Total RAM (MB)" ,
       ("SP"."total_ram_in_mb" - "SP"."free_ram_in_mb") "Used RAM (MB)" ,
       "SP"."free_ram_in_mb" "Free RAM (MB)" ,
       "SP"."total_disk_read_ops_per_sec" "Disk Read IOPS" ,
       "SP"."total_disk_bytes_written_per_sec_in_kbps" "Disk Write IOPS" ,
       "SP"."total_network_bytes_read_per_sec_in_kbps" "Network Reads (kbps)" ,
       "SP"."total_network_bytes_written_per_sec_in_kbps" "Network Write (kbps)"
FROM "sys_performance_agent" "SP" , "OS_INFO_agent" "OS"
WHERE ("SP"."agent_id" = "OS"."agent_id") limit 10;
```

Tieni traccia delle comunicazioni in uscita tra server in base al numero di porta e ai dettagli del processo

Questa query ottiene i dettagli sul traffico in uscita per ogni servizio, insieme al numero di porta e ai dettagli del processo.

Prima di eseguire la query, se non è già stata eseguita questa operazione, è necessario creare la tabella `iana_service_ports_import` contenente il database del registro delle porte IANA scaricato da IANA. Per informazioni su come creare questa tabella, consulta [Creazione della tabella di importazione del registro delle porte IANA](#).

Dopo aver creato la tabella `iana_service_ports_import`, creare due funzioni helper di visualizzazione per il monitoraggio del traffico in uscita. Per informazioni su come creare una visualizzazione, consulta [CREARE UNA VISUALIZZAZIONE](#) nel Guida per l'utente di Amazon Athena.

Per creare funzioni helper per il monitoraggio in uscita

1. Aprire la console Athena all'indirizzo <https://console.aws.amazon.com/athena/>.

2. Creazione del `valid_outbound_ips_helper` visualizza, utilizzando la seguente funzione di supporto che elenca tutti i distinti indirizzi IP di destinazione in uscita.

```
CREATE OR REPLACE VIEW valid_outbound_ips_helper AS
SELECT DISTINCT "destination_ip"
FROM outbound_connection_agent;
```

3. Creare la vista `outbound_query_helper` utilizzando la seguente funzione helper che determina la frequenza di comunicazione per il traffico in uscita.

```
CREATE OR REPLACE VIEW outbound_query_helper AS
SELECT "agent_id" ,
       "source_ip" ,
       "destination_ip" ,
       "destination_port" ,
       "agent_assigned_process_id" ,
       "count"(*) "frequency"
FROM outbound_connection_agent
WHERE (("ip_version" = 'IPv4')
       AND ("destination_ip" IN
           (SELECT *
            FROM valid_outbound_ips_helper )))
GROUP BY "agent_id", "source_ip", "destination_ip", "destination_port",
         "agent_assigned_process_id";
```

4. Dopo aver creato la tabella `iana_service_ports_import` e le due funzioni helper, è possibile eseguire la seguente query per ottenere i dettagli sul traffico in uscita per ciascun servizio, insieme al numero di porta e ai dettagli del processo.

```
SELECT hip1.host_name "Source Host Name",
       outbound_connections_results0.source_ip "Source IP Address",
       hip2.host_name "Destination Host Name",
       outbound_connections_results0.destination_ip "Destination IP Address",
       outbound_connections_results0.frequency "Connection Frequency",
       outbound_connections_results0.destination_port "Destination Communication
Port",
       outbound_connections_results0.servicename "Process Service Name",
       outbound_connections_results0.description "Process Service Description"
FROM
  (SELECT DISTINCT o.source_ip,
                  o.destination_ip,
                  o.frequency,
```

```

        o.destination_port,
        ianap.servicename,
        ianap.description
    FROM outbound_query_helper o, iana_service_ports_import ianap
    WHERE o.destination_port = TRY_CAST(ianap.portnumber AS integer)) AS
    outbound_connections_results0 LEFT OUTER
JOIN hostname_ip_helper hip1
    ON outbound_connections_results0.source_ip = hip1.ip_address LEFT OUTER
JOIN hostname_ip_helper hip2
    ON outbound_connections_results0.destination_ip = hip2.ip_address

```

Tieni traccia delle comunicazioni in entrata tra server in base al numero di porta e ai dettagli del processo

Questa query ottiene le informazioni sul traffico in ingresso per ogni servizio, insieme al numero di porta e ai dettagli del processo.

Prima di eseguire questa query, se non è già stato fatto, è necessario creare la tabella `iana_service_ports_import` contenente il database del registro delle porte IANA scaricato da IANA. Per informazioni su come creare questa tabella, consulta [Creazione della tabella di importazione del registro delle porte IANA](#).

Dopo aver creato la tabella `iana_service_ports_import`, creare due funzioni helper di visualizzazione per il monitoraggio del traffico in entrata. Per informazioni su come creare una visualizzazione, consulta [CREARE UNA VISUALIZZAZIONE](#) nel Guida per l'utente di Amazon Athena.

Per creare funzioni helper che consentano di importare il monitoraggio

1. Aprire la console Athena all'indirizzo <https://console.aws.amazon.com/athena/>.
2. Creare la vista `valid_inbound_ips_helper` utilizzando la seguente funzione helper che elenca tutti i distinti indirizzi IP di origine in entrata.

```

CREATE OR REPLACE VIEW valid_inbound_ips_helper AS
SELECT DISTINCT "source_ip"
FROM inbound_connection_agent;

```

3. Creare la vista `inbound_query_helper` utilizzando la seguente funzione helper che determina la frequenza di comunicazione per il traffico in entrata.

```

CREATE OR REPLACE VIEW inbound_query_helper AS

```

```

SELECT "agent_id" ,
       "source_ip" ,
       "destination_ip" ,
       "destination_port" ,
       "agent_assigned_process_id" ,
       "count"(*) "frequency"
FROM inbound_connection_agent
WHERE (("ip_version" = 'IPv4')
       AND ("source_ip" IN
           (SELECT *
            FROM valid_inbound_ips_helper )))
GROUP BY "agent_id", "source_ip", "destination_ip", "destination_port",
         "agent_assigned_process_id";

```

4. Dopo aver creato la tabella `iana_service_ports_import` e le due funzioni helper, è possibile eseguire la seguente query per ottenere i dettagli sul traffico in entrata per ciascun servizio, insieme al numero di porta e ai dettagli del processo.

```

SELECT hip1.host_name "Source Host Name",
       inbound_connections_results0.source_ip "Source IP Address",
       hip2.host_name "Destination Host Name",
       inbound_connections_results0.destination_ip "Destination IP Address",
       inbound_connections_results0.frequency "Connection Frequency",
       inbound_connections_results0.destination_port "Destination Communication
Port",
       inbound_connections_results0.servicename "Process Service Name",
       inbound_connections_results0.description "Process Service Description"
FROM
  (SELECT DISTINCT i.source_ip,
                  i.destination_ip,
                  i.frequency,
                  i.destination_port,
                  ianap.servicename,
                  ianap.description
   FROM inbound_query_helper i, iana_service_ports_import ianap
   WHERE i.destination_port = TRY_CAST(ianap.portnumber AS integer)) AS
inbound_connections_results0 LEFT OUTER
JOIN hostname_ip_helper hip1
  ON inbound_connections_results0.source_ip = hip1.ip_address LEFT OUTER
JOIN hostname_ip_helper hip2
  ON inbound_connections_results0.destination_ip = hip2.ip_address

```

Identifica il software in esecuzione in base al

Questa query identificherà il software in esecuzione in base ai numeri di porta.

Prima di eseguire questa query, se non è già stato fatto, è necessario creare la tabella `iana_service_ports_import` contenente il database del registro delle porte IANA scaricato da IANA. Per informazioni su come creare questa tabella, consulta [Creazione della tabella di importazione del registro delle porte IANA](#).

La seguente query può essere utilizzata per identificare il software in esecuzione in base ai numeri di porta.

```
SELECT o.host_name "Host Name",
       ianap.servicename "Service",
       ianap.description "Description",
       con.destination_port,
       con.cnt_dest_port "Destination Port Count"
FROM   (SELECT agent_id,
               destination_ip,
               destination_port,
               Count(destination_port) cnt_dest_port
        FROM   inbound_connection_agent
        GROUP  BY agent_id,
                 destination_ip,
                 destination_port) con,
       (SELECT agent_id,
               host_name,
               Max("timestamp")
        FROM   os_info_agent
        GROUP  BY agent_id,
                 host_name) o,
       iana_service_ports_import ianap
WHERE  ianap.transportprotocol = 'tcp'
       AND con.destination_ip NOT LIKE '172%'
       AND con.destination_port = ianap.portnumber
       AND con.agent_id = o.agent_id
ORDER BY cnt_dest_port DESC;
```

Creazione della tabella di importazione del registro delle porte IANA

Alcune delle query predefinite richiedono una tabella denominata `iana_service_ports_import` contenente informazioni scaricate da Internet Assigned Numbers Authority (IANA).

Per creare la tabella `iana_service_ports_import`

1. Scarica il database del registro delle porte IANACSVfile da [Nome del servizio e registro del numero di porta del protocollo](#) `disuliana.org`.
2. Carica il file in Amazon S3. Per ulteriori informazioni, consulta [Come caricare file e cartelle in un bucket S3](#).
3. Crea una nuova tabella in Athena denominata `iana_service_ports_import`. Per istruzioni, consulta [Creare una tabella](#) nel Guida per l'utente di Amazon Athena. Nell'esempio seguente, è necessario sostituire `my_bucket_name` con il nome del bucket S3 in cui è stato caricato il file CSV nella fase precedente.

```
CREATE EXTERNAL TABLE IF NOT EXISTS iana_service_ports_import (  
    ServiceName STRING,  
    PortNumber INT,  
    TransportProtocol STRING,  
    Description STRING,  
    Assignee STRING,  
    Contact STRING,  
    RegistrationDate STRING,  
    ModificationDate STRING,  
    Reference STRING,  
    ServiceCode STRING,  
    UnauthorizedUseReported STRING,  
    AssignmentNotes STRING  
)  
ROW FORMAT SERDE 'org.apache.hadoop.hive.serde2.lazy.LazySimpleSerDe'  
WITH SERDEPROPERTIES (  
    'serialization.format' = ',',  
    'quoteChar' = '"',  
    'field.delim' = ','  
) LOCATION 's3://my_bucket_name/'  
TBLPROPERTIES ('has_encrypted_data'='false','skip.header.line.count'='1');
```

AWS Application Discovery Service Procedure guidate console

AWS Application Discovery Service (Application Discovery Service) è integrato con AWS Migration Hub (Migration Hub) e i clienti possono visualizzare e gestire i propri strumenti di raccolta dati, server e applicazioni all'interno di Migration Hub. Quando si utilizza la console di Application Discovery Service, si viene reindirizzati alla console di Migration Hub. L'utilizzo della console Migration Hub non richiede passaggi o configurazioni aggiuntive da parte dell'utente.

In questa sezione viene descritto come gestire e monitorare Application Discovery Service Agentless Collector (Agentless Collector) e AWS Application Discovery Agent (Discovery Agent) utilizzando la console.

Argomenti

- [Pannello di controllo principale](#)
- [Strumenti di raccolta dei dati](#)
- [Visualizza, esporta ed esplora i dati del server](#)

Pannello di controllo principale

Per visualizzare la dashboard principale, scegli il Pannello di controllo di navigazione della console (Migration Hub) Nella dashboard principale di Migration Hub, è possibile visualizzare statistiche di alto livello su server, applicazioni e raccoglitori di dati come Application Discovery Service Agentless Collector (Agentless Collector) e AWS Application Discovery Agent (agente Discovery).

Pannello di controllo principale

Il pannello di controllo principale consente di raccogliere i dati dei pannelli di controllo Discover (Rileva) e Migrate (Migra) in una posizione centrale. Dispone di quattro riquadri di stato e di informazioni e di un elenco di collegamenti per l'accesso rapido. Utilizzando i riquadri, puoi visualizzare uno stato di riepilogo delle applicazioni aggiornate più di recente. Puoi anche accedere rapidamente a una qualsiasi delle applicazioni, ottenere una panoramica di applicazioni in stati diversi e monitorare l'avanzamento della migrazione nel tempo.

Per visualizzare la dashboard principale, scegli il riquadro di navigazione, che si trova sul lato sinistro della home page della console di Migration Hub.

Strumenti di raccolta dei dati

Application Discovery Service Agentless Collector (Agentless Collector) e AWS Application Discovery Agent (Discovery Agent) sono gli strumenti di raccolta dati che AWS Application Discovery Service (Application Discovery Service) viene utilizzato per aiutarti a scoprire l'infrastruttura esistente. Nei seguenti argomenti viene descritto come scaricare e implementare questi strumenti di raccolta dei dati di rilevamento, [Guida introduttiva a Agentless Collector](#) e [AWS Agente di individuazione delle applicazioni](#).

Questi strumenti di raccolta dati archiviano i dati nell'archivio dell'Application Discovery Service, fornendo dettagli su ciascun server e sui processi in esecuzione su di esso. Quando uno di questi strumenti viene implementato, è possibile avviare, interrompere e visualizzare i dati raccolti dalla AWS Migration Hub console (Migration Hub).

Argomenti

- [Avvio e arresto dei raccoglitori di dati](#)
- [Visualizzazione e ordinamento dei raccoglitori di dati](#)

Avvio e arresto dei raccoglitori di dati

Dopo il AWS Application Discovery Agent (Discovery Agent) è distribuito, è possibile avviare o interrompere il processo di raccolta dei dati sui Raccoglitori di dati della pagina della AWS Migration Hub console (Migration Hub).

Per avviare o arrestare gli strumenti di raccolta dei dati

1. Utilizzo dell'account AWS, accedi alla AWS Management Console e apri la console Migration Hub su <https://console.aws.amazon.com/migrationhub/>.
2. Nel pannello di navigazione della console Migration Hub sotto Scopri, scegli Raccoglitori di dati.
3. Selezionare la scheda Agents (Agenti).
4. Selezionare la casella di controllo dello strumento di raccolta che si desidera avviare o arrestare.
5. Selezionare Start data collection (Avvia raccolta dei dati) o Stop data collection (Arresta raccolta dei dati).

Visualizzazione e ordinamento dei raccoglitori di dati

Se hai distribuito molti raccoglitori di dati, puoi ordinare l'elenco visualizzato dei raccoglitori distribuiti sul Raccoglitori di pagina della console. Ordina l'elenco applicando filtri nella barra di ricerca. Puoi eseguire una ricerca e applicare filtri alla maggior parte dei criteri specificati nell'elenco Data Collectors (Agenti di raccolta dati).

Nella tabella riportata di seguito vengono mostrati i criteri di ricerca utilizzabili per Agenti, inclusi operatori, valori e una definizione dei valori.

Criterio di ricerca	Operatore	Valore: Definizione
Agent ID (ID agente)	==	Qualsiasi ID agente selezionato dall'elenco precompilato da cui è installato uno strumento di raccolta.
Hostname (Nome host)	==	Per agenti, qualsiasi nome host selezionato dall'elenco precompilato di host in cui è installato un agente.
	!=	
Collection status (Stato di raccolta)	==	Avvio delle I dati vengono raccolti e inviati all'Application Discovery Service
	!=	Avvio programmato: L'inizio della raccolta dei dati è pianificato. I dati verranno inviati all'Application Discovery Service al ping successivo e lo stato verrà modificato in Avvio.
		Interrotto: I dati non vengono raccolti o inviati al Application Discovery Service.
		Interruzione pianificata: È prevista l'interruzione della

Criterio di ricerca	Operatore	Valore: Definizione
		raccolta dei dati. I dati non verranno più inviati all'Application Discovery Service al ping successivo e lo stato verrà modificato in Interrotto.
Integrità	== !=	<p>Integro: La raccolta dei dati non è attivata. Lo strumento funziona correttamente.</p> <p>Malintegro: L'utensile è in stato di errore. I dati non vengono raccolti né segnalati.</p> <p>Sconosciuto: Nessuna connessione stabilita in più di un'ora.</p> <p>Arresto di tipo: L'ultimo strumento ha comunicato lo «spegnimento» a causa dell'arresto di un sistema, di un servizio o di un daemon. Se si è verificato un riavvio o un aggiornamento dello strumento, lo stato cambierà in un altro in corrispondenza del primo ciclo di reporting.</p> <p>In esecuzione: La raccolta dei dati è attivata. Lo strumento funziona correttamente.</p>

Critério di ricerca	Operatore	Valore: Definizione
Indirizzo IP	==	Qualsiasi indirizzo IP selezionato dall'elenco precompilato in cui è installato uno strumento di raccolta.
	!=	

Nella tabella riportata di seguito vengono mostrati i criteri di ricerca utilizzabili per Raccoglitori senza agenti, inclusi operatori, valori e una definizione dei valori.

Critério di ricerca	Operatore	Valore: Definizione
ID	==	Qualsiasi ID di raccolta senza agenti selezionato dall'elenco precompilato da cui è installato o uno strumento di raccolta.
Hostname (Nome host)	==	Per i raccoglitori senza agenti, qualsiasi nome host selezionato dall'elenco precompilato di host in cui è installato un raccoglitore senza agenti.
	!=	
Stato	==	Raccolta di dati: La raccolta dei dati è attivata. Lo strumento funziona correttamente.
	!=	Pronto per la configurazione: la raccolta dei dati non è attivata. Lo strumento funziona correttamente. Richiede attenzione: lo strumento è in stato di errore e richiede attenzione.

Critero di ricerca	Operatore	Valore: Definizione
		<p>Sconosciuto: Nessuna connessione stabilita in più di un'ora.</p> <p>Chiusura: L'ultimo strumento ha comunicato lo «spegnimento» a causa dell'arresto di un sistema, di un servizio o di un daemon. Se si è verificato un riavvio o un aggiornamento dello strumento, lo stato cambierà in un altro in corrispondenza del primo ciclo di reporting.</p>
Indirizzo IP	<p>==</p> <p>!=</p>	Qualsiasi indirizzo IP selezionato dall'elenco precompilato in cui è installato uno strumento di raccolta.

Per ordinare gli agenti di raccolta dati applicando filtri di ricerca

1. Utilizzo dellaAWSaccount, accedi alAWS Management Consolee apri la console Migration Hub su<https://console.aws.amazon.com/migrationhub/>.
2. Nel pannello di navigazione della console Migration Hub sottoScopri, scegliRaccoglitori di.
3. Scegli uno deiRaccoglitori senza agenteAgentiTabulatore.
4. Fare clic all'interno della barra di ricerca e scegliere un criterio di ricerca dall'elenco.
5. Selezionare un operatore dall'elenco successivo.
6. Selezionare un valore dall'ultimo elenco.

Visualizza, esporta ed esplora i dati del server

Nella pagina Servers (Server) vengono forniti la configurazione di sistema e i dati di prestazioni relativi a ogni istanza del server nota agli strumenti di raccolta dei dati. Puoi visualizzare informazioni

sul server, ordinare server con filtri, applicare tag a server come coppie chiave-valore ed esportare informazioni server e di sistema dettagliate.

Argomenti

- [Visualizzazione e ordinamento dei server](#)
- [Server di tagging](#)
- [Esportazione dei dati del server](#)
- [L'esplorazione dei dati in Athena](#)
- [Applicazioni](#)

Visualizzazione e ordinamento dei server

Puoi visualizzare informazioni relative ai server rilevati dagli strumenti di raccolta dei dati e scorrere i server utilizzando filtri.

Server di visualizzazione

Puoi ottenere una vista generale e una vista dettagliata dei server rilevati dagli strumenti di raccolta dei dati.

Per visualizzare i server rilevati

1. Utilizzo dellaAWSaccount, accedi alAWS Management Consolee apri la console Migration Hub su<https://console.aws.amazon.com/migrationhub/>.
2. Nel pannello di navigazione della console Migration Hub sottoScopri, scegliServer. I server rilevati vengono visualizzati nell'elenco dei server.
3. Per ulteriori informazioni su un server, selezionare il relativo collegamento server nella colonna Server info (Informazioni sul server). In questo modo viene visualizzata una schermata contenente una descrizione del server.

Nella schermata dei dettagli del server vengono visualizzate le informazioni di sistema e i parametri di prestazioni. Puoi anche trovare un pulsante per esportare dipendenze di rete e informazioni sui processi. Per esportare informazioni server dettagliate, consulta [Esportazione dei dati del server](#).

Ordinamento dei server con filtri di ricerca

Per trovare facilmente server specifici, applica filtri di ricerca per scorrere tutti i server rilevati dagli strumenti di raccolta. Puoi eseguire una ricerca e applicare un filtro su numerosi criteri.

Per ordinare i server applicando filtri di ricerca

1. Utilizzo dellaAWSaccount, accedi alAWS Management Consolee apri la console Migration Hub su<https://console.aws.amazon.com/migrationhub/>.
2. Nel pannello di navigazione della console Migration Hub sottoScopri, scegliServer.
3. Fare clic all'interno della barra di ricerca e scegliere un criterio di ricerca dall'elenco.
4. Selezionare un operatore dall'elenco successivo.
5. Digitare un valore che prevede una distinzione tra lettere maiuscole e minuscole per il criterio di ricerca selezionato e premere Invio.
6. Per applicare più filtri, ripetere le fasi da 2 a 4.

Server di tagging

Per facilitare la pianificazione della migrazione e rimanere organizzato, puoi creare più tag per ogni server. I tag sono coppie chiave-valore definite dall'utente che possono archiviare dati o metadati personalizzati relativi ai server. È possibile etichettare un singolo server o più server in un'unica operazione.AWS Application Discovery Service I tag (Application Discovery Service) sono simili aAWStag, ma i due tipi di tag non possono essere usati in modo intercambiabile.

Puoi aggiungere o rimuovere più tag per uno o più server dalla pagina principale Servers (Server). Nella pagina dei dettagli di un server, puoi aggiungere o rimuovere uno o più tag per il server selezionato. Puoi eseguire qualsiasi tipo di attività di applicazione tag che prevede più server o tag in un'unica operazione. Puoi anche rimuovere tag.

Per aggiungere tag a uno o più server

1. Utilizzo dellaAWSaccount, accedi alAWS Management Consolee apri la console Migration Hub su<https://console.aws.amazon.com/migrationhub/>.
2. Nel pannello di navigazione della console Migration Hub sottoScopri, scegliServer.
3. Nella colonna Server info (Informazioni sul server), selezionare il collegamento server per il server cui si desidera aggiungere tag. Per aggiungere tag a più di un server alla volta, fare clic all'interno delle caselle di controllo di più server.

4. Scegli **Aggiungere tag** quindi **End** **Aggiungere un nuovo tag**.
5. Nella finestra di dialogo, digitate una chiave nel **Chiave** campo e, facoltativamente, un valore nel **Valore**.

Aggiungi altri tag scegliendo **Aggiungere un nuovo tag** e aggiungendo ulteriori informazioni.

6. Seleziona **Salva**.

Per rimuovere tag da uno o più server

1. Utilizzo della **AWS** account, accedi al **AWS Management Console** e apri la console **Migration Hub** su <https://console.aws.amazon.com/migrationhub/>.
2. Nel pannello di navigazione della console **Migration Hub** sotto **Scopri**, scegli **Server**.
3. Nella colonna **Server info** (**Informazioni sul server**), selezionare il collegamento server per il server dal quale si desidera rimuovere tag. Seleziona le caselle di controllo di più server per rimuovere i tag da più di un server alla volta.
4. Scegli **Rimuovi tag**.
5. Seleziona ogni tag da rimuovere.
6. Scegliere **Confirm** (**Conferma**).

Esportazione dei dati del server

Per esportare dipendenze di rete e informazioni sul processo per un server alla volta, puoi utilizzare una schermata dei dettagli del server. I processi di esportazione per un server sono disponibili in una tabella che si trova nella sezione **Exports** (**Esportazioni**) della schermata dei dettagli del server. Se non esiste ancora alcun processo di esportazione, la tabella è vuota. Puoi esportare simultaneamente fino a cinque raccolte di dati.

Note

L'esportazione dei dati del server dalla console è disponibile solo per i dati raccolti da un agente in esecuzione su quel server. Se desideri esportare in blocco i dati per tutti i server su cui sono stati installati gli agenti, vedi [Esplorazione dei dati in Amazon Athena](#).

Per esportare dati server dettagliati

1. Utilizzo dellaAWSaccount, accedi alAWS Management Consolee apri la console Migration Hub su<https://console.aws.amazon.com/migrationhub/>.
2. Nel pannello di navigazione della console Migration Hub sottoScopri, scegliServer.
3. Nella colonna Server info (Informazioni server), scegli l'ID del server di cui desideri esportare i dati.
4. Nella sezione Exports (Esportazioni) nella parte inferiore della schermata, selezionare Export server details (Esporta dettagli server).
5. Per Export server details (Esporta dettagli server), compila i campi Start date (Data di inizio) e Time (Ora).

Note

L'ora di inizio non può essere più di 72 ore precedente all'ora corrente.

6. Scegli Export (Esporta) per avviare il processo. Lo stato iniziale è In-progress (In corso); per aggiornare lo stato, fare clic sull'icona di aggiornamento per la sezione Exports (Esportazioni).
7. Una volta completato il processo di esportazione, selezionare Download (Scarica) e salvare il file ZIP.
8. Decomprimi il file salvato. Un set di file CSV contiene i dati di esportazione, in maniera simile a quanto segue:
 - *<AWSID account >*_destinationProcessConnection.csv
 - *<AWSID account >*_networkInterface.csv
 - *<AWSID account >*_osInfo.csv
 - *<AWSID account >*_process.csv
 - *<AWSID account >*_sourceProcessConnection.csv
 - *<AWSID account >*_systemPerformance.csv

Puoi aprire i file CSV in Microsoft Excel e rivedere i dati server esportati.

Tra i file, puoi trovare un file JSON contenente dati sull'attività di esportazione e i relativi risultati.

L'esplorazione dei dati in Athena

L'esplorazione dei dati in Amazon Athena consente di analizzare i dati raccolti da tutti i server locali scoperti da Discovery Agent in un'unica posizione. Una volta abilitata l'esplorazione dei dati in Amazon Athena dalla console di Migration Hub (o utilizzando il StartContinuousExport API) e la raccolta dei dati per gli agenti è attivata, i dati raccolti dagli agenti vengono automaticamente archiviati nel bucket S3 a intervalli regolari. Per ulteriori informazioni, consulta la pagina [Esplorazione dei dati in Amazon Athena](#).

Applicazioni

Per mantenerne l'operatività, potrebbe essere necessario migrare alcuni dei tuoi server rilevati. In questo caso, puoi definire e raggruppare logicamente i server rilevati nelle applicazioni.

Come parte del processo di raggruppamento, puoi cercare, filtrare e aggiungere tag.

Per raggruppare i server in un'applicazione nuova o esistente

1. Utilizzo dellaAWSaccount, accedi alAWS Management Consolee apri la console Migration Hub su<https://console.aws.amazon.com/migrationhub/>.
2. Nel pannello di navigazione della console Migration Hub sottoScopri, scegliServer.
3. Nell'elenco dei server, selezionare i server che si desidera raggruppare in un'applicazione nuova o esistente.

Per semplificare la scelta dei server per il gruppo, è possibile eseguire una ricerca e filtrare su qualsiasi criterio specificato nell'elenco dei server. Fare clic all'interno della barra di ricerca e selezionare un elemento dall'elenco, selezionare un operatore dall'elenco successivo, quindi digitare i propri criteri.

4. Facoltativo: Per ogni server selezionato, scegliAggiungere tag, digitare un valore perChiavee quindi, facoltativamente, digitare un valore perValore.
5. Selezionare Group as application (Raggruppa come applicazione) per creare la propria applicazione o aggiungere a una esistente.
6. Nella finestra di dialogo Group as application (Raggruppa come applicazione), selezionare Group as a new application (Raggruppa come una nuova applicazione) o Add to an existing application (Aggiungi a un'applicazione esistente).

- a. Se si seleziona Group as a new application (Raggruppa come una nuova applicazione), digitare un nome per Application name (Nome applicazione). Facoltativamente, è possibile digitare una descrizione per Application description (Descrizione applicazione).
 - b. Se si sceglie Add to an existing application (Aggiungi a un'applicazione esistente), selezionare il nome dell'applicazione da aggiungere all'elenco.
7. Seleziona Salva.

Utilizzo dell'API Application Discovery Service per interrogare gli elementi di configurazione rilevati

Un elemento di configurazione è una risorsa IT scoperta nel data center da un agente o tramite un'importazione. Quando si utilizza AWS Application Discovery Service (Application Discovery Service), si utilizza l'API per specificare filtri e interrogare elementi di configurazione specifici per server, applicazioni, processi e risorse di connessione. Per informazioni sull'API, vedere [Application Discovery Service API Reference](#).

Le tabelle nelle seguenti sezioni elencano i filtri di input e le opzioni di ordinamento dell'output disponibili per due azioni di Application Discovery Service:

- `DescribeConfigurations`
- `ListConfigurations`

Le opzioni di filtraggio e ordinamento sono organizzate in base al tipo di asset a cui si applica (server, applicazione, processo o connessione).

Important

I risultati `DescribeConfigurations` restituiti `ListConfigurations` da `StartExportTask` potrebbero non contenere aggiornamenti recenti. Per ulteriori informazioni, consulta [Consistenza finale](#).

Utilizzo dell'`DescribeConfigurations`azione

L'operazione `DescribeConfigurations` recupera gli attributi per un elenco di ID di configurazione. Tutti gli ID forniti devono riguardare lo stesso tipo di asset (server, applicazione, processo o connessione). I campi di output sono specifici per il tipo di risorsa selezionato. Ad esempio, l'output per un elemento di configurazione di un server include un elenco di attributi relativi al server, come nome host, sistema operativo e numero di schede di rete. Per ulteriori informazioni sulla sintassi dei comandi, vedere [DescribeConfigurations](#).

L'operazione `DescribeConfigurations` non supporta il filtraggio.

Campi di output per **DescribeConfigurations**

Nelle tabelle seguenti, organizzate per tipo di asset, sono elencati i campi di output supportati dell'operazione DescribeConfigurations. Quelli contrassegnati come obbligatori sono sempre presenti nell'output.

Asset del server

Campo	Obbligatorio
<code>server.agentId</code>	
<code>server.applications</code>	
<code>server.applications.hasMoreValues</code>	
<code>server.configurationId</code>	x
<code>server.cpuType</code>	
<code>server.hostName</code>	
<code>server.hypervisor</code>	
<code>server.networkInterfaceInfo</code>	
<code>server.networkInterfaceInfo.hasMoreValues</code>	
<code>server.osName</code>	
<code>server.osVersion</code>	
<code>server.tags</code>	
<code>server.tags.hasMoreValues</code>	
<code>server.timeOfCreation</code>	x
<code>server.type</code>	

Campo	Obbligatorio
<code>server.performance.avgCpuUsagePct</code>	
<code>server.performance.avgDiskReadIOPS</code>	
<code>server.performance.avgDiskReadsPerSecondInKB</code>	
<code>server.performance.avgDiskWriteIOPS</code>	
<code>server.performance.avgDiskWritesPerSecondInKB</code>	
<code>server.performance.avgFreeRAMInKB</code>	
<code>server.performance.avgNetworkReadsPerSecondInKB</code>	
<code>server.performance.avgNetworkWritesPerSecondInKB</code>	
<code>server.performance.maxCpuUsagePct</code>	
<code>server.performance.maxDiskReadIOPS</code>	
<code>server.performance.maxDiskReadsPerSecondInKB</code>	
<code>server.performance.maxDiskWriteIOPS</code>	
<code>server.performance.maxDiskWritesPerSecondInKB</code>	

Campo	Obbligatorio
<code>server.performance.maxNetworkReadsPerSecondInKB</code>	
<code>server.performance.maxNetworkWritesPerSecondInKB</code>	
<code>server.performance.minFreeRAMInKB</code>	
<code>server.performance.numCores</code>	
<code>server.performance.numCpus</code>	
<code>server.performance.numDisks</code>	
<code>server.performance.numNetworkCards</code>	
<code>server.performance.totalRAMInKB</code>	

Asset di elaborazione

Campo	Obbligatorio
<code>process.commandLine</code>	
<code>process.configurationId</code>	x
<code>process.name</code>	
<code>process.path</code>	
<code>process.timeOfCreation</code>	x

Asset delle applicazioni

Campo	Obbligatorio
<code>application.configurationId</code>	x
<code>application.description</code>	
<code>application.lastModifiedTime</code>	x
<code>application.name</code>	x
<code>application.serverCount</code>	x
<code>application.timeOfCreation</code>	x

Utilizzo dell'azione **ListConfigurations**

L'operazione `ListConfigurations` recupera un elenco di elementi di configurazione in base ai criteri specificati in un filtro. Per ulteriori informazioni sulla sintassi dei comandi, vedere [ListConfigurations](#).

Campi di output per **ListConfigurations**

Nelle tabelle seguenti, organizzate per tipo di asset, sono elencati i campi di output supportati dell'operazione `ListConfigurations`. Quelli contrassegnati come obbligatori sono sempre presenti nell'output.

Asset del server

Campo	Obbligatorio
<code>server.configurationId</code>	x
<code>server.agentId</code>	
<code>server.hostName</code>	
<code>server.osName</code>	
<code>server.osVersion</code>	

Campo	Obbligatorio
<code>server.timeOfCreation</code>	x
<code>server.type</code>	

Asset di elaborazione

Campo	Obbligatorio
<code>process.commandLine</code>	
<code>process.configurationId</code>	x
<code>process.name</code>	
<code>process.path</code>	
<code>process.timeOfCreation</code>	x
<code>server.agentId</code>	
<code>server.configurationId</code>	x

Asset delle applicazioni

Campo	Obbligatorio
<code>application.configurationId</code>	x
<code>application.description</code>	
<code>application.name</code>	x
<code>application.serverCount</code>	x
<code>application.timeOfCreation</code>	x
<code>application.lastModifiedTime</code>	x

Asset di connessione

Campo	Obbligatorio
<code>connection.destinationIp</code>	x
<code>connection.destinationPort</code>	x
<code>connection.ipVersion</code>	x
<code>connection.latestTimestamp</code>	x
<code>connection.occurrence</code>	x
<code>connection.sourceIp</code>	x
<code>connection.transportProtocol</code>	
<code>destinationProcess.configurationId</code>	
<code>destinationProcess.name</code>	
<code>destinationServer.configurationId</code>	
<code>destinationServer.hostName</code>	
<code>sourceProcess.configurationId</code>	
<code>sourceProcess.name</code>	
<code>sourceServer.configurationId</code>	
<code>sourceServer.hostName</code>	

Filtri supportati per **ListConfigurations**

Nelle tabelle seguenti, organizzate per tipo di asset, sono elencati i filtri supportati per l'operazione `ListConfigurations`. I filtri e i valori sono in una relazione chiave/valore definita da una delle condizioni logiche supportate. È possibile ordinare l'output dei filtri indicati.

Asset del server

Filtro	Condizioni supportate	Valori supportati	Ordinamento supportato
<code>server.configurationId</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE 	<ul style="list-style-type: none"> Qualsiasi ID di configurazione server valido 	Nessuno
<code>server.hostName</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE CONTAINS NOT_CONTAINS 	<ul style="list-style-type: none"> Stringa 	<ul style="list-style-type: none"> ASC DESC
<code>server.osName</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE CONTAINS NOT_CONTAINS 	<ul style="list-style-type: none"> Stringa 	<ul style="list-style-type: none"> ASC DESC
<code>server.osVersion</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE CONTAINS NOT_CONTAINS 	<ul style="list-style-type: none"> Stringa 	<ul style="list-style-type: none"> ASC DESC
<code>server.agentId</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ 	<ul style="list-style-type: none"> Stringa 	Nessuno

Filtro	Condizioni supportate	Valori supportati	Ordinamento supportato
	<ul style="list-style-type: none"> • NE 		
<code>server.connectorId</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE 	<ul style="list-style-type: none"> • Stringa 	Nessuno
<code>server.type</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE 	Stringa con uno dei seguenti valori: <ul style="list-style-type: none"> • EC2 • OTHER • VMWARE_VM • VMWARE_HOST • VMWARE_VM_TEMPLATE 	Nessuno
<code>server.vmWareInfo.morefId</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • Stringa 	Nessuno
<code>server.vmWareInfo.vcenterId</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • Stringa 	Nessuno

Filtro	Condizioni supportate	Valori supportati	Ordinamento supportato
<code>server.vmWareInfo.hostId</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • Stringa 	Nessuno
<code>server.networkInterfaceInfo.portGroupId</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • Stringa 	Nessuno
<code>server.networkInterfaceInfo.portGroupName</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • Stringa 	Nessuno
<code>server.networkInterfaceInfo.virtualSwitchName</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • Stringa 	Nessuno

Filtro	Condizioni supportate	Valori supportati	Ordinamento supportato
<code>server.networkInterfaceInfo.ipAddress</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • Stringa 	Nessuno
<code>server.networkInterfaceInfo.macAddress</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • Stringa 	Nessuno
<code>server.performance.avgCpuUsagePct</code>	<ul style="list-style-type: none"> • GE • LE • GT • LT 	<ul style="list-style-type: none"> • Percentuale 	Nessuno
<code>server.performance.totalDiskFreeSizeInKB</code>	<ul style="list-style-type: none"> • GE • LE • GT • LT 	<ul style="list-style-type: none"> • Doppio 	Nessuno
<code>server.performance.avgFreeRAMInKB</code>	<ul style="list-style-type: none"> • GE • LE • GT • LT 	<ul style="list-style-type: none"> • Doppio 	Nessuno

Filtro	Condizioni supportate	Valori supportati	Ordinamento supportato
<code>server.tag.value</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • Stringa 	Nessuno
<code>server.tag.key</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • Stringa 	Nessuno
<code>server.application.name</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • Stringa 	Nessuno
<code>server.application.description</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • Stringa 	Nessuno

Filtro	Condizioni supportate	Valori supportati	Ordinamento supportato
<code>server.application.configurationId</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE 	<ul style="list-style-type: none"> Qualsiasi ID di configurazione valido dell'applicazione 	Nessuno
<code>server.process.configurationId</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE 	<ul style="list-style-type: none"> ProcessId 	Nessuno
<code>server.process.name</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE CONTAINS NOT_CONTAINS 	<ul style="list-style-type: none"> Stringa 	Nessuno
<code>server.process.commandLine</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE CONTAINS NOT_CONTAINS 	<ul style="list-style-type: none"> Stringa 	Nessuno

Asset delle applicazioni

Filtro	Condizioni supportate	Valori supportati	Ordinamento supportato
<code>application.configurationId</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE 	<ul style="list-style-type: none"> ApplicationId 	Nessuno
<code>application.name</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE CONTAINS NOT_CONTAINS 	<ul style="list-style-type: none"> Stringa 	<ul style="list-style-type: none"> ASC DESC
<code>application.description</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE CONTAINS NOT_CONTAINS 	<ul style="list-style-type: none"> Stringa 	<ul style="list-style-type: none"> ASC DESC
<code>application.serverCount</code>	Filtraggio non supportato.	Filtraggio non supportato.	<ul style="list-style-type: none"> ASC DESC
<code>application.timeOfCreation</code>	Filtraggio non supportato.	Filtraggio non supportato.	<ul style="list-style-type: none"> ASC DESC
<code>application.lastModifiedTime</code>	Filtraggio non supportato.	Filtraggio non supportato.	<ul style="list-style-type: none"> ASC DESC

Filtro	Condizioni supportate	Valori supportati	Ordinamento supportato
<code>server.configurationId</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE 	<ul style="list-style-type: none"> ServerId 	Nessuno

Asset di elaborazione

Filtro	Condizioni supportate	Valori supportati	Ordinamento supportato
<code>process.configurationId</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE 	<ul style="list-style-type: none"> ProcessId 	
<code>process.name</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE CONTAINS NOT_CONTAINS 	<ul style="list-style-type: none"> Stringa 	<ul style="list-style-type: none"> ASC DESC
<code>process.commandLine</code>	<ul style="list-style-type: none"> EQUALS NOT_EQUALS EQ NE CONTAINS NOT_CONTAINS 	<ul style="list-style-type: none"> Stringa 	<ul style="list-style-type: none"> ASC DESC

Filtro	Condizioni supportate	Valori supportati	Ordinamento supportato
<code>server.configurationId</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE 	<ul style="list-style-type: none"> • ServerId 	
<code>server.hostName</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • Stringa 	<ul style="list-style-type: none"> • ASC • DESC
<code>server.osName</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • Stringa 	<ul style="list-style-type: none"> • ASC • DESC
<code>server.osVersion</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • Stringa 	<ul style="list-style-type: none"> • ASC • DESC

Filtro	Condizioni supportate	Valori supportati	Ordinamento supportato
<code>server.agentId</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • Stringa 	

Asset di connessione

Filtro	Condizioni supportate	Valori supportati	Ordinamento supportato
<code>connection.sourceIp</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • IP 	<ul style="list-style-type: none"> • ASC • DESC
<code>connection.destinationIp</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • IP 	<ul style="list-style-type: none"> • ASC • DESC
<code>connection.destinationPort</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE 	<ul style="list-style-type: none"> • Numero intero 	<ul style="list-style-type: none"> • ASC • DESC

Filtro	Condizioni supportate	Valori supportati	Ordinamento supportato
sourceServer.configurationId	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE 	<ul style="list-style-type: none"> • ServerId 	
sourceServer.hostName	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • Stringa 	<ul style="list-style-type: none"> • ASC • DESC
destinationServer.osName	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • Stringa 	<ul style="list-style-type: none"> • ASC • DESC
destinationServer.osVersion	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • Stringa 	<ul style="list-style-type: none"> • ASC • DESC

Filtro	Condizioni supportate	Valori supportati	Ordinamento supportato
<code>destinationServer.agentId</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • Stringa 	
<code>sourceProcess.configurationId</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE 	<ul style="list-style-type: none"> • ProcessId 	
<code>sourceProcess.name</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • Stringa 	<ul style="list-style-type: none"> • ASC • DESC
<code>sourceProcess.commandLine</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS 	<ul style="list-style-type: none"> • Stringa 	<ul style="list-style-type: none"> • ASC • DESC
<code>destinationProcess.configurationId</code>	<ul style="list-style-type: none"> • EQUALS • NOT_EQUALS • EQ • NE 	<ul style="list-style-type: none"> • ProcessId 	

Filtro	Condizioni supportate	Valori supportati	Ordinamento supportato
<code>destinati onProcess.name</code>	<ul style="list-style-type: none">• EQUALS• NOT_EQUALS• EQ• NE• CONTAINS• NOT_CONTAINS	<ul style="list-style-type: none">• Stringa	<ul style="list-style-type: none">• ASC• DESC
<code>destinati onprocess .commandLine</code>	<ul style="list-style-type: none">• EQUALS• NOT_EQUALS• EQ• NE• CONTAINS• NOT_CONTAINS	<ul style="list-style-type: none">• Stringa	<ul style="list-style-type: none">• ASC• DESC

Eventuale coerenza nell'API AWS Application Discovery Service

Le seguenti operazioni di aggiornamento sono alla fine coerenti. Gli aggiornamenti potrebbero non essere immediatamente visibili alle operazioni di lettura [StartExportTask](#), [DescribeConfigurations](#), e [ListConfigurations](#).

- [AssociateConfigurationItemsToApplicazione](#)
- [CreateTags](#)
- [DeleteApplications](#)
- [DeleteTags](#)
- [DescribeBatchDeleteConfigurationCompito](#)
- [DescribeImportCompiti](#)
- [DisassociateConfigurationItemsFromApplicazione](#)
- [UpdateApplication](#)

Suggerimenti per la gestione dell'eventuale coerenza:

- Quando richiamate le operazioni di lettura [StartExportTask](#) o [ListConfigurations](#) (o i AWS CLI comandi corrispondenti), utilizzate un algoritmo di backoff esponenziale per consentire a qualsiasi operazione di aggiornamento precedente di propagarsi nel sistema. [DescribeConfigurations](#) A tale scopo, eseguite l'operazione di lettura ripetutamente, iniziando con un tempo di attesa di due secondi e aumentando gradualmente fino a cinque minuti di attesa.
- Aggiunge il tempo di attesa tra le operazioni successive, anche se un'operazione di aggiornamento restituisce una risposta di 200 - OK. Applica un algoritmo di backoff esponenziale a partire da un paio di secondi di attesa e aumenta gradualmente fino a circa cinque minuti di attesa.

Sicurezza in AWS Application Discovery Service

La sicurezza del cloud in AWS ha la massima priorità. In quanto cliente AWS, puoi trarre vantaggio da un'architettura di data center e di rete progettata per soddisfare i requisiti delle aziende più esigenti a livello di sicurezza.

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

- La sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che esegue i servizi AWS nel cloud AWS. AWS fornisce inoltre servizi che puoi utilizzare in sicurezza. L'efficacia della nostra sicurezza è regolarmente testata e verificata da revisori di terze parti come parte dei [programmi di conformità AWS](#).
- Sicurezza nel cloud: la tua responsabilità è determinata dal servizio AWS che viene utilizzato. L'utente è anche responsabile per altri fattori, tra cui la riservatezza dei dati, i requisiti dell'azienda e leggi e normative applicabili.

Per utilizzare AWS Application Discovery Agent o Application Discovery Service Agentless Collector è necessario fornire le chiavi di accesso al proprio account. AWS Queste informazioni vengono quindi archiviate nell'infrastruttura locale. Nell'ambito del modello di responsabilità condivisa, l'utente è responsabile della protezione dell'accesso alla propria infrastruttura.

Questa documentazione ti aiuterà a capire come applicare il modello di responsabilità condivisa quando usi Application Discovery Service. Negli argomenti seguenti viene illustrato come configurare Application Discovery Service per soddisfare gli obiettivi di sicurezza e conformità. Imparerai anche come utilizzare altri AWS servizi che possono aiutarti a monitorare e proteggere le risorse dell'Application Discovery Service.

Argomenti

- [Identity and Access Management per AWS Application Discovery Service](#)
- [Registrazione e monitoraggio in AWS Application Discovery Service](#)

Identity and Access Management per AWS Application Discovery Service

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 (dispone delle autorizzazioni) a utilizzare le risorse di Application Discovery Service. IAM è uno Servizio AWS strumento che puoi utilizzare senza costi aggiuntivi.

Argomenti

- [Destinatari](#)
- [Autenticazione con identità](#)
- [Gestione dell'accesso tramite policy](#)
- [Come AWS Application Discovery Service funziona con IAM](#)
- [AWS politiche gestite per AWS Application Discovery Service](#)
- [AWS Application Discovery Service Esempi di policy basate sull'identità](#)
- [Utilizzo di ruoli collegati ai servizi per Application Discovery Service Service](#)
- [Risoluzione dei problemi relativi a AWS Application Discovery Service identità e accesso](#)

Destinatari

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

Utente del servizio: se si utilizza il servizio Application Discovery Service per svolgere il proprio lavoro, l'amministratore fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più funzionalità di Application Discovery Service 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 è possibile accedere a una funzionalità di Application Discovery Service, vedere [Risoluzione dei problemi relativi a AWS Application Discovery Service identità e accesso](#).

Amministratore del servizio: se sei responsabile delle risorse di Application Discovery Service presso la tua azienda, probabilmente hai pieno accesso a Application Discovery Service. È compito dell'utente determinare a quali funzionalità e risorse di Application Discovery Service devono

accedere gli utenti del servizio. 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 Application Discovery Service, consulta [Come AWS Application Discovery Service funziona con IAM](#).

Amministratore IAM: se sei un amministratore IAM, potresti voler conoscere i dettagli su come scrivere policy per gestire l'accesso ad Application Discovery Service. Per visualizzare esempi di policy basate sull'identità di Application Discovery Service che è possibile utilizzare in IAM, vedere [AWS Application Discovery Service Esempi di policy basate sull'identità](#)

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi essere autenticato (aver effettuato l' Utente root dell'account AWS accesso 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 Gli utenti (IAM Identity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. 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 sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, consulta [Signing AWS API request](#) nella IAM User Guide.

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 \(MFA\) in AWS](#) 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.

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, è possibile avere un gruppo denominato IAMAdmins e concedere a tale 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 [Quando creare un utente IAM \(invece di un ruolo\)](#) 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. Puoi assumere temporaneamente un ruolo IAM in AWS Management Console [cambiando ruolo](#). 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 [Creazione di un ruolo per un provider di identità di terza parte](#) 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 conoscere la differenza tra ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta [Cross Account Resource Access in IAM nella IAM](#) User Guide.
- **Accesso tra servizi:** alcuni Servizi AWS utilizzano funzionalità in altri. Servizi AWS Ad esempio, quando effettui una chiamata in un servizio, è comune che tale servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
- **Sessioni di accesso diretto (FAS):** quando utilizzi un 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 la pagina [Forward access sessions](#).

- **Ruolo di servizio:** un ruolo di servizio è un [ruolo IAM](#) che un servizio assume per eseguire azioni 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 [Creazione di un ruolo per delegare le autorizzazioni a un 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'istanza EC2 e che AWS CLI effettuano richieste API. AWS Cloud è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un ruolo AWS a un'istanza EC2 e renderlo disponibile per tutte le sue applicazioni, crei un profilo di istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta [Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2](#) nella Guida per l'utente IAM.

Per informazioni sull'utilizzo dei ruoli IAM, consulta [Quando creare un ruolo IAM \(invece di un utente\)](#) nella Guida per l'utente IAM.

Gestione dell'accesso tramite 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 azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire 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 CLI o dall' AWS API.

Policy basate sulle 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 azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta [Creazione di policy IAM](#) 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 su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi più comuni di policy basate su 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 azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario [specificare un principale](#) in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o Servizi AWS.

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

Liste di controllo degli accessi (ACL)

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

Amazon S3 e Amazon VPC sono esempi di servizi che supportano gli ACL. AWS WAF Per maggiori informazioni sulle ACL, consulta [Panoramica delle liste di controllo degli accessi \(ACL\)](#) nella Guida per gli sviluppatori di Amazon Simple Storage Service.

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 dei servizi (SCP):** le SCP 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 Account AWS di proprietà dell'azienda. Se abiliti tutte le funzionalità in un'organizzazione, puoi applicare le policy di controllo dei servizi (SCP) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità negli account dei membri, inclusa ciascuna. Utente root dell'account AWS Per ulteriori informazioni su organizzazioni e policy SCP, consulta la pagina sulle [Policy di controllo dei servizi](#) nella Guida per l'utente di AWS Organizations .
- **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 una richiesta quando sono coinvolti più tipi di policy, consulta [Logica di valutazione delle policy](#) nella IAM User Guide.

Come AWS Application Discovery Service funziona con IAM

Prima di utilizzare IAM per gestire l'accesso ad Application Discovery Service, è necessario comprendere quali funzionalità IAM sono disponibili per l'uso con Application Discovery Service. Per avere una visione di alto livello di come Application Discovery Service e altri AWS servizi funzionano con IAM, consulta [AWS Services That Work with IAM nella IAM](#) User Guide.

Argomenti

- [Politiche basate sull'identità di Application Discovery Service](#)
- [Politiche basate sulle risorse di Application Discovery Service](#)
- [Autorizzazione basata sui tag di Application Discovery Service](#)
- [Ruoli IAM di Application Discovery Service](#)

Politiche basate sull'identità di Application Discovery Service

Con le policy basate su identità di IAM, è possibile specificare quali azioni e risorse sono consentite o rifiutate, nonché le condizioni in base alle quali le azioni sono consentite o rifiutate. Application Discovery Service supporta azioni, risorse e chiavi di condizione specifiche. Per informazioni su tutti gli elementi utilizzati in una policy JSON, consulta [Documentazione di riferimento degli elementi delle policy JSON IAM](#) nella Guida per l'utente IAM.

Azioni

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

L'elemento `Action` di una policy JSON descrive le azioni 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 azioni 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.

Le azioni politiche in Application Discovery Service utilizzano il seguente prefisso prima dell'azione: `discovery:`. Le istruzioni della policy devono includere un elemento `Action` o `NotAction`. Application Discovery Service definisce il proprio set di azioni che descrivono le attività che è possibile eseguire con questo servizio.

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

```
"Action": [  
    "discovery:action1",  
    "discovery:action2"
```

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

```
"Action": "discovery:Describe*"
```

Per visualizzare un elenco delle azioni dell'Application Discovery Service, consulta [Actions Defined by AWS Application Discovery Service](#) nella IAM User Guide.

Risorse

Application Discovery Service non supporta la specificazione degli ARN di risorse in una policy. Per separare l'accesso, crea e utilizza elementi separati. Account AWS

Chiavi di condizione

Application Discovery Service non fornisce chiavi di condizione specifiche del servizio, ma supporta l'utilizzo di alcune chiavi di condizione globali. Per visualizzare tutte le chiavi di condizione AWS globali, consulta [AWS Global Condition Context Keys](#) nella IAM User Guide.

Esempi

Per visualizzare esempi di policy basate sull'identità di Application Discovery Service, vedere. [AWS Application Discovery Service Esempi di policy basate sull'identità](#)

Politiche basate sulle risorse di Application Discovery Service

Application Discovery Service non supporta policy basate sulle risorse.

Autorizzazione basata sui tag di Application Discovery Service

Application Discovery Service non supporta l'etichettatura delle risorse o il controllo dell'accesso in base ai tag.

Ruoli IAM di Application Discovery Service

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

Utilizzo di credenziali temporanee con Application Discovery Service

Application Discovery Service non supporta l'utilizzo di credenziali temporanee.

Ruoli collegati al servizio

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

Application Discovery Service supporta i ruoli collegati ai servizi. Per informazioni dettagliate sulla creazione o la gestione dei ruoli collegati ai servizi di Application Discovery Service, vedere [Utilizzo di ruoli collegati ai servizi per Application Discovery Service](#)

Ruoli dei servizi

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

Application Discovery Service supporta i ruoli di servizio.

AWS politiche gestite per AWS Application Discovery Service

Per aggiungere autorizzazioni a utenti, gruppi e ruoli, è più facile utilizzare policy AWS gestite che scrivere policy personalizzate. 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 occasionalmente aggiungono altre autorizzazioni

a una policy gestita da AWS 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 policy gestita da AWS quando viene avviata 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: `AWSApplicationDiscoveryServiceFullAccess`

La `AWSApplicationDiscoveryServiceFullAccess` policy concede a un account utente IAM l'accesso alle API di Application Discovery Service e Migration Hub.

Un account utente IAM con questa policy allegata può configurare Application Discovery Service, avviare e arrestare gli agenti, avviare e interrompere il rilevamento senza agenti e interrogare i dati dal database AWS Discovery Service. Per un esempio di questa policy, consulta [Concessione dell'accesso completo a Application Discovery Service](#).

AWS politica gestita: `AWSApplicationDiscoveryAgentlessCollectorAccess`

La policy `AWSApplicationDiscoveryAgentlessCollectorAccess` gestita concede all'Application Discovery Service Agentless Collector (Agentless Collector) l'accesso per registrarsi e comunicare con l'Application Discovery Service e comunicare con altri servizi. AWS

Questa policy deve essere allegata all'utente IAM le cui credenziali vengono utilizzate per configurare Agentless Collector.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `arsenal`— Consente al raccoglitore di registrarsi con l'applicazione Application Discovery Service. Ciò è necessario per poter inviare i dati raccolti a AWS.

- **ecr-public**— Consente al raccoglitore di effettuare chiamate all'Amazon Elastic Container Registry Public (Amazon ECR Public) dove sono disponibili gli ultimi aggiornamenti per il raccoglitore.
- **mgh**— Consente al raccoglitore di effettuare una chiamata AWS Migration Hub per recuperare la regione di origine dell'account utilizzato per configurare il raccoglitore. Ciò è necessario per sapere a quale regione devono essere inviati i dati raccolti.
- **sts**— Consente al raccoglitore di recuperare un token del service bearer in modo da poter effettuare chiamate ad Amazon ECR Public per ottenere gli aggiornamenti più recenti.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "arsenal:RegisterOnPremisesAgent"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ecr-public:DescribeImages"
      ],
      "Resource": "arn:aws:ecr-
public::446372222237:repository/6e5498e4-8c31-4f57-9991-13b4b992ff7b"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ecr-public:GetAuthorizationToken"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "mgh:GetHomeRegion"
      ],
      "Resource": "*"
    }
  ]
}
```

```
    },
    {
      "Effect": "Allow",
      "Action": [
        "sts:GetServiceBearerToken"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS politica gestita: AWSApplicationDiscoveryAgentAccess

La `AWSApplicationDiscoveryAgentAccess` policy concede all'Application Discovery Agent l'accesso per registrarsi e comunicare con Application Discovery Service.

Questa politica viene allegata a qualsiasi utente le cui credenziali vengono utilizzate da Application Discovery Agent.

Questa policy inoltre autorizza l'utente ad accedere ad Arsenal. Arsenal è un servizio di agenti gestito e ospitato da AWS. L'Arsenal inoltra i dati all'Application Discovery Service nel cloud. Per un esempio di questa policy, consulta [Concessione dell'accesso ai Discovery Agents](#).

AWS politica gestita: AWSAgentlessDiscoveryService

La `AWSAgentlessDiscoveryService` policy concede all'AWS Agentless Discovery Connector in esecuzione nel VMware vCenter Server l'accesso alla registrazione, alla comunicazione e alla condivisione dei parametri di integrità del connettore con Application Discovery Service.

Colleghi questa policy a tutti gli utenti le cui credenziali vengono utilizzate dal connettore.

AWS politica ApplicationDiscoveryServiceContinuousExportServiceRole gestita: Policy

Se al tuo account IAM è allegata la `AWSApplicationDiscoveryServiceFullAccess` policy, questa `ApplicationDiscoveryServiceContinuousExportServiceRolePolicy` viene collegata automaticamente al tuo account quando attivi l'esplorazione dei dati in Amazon Athena.

Questa policy consente di AWS Application Discovery Service creare stream Amazon Data Firehose per trasformare e distribuire i dati raccolti dagli AWS Application Discovery Service agenti in un bucket Amazon S3 del tuo account. AWS

Inoltre, questa policy crea un AWS Glue Data Catalog nuovo database chiamato `application_discovery_service_database` e schemi di tabelle per la mappatura dei dati raccolti dagli agenti. Per un esempio di questa policy, consulta [Concessione delle autorizzazioni per la raccolta dei dati degli agenti](#).

AWS politica gestita: `AWSDiscoveryContinuousExportFirehosePolicy`

La `AWSDiscoveryContinuousExportFirehosePolicy` policy è necessaria per utilizzare l'esplorazione dei dati in Amazon Athena. Consente ad Amazon Data Firehose di scrivere i dati raccolti da Application Discovery Service su Amazon S3. Per informazioni sull'utilizzo di questa policy, consulta [Creazione del ruolo `AWSApplicationDiscoveryServiceFirehose`](#). Per un esempio di questa policy, consulta [Concessione delle autorizzazioni per l'esplorazione dei dati](#).

Creazione del ruolo `AWSApplicationDiscoveryServiceFirehose`

Un amministratore allega le policy gestite al tuo account utente IAM. Quando utilizza la `AWSDiscoveryContinuousExportFirehosePolicy` policy, l'amministratore deve prima creare un ruolo denominato `AWSApplicationDiscoveryServiceFirehoseFirehose` come entità attendibile e quindi allegare la `AWSDiscoveryContinuousExportFirehosePolicy` policy al ruolo, come illustrato nella procedura seguente.

Per creare il ruolo `AWSApplicationDiscoveryServiceFirehoseIAM`

1. Nella console IAM, scegli Ruoli nel riquadro di navigazione.
2. Selezionare Crea ruolo.
3. Scegliere Kinesis.
4. Scegliere Kinesis Firehose come caso d'uso.
5. Scegli Successivo: Autorizzazioni.
6. In Filter Policies cerca `AWSDiscoveryContinuousExportFirehosePolicy`.
7. Seleziona la casella accanto `AWSDiscoveryContinuousExportFirehosePolicy`, quindi scegli Avanti: Revisione.
8. Immettete `AWSApplicationDiscoveryServiceFirehose` come nome del ruolo, quindi scegliete Crea ruolo.

Aggiornamenti di Application Discovery Service alle policy AWS gestite

Visualizza i dettagli sugli aggiornamenti delle policy AWS gestite per Application Discovery Service da quando questo servizio ha iniziato a tenere traccia di queste modifiche. Per gli avvisi automatici sulle modifiche apportate alla pagina, iscriviti al feed RSS alla pagina [Cronologia dei documenti per AWS Application Discovery Service](#).

Modifica	Descrizione	Data
AWSApplicationDiscoveryAgentlessCollectorAccess — Nuova policy resa disponibile con il lancio di Agentless Collector	Application Discovery Service ha aggiunto la nuova policy gestita AWSApplicationDiscoveryAgentlessCollectorAccess che concede all'Agentless Collector l'accesso per registrarsi e comunicare con l'Application Discovery Service e comunicare con altri servizi. AWS	16 agosto 2022
Application Discovery Service ha iniziato a tenere traccia delle modifiche	Application Discovery Service ha iniziato a tenere traccia delle modifiche per le sue policy AWS gestite.	1 marzo 2021

AWS Application Discovery Service Esempi di policy basate sull'identità

Per impostazione predefinita, gli utenti e i ruoli IAM non dispongono dell'autorizzazione per creare o modificare le risorse di Application Discovery Service. Inoltre, non possono eseguire attività utilizzando l' AWS API AWS Management Console AWS CLI, o. Un amministratore IAM deve creare policy IAM che concedono a utenti e ruoli l'autorizzazione per eseguire operazioni API specifiche sulle risorse specificate di cui hanno bisogno. L'amministratore deve quindi allegare queste policy a utenti o IAM che richiedono tali autorizzazioni.

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

Argomenti

- [Best practice delle policy](#)
- [Concessione dell'accesso completo a Application Discovery Service](#)
- [Concessione dell'accesso ai Discovery Agents](#)
- [Concessione delle autorizzazioni per la raccolta dei dati degli agenti](#)
- [Concessione delle autorizzazioni per l'esplorazione dei dati](#)
- [Concessione delle autorizzazioni per l'uso del diagramma di rete della console Migration Hub](#)

Best practice delle policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare le risorse di Application Discovery Service 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 policy 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. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo 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 puoi 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 IAM Access Analyzer](#) 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 [Configurazione dell'accesso alle API protetto 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.

Concessione dell'accesso completo a Application Discovery Service

La policy `AWSApplicationDiscoveryServiceFullAccess` gestita concede all'account utente IAM l'accesso alle API di Application Discovery Service e Migration Hub.

Un utente IAM con questa policy associata al proprio account può configurare Application Discovery Service, avviare e arrestare gli agenti, avviare e interrompere il rilevamento senza agenti ed eseguire query sui dati dal database AWS Discovery Service. Per ulteriori informazioni su questa policy, consulta [AWS politiche gestite per AWS Application Discovery Service](#).

Example `AWSApplicationDiscoveryServiceFullAccess` politica

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "mgh:*",
        "discovery:*"
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Action": [
        "iam:GetRole"
      ],
      "Effect": "Allow",
```

```

        "Resource": "*"
    }
]
}

```

Concessione dell'accesso ai Discovery Agents

La policy `AWSApplicationDiscoveryAgentAccess` gestita concede all'Application Discovery Agent l'accesso per registrarsi e comunicare con Application Discovery Service. Per ulteriori informazioni su questa policy, consulta [AWS politiche gestite per AWS Application Discovery Service](#).

Allega questa policy a qualsiasi utente le cui credenziali vengono utilizzate da Application Discovery Agent.

Questa policy inoltre autorizza l'utente ad accedere ad Arsenal. Arsenal è un servizio di agenti gestito e ospitato da AWS. L'Arsenal inoltra i dati all'Application Discovery Service nel cloud.

Example `AWSApplicationDiscoveryAgentAccess` Politica

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "arsenal:RegisterOnPremisesAgent"
      ],
      "Resource": "*"
    }
  ]
}

```

Concessione delle autorizzazioni per la raccolta dei dati degli agenti

La policy `ApplicationDiscoveryServiceContinuousExportServiceRolePolicy` gestita consente di AWS Application Discovery Service creare flussi Amazon Data Firehose per trasformare e distribuire i dati raccolti dagli agenti di Application Discovery Service a un bucket Amazon S3 del tuo account. AWS

Inoltre, questa policy crea un catalogo AWS Glue dati con un nuovo database chiamato `application_discovery_service_database` e schemi di tabelle per la mappatura dei dati raccolti dagli agenti.

Per informazioni sull'utilizzo di questa policy, consulta [AWS politiche gestite per AWS Application Discovery Service](#).

Example ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue:CreateTable",
        "glue:UpdateTable",
        "firehose:CreateDeliveryStream",
        "firehose:DescribeDeliveryStream",
        "logs:CreateLogGroup"
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Action": [
        "firehose>DeleteDeliveryStream",
        "firehose:PutRecord",
        "firehose:PutRecordBatch",
        "firehose:UpdateDestination"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:firehose:*:*:deliverystream/aws-application-discovery-
service*"
    },
    {
      "Action": [
        "s3:CreateBucket",
        "s3:ListBucket",
        "s3:PutBucketLogging",
        "s3:PutEncryptionConfiguration"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::aws-application-discovery-service*"
    },
    {
      "Action": [
```

```

        "s3:GetObject"
    ],
    "Effect": "Allow",
    "Resource": "arn:aws:s3:::aws-application-discovery-service/*/*"
  },
  {
    "Action": [
      "logs:CreateLogStream",
      "logs:PutRetentionPolicy"
    ],
    "Effect": "Allow",
    "Resource": "arn:aws:logs:*:*:log-group:/aws/application-discovery-service/
firehose*"
  },
  {
    "Action": [
      "iam:PassRole"
    ],
    "Effect": "Allow",
    "Resource": "arn:aws:iam:*:*:role/AWSApplicationDiscoveryServiceFirehose",
    "Condition": {
      "StringLike": {
        "iam:PassedToService": "firehose.amazonaws.com"
      }
    }
  },
  {
    "Action": [
      "iam:PassRole"
    ],
    "Effect": "Allow",
    "Resource": "arn:aws:iam:*:*:role/service-role/
AWSApplicationDiscoveryServiceFirehose",
    "Condition": {
      "StringLike": {
        "iam:PassedToService": "firehose.amazonaws.com"
      }
    }
  }
]
}

```

Concessione delle autorizzazioni per l'esplorazione dei dati

La `AWSDiscoveryContinuousExportFirehosePolicy` policy è necessaria per utilizzare l'esplorazione dei dati in Amazon Athena. Consente ad Amazon Data Firehose di scrivere i dati raccolti da Application Discovery Service su Amazon S3. Per informazioni sull'utilizzo di questa policy, consulta [Creazione del ruolo `AWSApplicationDiscoveryServiceFirehose`](#).

Example `AWSDiscoveryContinuousExportFirehosePolicy`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "glue:GetTableVersions"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:AbortMultipartUpload",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:PutObject"
      ],
      "Resource": [
        "arn:aws:s3:::aws-application-discovery-service-*",
        "arn:aws:s3:::aws-application-discovery-service-*/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "logs:PutLogEvents"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:/aws/application-discovery-service/firehose:log-stream:*"
      ]
    }
  ]
}
```

```

    }
  ]
}

```

Concessione delle autorizzazioni per l'uso del diagramma di rete della console Migration Hub

Per concedere l'accesso al diagramma di rete della AWS Migration Hub console quando si crea una policy basata sull'identità che consente o nega l'accesso ad Application Discovery Service o Migration Hub, potrebbe essere necessario aggiungere l'`discovery:GetNetworkConnectionGraph` azione alla policy.

È necessario utilizzare l'`discovery:GetNetworkConnectionGraph` azione nelle nuove politiche o aggiornare le politiche precedenti se entrambe le condizioni sono valide per la politica:

- La policy consente o nega l'accesso ad Application Discovery Service o al Migration Hub.
- La politica concede le autorizzazioni di accesso utilizzando un'altra azione di scoperta specifica, ad esempio piuttosto che `discovery:action-name`. `discovery:*`

L'esempio seguente mostra come utilizzare l'`discovery:GetNetworkConnectionGraph` azione in una policy IAM.

Example

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["discovery:GetNetworkConnectionGraph"],
      "Resource": "*"
    }
  ]
}

```

Per informazioni sul diagramma di rete di Migration Hub, vedere [Visualizzazione delle connessioni di rete in Migration Hub](#).

Utilizzo di ruoli collegati ai servizi per Application Discovery Service

AWS Application Discovery Service utilizza [ruoli collegati al servizio AWS Identity and Access Management \(IAM\)](#). Un ruolo collegato ai servizi è un tipo di ruolo IAM univoco collegato direttamente ad Application Discovery Service. I ruoli collegati ai servizi sono definiti automaticamente da Application Discovery Service e includono tutte le autorizzazioni richieste dal servizio per eseguire chiamate agli altri AWS servizi per tuo conto.

Un ruolo collegato ai servizi semplifica la configurazione di Application Discovery Service perché evita di dover aggiungere manualmente le autorizzazioni necessarie. Application Discovery Service definisce le autorizzazioni dei relativi ruoli associati ai servizi e, salvo diversamente definito, solo Application Discovery Service potrà assumere i propri ruoli. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere collegata a nessun'altra entità IAM.

È possibile eliminare un ruolo collegato ai servizi solo dopo aver eliminato le risorse correlate. Questa procedura protegge le risorse di Application Discovery Service perché impedisce la rimozione involontaria delle autorizzazioni di accesso alle risorse.

Argomenti

- [Autorizzazioni del ruolo collegato ai servizi per Application Discovery Service](#)
- [Creazione di un ruolo collegato ai servizi per Application Discovery Service](#)
- [Eliminazione di un ruolo collegato ai servizi per Application Discovery Service](#)

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

Autorizzazioni del ruolo collegato ai servizi per Application Discovery Service

Application Discovery Service usa il ruolo collegato ai servizi denominato `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport`— Consente l'accesso a AWS Servizi e risorse utilizzati o gestiti da AWS Application Discovery Service.

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

- `continuousexport.discovery.amazonaws.com`

La policy delle autorizzazioni del ruolo consente ad Application Discovery Service di eseguire le seguenti operazioni:

glue

`CreateDatabase`

`UpdateDatabase`

`CreateTable`

`UpdateTable`

firehose

`CreateDeliveryStream`

`DeleteDeliveryStream`

`DescribeDeliveryStream`

`PutRecord`

`PutRecordBatch`

`UpdateDestination`

s3

`CreateBucket`

`ListBucket`

`GetObject`

log

`CreateLogGroup`

`CreateLogStream`

`PutRetentionPolicy`

iam

PassRole

Questa è la policy completa che mostra a quali risorse si applicano le operazioni descritte in precedenza:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue:CreateTable",
        "glue:UpdateTable",
        "firehose:CreateDeliveryStream",
        "firehose:DescribeDeliveryStream",
        "logs:CreateLogGroup"
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Action": [
        "firehose>DeleteDeliveryStream",
        "firehose:PutRecord",
        "firehose:PutRecordBatch",
        "firehose:UpdateDestination"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:firehose:*:*:deliverystream/aws-application-discovery-
service*"
    },
    {
      "Action": [
        "s3:CreateBucket",
        "s3:ListBucket",
        "s3:PutBucketLogging",
        "s3:PutEncryptionConfiguration"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::aws-application-discovery-service*"
    }
  ]
}
```

```

    },
    {
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::aws-application-discovery-service*/*"
    },
    {
      "Action": [
        "logs:CreateLogStream",
        "logs:PutRetentionPolicy"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:logs:*:*:log-group:/aws/application-discovery-service/
firehose*"
    },
    {
      "Action": [
        "iam:PassRole"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:iam::*:role/AWSApplicationDiscoveryServiceFirehose",
      "Condition": {
        "StringLike": {
          "iam:PassedToService": "firehose.amazonaws.com"
        }
      }
    },
    {
      "Action": [
        "iam:PassRole"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:iam::*:role/service-role/
AWSApplicationDiscoveryServiceFirehose",
      "Condition": {
        "StringLike": {
          "iam:PassedToService": "firehose.amazonaws.com"
        }
      }
    }
  ]

```

```
}
```

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 ai servizi per Application Discovery Service

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Il `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport` il ruolo collegato al servizio viene creato automaticamente quando l'esportazione continua viene attivata implicitamente da a) confermando le opzioni nella finestra di dialogo presentata dalla pagina Data Collectors dopo aver scelto «Avvia raccolta dati» o facendo clic sul cursore denominato «Esplorazione dei dati in Athena» o b) quando si chiama il `StartContinuousExport` API con `AWSSCLIP`.

Important

Questo ruolo collegato ai servizi può apparire nell'account se è stata completata un'operazione in un altro servizio che utilizza le funzionalità supportate dal ruolo. Per ulteriori informazioni, consulta [Un nuovo ruolo è apparso nel mio account IAM](#).

Creazione del ruolo collegato ai servizi dalla console di Migration Hub

Puoi utilizzare la console Migration Hub per creare il `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport` ruolo collegato ai servizi.

Per creare il ruolo collegato ai servizi (console)

1. Nel riquadro di navigazione, selezionare Data Collectors (Agenti di raccolta dati).
2. Selezionare la scheda Agents (Agenti).
3. Attiva o disattiva Esplorazione dei dati in Athena scorri fino alla posizione On.
4. Nella finestra di dialogo generata dal passaggio precedente, fare clic sulla casella di controllo dando il consenso ai costi associati e scegliere Continue (Continua) o Enable (Abilita).

Creazione del ruolo collegato ai servizi da AWS CLI

È possibile utilizzare i comandi di Application Discovery Service da AWS Command Line Interface per creare il `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport` ruolo collegato ai servizi.

Questo ruolo collegato al servizio viene creato automaticamente quando si avvia l'esportazione continua dalAWS CLI(ilAWS CLIdeve essere prima installato nel tuo ambiente).

Per creare il ruolo collegato ai servizi (CLI) avviando l'esportazione continua dalAWS CLI

1. Installare AWS CLI per il sistema operativo in uso (Linux, macOS o Windows). Consulta il [AWS Command Line Interface Guida per l'utente di](#) per istruzioni,
2. Aprire il prompt dei comandi (Windows) o Terminal (Linux o macOS).
 - a. Digitare `aws configure` e premere Invio.
 - b. Inserisci il tuoAWSID chiave di accesso eAWSChiave di accesso segreta.
 - c. Immettere `us-west-2` per Default Region Name (Nome della regione predefinito).
 - d. Immettere `text` per Default Output Format (Formato di output predefinito).
3. Digita il seguente comando:

```
aws discovery start-continuous-export
```

Puoi utilizzare la console IAM anche per creare un ruolo collegato ai servizi con Servizio Discovery - Esportazione continua caso d'uso. Nella CLI IAM o nell'API IAM, crea un ruolo collegato ai servizi con il nome servizio `continuousexport.discovery.amazonaws.com`. Per ulteriori informazioni, consulta [Creazione di un ruolo collegato ai servizi](#) nella Guida per l'utente IAM. Se elimini il ruolo collegato ai servizi, puoi utilizzare lo stesso processo per crearlo nuovamente.

Eliminazione di un ruolo collegato ai servizi per Application Discovery Service

Se non è più necessario utilizzare una caratteristica o un servizio che richiede un ruolo collegato ai servizi, ti consigliamo di eliminare il ruolo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente. Tuttavia, è necessario effettuare la pulizia delle risorse associate al ruolo collegato ai servizi prima di poterlo eliminare manualmente.

Pulizia del ruolo collegato ai servizi

Prima di utilizzare IAM; per eliminare un ruolo collegato al servizio, è necessario prima rimuovere qualsiasi risorsa utilizzata dal ruolo.

Note

Se Application Discovery Service sta utilizzando il ruolo quando provi a eliminare le risorse, è possibile che l'eliminazione non riesca. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare le risorse dell'Application Discovery Service utilizzate da `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport` ruolo collegato ai servizi dalla console Migration Hub

1. Nel riquadro di navigazione, selezionare Data Collectors (Agenti di raccolta dati).
2. Selezionare la scheda Agents (Agenti).
3. Attiva o disattiva Esplorazione dei dati in Athenacursore fino alla posizione Off.

Per eliminare le risorse dell'Application Discovery Service utilizzate da `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport` ruolo collegato ai servizi da parte del AWS CLI

1. Installare AWS CLI per il sistema operativo in uso (Linux, macOS o Windows). Consulta [il AWS Command Line Interface Guida per l'utente di](#) per istruzioni,
2. Aprire il prompt dei comandi (Windows) o Terminal (Linux o macOS).
 - a. Digitare `aws configure` e premere Invio.
 - b. Inserisci il tuo AWS ID chiave di accesso e AWS Chiave di accesso segreta.
 - c. Immettere `us-west-2` per Default Region Name (Nome della regione predefinito).
 - d. Immettere `text` per Default Output Format (Formato di output predefinito).
3. Digita il seguente comando:

```
aws discovery stop-continuous-export --export-id <export ID>
```

- Se non conosci l'ID esportazione dell'esportazione continua che vuoi arrestare, immetti il seguente comando per visualizzare l'ID dell'esportazione continua:

```
aws discovery describe-continuous-exports
```

4. Inserisci il seguente comando per assicurarti che l'esportazione continua sia stata interrotta verificando che lo stato di restituzione sia «INATTIVO»:

```
aws discovery describe-continuous-export
```

Eliminare manualmente il ruolo collegato al servizio

Puoi eliminare il `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport` ruolo collegato ai servizi tramite la console IAM, l'interfaccia a riga di comando IAM o l'API IAM. Se non è più necessario utilizzare le funzionalità Discovery Service - Esportazione continua che richiedono questo ruolo collegato ai servizi, ti consigliamo di eliminare quel ruolo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente. Per ulteriori informazioni, consulta [Eliminazione del ruolo collegato ai servizi](#) nella Guida per l'utente di IAM.

Note

Devi effettuare la pulizia del ruolo collegato ai servizi prima di poterlo eliminare. Per informazioni, consulta [Pulizia del ruolo collegato ai servizi](#).

Risoluzione dei problemi relativi a AWS Application Discovery Service identità e accesso

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con Application Discovery Service e IAM.

Argomenti

- [Non sono autorizzato a eseguire iam: PassRole](#)

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 passare un ruolo ad Application Discovery Service.

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.

Il seguente errore di esempio si verifica quando un utente IAM denominato `marymajor` tenta di utilizzare la console per eseguire un'azione in Application Discovery Service. Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare il ruolo al servizio.

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

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

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

Registrazione e monitoraggio in AWS Application Discovery Service

AWS Application Discovery Service è integrato con AWS CloudTrail. È possibile utilizzare CloudTrail per registrare, monitorare e mantenere continuamente l'attività dell'account per scopi di risoluzione dei problemi e audit. CloudTrail fornisce una cronologia eventi del tuoAWSattività del conto, comprese le azioni intraprese attraverso ilAWSConsole di gestione,AWSGli SDK e gli strumenti della riga di comando. L'argomento in questa sezione spiega come utilizzare CloudTrail con Application Discovery Service.

Argomenti

- [Registrazione delle chiamate API di Application Discovery Service conAWS CloudTrail](#)

Registrazione delle chiamate API di Application Discovery Service conAWS CloudTrail

AWS Application Discovery ServiceIntegrazione di conAWS CloudTrail, un servizio che offre un record delle operazioni eseguite da un utente, un ruolo o unAWSApplication Discovery Service.

CloudTrail acquisisce tutte le chiamate API per Application Discovery Service come eventi. Le chiamate acquisite includono le chiamate dalla console di Application Discovery Service e le chiamate di codice alle operazioni API di Application Discovery Service.

Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail Eventi su un bucket Amazon S3, inclusi gli eventi per Application Discovery Service. Se non configuri un trail, è comunque possibile visualizzare gli eventi più recenti in CloudTrail Console in Cronologia eventi. Utilizzo delle informazioni raccolte da CloudTrail, è possibile determinare la richiesta effettuata a Application Discovery Service, l'indirizzo IP da cui è stata eseguita la richiesta, l'autore della richiesta, il momento in cui è stata eseguita e altri dettagli.

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

Application Discovery Service in CloudTrail

CloudTrail è abilitato sul tuo AWS account quando crei l'account. Quando si verifica un'attività in Application Discovery Service, tale attività viene registrata in un CloudTrail evento insieme ad altri AWS Eventi del servizio in Cronologia eventi. È possibile visualizzare, cercare e scaricare gli eventi recenti nell'account AWS. Per ulteriori informazioni, consulta la pagina [Visualizzazione di eventi con CloudTrail Cronologia eventi](#).

Per una registrazione continuativa di attività ed eventi nel tuo AWS account, inclusi gli eventi per Application Discovery Service, crea un trail. Un trail abilita CloudTrail per distribuire i file di log in un bucket Amazon S3. Per impostazione predefinita, quando si crea un trail nella console, il trail sarà valido in tutte le regioni AWS. Il trail registra gli eventi di tutte le regioni nella partizione AWS e distribuisce i file di log nel bucket Amazon S3 specificato. Inoltre, è possibile configurarne altri AWS servizi per analizzare con maggiore dettaglio e usare i dati evento raccolti in CloudTrail registri. 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 CloudTrail File di log da più regioni](#) [Ricezione CloudTrail File di log da più account](#)

Tutte Application Discovery Service sono registrate da CloudTrail e sono documentati nel [Application Discovery Service](#). Ad esempio, le chiamate a `CreateTags`, `DescribeTags`, e `GetDiscoverySummary` le azioni generano voci nel CloudTrail file di log.

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 servizio AWS.

Per ulteriori informazioni, consulta [Elemento CloudTrail userIdentity](#).

Informazioni sulle voci dei file di registro del servizio Application

Un trail è una configurazione che consente la distribuzione di eventi come i file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di log possono contenere una o più voci di log. Un evento rappresenta una singola richiesta da un'origine e include informazioni sull'operazione richiesta, data e ora dell'operazione, parametri della richiesta e così via. CloudTrail i file di log non sono una traccia di stack ordinata delle chiamate API pubbliche e di conseguenza non appaiono in base a un ordine specifico.

Il seguente esempio mostra un CloudTrail voce di registro che dimostra laDescribeTagsOperazione.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAJBHC4H6EKEXAMPLE:sample-user",
    "arn": "arn:aws:sts::444455556666:assumed-role/ReadOnly/sample-user",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDAJQABLZS4A3QDU576Q",
        "arn": "arn:aws:iam::444455556666:role/ReadOnly",
        "accountId": "444455556666",
        "userName": "sampleAdmin"
      },
      "webIdFederationData": {},
    }
  }
}
```

```
        "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2020-05-05T15:19:03Z"
        }
    },
    "eventTime": "2020-05-05T17:02:40Z",
    "eventSource": "discovery.amazonaws.com",
    "eventName": "DescribeTags",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "20.22.33.44",
    "userAgent": "Coral/Netty4",
    "requestParameters": {
        "maxResults": 0,
        "filters": [
            {
                "values": [
                    "d-server-0315rfdjreyqsq"
                ],
                "name": "configurationId"
            }
        ]
    },
    "responseElements": null,
    "requestID": "mgh-console-eb1cf315-e2b4-4696-93e5-b3a3b9346b4b",
    "eventID": "7b32b778-91c9-4c75-9cb0-6c852791b2eb",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

Quote di AWS Application Discovery Service

La console Service Quotas fornisce le informazioni sulle quote di AWS Application Discovery Service. È possibile utilizzare la console Service Quotas per visualizzare le quote di servizio predefinite o [per richiedere aumenti delle quote](#) per quote regolabili.

Attualmente, l'unica quota che può essere aumentata è Server importati per account.

Application Discovery Service dispone delle quote predefinite riportate di seguito:

- Applicazioni 1.000 applicazioni per account.

Se si raggiunge questa quota e si desidera importare nuove applicazioni, è possibile eliminare le applicazioni esistenti con `DeleteApplications` Operazione API. Per ulteriori informazioni, consulta [DeleteApplications](#) nella Application Discovery Service Informazioni di riferimento.

- Ciascun file di importazione può avere una dimensione massima di 10 MB.
- 25.000 record di server importati per account.
- 25.000 eliminazioni di record di importazione al giorno.
- 10.000 server importati per account (puoi richiedere di aumentare questa quota).
- 1.000 agenti attivi, che raccolgono e inviano dati ad Application Discovery Service.
- 10.000 agenti inattivi, che rispondono ma non raccolgono dati.
- 400 server per applicazione.
- 30 tag per server.

Risoluzione dei problemi AWS Application Discovery Service

In questa sezione puoi trovare informazioni su come risolvere problemi comuni con AWS Application Discovery Service.

Argomenti

- [Interrompi la raccolta dei dati mediante l'esplorazione dei dati](#)
- [Rimuovi i dati raccolti dall'esplorazione dei dati](#)
- [Risolvi i problemi più comuni relativi all'esplorazione dei dati in Amazon Athena](#)
- [Risoluzione dei record di importazione non riusciti](#)

Interrompi la raccolta dei dati mediante l'esplorazione dei dati

Per interrompere l'esplorazione dei dati, puoi disattivare l'interruttore nella console Migration Hub nella scheda Discover > Data Collectors > Agents oppure richiamare l'API `StopContinuousExport`. Possono essere necessari fino a 30 minuti per interrompere la raccolta dei dati e, durante questa fase, l'interruttore a levetta sulla console e la chiamata all'API `DescribeContinuousExport` mostreranno lo stato di esplorazione dei dati come «Stop In Progress».

Note

Se dopo aver aggiornato la pagina della console l'interruttore non si disattiva e compare un messaggio di errore o se l'API `DescribeContinuousExport` restituisce lo stato "Stop_Failed", puoi riprovare disattivando l'interruttore o chiamando l'API `StopContinuousExport`. Se l' "esplorazione dei dati" mostra ancora un errore e non riesce a interrompersi correttamente, contatta l'assistenza. AWS

In alternativa, puoi interrompere manualmente la raccolta dei dati nel modo descritto nei seguenti passaggi.

Opzione 1: arrestare la raccolta dei dati da parte degli agenti

Se hai già completato il rilevamento utilizzando gli agenti ADS e non vuoi più raccogliere dati nel repository del database ADS:

1. Dalla console Migration Hub scegli Discover > Data Collectors > scheda Agenti.
2. Selezionare tutti gli agenti in esecuzione e scegliere Stop Data Collection (Interrompere la raccolta dei dati).

In questo modo gli agenti non raccoglieranno nuovi dati nel repository di dati ADS e nel bucket S3. I dati già esistenti rimangono accessibili.

Opzione 2: eliminare Amazon Kinesis Data Streams dell'esplorazione dei dati

Se desideri continuare a raccogliere dati dagli agenti nel repository di dati ADS, ma non desideri raccogliere dati nel tuo bucket Amazon S3 utilizzando l'esplorazione dei dati, puoi eliminare manualmente i flussi di Amazon Data Firehose creati dall'esplorazione dei dati:

1. Accedi ad Amazon Kinesis dalla AWS console e scegli Data Firehose dal pannello di navigazione.
2. Elimina i seguenti flussi creati dalla funzionalità di esplorazione dei dati:
 - aws-application-discovery-service-id_mapping_agent
 - aws-application-discovery-service-inbound_connection_agent
 - aws-application-discovery-service-network_interface_agent
 - aws-application-discovery-service-os_info_agent
 - aws-application-discovery-service-outbound_connection_agent
 - aws-application-discovery-service-processes_agent
 - aws-application-discovery-service-sys_performance_agent

Rimuovi i dati raccolti dall'esplorazione dei dati

Per rimuovere i dati raccolti mediante l'esplorazione dei dati

1. Rimuovi i dati dell'agente di rilevamento archiviati in Amazon S3.

I dati raccolti da AWS Application Discovery Service (ADS) vengono archiviati in un bucket S3 denominato. `aws-application-discover-discovery-service-uniqueid`

Note

L'eliminazione del bucket Amazon S3 o di uno qualsiasi degli oggetti in esso contenuti mentre l'esplorazione dei dati in Amazon Athena è abilitata causa un errore. Continua a inviare nuovi dati del Discovery Agent a S3. I dati eliminati non saranno più accessibili anche in Athena.

2. Rimuovi AWS Glue Data Catalog.

Quando l'esplorazione dei dati in Amazon Athena è attivata, crea un bucket Amazon S3 nel tuo account per archiviare i dati raccolti dagli agenti ADS a intervalli di tempo regolari. Inoltre, crea anche un file che AWS Glue Data Catalog consente di interrogare i dati archiviati in un bucket Amazon S3 da Amazon Athena. Quando disattivi l'esplorazione dei dati in Amazon Athena, non vengono archiviati nuovi dati nel bucket Amazon S3, ma i dati raccolti in precedenza persistono. Se non hai più bisogno di questi dati e desideri riportare il tuo account allo stato precedente all'attivazione dell'esplorazione dei dati in Amazon Athena.

- a. Visita Amazon S3 dalla AWS console ed elimina manualmente il bucket con il nome "-service-uniqueid» aws-application-discover-discovery
- b. Puoi rimuovere manualmente l'esplorazione dei dati AWS Glue Data Catalog eliminando il application-discovery-service-databasedatabase e tutte queste tabelle:
 - os_info_agent
 - network_interface_agent
 - sys_performance_agent
 - processes_agent
 - inbound_connection_agent
 - outbound_connection_agent
 - id_mapping_agent

Rimuovere i dati da AWS Application Discovery Service

Per far rimuovere tutti i dati da Application Discovery Service, contatta il [AWS supporto](#) e richiedi l'eliminazione completa dei dati.

Risolvi i problemi più comuni relativi all'esplorazione dei dati in Amazon Athena

In questa sezione, puoi trovare informazioni su come risolvere i problemi più comuni relativi all'esplorazione dei dati in Amazon Athena.

Argomenti

- [L'esplorazione dei dati in Amazon Athena non viene avviata perché non è possibile creare ruoli collegati ai servizi e risorse richieste AWS](#)
- [I dati dei nuovi agenti non vengono visualizzati in Amazon Athena](#)
- [Non disponi di autorizzazioni sufficienti per accedere ad Amazon S3, Amazon Data Firehose o AWS Glue](#)

L'esplorazione dei dati in Amazon Athena non viene avviata perché non è possibile creare ruoli collegati ai servizi e risorse richieste AWS

Quando attivi l'esplorazione dei dati in Amazon Athena, nel tuo account viene creato il ruolo `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport` collegato al servizio che gli consente di creare le risorse AWS necessarie per rendere accessibili i dati raccolti dall'agente in Amazon Athena, tra cui un bucket Amazon S3, Amazon Kinesis stream e AWS Glue Data Catalog. Se il tuo account non dispone delle autorizzazioni necessarie per l'esplorazione dei dati in Amazon Athena per creare questo ruolo, l'inizializzazione non riuscirà. Fai riferimento a [AWS politiche gestite per AWS Application Discovery Service](#).

I dati dei nuovi agenti non vengono visualizzati in Amazon Athena

Se non arrivano nuovi dati in Athena, sono trascorsi più di 30 minuti dall'avvio di un agente e lo stato di esplorazione dei dati è Attivo, controlla le soluzioni elencate di seguito:

- AWS Agenti Discovery

Verifica che lo stato della Collection (Raccolta) dell'agente venga contrassegnato come Started (Avviato) e lo stato di Health (Integrità) venga contrassegnato come Running (In esecuzione).

- Ruolo Kinesis

Verifica la presenza del ruolo `AWSApplicationDiscoveryServiceFirehose` nel tuo account.

- Stato Firehose

Assicuratevi che i seguenti flussi di distribuzione Firehose funzionino correttamente:

- `aws-application-discovery-service/os_info_agent`
- `aws-application-discovery-service-network_interface_agent`
- `aws-application-discovery-service-sys_performance_agent`
- `aws-application-discovery-service-processes_agent`
- `aws-application-discovery-service-inbound_connection_agent`
- `aws-application-discovery-service-outbound_connection_agent`
- `aws-application-discovery-service-id_mapping_agent`

- AWS Glue Data Catalog

Assicuratevi che il `application-discovery-service-database` database sia attivo. AWS Glue Assicuratevi che le seguenti tabelle siano presenti in AWS Glue:

- `os_info_agent`
- `network_interface_agent`
- `sys_performance_agent`
- `processes_agent`
- `inbound_connection_agent`
- `outbound_connection_agent`
- `id_mapping_agent`

- Bucket Amazon S3

Assicuratevi di avere un bucket Amazon S3 denominato `aws-application-discovery-service-uniqueid` nel tuo account. Se gli oggetti nel bucket sono stati spostati o eliminati, non verranno visualizzati correttamente in Athena.

- Server locali

Verifica che i server siano operativi in modo che gli agenti possano raccogliere e inviare dati a AWS Application Discovery Service.

Non disponi di autorizzazioni sufficienti per accedere ad Amazon S3, Amazon Data Firehose o AWS Glue

Se stai utilizzando AWS Organizations e l'inizializzazione per l'esplorazione dei dati in Amazon Athena non riesce, è possibile che non disponi delle autorizzazioni per accedere ad Amazon S3, Amazon Data Firehose, Athena o AWS Glue

Avrai bisogno di un utente IAM con autorizzazioni di amministratore per concederti l'accesso a questi servizi. Un amministratore può utilizzare il proprio account per autorizzare l'accesso. Per informazioni, consulta [AWS politiche gestite per AWS Application Discovery Service](#).

Per garantire che l'esplorazione dei dati in Amazon Athena funzioni correttamente, non modificare o eliminare AWS le risorse create dall'esplorazione dei dati in Amazon Athena, inclusi il bucket Amazon S3, Amazon Data Firehose Streams e AWS Glue Data Catalog. Se inavvertitamente elimini o modifichi queste risorse, arresta e avvia l'esplorazione dati e queste risorse verranno create automaticamente. Se elimini il bucket Amazon S3 creato dall'esplorazione dei dati, potresti perdere i dati raccolti nel bucket.

Risoluzione dei record di importazione non riusciti

L'importazione di Migration Hub consente di importare i dettagli dell'ambiente locale direttamente in Migration Hub senza utilizzare Discovery Connector o Discovery Agent. In questo modo è possibile eseguire la valutazione e pianificazione della migrazione direttamente dai dati importati. È anche possibile raggruppare i dispositivi come applicazioni e monitorarne lo stato di migrazione.

Durante l'importazione di dati, è possibile che si verifichino degli errori. In genere questi errori si verificano per uno dei seguenti motivi:

- È stata raggiunta una quota relativa all'importazione: esiste una quota associata alle attività di importazione. Se si effettua una richiesta di attività di importazione che supera le quote, la richiesta avrà esito negativo e restituirà un errore. Per ulteriori informazioni, consulta [Quote di AWS Application Discovery Service](#).
- Nel file di importazione è stata inserita una virgola aggiuntiva (,): le virgole nei file CSV vengono utilizzate per differenziare un campo dall'altro. Pertanto, una virgola all'interno di un campo

non è supportata perché dividerà sempre il campo. Questo può causare una serie di errori di formattazione. Le virgole devono essere utilizzate solo tra i campi e in nessun altro modo nei file di importazione.

- Un campo ha un valore al di fuori dell'intervallo supportato: alcuni campi, ad esempio, `CPU.NumberOfCores` devono avere un intervallo di valori che supportano. Se l'intervallo supportato non viene rispettato, il record non verrà importato.

Se si verificano errori per la richiesta di importazione, è possibile scaricare i record con esito negativo per l'attività di importazione, risolvere gli errori nel file `failed-entries.csv` ed effettuare nuovamente l'importazione.

Console

Per scaricare l'archivio dei record con esito negativo

1. Accedi a e apri AWS Management Console la console Migration Hub all'indirizzo <https://console.aws.amazon.com/migrationhub>.
2. Dal riquadro di navigazione a sinistra, in Discover (Rileva), scegli Tools (Strumenti).
3. Da Discovery Tools (Strumenti di rilevamento), scegli view imports (visualizza importazioni).
4. Dal pannello di controllo Imports (Importazioni), scegli il pulsante di opzione associato a una richiesta di importazione con alcuni Failed records (Record con errori).
5. Scegli Download failed records (Scarica record con errori) dalla tabella nel pannello di controllo. Si aprirà una finestra di dialogo del browser per scaricare il file di archivio.

AWS CLI

Per scaricare l'archivio dei record con esito negativo

1. Apri una finestra del terminale e digita il comando seguente, dove *ImportName* is the name of the import task with the failed entries that you want to correct.:

```
aws discovery describe-import-tasks - -name ImportName
```

2. Dall'output, copia l'intero contenuto del valore restituito per `errorsAndFailedEntriesZip`, senza le virgolette.

3. Apri un browser Web, incolla i contenuti nella casella di testo dell'URL e premi ENTER.
Questo scaricherà l'archivio dei record con esito negativo, compresso in un formato .zip.

Ora che hai scaricato l'archivio di record con errori, è possibile estrarre i due file all'interno e correggere gli errori. Si noti che se gli errori sono collegati a limiti dei servizi, è necessario richiedere un aumento del limite o eliminare alcune delle risorse associate per far rientrare l'account nel limite. L'archivio ha i file seguenti:

- `errors-file.csv`: questo file è il registro degli errori e tiene traccia della riga, del nome della colonna e di un messaggio di errore descrittivo per ogni record non riuscito di ogni immissione non riuscita. `ExternalId`
- `failed-entries-file.csv`: questo file contiene solo le voci non riuscite del file di importazione originale.

Per correggere gli non-limit-based errori riscontrati, utilizza il `errors-file.csv` per correggere i problemi del `failed-entries-file.csv` file, quindi importa il file. Per istruzioni sull'importazione di file, consulta [Importazione di dati](#).

Cronologia dei documenti per AWS Application Discovery Service

Ultimo aggiornamento della documentazione della Guida per l'utente: 16 maggio 2023

Nella tabella seguente sono descritte le modifiche importanti apportate alla Guida per l'utente di Application Discovery Service di a partire da 18 gennaio 2019. Per ricevere notifiche sugli aggiornamenti della documentazione, è possibile sottoscrivere il feed RSS.

Modifica	Descrizione	Data
Presentazione del database Agentless Collector e del modulo di raccolta dati di analisi	Il modulo di raccolta dei dati di database e analisi è il nuovo modulo di Application Discovery Service Agentless Collector (Agentless Collector). Puoi utilizzare questo modulo di raccolta dati per connetterti al tuo ambiente e raccogliere metadati e metadati delle prestazioni dal tuo database e dai server di analisi locali. Per ulteriori informazioni, vedere Modulo di raccolta dati di database e analisi .	16 maggio 2023
Presentazione di Application Discovery Service Agentless Collector	Application Discovery Service Agentless Collector (Agentless Collector) è la nuova applicazione AWS Application Discovery Service locale che raccoglie informazioni tramite metodi senza agenti sull'ambiente locale per aiutarti a pianificare in modo efficace	16 agosto 2022

la migrazione verso il. Cloud
AWS Per ulteriori informazioni,
consulta [Agentless Collector](#)
Collector Collector.

[Aggiornamento IAM](#)

L' discovery
:GetNetworkConnect
ionGraph azione AWS
Identity and Access
Management (IAM) è ora
disponibile per concedere
l'accesso al diagramma di
rete della AWS Migration Hub
console durante la creazione
di una policy basata sull'iden
tità. Per ulteriori informazioni,
vedere [Concessione delle
autorizzazioni per l'uso del
diagramma di rete.](#)

24 maggio 2022

[Presentazione della regione d'origine](#)

La regione di origine di
Migration Hub fornisce un
unico archivio di informazioni
sulla scoperta e sulla pianifica
zione della migrazione per
l'intero portafoglio e un'unica
visualizzazione delle migrazion
i in più regioni. AWS

20 novembre 2019

[Presentazione della funzionalità di importazione di Migration Hub](#)

L'importazione di Migration Hub consente di importare informazioni sui server e sulle applicazioni locali in Migration Hub, comprese le specifiche del server e i dati di utilizzo. È inoltre possibile utilizzare questi dati per monitorare lo stato delle migrazioni dell'applicazione. Per ulteriori informazioni, consulta [Migration Hub Import Import Import Import](#)

18 gennaio 2019

La tabella seguente descrive le versioni della documentazione per la Guida per l'utente di Application Discovery Service prima del 18 gennaio 2019:

Modifica	Descrizione	Data
Nuova caratteristica	Documenti aggiornati per supportare l'esplorazione dei dati in Amazon Athena e capitolo relativo alla risoluzione dei problemi.	09 agosto 2018
Revisione principale	Riscritture per dettagli di utilizzo e output; intero documento ristrutturato.	25 maggio 2018
Discovery Agent 2.0	È stata rilasciata una nuova versione migliorata dell'agente Application Discovery.	19 ottobre 2017
Console	È stato aggiunto AWS Management Console.	19 dicembre 2016
Rilevamento senza agente	In questa release viene descritto come impostare e	28 luglio 2016

Modifica	Descrizione	Data
	configurare il rilevamento senza agente.	
Nuovi dettagli per Microsoft Windows Server e correzioni e dei problemi relativi ai comandi	Questo aggiornamento aggiunge dettagli su Microsoft Windows Server. Documenta inoltre correzioni apportate a vari problemi relativi ai comandi.	20 maggio 2016
Pubblicazione iniziale	La prima versione della Guida per l'utente di Application Discovery Service Service Service Service Service Service per prima versione.	12 maggio 2016

Glossario per AWS

Per la terminologia AWS più recente, consultare il [glossario AWS](#) nella documentazione di riferimento per Glossario AWS.

Appendice

Questa sezione contiene informazioni supplementari su. AWS Application Discovery Service

Argomenti

- [Appendice: Transizione da Discovery Connector a Agentless Collector](#)
- [Appendice: AWS Agentless Discovery Connector](#)

Appendice: Transizione da Discovery Connector a Agentless Collector

Questa sezione descrive come passare da AWS Agentless Discovery Connector (Discovery Connector) a Application Discovery Service Agentless Collector (Agentless Collector).

Consigliamo ai clienti che attualmente utilizzano Discovery Connector di passare al nuovo Agentless Collector.

Per informazioni su come iniziare a utilizzare Agentless Collector, consulta. [Guida introduttiva a Agentless Collector](#)

Dopo aver distribuito Agentless Collector, è possibile eliminare la macchina virtuale Discovery Connector. Tutti i dati raccolti in precedenza continueranno a essere disponibili in AWS Migration Hub (Migration Hub).

Appendice: AWS Agentless Discovery Connector

Important

Consigliamo ai clienti che attualmente utilizzano Discovery Connector di passare al nuovo Agentless Collector. Per ulteriori informazioni, consulta [Appendice: Transizione da Discovery Connector a Agentless Collector](#).

Argomenti

- [Dati raccolti dal Discovery Connector](#)

- [Raccolta dati di Discovery Connector](#)
- [Risoluzione dei problemi del Discovery Connector](#)

Dati raccolti dal Discovery Connector

Il Discovery Connector raccoglie informazioni sugli host e sulle macchine virtuali VMware vCenter Server. Tuttavia, puoi acquisire questi dati solo se gli strumenti VMware vCenter Server sono installati. Per assicurarsi che l' AWS account che si sta utilizzando disponga dell'autorizzazione necessaria per questa attività, vedere. [AWS politiche gestite per AWS Application Discovery Service](#)

Di seguito, è possibile trovare un inventario delle informazioni raccolte da Discovery Connector.

Legenda della tabella per i dati raccolti da Discovery Connector:

- I dati raccolti sono misurati in kilobyte (KB) salvo diversamente specificato.
- I dati equivalenti nella console Migration Hub sono riportati in megabyte (MB).
- I campi dati contrassegnati da un asterisco (*) sono disponibili solo nei file.csv prodotti dalla funzione di esportazione API del connettore.
- Il periodo di polling è in intervalli di circa 60 minuti.
- Attualmente, i campi dati identificati con un asterisco (**) restituiscono un valore null.

Campo dati	Descrizione
applicationConfigurationId*	ID dell'applicazione di migrazione rispetto alla quale è raggruppata la macchina virtuale
avgCpuUsagePct	Percentuale di utilizzo medio della CPU nel periodo di polling
avgDiskBytesReadPerSecond	Il numero medio di byte letti dal disco nel periodo di polling.
avgDiskBytesWrittenPerSecond	Il numero medio di byte scritti su disco nel periodo di polling.
avgDiskReadOpsPerSecond**	Numero medio di operazioni I/O di lettura al secondo null

Campo dati	Descrizione
avgDiskWriteOpsPerSecond**	Numero medio di operazioni di I/O di scrittura al secondo
avgFreeRAM	RAM media libera espressa in MB
avgNetworkBytesReadPerSecond	Quantità media di throughput di byte letti al secondo
avgNetworkBytesWrittenPerSecond	Quantità media di throughput di byte scritti al secondo
configId	ID assegnato da Application Discovery Service alla macchina virtuale rilevata
configType	Tipo di risorsa rilevata
connectorId	ID dell'appliance virtuale Discovery Connector
cpuType	vCPU per una macchina virtuale, modello effettivo per un host
datacenterId	ID del vCenter
hostId*	ID dell'host della macchina virtuale
hostName	Nome dell'host che esegue il software di virtualizzazione
hypervisor	Tipo di hypervisor
id	ID di server
lastModifiedTime ^{Timbro *}	Data e ora dell'ultima raccolta dati prima dell'esportazione dei dati
macAddress	Indirizzo MAC della macchina virtuale
manufacturer	Maker del software di virtualizzazione

Campo dati	Descrizione
maxCpuUsagePct	Percentuale massima di utilizzo della CPU durante il periodo di polling
maxDiskBytesReadPerSecond	Numero massimo di byte letti dal disco nel periodo di polling.
maxDiskBytesWrittenPerSecond	Numero massimo di byte scritti su disco nel periodo di polling.
maxDiskReadOpsPerSecond ^{**}	Numero massimo di operazioni di I/O di lettura al secondo
maxDiskWriteOpsPerSecond ^{**}	Numero massimo di operazioni di I/O di scrittura al secondo
maxNetworkBytesReadPerSecond	Quantità massima di throughput di byte letti al secondo
maxNetworkBytesWrittenPerSecond	Quantità massima di throughput di byte scritti al secondo
memoryReservation [*]	Limite per evitare l'eccesso di impegno di memoria su macchina virtuale
moRefId	ID univoco di riferimento dell'oggetto vCenter gestito
name [*]	Nome della macchina virtuale o della rete (specificato dall'utente)
numCores	Numero di unità di elaborazione indipendenti all'interno della CPU
numCpus	Numero di unità di elaborazione centrali su macchina virtuale
numDisks ^{**}	Numero di dischi su macchina virtuale

Campo dati	Descrizione
numNetworkCards**	Numero di schede di rete su macchina virtuale
osName	Nome del sistema operativo su macchina virtuale
osVersion	Versione del sistema operativo su macchina virtuale
portGroupId*	ID di gruppo delle porte membro di VLAN
portGroupName*	Nome di gruppo delle porte membro di VLAN
powerState*	Stato di alimentazione
serverId	ID assegnato da Application Discovery Service alla macchina virtuale rilevata
smBiosId*	ID/versione del BIOS di gestione del sistema
state*	Stato dell'appliance virtuale Discovery Connector
toolsStatus	Stato operativo degli strumenti VMware (consulta Visualizzazione e ordinamento dei raccoglitori di dati per un elenco completo).
totalDiskSize	Capacità totale del disco espressa in MB
totalRAM	Quantità totale di RAM disponibile su macchina virtuale in MB
type (tipo)	Tipo di host
vCenterId	Numero ID univoco di una macchina virtuale
vCenterName*	Nome dell'host vCenter
virtualSwitchName*	Nome dello switch virtuale

Campo dati	Descrizione
vmFolderPath	Percorso di directory dei file della macchina virtuale
vmName	Nome della macchina virtuale

Raccolta dati di Discovery Connector

Dopo aver distribuito e configurato Discovery Connector nell'ambiente VMware, se la raccolta dei dati si interrompe, è possibile riavviarlo. È possibile avviare o interrompere la raccolta dei dati tramite la console o effettuando chiamate API tramite AWS CLI. Entrambi questi metodi sono descritti nelle procedure seguenti.

Using the Migration Hub Console

La procedura seguente mostra come avviare o interrompere il processo di raccolta dati di Discovery Connector, nella pagina Data Collectors della console Migration Hub.

Per avviare o interrompere la raccolta dei dati

1. Nel riquadro di navigazione, selezionare Data Collectors (Agenti di raccolta dati).
2. Seleziona la scheda Connectors (Connettori).
3. Seleziona la casella di controllo del connettore che desideri avviare o interrompere.
4. Selezionare Start data collection (Avvia raccolta dei dati) o Stop data collection (Arresta raccolta dei dati).

Note

Se non visualizzi le informazioni sull'inventario dopo aver avviato la raccolta dati con il connettore, conferma di aver registrato il connettore con vCenter Server.

Using the AWS CLI

Per avviare il processo di raccolta dati di Discovery Connector da AWS CLI, è AWS CLI necessario prima installarlo nell'ambiente e quindi impostare la CLI per utilizzare la regione [principale di Migration Hub](#) selezionata.

Per installare AWS CLI e avviare la raccolta dei dati

1. Installa il AWS CLI file per il tuo sistema operativo (Linux, macOS o Windows). Consulta la [Guida per AWS Command Line Interface l'utente](#) per le istruzioni.
2. Aprire il prompt dei comandi (Windows) o Terminal (Linux o macOS).
 - a. Digitare `aws configure` e premere Invio.
 - b. Inserisci AWS l'ID della chiave di accesso e la chiave di accesso AWS segreta.
 - c. Inserisci la tua regione d'origine per il nome predefinito della regione. Ad esempio, `us-west-2`.
 - d. Immettere `text` per Default Output Format (Formato di output predefinito).
3. Per trovare l'ID del connettore per il quale desideri avviare o interrompere la raccolta dei dati, digita il seguente comando per visualizzare l'ID del connettore:

```
aws discovery describe-agents --filters  
condition=EQUALS,name=hostName,values=connector
```

4. Per avviare la raccolta dei dati da parte del connettore, digita il seguente comando:

```
aws discovery start-data-collection-by-agent-ids --agent-ids <connector ID>
```

Note

Se non visualizzi le informazioni sull'inventario dopo aver avviato la raccolta dati con il connettore, conferma di aver registrato il connettore con vCenter Server.

Per interrompere la raccolta dei dati da parte del connettore, digitate il seguente comando:

```
aws discovery stop-data-collection-by-agent-ids --agent-ids <connector ID>
```


Risoluzione dei problemi del Discovery Connector

Questa sezione contiene argomenti che possono aiutarti a risolvere i problemi noti relativi ad Application Discovery Service Discovery Connector.

Impossibile risolvere il problema di Discovery Connector durante la configurazione AWS

Quando si configura l' AWS Agentless Discovery Connector nella console, è possibile che venga visualizzato il seguente messaggio di errore:

Impossibile raggiungere AWS

AWS impossibile da raggiungere (ripristino della connessione). Verifica le impostazioni di rete e proxy.

Questo errore si verifica a causa di un tentativo fallito da parte di Discovery Connector di stabilire una connessione HTTPS a un AWS dominio con cui il connettore deve comunicare durante il processo di configurazione. La configurazione di Discovery Connector fallisce se non è possibile stabilire una connessione.

Per correggere la connessione a AWS

1. Rivolgiti all'amministratore IT per verificare se il firewall aziendale sta bloccando il traffico in uscita sulla porta 443 verso uno dei AWS domini che richiedono l'accesso in uscita.

I seguenti AWS domini richiedono l'accesso in uscita:

- `awsconnector.Migration Hub home Region.amazonaws.com`
- `sns.Migration Hub home Region.amazonaws.com`
- `arsenal-discovery.Migration Hub home Region.amazonaws.com`
- `iam.amazonaws.com`
- `aws.amazon.com`
- `ec2.amazonaws.com`

Se il firewall blocca il traffico in uscita, sbloccalo. Dopo aver aggiornato il firewall, riconfigura il connettore.

2. Se l'aggiornamento del firewall non risolve il problema di connessione, assicurati che la macchina virtuale del connettore disponga di connettività di rete in uscita ai domini elencati. Se la macchina virtuale dispone di connettività in uscita, verifica la connessione ai domini elencati eseguendo telnet sulle porte 443, come mostrato nell'esempio seguente.

```
telnet ec2.amazonaws.com 443
```

3. Se la connettività in uscita dalla macchina virtuale è abilitata, è necessario contattare l'[AWS assistenza](#) per un'ulteriore risoluzione dei problemi.

Correzione di connettori non integri

Le informazioni sanitarie per ogni Discovery Connector sono disponibili nella pagina [Data Collector](#) della console Migration Hub. È possibile identificare i connettori con problemi individuando quelli con lo stato di integrità Unhealthy (Non integro). Nella procedura seguente viene descritto come accedere alla console del connettore per identificare i problemi di integrità.

Accedere alla console di un connettore

1. Apri la console Migration Hub in un browser Web e scegli Data Collectors dalla barra di navigazione a sinistra.
2. Dalla scheda Connectors (Connettori) prendere nota dell'indirizzo IP di ogni connettore con stato di integrità Unhealthy (Non integro).
3. Apri un browser su qualsiasi computer in grado di connettersi alla macchina virtuale del connettore e inserisci l'URL della console del connettore `https://ip_address_of_connector`, dove `ip_address_of_connector` trova l'indirizzo IP di un connettore non funzionante.
4. Immettere la password della console di gestione del connettore, impostata al momento della configurazione del connettore.

Dopo aver effettuato l'accesso alla console del connettore, puoi eseguire le operazioni per risolvere uno stato non integro. Qui puoi scegliere View Info (Visualizza informazioni) per vCenter connectivity (Connettività vCenter). Viene visualizzata una finestra di dialogo con un messaggio di diagnostica. Il collegamento View Info (Visualizza informazioni) è disponibile solo sui connettori versione 1.0.3.12 o successiva.

Dopo aver corretto i problemi di integrità, il connettore ristabilirà la connettività con il server vCenter e lo stato del connettore diventa HEALTHY (INTEGRO). Se il problema persiste, contatta l'[AWS assistenza](#).

Le cause più comuni per i connettori non integri sono problemi di indirizzo IP e problemi di credenziali. Nelle sezioni seguenti è possibile risolvere questi problemi e ripristinare lo stato integro di un connettore.

Argomenti

- [Problemi relativi all'indirizzo IP](#)
- [Problemi con le credenziali](#)

Problemi relativi all'indirizzo IP

Un connettore può passare nello stato non integro se l'endpoint vCenter fornito durante l'installazione del connettore è errato, non valido o se il server vCenter è attualmente inattivo e non raggiungibile. In questo caso, quando si sceglie View Info (Visualizza informazioni) per vCenter connectivity (Connettività vCenter) viene visualizzata una finestra di dialogo con il messaggio che richiede di confermare lo stato operativo del server vCenter o scegliere Modifica impostazioni per aggiornare l'endpoint vCenter.

La procedura seguente consente di risolvere i problemi relativi all'indirizzo IP.

1. Dalla console del connettore (https://ip_address_of_connector), scegliere Edit Settings (Modifica impostazioni).
2. Dalla barra di navigazione a sinistra, scegliere Step 5: Discovery Connector Set Up (Fase 5: configurazione di Discovery Connector).
3. Da Configure vCenter credentials (Configura credenziali vCenter), prendere nota dell'indirizzo IP di vCenter Host (Host vCenter).
4. Utilizzando uno strumento a riga di comando separato come `ping` o `tracert`, verifica che il server vCenter associato sia attivo e che l'IP sia raggiungibile dalla macchina virtuale del connettore.
 - Se l'indirizzo IP non è corretto e il servizio vCenter è attivo, aggiornare l'indirizzo IP nella console del connettore e scegliere Next (Successivo).
 - Se l'indirizzo IP è corretto ma il server vCenter non è attivo, attivarlo.

- Se l'indirizzo IP è corretto e il server vCenter è attivo, verificare se blocca le connessioni di rete in ingresso a causa di problemi di firewall. In caso affermativo, aggiornare le impostazioni del firewall per consentire le connessioni in ingresso dalla macchina virtuale del connettore.

Problemi con le credenziali

I connettori possono essere in uno stato non integro se le credenziali utente di vCenter fornite durante l'installazione del connettore non sono valide o non dispongono dei privilegi per l'account vCenter di lettura e visualizzazione. In questo caso, quando scegli View Info (Visualizza informazioni) per vCenter connectivity (Connettività vCenter) viene visualizzata una finestra di dialogo con il messaggio indicante di scegliere Modifica impostazioni per aggiornare il tuo nome utente e la password vCenter per il tuo account con privilegi di lettura e visualizzazione.

La procedura seguente consente di risolvere i problemi relativi alle credenziali. Come prerequisito, assicurati di aver creato un utente vCenter che disponga di autorizzazioni per l'account in lettura e visualizzazione sul server vCenter.

1. Dalla console del connettore (https://ip_address_of_connector), scegliere Edit Settings (Modifica impostazioni).
2. Dalla barra di navigazione a sinistra, scegliere Step 5: Discovery Connector Set Up (Fase 5: configurazione di Discovery Connector).
3. Da Configure vCenter credentials (Configura credenziali vCenter), aggiornare vCenter Username (Nome utente vCenter) e vCenter Password (Password vCenter) fornendo le credenziali per un utente vCenter con le autorizzazioni di lettura e visualizzazione.
4. Scegliere Next (Successivo) per completare la configurazione.

Supporto per host ESX autonomi

Il Discovery Connector non supporta un host ESX autonomo. L'host ESX deve essere parte dell'istanza di vCenter Server.

Ottenere supporto aggiuntivo per i problemi relativi ai connettori

Se riscontri problemi e hai bisogno di aiuto, contatta l'[AWS assistenza](#). Verrai contattato e ti potrebbe essere chiesto di inviare i log del connettore. Per ottenere i log, procedi come indicato di seguito.

- Accedi nuovamente alla console AWS Agentless Discovery Connector e scegli Scarica il pacchetto di log.

- Dopo che il download del pacchetto di log è terminato, invialo come da indicato da AWS Support.

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.