



Guida per l'utente

AWS Servizio Application Discovery



AWS Servizio Application Discovery: Guida per l'utente

Copyright © 2026 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 dei rispettivi proprietari, che possono o meno essere affiliati, collegati o sponsorizzati da Amazon.

Table of Contents

Che cos'è AWS Application Discovery Service?	1
VMware Discovery	2
Individuazione dei database	3
Confronta Agentless Collector e Discovery Agent	3
Presupposti	7
AWS Application Discovery Service modifica della disponibilità	8
Dettagli sulla disponibilità del servizio	8
AWS Transform transizione	8
Domande frequenti	9
Configurazione	11
Registrazione ad Amazon Web Services	11
Crea utenti IAM	11
Creazione di un utente amministrativo IAM	12
Creazione di un utente IAM non amministrativo	12
Accedi a Migration Hub e scegli una regione d'origine	13
Agente Discovery	14
Come funziona	14
Dati raccolti	15
Prerequisiti	18
Installazione di Discovery Agent	19
Installazione del su Linux	20
Installazione su Microsoft Windows	23
Gestione del processo di Discovery Agent	27
Gestisci il processo su Linux	28
Gestisci il processo su Microsoft Windows	29
Disinstallazione di Discovery Agent	30
Disinstalla su Linux	30
Disinstallazione su Microsoft Windows	30
Avvio e arresto della raccolta dei dati	31
Risoluzione problemi di Discovery Agent	32
Risoluzione dei problemi di Discovery Agent su Linux	33
Risoluzione dei problemi di Discovery Agent su Microsoft Windows	33
Agentless Collector	35
Prerequisiti	35

Configura il perimetro dei dati	36
Configurare il firewall	37
Implementazione di un raccoglitore	38
Creare un utente IAM	38
Scarica il raccoglitore	41
Distribuisci il raccoglitore	42
Accesso alla console Collector	43
Configurazione del raccoglitore	44
(Facoltativo) Configurare un indirizzo IP statico per la macchina virtuale collector	45
(Facoltativo) Reimposta la VM del collettore all'utilizzo di DHCP	51
(Facoltativo) Configurare Kerberos	53
Utilizzo del modulo Network Data Collection	54
Configurazione del modulo Network Data Collection	55
Tentativi di raccolta di dati di rete	57
Stato del server nel modulo Network Data Collection	57
Utilizzo del modulo di raccolta dati VMware	58
Configurazione della raccolta dati vCenter	58
Visualizzazione VMware dei dettagli della raccolta dei dati	59
Controllo dell'ambito della raccolta dei dati	60
Dati raccolti dal modulo VMware	62
Utilizzo del database e del modulo di raccolta dei dati di analisi	66
Server supportati	67
Creazione del raccoglitore di AWS DMS dati	68
Configurazione dell'inoltro dei dati	70
Aggiungere i server LDAP e OS	70
Alla scoperta dei tuoi database	73
Dati raccolti dal database e dal modulo di analisi	78
Visualizzazione dei dati raccolti	79
Accesso all'Agentless Collector	80
Dashboard Collector	80
Modifica delle impostazioni del raccoglitore	83
Modifica delle credenziali vCenter	84
Aggiornamento di Agentless Collector	84
Risoluzione dei problemi	86
Riparazione Unable to retrieve manifest or certificate file error	86

Risoluzione dei problemi di certificazione autofirmata durante la configurazione dei certificati	
WinRM	87
Fixing Agentless Collector non riesce a raggiungerlo durante la configurazione AWS	88
Risoluzione dei problemi di certificazione autofirmata durante la connessione all'host	
proxy	89
Trovare collezionisti malsani	90
Risoluzione dei problemi relativi all'indirizzo IP	91
Risoluzione dei problemi relativi alle credenziali vCenter	92
Risoluzione dei problemi di inoltro dei dati	92
Risoluzione dei problemi di connessione	93
Supporto per host ESX autonomi	95
Contattare AWS Support	95
Importazione di dati in Migration Hub	96
Formati di importazione supportati	96
RVTools	97
Modello di importazione Migration Hub	97
Configurazione delle autorizzazioni di importazione	103
Caricamento del file di importazione su Amazon S3	106
Importazione dei dati	107
Monitoraggio delle richieste di importazione di Migration Hub	110
Visualizza ed esplora i dati	112
Visualizza i dati raccolti	112
Logica di corrispondenza	113
Esplorazione dei dati in Athena	114
Attivazione dell'esplorazione dei dati	114
Esplorazione dei dati	116
Visualizzazione dei dati	117
Utilizzo di query predefinite	118
Alla scoperta dei dati con la console Migration Hub	127
Visualizzazione dei dati nella dashboard	127
Avvio e arresto dei raccoglitori di dati	128
Ordinamento dei raccoglitori di dati	129
Visualizzazione dei server	133
Ordinamento dei server	134
Server di etichettatura	134
Esportazione dei dati del server	136

Raggruppamento dei server	138
Utilizzo dell'API per interrogare gli elementi scoperti	140
Utilizzo dell'DescribeConfigurationsazione	140
Utilizzo dell'azione ListConfigurations	144
Consistenza finale	159
AWS PrivateLink	161
Considerazioni	161
Creazione di un endpoint di interfaccia	161
Creazione di una policy dell'endpoint	162
Utilizzo dell'endpoint VPC per Agentless Collector e Application Discovery Agent AWS	163
Sicurezza	165
Identity and Access Management	166
Destinatari	166
Autenticazione con identità	167
Gestione dell'accesso tramite policy	168
Come AWS Application Discovery Service funziona con IAM	170
AWS politiche gestite	172
Esempi di policy basate su identità	177
Comprensione e utilizzo dei ruoli collegati ai servizi	185
Risoluzione dei problemi di IAM	193
Registrazione delle chiamate API di CloudTrail con	194
Informazioni su Application Discovery Service in CloudTrail	194
Informazioni sulle voci dei file di registro di Application Discovery Service	195
Formati ARN	197
Quote	198
Risoluzione dei problemi	199
Interrompi la raccolta dei dati mediante l'esplorazione dei dati	199
Rimuovi i dati raccolti dall'esplorazione dei dati	200
Risolvi i problemi più comuni relativi all'esplorazione dei dati in Amazon Athena	202
L'esplorazione dei dati in Amazon Athena non viene avviata perché non è possibile creare ruoli collegati ai servizi e risorse richieste AWS	202
I dati dei nuovi agenti non vengono visualizzati in Amazon Athena	202
Non disponi di autorizzazioni sufficienti per accedere ad Amazon S3, Amazon Data Firehose o AWS Glue	204
Risoluzione dei record di importazione non riusciti	204
Cronologia dei documenti	207

AWS Glossario	212
.....	ccxiii

Che cos'è AWS Application Discovery Service?

AWS Application Discovery Service ti aiuta a pianificare la migrazione al AWS cloud raccogliendo dati di utilizzo e configurazione sui server e sui database locali. Application Discovery Service è integrato con AWS Migration Hub AWS Database Migration Service Fleet Advisor. Migration Hub semplifica il monitoraggio della migrazione in quanto aggrega le informazioni sullo stato della migrazione in un'unica console. È possibile visualizzare i server rilevati, raggrupparli in applicazioni e quindi tenere traccia dello stato della migrazione di ciascuna applicazione dalla console Migration Hub nella propria area geografica. 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 AWS Migration Hub regione di origine. Pertanto, è necessario impostare la propria regione di origine 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 Quick.

Utilizzando Application Discovery Service APIs, 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 esecuzione di tali 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 regione di residenza deve essere impostata AWS Migration Hub prima di iniziare il processo di scoperta, poiché i dati verranno archiviati nella regione di origine. Per ulteriori informazioni su come lavorare con una regione d'origine, vedi [Home Region](#).

Application Discovery Service offre tre modi per eseguire il rilevamento e la raccolta di dati sui server locali:

- Il rilevamento senza agente può essere eseguito distribuendo l'Application Discovery Service Agentless Collector (Agentless Collector) (file OVA) tramite vCenter. VMware Una volta configurato, Agentless Collector identifica le macchine virtuali (VMs) 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 su disco, versioni dei motori di database e schemi di

database. Inoltre, raccoglie i dati di utilizzo per ogni macchina virtuale e database, fornendo l'utilizzo medio e di picco per metriche quali CPU, RAM e I/O del disco.

- L'individuazione basata su agenti può essere eseguita implementando AWS Application Discovery Agent (Discovery Agent) su ciascuno dei tuoi server e su quelli fisici. VMs 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.
- L'importazione basata su file consente di importare i dettagli dell'ambiente locale direttamente in Migration Hub senza utilizzare Agentless Collector o Discovery Agent, in modo da poter eseguire la valutazione e la pianificazione della migrazione direttamente dai dati importati. I dati acquisiti dipendono dai dati forniti.

Application Discovery Service si integra con le soluzioni di scoperta delle applicazioni dei AWS partner Partner Network (APN). Queste soluzioni di terze parti possono aiutarti a importare i dettagli del tuo ambiente locale direttamente in Migration Hub, senza utilizzare alcun agente di raccolta o discovery agent senza agente. Gli strumenti di rilevamento delle applicazioni di terze parti possono interrogare AWS Application Discovery Service e 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.

VMware Discovery

Se si dispone di macchine virtuali (VMs) in esecuzione nell'ambiente VMware vCenter, è possibile utilizzare Agentless Collector per raccogliere informazioni di sistema senza dover installare un agente su ogni macchina virtuale. Invece, si carica questa appliance locale in vCenter e le si consente di scoprire tutti i suoi host e VMs

Agentless Collector acquisisce informazioni sulle prestazioni del sistema e sull'utilizzo delle risorse per ogni macchina virtuale in esecuzione nel vCenter, indipendentemente dal sistema operativo in uso. Tuttavia, non può «guardare all'interno» di ciascuna macchina virtuale e VMs, pertanto, non è in grado di capire quali processi sono in esecuzione su ciascuna macchina virtuale né quali connessioni di rete esistono. Pertanto, se avete bisogno di questo livello di dettaglio e desiderate esaminare più da vicino alcuni dei vostri sistemi esistenti VMs per aiutarvi a pianificare la migrazione, potete installare Discovery Agent in base alle esigenze.

Inoltre, se VMs ospitato su VMware, è possibile utilizzare sia Agentless Collector che Discovery Agent per eseguire il rilevamento contemporaneamente. Per informazioni dettagliate sui tipi esatti di

dati che ogni strumento di rilevamento raccoglierà, consulta. [Utilizzo del modulo di VMware raccolta dati vCenter Agentless Collector](#)

Individuazione dei 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 dell'ambiente.

Il modulo di raccolta dei dati di analisi e database Agentless Collector acquisisce metadati e metriche prestazionali che forniscono informazioni dettagliate sull'infrastruttura di 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 delle query per raccogliere i parametri di utilizzo effettivo della CPU, della memoria e della capacità del disco per i database e i server di analisi. Per i dettagli sulle 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 la AWS DMS console per ulteriori analisi e per pianificare la migrazione. Ad esempio, per scegliere un obiettivo di migrazione ottimale in Cloud AWS, è possibile generare raccomandazioni sulle destinazioni per i database di origine. Per ulteriori informazioni, consulta [Utilizzo del database e del modulo di raccolta dei dati di analisi](#).

Confronta Agentless Collector e Discovery Agent

La tabella seguente fornisce un rapido confronto dei metodi di raccolta dati supportati da Application Discovery Service.

	Agentless Collector	Agente Discovery	Modello Migration Hub	RVTtools esportazione
Supported server types				
VMware macchina virtuale	Si	Si	Si	Si

	Agentless Collector	Agente Discovery	Modello Migration Hub	RVTools esportazione
Server fisico	No	Si	Si	Si
Deployment				
Per server	No	Si	N/D	No
Per vCenter	Si	No	N/D	Si
Per data center sulla stessa rete	No	No	N/D	No
Collected data				
Dati del profilo del server (configurazione statica)	Si	Si	Si	Si
Metriche di utilizzo del server fornite da Hypervisor (CPU, RAM, ecc.)	Si	Si	Si	No
Metriche di utilizzo del server ricavate dal server (CPU, RAM, ecc.)	Si	Si	Si	No
Connessioni di rete al server (solo TCP)	Si	Si	No	No

	Agentless Collector	Agente Discovery	Modello Migration Hub	RVTools esportazione
Processi in esecuzione	No	Si	No	No
Intervallo di raccolta	-60 minuti	-15 secondi	Istantanea singola	Istantanea singola
Server data use cases				
Visualizza i dati del server in Migration Hub	Si	Si	Solo profilo	No
Genera raccomandazioni Amazon EC2 in base al profilo del server	Si	Si	Si	Si
Genera raccomandazioni Amazon EC2 in base ai dati di utilizzo	Si	Si	Si	No
Esportazione dei dati degli snapshot di utilizzo più recenti	Si	Si	Si	No
Esportazione dei dati di utilizzo delle serie temporali	No	Si	No	No
Network data use cases				

	Agentless Collector	Agente Discovery	Modello Migration Hub	RVTools esportazione
Visualizzazione in Migration Hub	Si	Si	No	No
Esporta in Amazon Athena per ulteriori esplorazioni	No	Si	No	No
Esporta in un file CSV	No	Si	No	No
Database use cases				
Dati del profilo del server di database (configurazione statica)	Si	No	No	No
Motori di database supportati	Oracle, SQL Server, MySQL, PostgreSQL	Nessuno	Nessuna	Nessuno
Complessità e duplicati dello schema del database	Si	No	No	No
Oggetti dello schema del database	Si	No	No	No
Platform support				

	Agentless Collector	Agente Discovery	Modello Migration Hub	RVTools esportazione
Sistemi operativi supportati	Qualsiasi sistema operativo in esecuzione su VMware Center v5.5 o versioni successive	Qualsiasi server Linux o Windows	Qualsiasi server Linux o Windows	Qualsiasi server Linux, server Windows o versione VMware v5.5 o più recente

Presupposti

Per utilizzare Application Discovery Service, si presuppone quanto segue:

- Ti sei registrato per AWS. Per ulteriori informazioni, consulta [Configurazione di Application Discovery Service](#).
- Hai selezionato una regione di origine di Migration Hub. Per ulteriori informazioni, consulta [la documentazione relativa alle regioni d'origine](#).

Ecco cosa aspettarsi:

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

AWS Application Discovery Service modifica della disponibilità

Dopo un'attenta valutazione, abbiamo deciso di chiudere AWS Application Discovery Service a nuovi clienti a partire dal 7 novembre 2025. Se desideri utilizzare il servizio, registrati prima di tale data. I clienti esistenti possono continuare a utilizzare il servizio normalmente.

Questo argomento fornisce informazioni sulla modifica della disponibilità e linee guida per la transizione a AWS Transform.

Dettagli sulla disponibilità del servizio

Application Discovery Service smetterà di accettare nuovi clienti a partire dal 7 novembre 2025. AWS Transform è il nostro servizio di intelligenza artificiale agentica di nuova generazione che offre funzionalità simili e funzionalità avanzate di scoperta e valutazione delle VM. I clienti esistenti di Application Discovery Service possono continuare a utilizzare il servizio per completare i progetti di discovery in corso, che in genere hanno un ciclo di vita di 4 mesi. Le funzionalità principali del servizio per l'individuazione e la raccolta di dati su server e applicazioni locali sono ora disponibili AWS Transform con funzionalità migliorate, che non richiedono alcun intervento da parte del cliente per la transizione.

Fino al 7 novembre 2025, continueremo a mantenere la sicurezza e l'affidabilità di Application Discovery Service. Sebbene non aggiungeremo nuove funzionalità al servizio, restiamo impegnati a fornire aggiornamenti di sicurezza e a mantenere la disponibilità del servizio per garantire che i progetti di migrazione in corso continuino a funzionare senza intoppi. Il nostro obiettivo è garantire un ambiente stabile in cui i clienti esistenti possano completare le loro iniziative di migrazione in volo preparandosi al contempo alle funzionalità avanzate disponibili in AWS Transform.

AWS Transform transizione

AWS Transform è la nostra soluzione consigliata che riunisce tutte le funzionalità di Application Discovery Service introducendo nuove potenti funzionalità. Fornisce funzionalità complete di scoperta e valutazione tramite raccoglitori basati su agenti e senza agenti, con analisi ambientale avanzata. VMware Il servizio consente la mappatura automatizzata delle dipendenze delle applicazioni e la pianificazione delle ondate, offrendo al contempo una logica di scoperta migliorata con analisi ipotetiche e stime dei costi. Con funzionalità avanzate tra cui storage integrato e rilevamento dei

database, integrazione consolidata degli strumenti 3P e analisi completa della configurazione delle macchine virtuali, AWS Transform è progettato per rendere il processo di valutazione e pianificazione della migrazione dei clienti più efficiente e efficace.

La transizione a AWS Transform è semplice e non richiede la migrazione dei dati. I progetti di discovery esistenti in Application Discovery Service continueranno a funzionare normalmente fino al completamento. Quando i clienti sono pronti per avviare nuovi progetti di scoperta, possono iniziare a utilizzarli AWS Transform direttamente: tutte le funzionalità di scoperta e valutazione di Application Discovery Service sono disponibili lì con funzionalità avanzate. Per iniziare a utilizzarlo, AWS Transform consulta la [Guida introduttiva](#). AWS Il team di supporto è disponibile tramite la console di AWS supporto per fornire assistenza in caso di AWS Transform accesso o domande sui progetti di scoperta in corso.

Domande frequenti

Cosa significa questo per il servizio (avete intenzione di chiudere il servizio)?

Application Discovery Service smetterà di accettare nuovi clienti a partire dal 7 novembre 2025. Il servizio continuerà a funzionare per consentire ai clienti esistenti di completare i loro progetti di migrazione in corso.

In che modo verranno influenzati i clienti esistenti?

I clienti esistenti non subiranno alcuna interruzione dei loro attuali progetti di migrazione. Possono continuare a utilizzare Application Discovery Service normalmente fino al completamento dei progetti. Tutti i progetti in corso rimarranno accessibili e gli aggiornamenti di sicurezza continueranno a essere implementati per mantenere l'affidabilità del servizio.

Il 7 novembre 2025, il cliente sta riscontrando dei problemi, come possono aggravarsi?

I clienti che riscontrano problemi possono contattare l'AWS assistenza tramite la console di AWS supporto. Il team di AWS supporto è a disposizione per rispondere a qualsiasi domanda o dubbio relativo al servizio.

Quali alternative possono esplorare i clienti?

AWS Transform è il servizio alternativo consigliato. Lanciato nel 2025, AWS Transform include funzionalità simili per Application Discovery Service. Offre funzionalità avanzate con una migliore analisi VMware dell'ambiente e una mappatura automatizzata delle dipendenze. Fornisce funzionalità

integrate di storage e individuazione dei database e strumenti di valutazione completi. Non sono necessari strumenti speciali durante la transizione a AWS Transform

In che modo i clienti possono migrare da Application Discovery Service?

Non è richiesto alcun processo di migrazione formale. I progetti esistenti possono continuare in Application Discovery Service fino al completamento. Per i nuovi progetti, i clienti possono iniziare direttamente AWS Transform, il che fornisce tutte le funzionalità familiari di Application Discovery Service con funzionalità avanzate. Non è necessaria alcuna migrazione dei dati e AWS il servizio Support è disponibile per assisterti nella transizione.

Se hai altre domande, contattaci tramite [AWS Support](#) o leggi il nostro FAQs.

Configurazione di Application Discovery Service

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

[Registrazione ad Amazon Web Services](#)

[Crea utenti IAM](#)

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

Registrazione ad Amazon Web Services

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

Per iscriverti a un Account AWS

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

Nel corso della procedura di registrazione riceverai una telefonata o un messaggio di testo e ti verrà chiesto di inserire un codice di verifica attraverso la tastiera del telefono.

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

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 Console di gestione AWS 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 Console di gestione AWS, 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 relativa alla pagina Imposta le autorizzazioni, 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 (chiave di accesso IDs e chiavi di accesso segrete), segui le indicazioni contenute nella Nota importante sul salvataggio dell'ID della nuova chiave di accesso e della chiave di accesso segreta dell'utente in un luogo sicuro e protetto.
3. Dopo aver creato l'utente, forniscigli l'accesso programmatico come descritto in [Support programmatic user](#) access.

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 una regione d'origine

1. Utilizzando il tuo AWS account, accedi Console di gestione AWS e apri la console Migration Hub all'indirizzo <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 il proprio agente nella propria regione d'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 origine, si registra `arsenal-discovery.eu-central-1.amazonaws.com` con Application Discovery Service.
- Oppure, se necessario, sostituisci la tua regione di origine con tutte le altre regioni tranne `us-west-2`.
- Se `us-west-2` è la tua regione di origine, 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](#)

Dati raccolti da Discovery Agent

AWS Application Discovery Agent (Discovery Agent) è un software che si installa su server locali e VMs. 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	Description
agentAssignedProcess ^{ld (*)}	ID processo dei processi rilevati dall'agente
agentId	ID univoco dell'agente
agentProvidedTime ^{Timbro *}	Data e ora dell'osservazione dell'agente () mm/dd/yyyy hh:mm:ss am/pm
cmdLine [*]	Processo inserito dalla riga di comando

Campo dati	Description
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 a data/request cui deve essere inviato
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
osVersion	Versione del sistema operativo su host

Campo dati	Description
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 data/request proviene
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 I/O operazioni di lettura al secondo
totalDiskSize (GB)	Capacità totale del disco espressa in GB
totalDiskWriteOpsPerSecond	Numero totale di I/O operazioni 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
totalNumCpus	Numero totale di unità di elaborazione centrali

Campo dati	Description
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

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).
- Genera [le chiavi di accesso](#) necessarie per installare Discovery Agent.
- Verificare che l'ambiente del sistema operativo (OS) sia supportato:

Linux

Amazon Linux 2012.03, 2015.03

Amazon Linux 2 (aggiornamento 25/9/2018 e versioni successive)

Ubuntu 12.04, 14.04, 16.04, 18.04, 20.04

Red Hat Enterprise Linux 5.11, 6.10, 7.3, 7.7, 8.1

CentOS 5.11, 6.9, 7.3

SUSE 11, 12, 15 SP4 SP5 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 tua regione di residenza 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.

Installazione di Discovery Agent

Questa pagina spiega come installare Discovery Agent su Linux e Microsoft Windows.

Installare 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 [Considerazioni relative alle 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.region.amazonaws.com/aws-discovery-agent.region/linux/latest/aws-discovery-agent.tar.gz
```

- b. Per effettuare il download dalla console Migration Hub, procedi come segue:
 - i. Accedi Console di gestione AWS e apri la console Migration Hub all'indirizzo <https://console.aws.amazon.com/migrationhub/>.
 - ii. Nella pagina di navigazione a sinistra, in Discover, scegli Strumenti.
 - iii. Nella casella AWS Discovery Agent, scegli Scarica agenti, quindi scegli Scarica per Linux. Il download inizia immediatamente.
3. Verificare la firma crittografica del pacchetto di installazione con i seguenti tre comandi:

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

```
curl -o ./discovery.gpg https://s3.region.amazonaws.com/aws-discovery-agent.region/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...
<p>Installa Discovery Agent</p>	<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 tua regione d'origine è `eu-central-1`, dovresti usare `https://arsenal-discovery.eu-central-1.amazonaws.com:443`

Considerazioni relative alle 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 caratterizzate da 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
```

Installare Discovery Agent su Microsoft Windows

Completare la procedura seguente per installare un agente su Microsoft Windows. 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 specificando il percorso della cartella <i>C:\install-location</i> per il parametro <code>INSTALLLOCATION</code>. Ad esempio, <code>INSTALLLOCATION=" C:\install-location "</code>. La gerarchia di cartelle risultante sarà <code>[INSTALLLOCATION path]\Discovery.AWS</code> Per impostazione predefini</p>

A...

Esegui questa operazione...

ta, 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`

 Warning

La disabilitazione degli aggiornamenti automatici impedirà l'installazione delle patch di sicurezza più recenti.

A...	Esegui questa operazione...
(Facoltativo) Installa Discovery Agent e configura un proxy non trasparente	<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 d'origine 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 SHA256 certificato. Per gli aggiornamenti automatici con SHA2 firma elettronica su Windows Server 2008 SP2, assicurati che sugli host sia installato un hotfix per supportare l'autenticazione delle firme. SHA2 L'ultimo [hotfix di supporto di Microsoft aiuta a](#) supportare l'autenticazione su Windows Server 2008 SHA2 . SP2

Note

Gli aggiornamenti rapidi per il SHA256 supporto di 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. Eseguire il seguente comando seguente.

```
AWSDiscoveryAgentUpdater.exe /Q
```

Gestione del processo di Discovery Agent

Questa pagina spiega come gestire Discovery Agent su Linux e Microsoft Windows.

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`, or. Le seguenti schede delineare i comandi per le attività supportate in ciascuno dei rispettivi strumenti.

systemd

Comandi di gestione per Application Discovery Agent

Operazione	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

Operazione	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

Operazione	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>

Gestire il processo di Discovery Agent su Microsoft 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.

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

Disinstallazione di Discovery Agent

Questa pagina spiega come disinstallare Discovery Agent su Linux e Microsoft Windows.

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
```

Disinstallare Discovery Agent su Microsoft Windows

Questa sezione descrive come disinstallare Discovery Agent su Microsoft Windows.

Per disinstallare Discovery Agent su Windows

1. Aprire 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
```

Note

Se il `.exe` file è presente sul server, è possibile disinstallare completamente l'agente dal server utilizzando il comando seguente. Se si utilizza questo comando per la disinstallazione, non è necessario utilizzare le `/norestart` opzioni `/repair` and quando si reinstalla l'agente.

```
.\AWSDiscoveryAgentInstaller.exe /quiet /uninstall
```

Avvio e arresto della 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 seguendo i passaggi indicati o effettuando chiamate API tramite. [Avvio e arresto dei raccoglitori di dati nella](#)

[console AWS Migration Hub](#) AWS CLI Prima di iniziare, assicurati di generare [le chiavi di accesso](#) necessarie per gestire Discovery Agent.

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. Inserisci la tua regione d'origine per il nome predefinito della regione, ad esempio `us-west-2`. (In questo esempio, supponiamo che questa `us-west-2` sia la tua 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>
```

Risoluzione problemi di Discovery Agent

Questa pagina descrive la risoluzione dei problemi relativi a Discovery Agent su Linux e Microsoft Windows.

Risoluzione dei problemi di Discovery Agent su Linux

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](#)

Risoluzione dei problemi di Discovery Agent su Microsoft Windows

In caso di problemi durante l'installazione o l'utilizzo di AWS Application Discovery Agent su Microsoft Windows, consulta la seguente guida sulla registrazione e la configurazione. Supporto AWS 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](#)

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, quantità di RAM), metadati del database, metriche di CPU utilizzo e dati sul traffico di rete tra i server locali. Agentless Collector viene installato 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 fornisce moduli per la raccolta di dati da e verso database e server di analisi. VMware VMs Fornisce inoltre un modulo per la raccolta di dati sul traffico di rete tra i server locali.

Agentless Collector supporta la raccolta di dati per AWS Application Discovery Service (Application Discovery Service) raccogliendo dati di utilizzo e configurazione sui server e database locali, nonché dati sul traffico di rete tra i server locali.

Application Discovery Service è integrato con AWS Migration Hub un servizio 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.

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' AWS account configurato per utilizzare la policy AWS `gestitaAWSApplicationDiscoveryAgentlessCollectorAccess`. 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 [Implementazione di Application Discovery Service 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, ma attualmente testiamo con le versioni 6.7 e 7.0 VMware.

- 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. [Configurare 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 [Creazione di un bucket](#) nella Guida per l'utente di Amazon S3.
- La versione 2 di Agentless Collector richiede ESXi la versione 6.5 o successiva.

Configura il perimetro dei dati per l'accesso alle risorse di proprietà dei servizi AWS

La funzione di aggiornamento automatico di Agentless Collector recupera gli aggiornamenti sotto forma di immagini Docker da un archivio ECR pubblico di proprietà del servizio. AWS Se utilizzi perimetri di dati per controllare l'accesso ad Amazon ECR nel tuo ambiente, potresti dover consentire esplicitamente l'accesso a quanto segue per utilizzare la funzionalità di aggiornamento automatico:

- Risorse ARNs che richiedono l'accesso: `arn:aws:ecr-public::44637222237:repository/6e5498e4-8c31-4f57-9991-13b4b992ff7b`
- Autorizzazioni richieste: `ecr-public:DescribeImages`

Configurare 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. AWS I domini che richiedono l'accesso in uscita dipendono dal fatto che la regione di origine di Migration Hub sia la regione 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`— Il raccoglitore utilizza questo dominio per verificare che sia configurato con le credenziali utente IAM richieste. Il raccoglitore 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 raccoglitore utilizza questo dominio per determinare a quale regione di origine il raccoglitore invia 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.
- `sts.amazonaws.com`— Il raccoglitore utilizza questo dominio per capire con quale account è stato configurato.

I seguenti domini richiedono l'accesso in uscita se la regione di residenza AWS dell'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.
- `sts.amazonaws.com`— Il raccoglitore utilizza questo dominio per capire con quale account è stato configurato.

Durante la configurazione di Agentless Collector, potresti ricevere errori del tipo Configurazione non riuscita: controlla le tue credenziali e riprova oppure 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 riesce a raggiungerlo durante la configurazione AWS](#)

Implementazione di Application Discovery Service Agentless Collector

Per distribuire Application Discovery Service Agentless Collector, devi prima creare un utente IAM e scaricare il raccoglitore. Questa pagina illustra i passaggi da eseguire per implementare un collector.

Crea un utente IAM per Agentless Collector

Per utilizzare Agentless Collector, nell' AWS account 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](#) Allegghi 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.

JSON

```
{
  "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.

JSON

```
{
  "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 Console di gestione AWS, 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 (chiave di accesso IDs e chiavi di accesso segrete), segui le indicazioni contenute nella Nota importante sul salvataggio dell'ID della nuova chiave di accesso e della chiave di accesso segreta dell'utente in un luogo sicuro e protetto. Avrai bisogno di queste chiavi di accesso [Configurazione di 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](#).

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 locale. VMware 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. Accedere a vCenter come VMware amministratore e passare alla directory in cui si desidera 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 utilizzato nell'ambiente di sistema, scaricate [MD5](#) o scaricate il file contenente [SHA256](#) il valore del checksum. Utilizzate il valore scaricato per verificare il `ApplicationDiscoveryServiceAgentlessCollector` file scaricato nel passaggio precedente.
4. A seconda della variante di Linux in uso, esegui il MD5 comando o SHA256 il comando appropriato per la versione per verificare che la firma crittografica del `ApplicationDiscoveryServiceAgentlessCollector.ova` file corrisponda al valore del rispettivo SHA256 file MD5/scaricato.

```
$ md5sum ApplicationDiscoveryServiceAgentlessCollector.ova
```

```
$ sha256sum ApplicationDiscoveryServiceAgentlessCollector.ova
```

Implementa Agentless Collector

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

Specifiche della macchina virtuale Agentless Collector

Agentless Collector version 2

- Sistema operativo — Amazon Linux 2023
- RAM: 16 GB
- CPU: 4 core
- VMware requisiti: vedi i [requisiti VMware dell'host per l'esecuzione su AL2023 VMware](#)

Agentless Collector version 1

- Sistema operativo: Amazon Linux 2
- RAM: 16 GB
- CPU: 4 core

La procedura seguente illustra la distribuzione del file OVA Agentless Collector nel proprio ambiente. VMware

Per distribuire Agentless Collector

1. Accedere a vCenter come amministratore. VMware
2. Utilizza uno dei seguenti modi 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. Assicurati che le impostazioni del proxy nella dashboard di gestione del server siano configurate correttamente.
 - Usa la riga di comando: per installare il file Collector OVA dalla riga di comando, scarica e usa 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 **replaceable** valori dell'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.
 - Queste username/password sono le tue credenziali vCenter.
 - Il vcenterurl è l'URL del tuo vCenter.
 - Il percorso vi è il percorso verso il vostro 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.

Accesso 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. [Implementa 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, lo farai. [Configurazione di Agentless Collector](#) Altrimenti, vedrete dopo. [La dashboard di Agentless Collector](#)

Configurazione di 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 Collector name, inserisci un nome per il raccogliitore 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'AWS account che l'utente IAM deve specificare come account di destinazione per ricevere i dati scoperti dal raccogliitore. Per informazioni sui requisiti per l'utente IAM, consulta. [Implementazione di Application Discovery Service Agentless Collector](#)
 - a. Per la AWS chiave di accesso, inserisci la chiave di accesso dell'utente IAM dell'AWS account che stai specificando come account di destinazione.
 - b. Per la AWS chiave segreta, inserisci la chiave segreta dell'AWS account utente IAM che stai specificando come account di destinazione.
 - c. (Facoltativo) Se la tua rete richiede l'uso di un proxy per accedere AWS, 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, imposta 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 Application Discovery Service 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

Agentless Collector version 2

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 CIDR: per ottenere la maschera di rete CIDR, controlla l'impostazione dell'indirizzo IP dell'host VMware vCenter che ospita la macchina virtuale del collettore. Ad esempio, /24.
 - Gateway predefinito: per ottenere il gateway predefinito, controllare l'impostazione dell'indirizzo IP dell'host VMware vCenter che ospita la macchina virtuale del collettore. Ad esempio, 192.168.1.1.
 - DNS primario: per ottenere il DNS primario, controlla 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 ip link set ens192 down
```

4. Aggiornare la configurazione dell'interfaccia utilizzando i seguenti passaggi.

- a. Aprire 10- cloud-init-ens 192.network nell'editor vi utilizzando il seguente comando.

```
sudo vi /etc/systemd/network/10-cloud-init-ens192.network
```

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

```
[Match]
Name=ens192

[Network]
DHCP=no
Address=static-ip-value/CIDR-netmask
Gateway=gateway-value
DNS=dnserver-value
```

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 dnserver-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 ip link set ens192 up
```

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
```

Agentless Collector version 1

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: per ottenere la maschera di rete, controlla l'impostazione dell'indirizzo IP dell'host VMware vCenter che ospita la macchina virtuale del collettore. Ad esempio, 255.255.255.0.
- Gateway predefinito: per ottenere il gateway predefinito, controllare l'impostazione dell'indirizzo IP dell'host VMware vCenter che ospita la macchina virtuale del collettore. Ad esempio, 192.168.1.1.

- DNS primario: per ottenere il DNS primario, controlla 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 raccogliitore di raggiungere l'URL dell'host vCenter senza il nome di dominio.
2. Apri la console VM del raccogliitore 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 dnserver-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.

Agentless Collector version 2

Per configurare la VM collector per l'utilizzo di DHCP

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

```
sudo ip link set ens192 down
```

2. Aggiornare la configurazione dell'interfaccia utilizzando i seguenti passaggi.
 - a. Aprire il `10-cloud-init-ens192.network` file nell'editor vi utilizzando il seguente comando.

```
sudo vi /etc/systemd/network/10-cloud-init-ens192.network
```

- b. Aggiornate i valori come illustrato nell'esempio seguente.

```
[Match]
Name=ens192

[Network]
```

```
DHCP=yes  
  
[DHCP]  
ClientIdentifier=mac
```

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 ip link set ens192 up
```

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

```
sudo reboot
```

Agentless Collector version 1

Per configurare la VM del collettore per l'utilizzo di DHCP

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

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

2. Aggiornare 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 mostrato 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 raccoglitore e accedi **ec2-user** utilizzando la password, come mostrato nell'**collector** 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
```

Utilizzo del modulo Agentless Collector Network Data Collection

Il modulo Network Data Collection consente di scoprire le dipendenze tra i server del data center locale. Questi dati di rete accelerano la pianificazione della migrazione fornendo visibilità sul modo in cui le applicazioni comunicano tra i server.

Il modulo Network Data Collection si connette ai server identificati VMware dal modulo vCenter e analizza l'IP di origine e il IP/port traffico di destinazione per tali server.

Argomenti

- [Configurazione del modulo Network Data Collection](#)
- [Tentativi di raccolta di dati di rete](#)
- [Stato del server nel modulo Network Data Collection](#)

Configurazione del modulo Network Data Collection

Il modulo Network Data Collection raccoglie i dati di rete per l'inventario dei server provenienti dal modulo VMware vCenter. Pertanto, per utilizzare il modulo Network Data Collection, è necessario prima configurare il modulo VMware vCenter. Per istruzioni, segui le indicazioni riportate nei seguenti argomenti:

1. [the section called “Implementazione di un raccoglitore”](#)
2. [the section called “Accesso alla console Collector”](#)
3. [the section called “Configurazione del raccoglitore”](#)
4. [the section called “Utilizzo del modulo di raccolta dati VMware ”](#)

Per configurare il modulo Network Data Collection

1. Nella dashboard di Agentless Collector, nella sezione Raccolta dati di rete, scegli Visualizza connessioni di rete.
2. Nella pagina Connessioni di rete, scegli Modifica raccoglitore.
3. Nella sezione credenziali, inserisci almeno un set di credenziali. Puoi inserire fino a 10 set di credenziali. La prima volta che il modulo tenta di raccogliere dati per un server, prova tutte le credenziali finché non trova un set di credenziali che funzioni; quindi salva quel set e lo riutilizza nei tentativi successivi. Per informazioni sulla configurazione delle credenziali, vedere. [the section called “Impostazione delle credenziali”](#)
4. Nella sezione Preferenze di raccolta dati, per iniziare automaticamente la raccolta dei dati al riavvio di un server, seleziona Avvia automaticamente la raccolta dati.
5. Se non hai configurato i certificati WinRM, seleziona Disabilita i controlli dei certificati WinRM.
6. Scegli Save (Salva).
7. La raccolta avviene sui server ogni 15 secondi. Per visualizzare i dettagli dei tentativi di raccolta per un determinato server, seleziona la casella di controllo a sinistra del server nella tabella Server.

Impostazione delle credenziali

Il modulo Network Data Collection utilizza WinRM per raccogliere dati dai server Windows. Utilizza SNMPv2 e SNMPv3 raccoglie dati dai server Linux.

Credenziali WinRM:

- Specificare il nome utente e la password di un account Windows con le seguenti caratteristiche:
 - Accesso in lettura al `\root\standardcimv2` namespace
 - Autorizzazioni di lettura per la classe `MSFT_NetTCPConnection`
 - Accesso WMI remoto
- Si consiglia di creare un account di servizio dedicato con autorizzazioni minime richieste.
- Evita di utilizzare account di amministratore di dominio o amministratore locale.
- La porta 5986 (HTTPS) deve essere aperta tra i server di raccolta e di destinazione.
- Evitare di disabilitare il controllo dei certificati WinRM. Per informazioni sulla configurazione dei certificati WinRM, vedere. [the section called "Risoluzione dei problemi di certificazione autofirmata durante la configurazione dei certificati WinRM"](#)

SNMPv2 credenziali:

- Fornisci una stringa di community di sola lettura che può accedere a 1.3.6.1.2.1.6.13.* OID
- SNMPv3 è SNMPv2 preferibile a causa della maggiore sicurezza in SNMPv3
- La porta 161/UDP deve essere aperta tra i server di raccolta e di destinazione
- Usa stringhe di community complesse e non predefinite
- Evita stringhe comuni come «public» o «private»
- Tratta le stringhe della community come password

SNMPv3 credenziali

- Fornisci un'autorizzazione di sola lettura username/password e auth/privacy dettagli per accedere all'OID 1.3.6.1.2.1.6.13.*.
- La porta 161/UDP deve essere aperta tra i server di raccolta e di destinazione
- Abilita sia l'autenticazione che la privacy
- Utilizza protocolli di autenticazione avanzati (preferibilmente SHA) MD5
- Utilizza protocolli di crittografia avanzati (AES preferito rispetto a DES)
- Utilizza password complesse sia per l'autenticazione che per la privacy
- Usa nomi utente univoci (evita nomi comuni)

Le migliori pratiche generali per la gestione delle credenziali

- Archivia le credenziali in modo sicuro
- Ruota regolarmente tutte le credenziali
- Usa gestori di password o casseforti sicuri
- Monitora l'utilizzo delle credenziali
- Segui il principio del privilegio minimo e concedi solo le autorizzazioni minime necessarie

Tentativi di raccolta di dati di rete

Quando viene scoperto un nuovo server, il raccoglitore tenta ogni credenziale configurata per ogni indirizzo IP. Dopo che il raccoglitore ha trovato una credenziale valida, utilizza solo quella credenziale. Dopo due errori consecutivi, il raccoglitore tenta di raccogliere i dati di rete per un server dopo 30 minuti, 2 ore, 8 ore e poi 24 ore. Dopo 6 tentativi falliti, il raccoglitore continua a provare tutte le credenziali configurate una volta al giorno. Per risolvere il problema, modifica le credenziali correnti o aggiungine altre scegliendo Modifica raccoglitore oppure apporta modifiche al server di destinazione monitorato.

Stato del server nel modulo Network Data Collection

La tabella seguente illustra i valori dello stato della raccolta.

Status	Significato
Raccolta o raccolta	L'ultimo tentativo di raccolta delle connessioni di rete è riuscito.
Errore o errore	L'ultimo tentativo di raccolta delle connessioni di rete non è riuscito a causa di un problema di rete o di autorizzazioni. Per ulteriori informazioni, seleziona la casella di controllo a sinistra del server che presenta l'errore.
Saltato	Server per i quali non sono state fornite credenziali valide. Aggiorna o configura credenziali server aggiuntive.

Status	Significato
Nessun dato	La raccolta dei dati per il server non è stata avviata. Per iniziare a raccogliere dati, scegli Avvia raccoglitore.
Pending (In attesa)	La raccolta è stata avviata ma non è stato effettuato alcun tentativo di raccolta. Attendi qualche minuto, quindi aggiorna l'elenco.

Utilizzo del modulo di VMware raccolta dati vCenter Agentless Collector

Questa sezione descrive il modulo di raccolta dati VMware vCenter di Application Discovery Service Agentless Collector (Agentless Collector), utilizzato per raccogliere dati di inventario, profilo e utilizzo del server dall'utente. VMware VMs

Argomenti

- [Configurazione del modulo di raccolta dati Agentless Collector per vCenter VMware](#)
- [Visualizzazione VMware dei dettagli della raccolta dei dati](#)
- [Controllo dell'ambito della raccolta dei dati vCenter](#)
- [Dati raccolti dal modulo di raccolta dati Agentless Collector VMware vCenter](#)

Configurazione del modulo di raccolta dati Agentless Collector per vCenter VMware

Questa sezione descrive come configurare il modulo di raccolta dati Agentless Collector VMware vCenter per raccogliere dati di inventario, profilo e utilizzo del server dal tuo. VMware VMs

Note

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

Per configurare il modulo di VMware raccolta dati vCenter

1. Nella pagina dashboard di Agentless Collector, in Raccolta dati, scegli Configura nella sezione VMware vCenter.
2. Nella pagina Configurazione della raccolta dati di VMware vCenter, effettuare le seguenti operazioni:
 - a. In base alle credenziali vCenter:
 - i. Per vCenter URL/IP, inserire l'indirizzo IP dell'host VMware vCenter Server.
 - ii. Per vCenter Username, immettere il nome di un utente locale o di dominio utilizzato dal raccogliatore 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 iniziare automaticamente la raccolta dei dati subito dopo una corretta configurazione, seleziona Avvia automaticamente la raccolta dati.
 - c. Scegliere Set up (Configura).

Successivamente, vedrai la pagina dei dettagli della raccolta VMware dei dati, descritta nell'argomento successivo.

Visualizzazione VMware dei dettagli della raccolta dei dati

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

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

- L'indirizzo IP del server vCenter.
- Il numero di server nel vCenter.
- Lo stato della raccolta dei dati.
- Quanto tempo è passato dall'ultimo aggiornamento.

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

Se non hai scelto di avviare automaticamente la raccolta dei dati, 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 la raccolta dei 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 visualizzati 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 Migration Hub, consulta [Visualizzazione dei dati raccolti](#).

Di seguito sono riportate le linee guida per la durata consigliata per la 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

Controllo dell'ambito della raccolta dei dati vCenter

L'utente vCenter richiede autorizzazioni di sola lettura su ogni host ESX o VM per effettuare l'inventario utilizzando Application Discovery Service. Utilizzando le impostazioni di autorizzazione, è possibile controllare quali host VMs sono inclusi nella raccolta dei dati. È possibile consentire l'inventario di tutti gli host e dell'attuale vCenter oppure concedere le autorizzazioni su VMs base individuale. case-by-case

Note

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

Nelle procedure seguenti sono descritti gli scenari di configurazione ordinati a partire dal meno granulare al più granulare. Queste procedure si riferiscono a 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 scoprire i dati su tutti gli host ESX e VMs con l'attuale vCenter

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

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

1. Nel client VMware vSphere, selezionare vCenter, quindi scegliere Hosts and Clusters o Templates. VMs
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 su uno specifico host ESX o una macchina virtuale secondaria

1. Nel client VMware vSphere, selezionare vCenter, quindi scegliere Hosts and Clusters o Templates. VMs
2. Scegli Related Objects.
3. Scegliere Host (che mostra un elenco di host ESX noti a vCenter) o Macchine virtuali (che mostra un elenco VMs di 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 Propagate to children, è comunque possibile rimuovere l'autorizzazione di sola lettura dagli host ESX e su base individuale. VMs case-by-case Questa opzione non ha alcun effetto sulle autorizzazioni ereditate che si applicano ad altri host ESX e. VMs

Dati raccolti dal modulo di raccolta dati Agentless Collector VMware vCenter

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

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	Description
applicationConfigurationId*	ID dell'applicazione di migrazione in cui è raggruppata la macchina virtuale.
avgCpuUsagePct	Percentuale media di utilizzo della CPU durante il periodo di polling.

Campo dati	Description
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 I/O operazioni di lettura al secondo nullo.
avgDiskWriteOpsPerSecond ^{**}	Numero medio di I/O operazioni 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 computerizzato 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.
hostId [*]	ID dell'host VM.

Campo dati	Description
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 lettura I/O al secondo.
maxDiskWriteOpsPerSecond ^{**}	Numero massimo di I/O operazioni 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.
memoryReservation [*]	Limite per evitare un sovraccarico di memoria sulla VM.

Campo dati	Description
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.
totalDiskSize	Capacità totale del disco espressa in MB.

Campo dati	Description
totalRAM	Quantità totale di RAM disponibile sulla macchina virtuale in MB.
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 VM.
vmName	Nome della macchina virtuale.

Utilizzo del database e del modulo di raccolta dei dati di analisi

Questa sezione descrive come impostare, configurare e utilizzare un database e un modulo di raccolta dati di 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 puoi raccogliere con questo modulo, consulta [Dati raccolti dal database Agentless Collector e dal modulo di raccolta dati di analisi](#)

Important

Avviso di fine del supporto: il 20 maggio 2026, AWS terminerà il supporto per AWS Database Migration Service Fleet Advisor. Dopo il 20 maggio 2026, non sarà più possibile accedere alla console di Fleet Advisor o alle risorse di AWS DMS AWS DMS Fleet Advisor. Per ulteriori informazioni, consulta [AWS DMS Fine del supporto di Fleet Advisor](#).

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

1. Completa i passaggi preliminari, configura il tuo utente IAM e crea il AWS DMS data collector.

2. Configura l'inoltro dei dati per assicurarti che il 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 sistema operativo manualmente o utilizza [il Utilizzo del modulo di raccolta dati VMware](#).
4. Configura le credenziali di connessione ai server del tuo sistema operativo e poi usale per scoprire i server di 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 database e analisi](#).
6. Visualizza i dati raccolti nella AWS DMS console e usali per generare raccomandazioni mirate per una migrazione verso Cloud AWS. Per ulteriori informazioni, consulta [Raccolta di dati di database e analisi](#).

Argomenti

- [Sistemi operativi, database e server di analisi supportati](#)
- [Creazione del raccogliatore di AWS DMS dati](#)
- [Configurazione dell'inoltro dei dati](#)
- [Aggiungere i server LDAP e OS](#)
- [Alla scoperta dei tuoi server di database](#)
- [Dati raccolti dal database Agentless Collector e dal modulo di raccolta dati di analisi](#)

Sistemi operativi, database e server di analisi supportati

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

Questo modulo di raccolta dati supporta i seguenti server del sistema operativo.

- 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 versioni successive
- Windows XP e versioni successive

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

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

Creazione del raccogliatore di AWS DMS dati

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

Prima di creare un raccogliatore di AWS DMS dati, crea un ruolo IAM da utilizzare per accedere al bucket Amazon S3. AWS DMS Hai creato questo bucket Amazon S3 dopo aver completato i prerequisiti in: [Prerequisiti per Agentless Collector](#)

Per creare un ruolo IAM per il tuo raccogliatore di AWS DMS dati per accedere ad Amazon S3

1. Accedi Console di gestione AWS 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 un'entità attendibile scegli Servizio AWS per Tipo di entità attendibile. Per i casi d'uso per altri AWS servizi, scegli DMS.
4. Seleziona la casella di controllo DMS e scegli Successivo.
5. Nella pagina Aggiungi autorizzazioni, scegli FleetAdvisorS3Policy che hai creato in precedenza. Scegli Next (Successivo).
6. Nella pagina Nomina, verifica e crea immetti **FleetAdvisorS3Role** per Nome ruolo e scegli Crea ruolo.
7. Apri il ruolo che hai creato e scegli la scheda Relazioni di fiducia. Seleziona Modifica policy di attendibilità.

8. Nella pagina Modifica politica di fiducia, incolla il seguente codice JSON nell'editor, sostituendo il codice esistente.

JSON

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

9. Scegli Aggiorna policy.

Ora crea un raccogliatore di dati nella AWS DMS console.

Per creare un raccogliatore di AWS DMS dati

1. Accedi a Console di gestione AWS e apri la AWS DMS console su <https://console.aws.amazon.com/dms/v2/>.
2. Scegli quella Regione AWS che hai impostato come regione di origine di Migration Hub. Per ulteriori informazioni, consulta [Accedi a Migration Hub e scegli una regione d'origine](#).
3. Nel riquadro di navigazione, scegli Raccoglitori di dati in Scopri. Viene visualizzata la pagina Raccoglitori di dati.
4. Scegli Crea raccogliatore di dati. Viene visualizzata la pagina Crea raccogliatore di dati.
5. Per Nome nella sezione Configurazione generale, inserisci il nome del raccogliatore di dati.
6. Nella sezione Connettività scegli Sfoglia S3. Scegli il bucket Amazon S3 che hai creato in precedenza dall'elenco.
7. Per il ruolo IAM, scegli FleetAdvisorS3Role quello che hai creato in precedenza.
8. Scegli Crea raccogliatore di dati.

Configurazione dell'inoltro dei dati

Dopo aver creato AWS le risorse richieste, configura l'inoltro dei dati dal database e dal modulo di raccolta dei dati di analisi al tuo raccoglitore. AWS DMS

Per configurare l'inoltro dei dati

1. Apri la console Agentless Collector. Per ulteriori informazioni, consulta [Accesso 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 che hai configurato in precedenza. Per ulteriori informazioni, consultare [Accedi a Migration Hub e scegli una regione d'origine](#) e [Implementazione di un raccoglitore](#).
5. Per Connected DMS data collector, scegli il raccoglitore di dati che hai creato nella console. AWS DMS
6. Scegli Save (Salva).

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

for Access to DMS e Access to S3.


Aggiungere i 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 distribuite sulla rete IP.

È possibile aggiungere un server LDAP esistente al database e al modulo di raccolta dei dati di analisi per individuare automaticamente i server del sistema operativo presenti nella rete. Se non utilizzi LDAP, puoi aggiungere i server del sistema operativo manualmente.

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

1. Apri la console Agentless Collector. Per ulteriori informazioni, consulta [Accesso alla console Collector](#).
2. Scegli Visualizza database e raccoglitore di analisi, quindi scegli i server LDAP in Discovery nel riquadro di navigazione.
3. Scegli Aggiungi server LDAP. Viene visualizzata la pagina Aggiungi server LDAP.
4. Per Hostname, inserisci il nome host del tuo server LDAP.
5. Per Porta, inserisci il numero di porta utilizzato per le richieste LDAP.
6. Per Nome utente, inserisci il nome utente che usi per connetterti al tuo server LDAP.
7. Per Password, inserisci la password che usi per connetterti al tuo 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 Scopri i server del sistema operativo.

 Important

Per l'individuazione del sistema operativo, il modulo di raccolta dati necessita delle credenziali del server di dominio per eseguire 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, puoi visualizzare l'elenco dei server del sistema operativo rilevati selezionando Visualizza server OS.

In alternativa, puoi aggiungere i server del sistema operativo manualmente o importare l'elenco dei server da un file con valori separati da virgole (CSV). Inoltre, è possibile utilizzare il modulo di raccolta dati VMware vCenter Agentless Collector per scoprire i server del sistema operativo. Per ulteriori informazioni, consulta [Utilizzo del modulo di raccolta dati VMware](#).

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

1. Nella pagina Database and analytics collector, scegli Server OS 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. Per Hostname/IP, inserite il nome host o l'indirizzo IP del server del sistema operativo.
 - c. Per Porta, inserisci il numero di porta utilizzato per le interrogazioni remote.
 - d. Per Tipo di autenticazione, scegli il tipo di autenticazione utilizzato dal server del sistema operativo.
 - e. Per Nome utente, inserisci il nome utente che usi per connetterti al server del sistema operativo.
 - f. Per Password, inserisci la password che usi per connetterti al server del tuo 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 sistema operativo nel file in base al modello. L'esempio seguente mostra come è possibile fornire le credenziali di connessione al server OS 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 Scopri i server di database.

Alla scoperta dei tuoi server di database

Questa sezione illustra i passaggi da eseguire per configurare il sistema operativo e i server di database. Quindi, scoprirai i tuoi server e avrai la possibilità di aggiungere manualmente un database o un server di analisi.

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

Configurazione e configurazione

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. Questa pagina descrive i passaggi da eseguire per assicurarsi che il database sia accessibile dalla porta specificata nelle impostazioni di connessione. Attiverai anche l'autenticazione remota sul tuo server di database e fornirai le autorizzazioni al modulo di raccolta dati.

Configura e configura su Linux

Completa la seguente procedura per configurare la configurazione per scoprire i server di database su Linux.

Per configurare Linux per scoprire i server di database

1. Fornisci l'accesso sudo ai netstat comandi ss and.

Il seguente esempio di codice concede a sudo l'accesso ai comandi and. ss netstat

```
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, sostituitelo *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 dei comandi `and. ss netstat`. Questo percorso potrebbe essere diverso nel tuo ambiente. Per determinare il percorso dei `netstat` comandi `ss and`, esegui `which netstat` i comandi `which ss and`.

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

Configurare la configurazione su Microsoft Windows

Completare la procedura seguente per configurare la configurazione per l'individuazione dei server di database su Microsoft Windows.

Per configurare Microsoft Windows per l'individuazione dei server di database

1. Fornisci le credenziali e le autorizzazioni per eseguire le query di Windows Management Instrumentation (WMI) e WMI Query Language (WQL) e leggere il registro.
2. Aggiungere l'utente Windows specificato nelle credenziali di connessione del server OS ai seguenti gruppi: utenti COM distribuiti, utenti del registro delle prestazioni, utenti di monitoraggio delle prestazioni e lettori del registro eventi. A tale scopo, utilizzare 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, sostituitelo *username* con il nome dell'utente Windows specificato nelle credenziali di connessione al server del sistema operativo.

3. Concedi le autorizzazioni richieste per l'utente Windows che hai 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 il controllo WMI, scegli le autorizzazioni Execute Methods, Enable Account, Remote Enable e Read Security per i namespaceCIMV2,DEFAULT, StandartCimv2 e WMI
 - Per il plug-in WMI, esegui e scegli Leggi **winrm configsddl default** 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
```

Alla scoperta di un server di database

Completa il seguente set di attività per individuare e aggiungere server di database sulla console.

Per iniziare l'individuazione dei server di database

1. Nella pagina Database and analytics collector, scegli Server OS 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 di connettività non riuscito, modifica le credenziali di connessione.
 - a. Seleziona uno o più server quando hanno credenziali identiche, quindi scegli Modifica nel menu Azioni. Viene visualizzata la pagina Modifica server OS.
 - b. In Porta, inserisci 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. Per Nome utente, inserisci il nome utente che usi per connetterti al server del sistema operativo.
 - e. Per Password, inserisci la password che usi per connetterti al server del tuo 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 **Scopri** i server di database.

Il modulo di raccolta dei dati di database e analisi si collega ai server del sistema operativo e rileva i database e i server di analisi supportati. Dopo che il modulo di raccolta dati ha completato l'individuazione, puoi 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. Puoi saltare questo passaggio 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 **Database and analytics**, 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 di database.
 - a. Per **Motore di database**, scegli il motore di database del tuo server. Per ulteriori informazioni, consulta [Sistemi operativi, database e server di analisi supportati](#).
 - b. Per **Hostname/IP**, inserisci il nome host o l'indirizzo IP del database o del server di analisi.
 - c. Per **Port**, inserisci la porta su cui è in esecuzione il server.
 - d. Per **Tipo di autenticazione**, scegli il tipo di autenticazione utilizzato dal database o dal server di analisi.
 - e. Per **Nome utente**, inserisci il nome utente che usi per connetterti al tuo server.
 - f. Per **Password**, inserisci la password che usi per connetterti al tuo 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 **Importa server di database 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 database e i server di analisi nel file in base al modello. L'esempio seguente mostra come è possibile fornire le credenziali di connessione al database o al server di analisi in un file 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,,postgres,,TRUE,
MSSQL,203.0.113.1,1433,Login/Password authentication,USER3-
EXAMPLE,h3yCo8nvbEXAMPLE,,,,,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 Scopri i server di database.

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

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

1. Nella pagina Database and analytics collector, scegli Database servers 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 database e i server di analisi al tuo inventario, puoi iniziare a raccogliere metadati e metriche delle prestazioni. Per ulteriori informazioni, consulta [Raccolta di dati di database e analisi](#).

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

Il modulo di raccolta dati di analisi e database di Application Discovery Service Agentless Collector (Agentless Collector) raccoglie le seguenti metriche dall'ambiente di dati dell'utente. Per informazioni sulla configurazione della raccolta dei dati, vedere. [Utilizzo del database e del modulo di raccolta dei dati di analisi](#)

Quando si utilizza il modulo di raccolta dei dati di database e analisi per raccogliere i metadati e la 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 server del CPUs sistema operativo
- Numero di schemi
- Numero di stored procedure
- Numero di tabelle
- Numero di trigger
- Numero di viste
- Struttura dello schema

Dopo aver avviato l'analisi dello schema nella AWS 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 utilizzi il modulo di raccolta dei dati di database e analisi per raccogliere metadati, capacità del database e utilizzo delle risorse, acquisisce le seguenti metriche.

- Velocità di trasmissione effettiva di I/O sui server di database

- Operazioni di input/output al secondo (IOPS) sui server database
- Numero di dati utilizzati dai server del CPUs 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.

Visualizzazione dei dati raccolti

Important

Avviso di fine del supporto: il 20 maggio 2026, AWS terminerà il supporto per Fleet Advisor. AWS Database Migration Service Dopo il 20 maggio 2026, non sarà più possibile accedere alla console di Fleet Advisor o alle risorse di AWS DMS AWS DMS Fleet Advisor. Per ulteriori informazioni, consulta [AWS DMS Fine del supporto di Fleet Advisor](#).

Puoi visualizzare i dati raccolti dal tuo Application Discovery Service Agentless Collector (Agentless Collector) nella console Migration Hub seguendo la procedura riportata di seguito. [Visualizzazione dei server nella console AWS Migration Hub](#)

È inoltre possibile visualizzare le metriche raccolte per i server di database e analisi nella console procedendo come segue AWS DMS .

Per visualizzare i dati rilevati dal database e dal modulo di raccolta dei dati di analisi nella console AWS DMS

1. Accedi a Console di gestione AWS e apri la AWS DMS console su <https://console.aws.amazon.com/dms/v2/>.
2. Scegli Inventario in Scopri. Viene visualizzata 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.

Accesso a Agentless Collector

Questa sezione descrive come utilizzare l'Application Discovery Service Agentless Collector (Agentless Collector).

Argomenti

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

La dashboard di Agentless Collector

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

Argomenti

- [Stato del raccoglitore](#)
- [Raccolta dei dati](#)

Stato del raccoglitore

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

In caso di problemi di AWS connessione, potrebbe essere necessario modificare le impostazioni di configurazione di Agentless Collector.

Per modificare le impostazioni di configurazione del collettore, scegliete Modifica impostazioni del raccoglitore e seguite le istruzioni descritte in [Modifica delle impostazioni di Agentless Collector](#)

Raccolta dei dati

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

Argomenti

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

VMware Raccolta dati vCenter

Per raccogliere dati di inventario, profilo e utilizzo dei server dal tuo VMware VMs, configura le connessioni ai tuoi server vCenter. Per configurare le connessioni, scegli Configura nella sezione VMware vCenter e segui le istruzioni descritte in [Utilizzo del modulo di VMware raccolta dati vCenter Agentless Collector](#)

Dopo aver configurato la raccolta dei dati vCenter, dal dashboard è possibile eseguire le seguenti operazioni:

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

Note

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

Raccolta di dati di database e analisi

È possibile eseguire il database e il modulo di raccolta dei dati di 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 dai server di database e di analisi. È possibile utilizzare queste informazioni raccolte per calcolare i consigli sugli obiettivi nella console. AWS DMS Se il provisioning del database di origine è eccessivo o insufficiente, anche le raccomandazioni di destinazione verranno fornite 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 i parametri di utilizzo effettivo di CPU, memoria e 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 Database and analytics, 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. Scegliete 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 nei successivi 7 giorni o impostare unintervallo personalizzato compreso tra 1 e 60 giorni.

5. Scegli Esegui raccolta dati. Si apre la pagina di raccolta dati.
6. Scegli la scheda Integrità della raccolta per visualizzare lo stato della raccolta dei dati.

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

Modifica delle impostazioni di Agentless Collector

Hai configurato il raccoglitore quando hai configurato per la prima volta Application Discovery Service Agentless Collector (Agentless Collector) come descritto in [Configurazione di Agentless Collector](#). La procedura seguente descrive come modificare le impostazioni di configurazione di Agentless Collector.

Per modificare le impostazioni di configurazione del collettore

- Scegliete il pulsante Modifica le impostazioni del raccoglitore nella dashboard di Agentless Collector.

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

- a. Per Nome del raccoglitore, inserite un nome per identificare il raccoglitore. Il nome può contenere spazi ma non può contenere caratteri speciali.
- b. In AWS Account di destinazione per i dati di rilevamento, inserisci la chiave di AWS accesso e la chiave segreta dell' AWS account da specificare come account di destinazione per ricevere i dati scoperti dal raccoglitore. Per informazioni sui requisiti per l'utente IAM, consulta [Implementazione di Application Discovery Service Agentless Collector](#).
 - i. Per la AWS chiave di accesso, inserisci la chiave di accesso dell'utente IAM dell' AWS account che stai specificando come account di destinazione.
 - ii. Per la AWS chiave segreta, inserisci la chiave segreta dell' AWS account utente IAM che stai specificando come account di destinazione.
- c. In Password Agentless Collector, modifica la password da utilizzare per autenticare l'accesso ad Agentless Collector.
 - i. Per la password di Agentless Collector, inserisci una password da utilizzare per autenticare l'accesso ad 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 VMware credenziali vCenter

Per raccogliere dati di inventario, profilo e utilizzo dei server dai tuoi VMware VMs, configura le connessioni ai tuoi server vCenter. Per informazioni sulla configurazione delle connessioni VMware vCenter, vedere. [Utilizzo del modulo di VMware raccolta dati vCenter Agentless Collector](#)

Questa sezione descrive 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 VMware credenziali vCenter

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

- Nella pagina Modifica vCenter, effettuare le seguenti operazioni:
 - a. In base alle credenziali vCenter:
 - i. Per vCenter URL/IP, inserire 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. Scegli Save (Salva).

Aggiornamento manuale di Application Discovery Service Agentless Collector

Quando si configura Application Discovery Service Agentless Collector (Agentless Collector), è possibile scegliere di abilitare gli aggiornamenti automatici come descritto in. [Configurazione di 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. Segui i passaggi indicati in [Implementa 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 vCenter. VMware
2. Apri la console VM del raccoglitore e accedi **ec2-user** utilizzando la password, come mostrato nell'**collector** esempio seguente.

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

3. Segui le istruzioni riportate in [Update instance software on your AL2 instance](#) nella Amazon Linux 2 User Guide.

Kernel Live Patching

Agentless Collector version 2

La macchina virtuale Agentless Collector versione 2 utilizza Amazon Linux 2023 come descritto in [Implementa Agentless Collector](#)

Per abilitare e utilizzare Live Patching per Amazon Linux 2023, consulta [Kernel Live Patching on AL2023](#) nella Amazon EC2 User Guide.

Agentless Collector version 1

La macchina virtuale Agentless Collector versione 1 utilizza Amazon Linux 2 come descritto in [Implementa Agentless Collector](#)

Per abilitare e utilizzare Live Patching per Amazon Linux 2, consulta [Kernel Live Patching on AL2](#) nella Amazon EC2 User Guide.

Per eseguire l'aggiornamento dalla versione 1 di Agentless Collector alla versione 2

1. Installa un nuovo Agentless Collector OVA utilizzando l'immagine più recente.
2. Configura le credenziali.
3. Eliminare la vecchia appliance virtuale.

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

- [Riparazione Unable to retrieve manifest or certificate file error](#)
- [Risoluzione dei problemi di certificazione autofirmata durante la configurazione dei certificati WinRM](#)
- [Fixing Agentless Collector non riesce a raggiungerlo durante la configurazione AWS](#)
- [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](#)

Riparazione **Unable to retrieve manifest or certificate file error**

Se ricevi questo errore quando tenti di distribuire l'OVA dall'URL di Amazon S3 nell'interfaccia utente VMware vCenter, assicurati che il tuo server vCenter soddisfi i seguenti requisiti:

- VMware vCenter Server versione 8.0 update 1 o successiva
- VMware vCenter Server 7.0 Update 3q (build ISO 23788036) o versione successiva

Risoluzione dei problemi di certificazione autofirmata durante la configurazione dei certificati WinRM

Se si abilitano i controlli dei certificati WinRM, potrebbe essere necessario importare un'autorità di certificazione autofirmata in Agentless Collector.

Per importare un'autorità di certificazione autofirmata

1. Apri la console web VM di Collector in VMware vCenter e accedi `ec2-user` con la password, `collector` come mostrato nell'esempio seguente.

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

2. Assicurati che tutti i certificati CA autofirmati utilizzati per firmare i certificati WinRM si trovino nella directory. `/etc/pki/ca-trust/source/anchors` Esempio:

```
/etc/pki/ca-trust/source/anchors/https-winrm-ca-1.pem
```

3. Per installare i nuovi certificati, esegui il comando seguente.

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

4. Riavvia Agentless Collector eseguendo il comando seguente

```
sudo shutdown -r now
```

5. (Facoltativo) Per verificare che i certificati siano stati importati correttamente, è possibile eseguire il comando seguente.

```
sudo trust list --filter=ca-anchors | less
```

Fixing Agentless Collector non riesce a raggiungerlo durante la configurazione AWS

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 raccogliatore 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. 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. 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 vCenter. VMware
 - b. Apri la console web VM del raccogliitore e accedi **ec2-user** utilizzando la password, come mostrato nell'**collectoresempio** seguente.

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

- c. Verificate 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 vCenter. VMware

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

```
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 Console di gestione AWS e apri la console Migration Hub all'indirizzo <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. [Configurazione di 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 VMware credenziali 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 vCenter. VMware
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. [Implementa Agentless Collector](#)
3. Scegliete Accedi, quindi immettete la password di Agentless Collector, che è stata impostata al momento della configurazione del raccoglitore. [Configurazione di 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 VMware dati, 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 VMware credenziali 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 DMSCollectorpolitiche Policy e FleetAdvisorS3Policy al tuo utente IAM. Per ulteriori informazioni, consulta [Implementazione di Application Discovery Service 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 *replaceable* i valori con i tuoi valori.

- Per verificare che sia possibile connettersi al server LDAP, installate 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 [Alla scoperta dei 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 vCenter. VMware
2. Apri la console web VM del raccoglitore e accedi **ec2-user** utilizzando la password, come mostrato nell'**collectore**sempio seguente.

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

3. Utilizzate 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.

Importazione di dati in Migration Hub

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.

Questa pagina descrive i passaggi per completare una richiesta di importazione. Innanzitutto, si utilizza una delle due opzioni seguenti per preparare i dati del server locale.

- Utilizza strumenti comuni di terze parti per generare un file contenente i dati del server locale.
- Scarica il nostro modello di importazione con valori separati da virgole (CSV) e compilalo con i dati del tuo server locale.

Dopo aver utilizzato uno dei due metodi descritti in precedenza per creare il file di dati locale, carichi il file su Migration Hub utilizzando la console Migration Hub o uno dei AWS SDKs. AWS CLI Per ulteriori informazioni sulle due opzioni, consulta [the section called “Formati di importazione supportati”](#).

È possibile inviare più richieste di importazione. Ogni richiesta viene elaborata in sequenza. Puoi controllare lo stato delle tue richieste di importazione in qualsiasi momento, tramite la console o l'importazione APIs.

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 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.

Errori di gestione: viene fornito un collegamento per scaricare i file di log degli errori e dei record non riusciti 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 [AWS Application Discovery Service Quote](#).

Formati di importazione supportati

Migration Hub supporta i seguenti formati di importazione.

- [RVTools](#)
- [Modello di importazione Migration Hub](#)

RVTools

Migration Hub supporta l'importazione di esportazioni di VMware RVTools vSphere tramite. Quando salvate i dati da RVTools, scegliete prima l'opzione Esporta tutto in csv o l'opzione Esporta tutto in Excel, quindi ZIP la cartella e importate il file ZIP in Migration Hub. Nello ZIP sono richiesti i seguenti file: vInfo, vNetwork, vCPU, vMemory, vDisk, vPartition, vSource, vTools, vHost, vNIC, vsc_VMK.

Modello di importazione Migration Hub

L'importazione da Migration Hub consente di importare dati da qualsiasi fonte. 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 seguente indica che si tratta di 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.

Il cursore (^) accanto al nome di un file di importazione nella tabella seguente indica che è di sola lettura se viene fornito un ServerID.

Note

Se stai usando uno dei due. VMware MoRefId oppure VMWare. VCenterId, per identificare un record, è necessario disporre di entrambi i campi nello stesso record.


Nome del campo di importazione	Description	Esempi
ExternalId [^]	Un identificatore personalizzato che consente di contrassegnare ciascun record	Inventory Id 1 Server 2

Nome del campo di importazione	Description	Esempi
	come univoco. Ad esempio, ExternalId può essere l'ID di inventario del server nel data center.	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
VMware.MoRefId*^	L'ID di riferimento dell'oggetto gestito. Deve essere fornito con un VMware.VCenterId.	
VMware.VCenterID*^	Identificatore univoco della macchina virtuale. Deve essere fornito con un VMware MoRefId.	
TAZZA.NumberOfProcessors^	Il numero di CPUs.	4
TAZZA.NumberOfCores^	Il numero totale di core fisici.	8

Nome del campo di importazione	Description	Esempi
COPPA. NumberOfLogicalCores^	Il numero totale di thread che possono essere eseguiti contemporaneamente su tutti i thread di un CPUs server. Alcuni CPUs supportano l'esecuzione simultanea di più thread su un singolo core della CPU. In questi casi, questo numero sarà superiore al numero di core (fisico o virtuale).	16
Nome del sistema operativo^	Il nome del sistema operativo.	Linux Windows.Hat
Versione del sistema operativo^	La versione del sistema operativo.	16.04.3 NT 6.2.8
VMware.VMName^	Il nome della macchina virtuale.	Corp1
RAM. TotalSizeInMB^	La RAM totale disponibile sul server in MB.	64 128
ARIETE. UsedSizeInMB.avg^	La quantità media di RAM utilizzata sul server, in MB.	64 128
ARIETE. UsedSizeInMB.max^	La quantità massima di RAM utilizzata disponibile sul server, in MB.	64 128

Nome del campo di importazione	Description	Esempi
CPU. UsagePct.Media^	L'utilizzo medio della CPU quando lo strumento di rilevamento raccoglieva i dati.	45 23.9
COPPA. UsagePct.Massimo^	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
DiskReadsOpsPerSecond.Media^	Il numero medio di operazioni di lettura del disco al secondo.	45 28
DiskWritesOpsPerSecond.Media^	Il numero medio di operazioni di scrittura su disco al secondo.	8 3
DiskReadsOpsPerSecond.Massimo^	Il numero massimo di operazioni di lettura del disco al secondo.	1083 176

Nome del campo di importazione	Description	Esempi
DiskWritesOpsPerSecond.Massimo^	Il numero massimo di operazioni di scrittura su disco al secondo.	535 71
NetworkReadsPerSecondInKB.avg^	Il numero medio di operazioni di lettura sulla rete al secondo, in KB.	45 28
NetworkWritesPerSecondInKB.avg^	Il numero medio di operazioni di scrittura sulla rete al secondo, in KB.	8 3
NetworkReadsPerSecondInKB.max^	Il numero massimo di operazioni di lettura sulla rete al secondo, in KB.	1083 176
NetworkWritesPerSecondInKB.max^	Il numero massimo di operazioni di scrittura sulla rete al secondo, in KB.	535 71
Applicazioni	Un elenco separato da virgole di applicazioni che includono questo server, tra virgolette. Questo valore può includere applicazioni esistenti, and/or nuove applicazioni create al momento dell'importazione.	Application1 "Application2, Application3"
ApplicationWave	L'ondata di migrazione per questo server.	

Nome del campo di importazione	Description	Esempi
Tag^	Un elenco separato da virgole di tag formattati come nome:valore. <div 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"
ServerId	L'identificatore del server visualizzato nell'elenco dei server Migration Hub.	d-server-01kk9i6yw waxmp

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 di corrispondenza per i server e le applicazioni rilevati](#).

Note

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

Configurazione delle autorizzazioni di importazione

Prima di poter importare i dati, assicurati che il tuo utente IAM disponga delle autorizzazioni Amazon S3 necessarie per caricare (`s3:PutObject`) il file di importazione su Amazon S3 e leggere l'oggetto (`s3:GetObject`). Inoltre, devi stabilire l'accesso programmatico (per il AWS CLI) o l'accesso alla console, creando una policy IAM e collegandola all'utente IAM che esegue le importazioni nel tuo account. AWS

Console Permissions

Utilizza la seguente procedura per modificare la politica di autorizzazione per l'utente IAM che effettuerà le richieste di importazione nel tuo AWS account utilizzando la console.

Per modificare le policy gestite collegate a un utente

1. Accedi Console di gestione AWS e apri la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel pannello di navigazione, seleziona 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.

JSON

```
{
  "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. Scegliere Esamina policy.
 - c. Assegna alla policy un nuovo Nome e una descrizione facoltativa prima di esaminare il riepilogo della policy.
 - d. Scegli Crea policy.
6. Torna alla pagina Concedi le autorizzazioni della console IAM per l'utente che effettuerà le richieste di importazione nel tuo AWS account.
 7. Aggiorna la tabella di policy e cerca il nome della policy appena creata.
 8. Scegli Prossimo: Rivedi.
 9. Scegli Add Permissions (Aggiungi autorizzazioni).

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

AWS CLI Permissions

Utilizza la seguente procedura per creare le politiche gestite necessarie a fornire a un utente IAM le autorizzazioni per effettuare richieste di importazione di dati utilizzando. AWS CLI

Per creare e allegare le politiche gestite

1. Utilizza il `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.

JSON

```
{
  "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 [create-policy](#) nel Command Reference.AWS CLI

2. Utilizza il `aws iam create-policy` AWS CLI comando per creare una politica IAM aggiuntiva con le seguenti autorizzazioni.

JSON

```
{
  "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. Utilizza il `aws iam attach-user-policy` AWS CLI comando per allegare le politiche create nei due passaggi precedenti all'utente IAM che eseguirà le richieste di importazione nel tuo AWS account utilizzando il AWS CLI. Per ulteriori informazioni sull'utilizzo di questo comando, consulta [attach-user-policy](#) la sezione AWS CLI Command Reference.

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

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

Caricamento del file di importazione su Amazon S3

Successivamente, devi caricare il file di importazione in formato CSV in Amazon S3 in modo che possa essere importato. Prima di iniziare, dovresti disporre di un bucket Amazon S3 in cui archiviare il file di importazione creato e and/or scelto in precedenza.

Console S3 Upload

Per caricare il file di importazione su Amazon S3

1. Accedi a Console di gestione AWS e apri la console 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. Scegli 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. Scegli 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. Vai alla pagina Importa nella console Migration Hub come descritto in [Importazione dei dati](#). Quindi, incolla l'URL dell'oggetto nel campo URL dell'oggetto Amazon S3.

AWS CLI S3 Upload

Per caricare il file di importazione su Amazon S3

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

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

3. Ciò restituisce i seguenti risultati:

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

4. Copia il percorso completo dell'oggetto Amazon S3 che è stato restituito. Ti servirà quando creerai la tua richiesta di importazione.

Importazione dei dati

Dopo aver scaricato il modello di importazione dalla console di Migration Hub e averlo compilato con i dati del server locale esistente, sei pronto per iniziare a importare i dati in Migration Hub. Le seguenti istruzioni descrivono due modi per eseguire questa operazione, utilizzando la console o effettuando chiamate API tramite AWS CLI

Console Import

Avvia l'importazione dei dati nella pagina Strumenti della console 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. [Puoi anche scaricare il modello di importazione dal nostro bucket Amazon S3 all'indirizzo import_template.csv https://s3.us-west-2.amazonaws.com/templates-7cfcf56-bd96-4b1c-b45b-a5b42f282e46/](https://s3.us-west-2.amazonaws.com/templates-7cfcf56-bd96-4b1c-b45b-a5b42f282e46/)
3. Per aprire la pagina di importazione, scegli Importa nella casella Importa.
4. In Nome di importazione, specificate un nome per l'importazione.
5. Compila il campo URL dell'oggetto Amazon S3. Per eseguire questo passaggio, devi caricare il file di dati di importazione su Amazon S3. Per ulteriori informazioni, consulta [Caricamento del file di importazione su 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 navighi dalla pagina Importazioni (cronologia delle importazioni) selezionando il nome dell'importazione elencato nella colonna Nome, verrai indirizzato alla pagina Server in cui viene applicato un filtro basato sul set di dati dell'importazione selezionata. Quindi, vedrai 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 da AWS CLI, è AWS CLI necessario prima installarlo nel proprio ambiente. Per ulteriori informazioni, vedere [Installazione dell'interfaccia a riga di AWS comando](#) nella Guida AWS Command Line Interface per l'utente.

Note

[Se non hai già compilato un modello di importazione, puoi scaricarlo dal nostro bucket Amazon S3 qui: import_template.csv https://s3.us-west-2.amazonaws.com/templates-7cffcf56-bd96-4b1c-b45b-a5b42f282e46/](#)

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"  
  }  
}
```

Monitoraggio delle richieste di importazione di Migration Hub

Puoi monitorare lo stato delle tue richieste di importazione di Migration Hub utilizzando la console o una delle AWS SDKs. AWS CLI

Console Tracking

Dalla dashboard Imports nella console Migration Hub, troverai i seguenti elementi.

- Nome: il nome della richiesta di importazione.
- ID di importazione: l'ID univoco della richiesta di importazione.
- Ora di importazione: data e ora di creazione della richiesta di importazione.
- Stato dell'importazione: lo stato della richiesta di importazione. Può essere uno dei seguenti valori:
 - Importazione: questo file di dati è attualmente in fase di importazione.
 - Importato: l'intero file di dati è stato importato correttamente.
 - Importato con errori: uno o più record nel 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.
 - Importazione non riuscita: nessuno dei record nel 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 un file di dati specifico che sono stati importati correttamente.
- Record non riusciti: il numero di record in un file di dati specifico che non sono stati importati.

CLI Tracking

È possibile tenere traccia dello stato delle attività di importazione con il `aws discovery describe-import-tasks` AWS CLI comando.

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 ed esplora i dati scoperti

Sia Application Discovery Service Agentless Collector (Agentless Collector) che Discovery Agent (AWS Discovery Agent) forniscono dati sulle prestazioni del sistema basati sull'utilizzo medio e di picco. 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, tra cui dati di serie temporali per informazioni sulle prestazioni del sistema, connessioni di rete in entrata e in uscita e 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 troverai le istruzioni su come visualizzare e utilizzare i dati scoperti da Agentless Collector e Discovery Agent sia dalla console che dal. AWS CLI

Argomenti

- [Visualizza i dati raccolti utilizzando la console Migration Hub](#)
- [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, puoi utilizzare la console per visualizzare i dati raccolti sui tuoi server e VMs I dati vengono visualizzati nella console circa 15 minuti dopo l'inizio della raccolta dei dati. È inoltre possibile visualizzare questi dati in formato CSV esportando i dati raccolti effettuando chiamate API utilizzando. AWS CLI

Per visualizzare i dati raccolti sui server rilevati nella console, procedi nel seguente modo.

[Visualizzazione dei server nella console AWS Migration Hub](#) Per ulteriori informazioni sull'utilizzo della console per visualizzare, ordinare ed etichettare i server scoperti dai tuoi Agentless Collector o Discovery Agent, consulta. [Scoperta dei dati con la AWS Migration Hub console](#)

Il database Agentless Collector e il modulo di raccolta dei dati di analisi caricano i dati raccolti nel bucket Amazon S3. Puoi visualizzare i dati di questo bucket nella console DMS. AWS Per visualizzare i dati raccolti sui database e sui server di analisi scoperti, procedi nel seguente modo.

[Visualizzazione dei dati raccolti](#)

Logica di corrispondenza 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 rilevati 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, vedere [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 si visualizza questo server nella console Migration Hub, si trova 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 corrisponde alle due voci, indipendentemente dal fatto che gli altri campi corrispondano o meno.
- IPAddress
- HostName
- MacAddress

- VMware. MoRefId VMware. vCenterId — Entrambi questi valori devono essere identici ai rispettivi campi di un'altra voce affinché Application Discovery Service esegua una corrispondenza.

Esplorazione dei dati in Amazon Athena

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

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

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

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.

Attivazione dell'esplorazione dei dati in Amazon Athena

L'esplorazione dei dati in Amazon Athena è abilitata attivando Continuous Export 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'esportazione continua, il ruolo collegato al servizio `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport` viene utilizzato automaticamente dal tuo account. Per ulteriori informazioni sul ruolo collegato a questo servizio, consulta [Autorizzazioni di ruolo collegate ai servizi per Application Discovery Service](#).

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

Turn on 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'opzione «Esplorazione dei dati in Amazon Athena» nella pagina Data Collectors della console Migration Hub.

Per attivare 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 dati oppure, se hai già attivato la raccolta dati, fai clic sull'interruttore Esplorazione dei dati in Amazon Athena.
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 ora funzionano 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 dati vengano visualizzati in Amazon Athena.

Enable with the AWS CLI

L'esplorazione dei dati in Amazon Athena è abilitata dall'attivazione esplicita di Continuous Export tramite una chiamata API da. AWS CLI A tale scopo, è AWS CLI necessario prima installarlo nel proprio ambiente.

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

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. 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 ora funzionano 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 dati vengano visualizzati in Amazon Athena.

Esplorazione dei dati direttamente in Amazon Athena

Dopo aver attivato 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.

Le seguenti istruzioni spiegano come esplorare i dati degli agenti direttamente nella console Athena. Se non disponi di dati in Athena o non hai abilitato l'esplorazione dei dati in Amazon Athena, una finestra di dialogo ti chiederà di abilitare l'esplorazione dei dati in Amazon Athena, come spiegato in.

[Attivazione dell'esplorazione dei dati in Amazon Athena](#)

Per esplorare i dati scoperti dagli agenti direttamente in Athena

1. Nella AWS Migration Hub console, scegli Server nel riquadro di navigazione.
2. Per aprire la console Amazon Athena, scegli Esplora 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 query SQL in 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 [Utilizzo di query predefinite in Amazon Athena](#).

Visualizzazione dei dati di Amazon Athena

Per visualizzare i dati, è possibile trasferire una query su un programma di visualizzazione come Amazon Quick o altri strumenti di visualizzazione open source come Cytoscape, yEd o Gephi. 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 con Quick

1. Accedi ad [Amazon Quick](#).
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. Viene visualizzata la finestra di dialogo Nuova origine dati Athena.

4. Immetti un nome nel campo Data source name (Nome origine dati).
5. Seleziona Create data source (Crea origine dati).
6. Selezionate la gents-servers-os tabella A nella finestra di dialogo Scegli la tabella e scegliete Seleziona.
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.

Utilizzo di query predefinite in Amazon 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. Nella AWS Migration Hub console, scegli Server nel riquadro di navigazione.
2. Per aprire la console Amazon Athena, scegli Esplora 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 vista, consulta [CREATE VIEW nella 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 sulle prestazioni del sistema per i server con agenti

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 i 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 vista, consulta [CREATE VIEW nella Guida per l'utente di Amazon Athena](#).

Per creare funzioni helper per il monitoraggio in uscita

1. Apri la console Athena all'indirizzo <https://console.aws.amazon.com/athena/>.
2. Crea la `valid_outbound_ips_helper` vista utilizzando la seguente funzione di supporto che elenca tutti gli indirizzi IP di destinazione in uscita distinti.

```
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 i 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 vista, consulta [CREATE VIEW nella Guida per l'utente di Amazon Athena](#).

Per creare funzioni helper che consentano di importare il monitoraggio

1. Apri 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 numero di porta

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 file CSV del database del registro delle porte IANA da [Service Name and Transport Protocol Port Number Registry](#) su [iana.org](#).
2. Carica il file su 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 [Crea una tabella nella 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");
```

Scoperta dei dati con la AWS Migration Hub 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 raccoglitori di dati, server e applicazioni all'interno di Migration Hub. Quando si utilizza la console Application Discovery Service, si viene reindirizzati alla console Migration Hub. Lavorare con la console Migration Hub non richiede passaggi o configurazioni aggiuntivi da parte dell'utente.

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

Argomenti

- [Visualizzazione dei dati nella dashboard della console AWS Migration Hub](#)
- [Avvio e arresto dei raccoglitori di dati nella console AWS Migration Hub](#)
- [Ordinamento dei raccoglitori di dati nella console AWS Migration Hub](#)
- [Visualizzazione dei server nella console AWS Migration Hub](#)
- [Ordinamento dei server nella console AWS Migration Hub](#)
- [Etichettatura dei server nella console AWS Migration Hub](#)
- [Utilizzo AWS Migration Hub per esportare i dati del server](#)
- [Raggruppamento dei server nella console AWS Migration Hub](#)

Visualizzazione dei dati nella dashboard della console AWS Migration Hub

Per visualizzare la dashboard principale, scegli Dashboard dal riquadro di navigazione della console AWS Migration Hub (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 (Discovery Agent).

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 Dashboard dal pannello di navigazione, che si trova sul lato sinistro della home page della console Migration Hub.

Avvio e arresto dei raccoglitori di dati nella console AWS Migration Hub

Application Discovery Service Agentless Collector (Agentless Collector) e AWS Application Discovery Agent (Discovery Agent) sono gli strumenti di raccolta dati che (Application Discovery AWS Application Discovery Service Service) utilizza per aiutarti a scoprire l'infrastruttura esistente. I passaggi seguenti spiegano come scaricare e distribuire questi strumenti di raccolta dei dati di rilevamento e [Implementa Agentless Collector 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 distribuito, è possibile avviare, interrompere e visualizzare i dati raccolti dalla console AWS Migration Hub (Migration Hub).

Dopo la distribuzione di AWS Application Discovery Agent (Discovery Agent), è possibile avviare o interrompere il processo di raccolta dati nella pagina Data Collectors della console AWS Migration Hub (Migration Hub).

Per avviare o arrestare gli strumenti di raccolta dei dati

1. Utilizzando il tuo AWS account, accedi Console di gestione AWS e apri la console Migration Hub all'indirizzo <https://console.aws.amazon.com/migrationhub/>.
2. Nel pannello di navigazione della console Migration Hub sotto Discover, 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).

Ordinamento dei raccoglitori di dati nella console AWS Migration Hub

Se hai distribuito molti raccoglitori di dati, puoi ordinare l'elenco visualizzato dei raccoglitori distribuiti nella pagina Data Collector della console. Ordina l'elenco applicando i 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).

La tabella seguente mostra i criteri di ricerca che è possibile utilizzare per gli 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)	==	Avviato: i dati vengono raccolti e inviati a Application Discovery Service
	!=	Start scheduled (Avvio pianificato): è stato pianificato l'avvio della raccolta dati. I dati verranno inviati ad Application Discovery Service al ping successivo e lo stato cambierà in Avviato. Interrotto: i dati non vengono raccolti o inviati ad Application Discovery Service.

Criterio di ricerca	Operatore	Valore: definizione
		Stop scheduled (Arresto pianificato): è stato pianificato l'arresto della raccolta dati. I dati smetteranno di essere inviati ad Application Discovery Service al ping successivo e lo stato cambierà in Stopped.

Criterio di ricerca	Operatore	Valore: definizione
Integrità	== !=	<p>Healthy (Integro): la raccolta dei dati non è attiva. Lo strumento funziona correttamente.</p> <p>Unhealthy (Non integro): lo strumento è in uno stato di errore. I dati non vengono raccolti né segnalati.</p> <p>Unknown (Sconosciuto): nessuna connessione stabilita in oltre un'ora.</p> <p>Shutdown (Arresto): l'ultima comunicazione dello strumento è stata "shutting down (arresto in corso)" a causa di un arresto del sistema, del servizio o del 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>Running (In esecuzione): la raccolta dei dati è attiva. Lo strumento funziona correttamente.</p>
IP address (Indirizzo IP)	== !=	<p>Qualsiasi indirizzo IP selezionato dall'elenco precompilato in cui è installato uno strumento di raccolta.</p>

La tabella seguente mostra i criteri di ricerca che è possibile utilizzare per i raccoglitori Agentless, inclusi operatori, valori e una definizione dei valori.

Criterio di ricerca	Operatore	Valore: definizione
ID	==	Qualsiasi ID di raccolta senza agente selezionato dall'elenco precompilato da cui è installato 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.
	!=	
Status	==	Raccolta 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 uno stato di errore e richiede attenzione.
		Unknown (Sconosciuto): nessuna connessione stabilita in oltre un'ora.
		Arresto: lo strumento ha comunicato l'ultima volta che si è «spento» a causa dell'arresto di un sistema, di un servizio o di un demone. Se si è verificato un riavvio

Critero di ricerca	Operatore	Valore: definizione
		o un aggiornamento dello strumento, lo stato cambierà in un altro in corrispondenza del primo ciclo di reporting.
IP address (Indirizzo IP)	== !=	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. Utilizzando il tuo AWS account, accedi Console di gestione AWS e apri la console Migration Hub all'indirizzo <https://console.aws.amazon.com/migrationhub/>.
2. Nel pannello di navigazione della console Migration Hub sotto Discover, scegli Data Collectors.
3. Scegli la scheda Agentless Collector o Agents.
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.

Visualizzazione dei server nella console AWS Migration Hub

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.

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

Per visualizzare i server rilevati

1. Utilizzando il tuo AWS account, accedi Console di gestione AWS e apri la console Migration Hub all'indirizzo <https://console.aws.amazon.com/migrationhub/>.

2. Nel pannello di navigazione della console Migration Hub sotto Discover, scegli Server. 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 [Utilizzo AWS Migration Hub per esportare i dati del server](#).

Ordinamento dei server nella console AWS Migration Hub

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. Utilizzando il tuo AWS account, accedi Console di gestione AWS e apri la console Migration Hub all'indirizzo <https://console.aws.amazon.com/migrationhub/>.
2. Nel pannello di navigazione della console Migration Hub sotto Discover, scegli Server.
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.

Etichettatura dei server nella console AWS Migration Hub

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 ai AWS tag, 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. Utilizzando il tuo AWS account, accedi Console di gestione AWS e apri la console Migration Hub all'indirizzo <https://console.aws.amazon.com/migrationhub/>.
2. Nel pannello di navigazione della console Migration Hub sotto Discover, scegli Server.
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 Aggiungi tag, quindi scegli Aggiungi nuovo tag.
5. Nella finestra di dialogo, digita una chiave nel campo Chiave e, facoltativamente, un valore nel campo Valore.

Aggiungi altri tag selezionando Aggiungi nuovo tag e aggiungendo altre informazioni.

6. Scegli Save (Salva).

Per rimuovere tag da uno o più server

1. Utilizzando il tuo AWS account, accedi Console di gestione AWS e apri la console Migration Hub all'indirizzo <https://console.aws.amazon.com/migrationhub/>.
2. Nel pannello di navigazione della console Migration Hub sotto Discover, 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 che desideri rimuovere.
6. Scegli Conferma.

Utilizzo AWS Migration Hub per esportare i dati del server

Questo argomento spiega come esportare i dati del server utilizzando l' Console di gestione AWS, l'AWS Command Line Interface, o l'API.

Da utilizzare per Console di gestione AWS esportare i dati del server per tutti i server

1. Accedi Console di gestione AWS e apri la console Migration Hub all'indirizzo <https://console.aws.amazon.com/migrationhub/>.
2. Nel riquadro di navigazione a sinistra sotto Discover, scegli Server.
3. Scegli Azioni, quindi scegli Esporta dati di rilevamento.
4. Nella sezione Exports (Esportazioni) nella parte inferiore della schermata, selezionare Export server details (Esporta dettagli server). Questa azione genera un file.zip che include i file.csv descritti nella tabella seguente.

Nome file	Description
{account_id} _Application.csv	Dettagli di ogni applicazione, inclusi il numero, il nome e la descrizione del server.
{account_id} _ApplicationResourceAssociation.csv	La relazione tra server e applicazioni.
{account_id} _ImportTemplate	Il riepilogo dell'applicazione e dei tag di ogni server. Questo file può essere modificato e reimportato per aggiornare l'applicazione associata al server.
{account_id} _NetworkInterface.csv	Dettagli di ogni interfaccia di rete, inclusi il server, l'indirizzo e lo switch associati.
{account_id} _Server.csv	Dettagli di ogni server, inclusi sistema operativo, nome host e hypervisor.
{account_id} _SystemPerformance.csv	Dettagli di ciascun server, tra cui la configurazione e le prestazioni di CPU, memoria e storage.

Nome file	Description
{account_id} _Tags.csv	Dettagli di ogni tag associato a un server.
{account_id} _ Info.csv VMware	Dettagli di ogni VMware configurazione, inclusi moreF, VMName e vCenter.

Da utilizzare per Console di gestione AWS esportare i dati dell'agente per un server specifico

1. Accedi Console di gestione AWS e apri la console Migration Hub all'indirizzo <https://console.aws.amazon.com/migrationhub/>.
2. Nel riquadro di navigazione a sinistra sotto Discover, scegli Server.
3. Posiziona il cursore nel campo di ricerca sotto Server. Viene visualizzato un elenco a discesa. In tale elenco, in Proprietà, scegli Sorgente, quindi scegli l'operatore = e quindi scegli Sorgente = Agente.
4. Nei risultati della ricerca, scegli il nome del server per il quale desideri esportare i dati. Questa azione porta alla pagina dei dettagli di quel server.
5. Inserisci un'ora di inizio e un'ora di fine, quindi scegli Esporta. Il file.zip esportato include i file.csv descritti nella tabella seguente.

{account_id} _ .csv destinationProcess Connection	Dettagli delle connessioni in entrata al server.
{account_id} _networkInterface.csv	Dettagli di ciascuna interfaccia di rete, inclusi indirizzo, maschera e nome
{account_id} _osInfo.csv	Dettagli del sistema operativo, inclusi il tipo di CPU, l'hypervisor e il nome del sistema operativo.
{account_id} _process.csv	Dettagli dei processi in esecuzione sul server.

{account_id} _ .csv sourceProcessConne ction	Dettagli della connessione in uscita proveniente dal server.
{account_id} _systemPerformance.csv	Dettagli sulla configurazione e sulle prestazio ni di CPU, memoria e storage per il server.

Per utilizzare l'API AWS Command Line Interface o l'API per esportare i dati del server

1. Esegui [start-export-task](#). L'operazione API corrispondente è [StartExportTask](#)
2. Esegui [describe-export-tasks](#). L'operazione API corrispondente è [DescribeExportTasks](#).

Raggruppamento dei server nella console AWS Migration Hub

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. Utilizzando il tuo AWS account, accedi Console di gestione AWS e apri la console Migration Hub all'indirizzo <https://console.aws.amazon.com/migrationhub/>.
2. Nel pannello di navigazione della console Migration Hub sotto Discover, scegli Server.
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. Opzionale: per ciascun server selezionato, selezionare Add tag (Aggiungi tag), digitare un valore per il campo Key (Chiave), quindi, facoltativamente, digitare un valore per il campo Value (Valore).

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. Scegli Save (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 [the section called "Consistenza finale"](#).

Utilizzo dell'`DescribeConfigurations`azione

L'`DescribeConfigurations`azione recupera gli attributi per un elenco di configurazioni IDs. Tutti i dati forniti IDs devono riguardare lo stesso tipo di risorsa (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 si trovano in una key/value relazione 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"> • Double 	Nessuno
<code>server.performance.avgFreeRAMInKB</code>	<ul style="list-style-type: none"> • GE • LE • GT • LT 	<ul style="list-style-type: none"> • Double 	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 [StartExportTaskDescribeConfigurations](#), e [ListConfigurations](#).

- [AssociateConfigurationItemsToApplication](#)
- [CreateTags](#)
- [DeleteApplications](#)
- [DeleteTags](#)
- [DescribeBatchDeleteConfigurationTask](#)
- [DescribeImportTasks](#)
- [DisassociateConfigurationItemsFromApplication](#)
- [UpdateApplication](#)

Suggerimenti per gestire l'eventuale coerenza:

- Quando richiamate le operazioni di lettura o [ListConfigurations](#) (o i AWS CLI comandi corrispondenti) [StartExportTaskDescribeConfigurations](#), utilizzate un algoritmo di backoff esponenziale per concedere tempo sufficiente per consentire a qualsiasi operazione di aggiornamento precedente di propagarsi nel sistema. 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.

Accesso AWS Application Discovery Service tramite un endpoint di interfaccia ()AWS PrivateLink

Puoi usarlo AWS PrivateLink per creare una connessione privata tra il tuo VPC e. AWS Application Discovery Service Puoi accedere ad Application Discovery Service come se fosse nel tuo VPC, senza l'uso di un gateway Internet, un dispositivo NAT, una connessione VPN o una connessione. Direct Connect Le istanze nel tuo VPC non necessitano di indirizzi IP pubblici per accedere all'Application Discovery Service.

Stabilisci questa connessione privata creando un endpoint di interfaccia attivato da AWS PrivateLink. In ciascuna sottorete viene creata un'interfaccia di rete endpoint da abilitare per l'endpoint di interfaccia. Si tratta di interfacce di rete gestite dai richiedenti che fungono da punto di ingresso per il traffico destinato all'Application Discovery Service.

Per ulteriori informazioni, consulta la sezione [Accesso a Servizi AWS tramite AWS PrivateLink](#) nella Guida di AWS PrivateLink .

Considerazioni per Application Discovery Service

Prima di configurare un endpoint di interfaccia per Application Discovery Service, consulta [Accedere a un AWS servizio utilizzando un endpoint VPC di interfaccia](#) nella Guida.AWS PrivateLink

Application Discovery Service supporta due interfacce: una per effettuare chiamate a tutte le sue azioni API e una seconda per Agentless Collector e AWS Application Discovery Agent per inviare dati di discovery.

Creazione di un endpoint di interfaccia

È possibile creare un endpoint di interfaccia utilizzando la console Amazon VPC o AWS Command Line Interface (AWS CLI). Per ulteriori informazioni, consulta [Accedere a un AWS servizio utilizzando un endpoint VPC di interfaccia nella Guida](#).AWS PrivateLink

For Application Discovery Service

Crea un endpoint di interfaccia per Application Discovery Service utilizzando il seguente nome di servizio:

```
com.amazonaws.region.discovery
```

Se abiliti il DNS privato per l'endpoint dell'interfaccia, puoi effettuare richieste API ad Application Discovery Service utilizzando il nome DNS regionale predefinito. Ad esempio, `discovery.us-east-1.amazonaws.com`.

For Agentless Collector and AWS Application Discovery Agent

Crea un endpoint di interfaccia utilizzando il seguente nome di servizio:

```
com.amazonaws.region.arsenal-discovery
```

Se abiliti il DNS privato per l'endpoint di interfaccia, puoi effettuare richieste API a Application Discovery Arsenal utilizzando il nome DNS regionale predefinito. Ad esempio, `arsenal-discovery.us-east-1.amazonaws.com`.

Creazione di una policy dell' endpoint per l'endpoint dell'interfaccia

Una policy dell'endpoint è una risorsa IAM che è possibile allegare all'endpoint dell'interfaccia. La policy predefinita per gli endpoint consente l'accesso completo a un AWS servizio tramite l'endpoint dell'interfaccia. Per controllare l'accesso consentito a un AWS servizio dal tuo VPC, collega una policy endpoint personalizzata all'endpoint di interfaccia.

Una policy di endpoint specifica le informazioni riportate di seguito:

- I principali che possono eseguire azioni (Account AWS, utenti IAM e ruoli IAM).
- Le azioni che possono essere eseguite.

Per ulteriori informazioni, consulta la sezione [Controllo dell'accesso ai servizi con policy di endpoint](#) nella Guida di AWS PrivateLink .

Esempio: policy degli endpoint VPC

Di seguito è riportato l'esempio di una policy dell'endpoint personalizzata. Se collegata a un endpoint dell'interfaccia, questa policy concede l'accesso alle operazioni elencate per tutti i principali su tutte le risorse.

Example policy for Application Discovery Service

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "discovery:action-1",
        "discovery:action-2",
        "discovery:action-3"
      ],
      "Resource": "*"
    }
  ]
}
```

Example policy for the Agentless Collector and AWS Application Discovery Agent

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "arsenal:RegisterOnPremisesAgent"
      ],
      "Resource": "*"
    }
  ]
}
```

Utilizzo dell'endpoint VPC per Agentless Collector e Application Discovery Agent AWS

Agentless Collector e AWS Application Discovery Agent non supportano endpoint configurabili. Utilizza invece la funzionalità DNS privata per l'endpoint `arsenal-discovery` Amazon VPC.

- Configura la tabella di Direct Connect routing per indirizzare gli indirizzi IP AWS privati al VPC. Ad esempio, destination = 10.0.0.0/8 e target = local. Per questa configurazione è necessario almeno indirizzare gli indirizzi IP privati degli endpoint arsenal-discovery Amazon VPC al VPC.
- Utilizza la funzionalità DNS privato degli endpoint arsenal-discovery Amazon VPC perché Agentless Collector non supporta endpoint Arsenal configurabili.
- Configura l'endpoint arsenal-discovery Amazon VPC in una sottorete privata con lo stesso VPC verso cui stai instradando il traffico. Direct Connect
- Configura l'endpoint arsenal-discovery Amazon VPC con un gruppo di sicurezza che abiliti il traffico in entrata dall'interno del VPC (ad esempio, 10.0.0.0/8).
- Configura un resolver in ingresso Amazon Route 53 per instradare la risoluzione DNS per il nome DNS privato dell'endpoint Amazon arsenal-discovery VPC, che verrà risolto nell'IP privato dell'endpoint VPC. In caso contrario, il raccoglitore eseguirà la risoluzione DNS utilizzando il resolver locale e utilizzerà l'endpoint pubblico Arsenal e il traffico non passerà attraverso il VPC.
- Se hai disabilitato tutto il traffico pubblico, la funzionalità di aggiornamento automatico non funzionerà. Questo perché Agentless Collector recupera gli aggiornamenti inviando richieste all'endpoint Amazon ECR. Per far funzionare la funzionalità di aggiornamento automatico senza inviare richieste su Internet pubblico, configura un endpoint VPC per il servizio Amazon ECR e abilita la funzionalità DNS privato per questo endpoint.

Sicurezza in AWS Application Discovery Service

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

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

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi nel AWS cloud. AWS ti fornisce anche servizi che puoi utilizzare in modo sicuro. L'efficacia della nostra sicurezza è regolarmente testata e verificata da revisori di terze parti come parte dei [programmi di conformitàAWS](#).
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. 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 delle chiamate API di Application Discovery Service con AWS CloudTrail](#)

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 politiche basate sull'identità](#)
- [Utilizzo di ruoli collegati ai servizi per Application Discovery 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 in base al tuo ruolo:

- Utente del servizio: richiedi le autorizzazioni all'amministratore se non riesci ad accedere alle funzionalità (consulta [Risoluzione dei problemi relativi a AWS Application Discovery Service identità e accesso](#))
- Amministratore del servizio: determina l'accesso degli utenti e invia le richieste di autorizzazione (consulta [Come AWS Application Discovery Service funziona con IAM](#))
- Amministratore IAM: scrivi policy per gestire l'accesso (consulta [AWS Application Discovery Service esempi di politiche basate sull'identità](#))

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi autenticarti come utente IAM o assumendo un ruolo IAM. Utente root dell'account AWS

Puoi accedere come identità federata utilizzando credenziali provenienti da una fonte di identità come AWS IAM Identity Center (IAM Identity Center), autenticazione Single Sign-On o credenziali. Google/Facebook Per ulteriori informazioni sull'accesso, consulta [Come accedere all' Account AWS](#) nella Guida per l'utente di Accedi ad AWS .

Per l'accesso programmatico, AWS fornisce un SDK e una CLI per firmare crittograficamente le richieste. Per ulteriori informazioni, consulta [AWS Signature Version 4 per le richieste API](#) nella Guida per l'utente di IAM.

Account AWS utente root

Quando si crea un Account AWS, si inizia con un'identità di accesso denominata utente Account AWS root che ha accesso completo a tutte Servizi AWS le risorse. Consigliamo vivamente di non utilizzare l'utente root per le attività quotidiane. Per le attività che richiedono le credenziali come utente root, consulta [Attività che richiedono le credenziali dell'utente root](#) nella Guida per l'utente di IAM.

Utenti e gruppi IAM

Un [utente IAM](#) è una identità che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ti consigliamo di utilizzare credenziali temporanee invece di utenti IAM con credenziali a lungo termine. Per ulteriori informazioni, consulta [Richiedere agli utenti umani di utilizzare la federazione con un provider di identità per accedere AWS utilizzando credenziali temporanee nella Guida](#) per l'utente IAM.

Un [gruppo IAM](#) specifica una raccolta di utenti IAM e semplifica la gestione delle autorizzazioni per gestire gruppi di utenti di grandi dimensioni. Per ulteriori informazioni, consulta [Casi d'uso per utenti IAM](#) nella Guida per l'utente di IAM.

Ruoli IAM

Un [ruolo IAM](#) è un'identità con autorizzazioni specifiche che fornisce credenziali temporanee. Puoi assumere un ruolo [passando da un ruolo utente a un ruolo IAM \(console\)](#) o chiamando un'operazione AWS CLI o AWS API. Per ulteriori informazioni, consulta [Metodi per assumere un ruolo](#) nella Guida per l'utente di IAM.

I ruoli IAM sono utili per l'accesso degli utenti federati, le autorizzazioni utente IAM temporanee, l'accesso multi-account, l'accesso multi-servizio e le applicazioni in esecuzione su Amazon EC2. Per maggiori informazioni, consultare [Accesso a risorse multi-account in IAM](#) nella Guida per l'utente IAM.

Gestione dell'accesso tramite policy

Puoi controllare l'accesso AWS creando policy e associandole a AWS identità o risorse. Una policy definisce le autorizzazioni quando è associata a un'identità o a una risorsa. AWS valuta queste politiche quando un preside effettua una richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per maggiori informazioni sui documenti delle policy JSON, consulta [Panoramica delle policy JSON](#) nella Guida per l'utente IAM.

Utilizzando le policy, gli amministratori specificano chi ha accesso a cosa definendo quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Un amministratore IAM crea le policy IAM e le aggiunge ai ruoli, che gli utenti possono quindi assumere. Le policy IAM definiscono le autorizzazioni indipendentemente dal metodo utilizzato per eseguirle.

Policy basate sull'identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile collegare a un'identità (utente, gruppo o ruolo). Tali policy controllano le operazioni autorizzate per l'identità, nonché le risorse e le condizioni in cui possono essere eseguite. Per informazioni su come creare una policy basata su identità, consultare [Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente](#) nella Guida per l'utente IAM.

Le policy basate su identità possono essere policy in linea (con embedding direttamente in una singola identità) o policy gestite (policy autonome collegate a più identità). Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta [Scegliere tra policy gestite e policy in linea](#) nella Guida per l'utente di IAM.

Policy basate sulle risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi includono le policy di trust dei ruoli IAM e le policy dei bucket di Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. In una policy basata sulle risorse è obbligatorio [specificare un'entità principale](#).

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

Elenchi di controllo degli accessi () ACLs

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

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

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi che possono impostare le autorizzazioni massime concesse dai tipi di policy più comuni:

- Limiti delle autorizzazioni: imposta il numero massimo di autorizzazioni che una policy basata su identità ha la possibilità di concedere a un'entità IAM. Per ulteriori informazioni, consulta [Limiti delle autorizzazioni per le entità IAM](#) nella Guida per l'utente di IAM.
- Politiche di controllo del servizio (SCPs): specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa in. AWS Organizations Per ulteriori informazioni, consultare [Policy di controllo dei servizi](#) nella Guida per l'utente di AWS Organizations .
- Politiche di controllo delle risorse (RCPs): imposta le autorizzazioni massime disponibili per le risorse nei tuoi account. Per ulteriori informazioni, consulta [Politiche di controllo delle risorse \(RCPs\)](#) nella Guida per l'AWS Organizations utente.
- Policy di sessione: policy avanzate passate come parametro quando si crea una sessione temporanea per un ruolo o un utente federato. Per maggiori informazioni, consultare [Policy di sessione](#) nella Guida per l'utente IAM.

Più tipi di policy

Quando a una richiesta si applicano più tipi di policy, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire o meno una richiesta quando sono coinvolti più tipi di policy, consulta [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 sull'identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. 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. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Action` di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso in una policy. Includere 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.

Resources

Application Discovery Service non supporta la specificazione di risorse ARNs in una policy. Per separare l'accesso, crea e usa un accesso separato 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 politiche 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 ai servizi

[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 funzionalità 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. La [creazione di policy gestite dai clienti IAM](#) che forniscono al 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 nell'account 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, consultare 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 ad Application Discovery Service e Migration Hub APIs.

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 delle autorizzazioni

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.

JSON

```
{
  "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: AWSApplication DiscoveryAgentAccess

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: AWSAgentless DiscoveryService

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 relativi allo stato del connettore con Application Discovery Service.

Colleghi questa policy a tutti gli utenti le cui credenziali vengono utilizzate dal connettore.

AWS politica gestita: ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

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 politiche 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 Console di gestione AWS 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 si creano o modificano policy basate sull'identità, seguire 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 maggiori informazioni, consulta [Policy gestite da AWS](#) o [Policy gestite da AWS per le funzioni dei processi](#) nella Guida per l'utente di IAM.
- Applicazione delle autorizzazioni con privilegio minimo - Quando si impostano le autorizzazioni con le policy IAM, concedere solo le autorizzazioni richieste per eseguire un'attività. È possibile farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegio minimo. Per maggiori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta [Policy e autorizzazioni in IAM](#) nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso - Per limitare l'accesso ad azioni e risorse è possibile aggiungere una condizione alle 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 CloudFormation. Per maggiori informazioni, consultare la sezione [Elementi delle policy JSON di IAM: condizione](#) nella Guida per l'utente di IAM.

- Utilizzo dello strumento di analisi degli accessi IAM per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali - Lo strumento di analisi degli accessi IAM convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio (JSON) della policy IAM e alle best practice di IAM. Lo strumento di analisi degli accessi IAM offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per maggiori informazioni, consultare [Convalida delle policy per il Sistema di analisi degli accessi IAM](#) nella Guida per l'utente di 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, aggiungere le condizioni MFA alle policy. Per maggiori informazioni, consultare [Protezione dell'accesso API con MFA](#) nella Guida per l'utente di 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 all'Application Discovery Service e Migration Hub APIs.

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

JSON

```
{
  "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

JSON

```
{
  "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`

JSON

```
{
  "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`

JSON

```

{
  "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 `discovery:GetNetworkConnectionGraphazione` alla policy.

È necessario utilizzare `discovery:GetNetworkConnectionGraphazione` 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 `discovery:action-name`. `discovery:*`

L'esempio seguente mostra come utilizzare `discovery:GetNetworkConnectionGraphazione` in una policy IAM.

Example

JSON

```
{
  "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 ai [servizi AWS Identity and Access Management](#) (IAM). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM collegato direttamente ad Application Discovery Service. I ruoli collegati ai servizi sono predefiniti da Application Discovery Service e includono tutte le autorizzazioni richieste dal servizio per chiamare altri AWS servizi per conto dell'utente.

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

È possibile eliminare un ruolo collegato al servizio solo dopo avere eliminato le risorse correlate. Ciò protegge le risorse dell'Application Discovery Service perché non è possibile rimuovere inavvertitamente l'autorizzazione ad accedere alle risorse.

Argomenti

- [Autorizzazioni di ruolo collegate ai servizi per Application Discovery Service](#)

- [Creazione di un ruolo collegato ai servizi per Application Discovery Service](#)
- [Eliminazione di un ruolo collegato al servizio per Application Discovery Service](#)

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

Autorizzazioni di ruolo collegate ai servizi per Application Discovery Service

Application Discovery Service utilizza il ruolo collegato al servizio denominato `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport`: consente l'accesso ai AWS servizi e alle risorse utilizzati o gestiti da. AWS Application Discovery Service

Il ruolo `AWSService RoleForApplicationDiscoveryServiceContinuousExport` collegato al servizio prevede che i seguenti servizi assumano il ruolo:

- `continuousexport.discovery.amazonaws.com`

La politica di autorizzazione dei ruoli consente ad Application Discovery Service di completare le seguenti azioni:

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:

JSON

```
{
  "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 al servizio è necessario 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 ruolo `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport` collegato al servizio viene creato automaticamente quando l'esportazione continua viene attivata implicitamente a) confermando le opzioni nella finestra di dialogo presentata dalla pagina Data Collector dopo aver scelto «Avvia raccolta dati» o facendo clic sul cursore denominato «Esplorazione dei dati in Athena» o b) quando si chiama l'API utilizzando la CLI. `StartContinuousExport AWS`

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 al servizio dalla console Migration Hub

È possibile utilizzare la console Migration Hub per creare il ruolo `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport` collegato al servizio.

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 il cursore **Esplorazione dati in Athena** sulla 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 al servizio da AWS CLI

È possibile utilizzare i comandi di Application Discovery Service da AWS Command Line Interface per creare il ruolo `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport` collegato al servizio.

Questo ruolo collegato al servizio viene creato automaticamente quando si avvia Continuous Export da AWS CLI (AWS CLI deve prima essere installato nell'ambiente).

Per creare il ruolo collegato al servizio (CLI) avviando Continuous Export da AWS CLI

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. 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 anche utilizzare la console IAM per creare un ruolo collegato al servizio con lo use case Discovery Service - Continuous Export. Nella CLI IAM o nell'API IAM, crea un ruolo collegato al servizio 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, è possibile utilizzare lo stesso processo per crearlo nuovamente.

Eliminazione di un ruolo collegato al servizio per Application Discovery Service

Se non è più necessario utilizzare una funzionalità o un servizio che richiede un ruolo collegato al servizio, 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 utilizza il ruolo quando si tenta di eliminare le risorse, l'eliminazione potrebbe non riuscire. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare le risorse di Application Discovery Service utilizzate dal ruolo `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport` collegato al servizio dalla console di Migration Hub

1. Nel riquadro di navigazione, selezionare Data Collectors (Agenti di raccolta dati).
2. Selezionare la scheda Agents (Agenti).
3. Sposta il cursore Esplorazione dati in Athena in posizione Off.

Per eliminare le risorse di Application Discovery Service utilizzate dal ruolo `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport` collegato al servizio dal AWS CLI

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. 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. Immettete il seguente comando per assicurarvi che l'esportazione continua sia interrotta verificando che lo stato di restituzione sia «INATTIVO»:

```
aws discovery describe-continuous-export
```

Eliminazione manuale del ruolo collegato ai servizi

Puoi eliminare il ruolo `AWSService RoleForApplicationDiscoveryServiceContinuousExport` collegato al servizio utilizzando la console IAM, la CLI IAM o l'API IAM. Se non hai più bisogno di utilizzare le funzionalità di Discovery Service - Continuous Export che richiedono questo ruolo collegato al servizio, 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 al servizio](#) 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 policy 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 invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

Il seguente errore di esempio si verifica quando un 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 trasmettere 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 delle chiamate API di Application Discovery Service con AWS CloudTrail

AWS Application Discovery Service è integrato con AWS CloudTrail, un servizio che fornisce una registrazione delle azioni intraprese da un utente, un ruolo o un AWS servizio in Application Discovery Service. È possibile utilizzarlo CloudTrail per registrare, monitorare continuamente e conservare l'attività dell'account per scopi di risoluzione dei problemi e di controllo. CloudTrail fornisce una cronologia degli eventi dell'attività dell' AWS account, comprese le azioni intraprese tramite la console di AWS gestione e AWS SDKs gli strumenti da riga di comando.

CloudTrail acquisisce tutte le chiamate API per Application Discovery Service come eventi. Le chiamate acquisite includono chiamate dalla console di Application Discovery Service e chiamate di codice alle operazioni dell'API Application Discovery Service.

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

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

Informazioni su Application Discovery Service in CloudTrail

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

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

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

Tutte le azioni di Application Discovery Service vengono registrate CloudTrail e documentate nell'[Application Discovery Service API Reference](#). Ad esempio, le chiamate alle `GetDiscoverySummary` azioni `CreateTagsDescribeTags`, e generano voci nei file di CloudTrail registro.

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

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

Per ulteriori informazioni, consulta [Elemento CloudTrail userIdentity](#).

Informazioni sulle voci dei file di registro di Application Discovery Service

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

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'`DescribeTags` azione.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
```

```

    "principalId": "AR0AJBHMC4H6EKEXAMPLE: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"
}

```

AWS Application Discovery Service Formati ARN

Un Amazon Resource Name (ARN) è una stringa che identifica in modo univoco una risorsa. AWS richiede un ARN quando si desidera specificare una risorsa in modo inequivocabile per tutti. AWS Application Discovery Service definisce quanto segue. ARNs

- Agente Discovery: `arn:aws:discovery:region:account:agent/discovery-agent/agentId`
- Collezionista senza agenti: `arn:aws:discovery:region:account:agent/agentless-collector/agentId`
- Collettore Migration Evaluator: `arn:aws:discovery:region:account:agent/migration-evaluator-collector/agentId`
- Connettore Discovery: `arn:aws:discovery:region:account:agent/discovery-connector/agentId`

AWS Application Discovery Service Quote

La console Service Quotas fornisce informazioni sulle AWS Application Discovery Service quote. È possibile utilizzare la console Service Quotas per visualizzare le quote di servizio predefinite o per [richiedere aumenti delle quote per le quote regolabili](#).

Attualmente, l'unica quota che può essere aumentata sono i server importati per account.

Application Discovery Service ha le seguenti quote predefinite:

- 1.000 applicazioni per account.

Se raggiungi questa quota e desideri importare nuove applicazioni, puoi eliminare le applicazioni esistenti con l'azione `DeleteApplications` API. Per ulteriori informazioni, vedere [DeleteApplications](#) Application Discovery Service API Reference.

- Ogni 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-database 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 [AWS Application Discovery Service Quote](#).
- 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 Console di gestione AWS 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 dei dati](#).

Cronologia dei documenti per AWS Application Discovery Service

Ultimo aggiornamento della documentazione della Guida per l'utente: 16 maggio 2023

La tabella seguente descrive le modifiche importanti alla Application Discovery Service User Guide dopo il 18 gennaio 2019. Per ricevere notifiche sugli aggiornamenti della documentazione, è possibile sottoscrivere il feed RSS.

Modifica	Descrizione	Data
Modalità di manutenzione	AWS Application Discovery Service non è più aperto a nuovi clienti. In alternativa, utilizza AWS Transform che offre funzionalità simili. Per ulteriori informazioni, vedere Modifica della disponibilità di AWS Application Discovery Service .	7 novembre 2025
Transizione da Discovery Connector a Agentless Collector	Consigliamo ai clienti che attualmente utilizzano Discovery Connector di passare al nuovo Agentless Collector. A partire dal 17 novembre 2025, AWS Application Discovery Service smetterà di accettare nuovi dati da Discovery Connector s. Per ulteriori informazioni, vedere Discovery Connector .	12 novembre 2024
Rilasciato il modulo Agentless Collector Network Data Collection	Il modulo Network Data Collection consente di scoprire le dipendenze tra i server	8 novembre 2024

	del data center locale. Per ulteriori informazioni, consulta Utilizzo del modulo Agentless Collector Network Data Collection .	
Support per la raccolta senza agenti per la mappatura delle dipendenze	Per ulteriori informazioni, vedere Utilizzo del modulo di raccolta dati VMware vCenter Agentless Collector .	24 ottobre 2024
Rilasciata la versione 2 di Agentless Collector basata su Amazon Linux 2023	Per ulteriori informazioni, consulta Prerequisiti per Agentless Collector.	26 settembre 2024
Prerequisiti aggiornati di Agentless Collector	Per ulteriori informazioni, consulta Prerequisiti per Agentless Collector.	9 settembre 2024
Eventuale coerenza nell'API	Per ulteriori informazioni, consulta Eventuale coerenza nell' AWS Application Discovery Service API .	20 giugno 2024
Aggiornamenti di Agentless Collector	Sono stati aggiunti <code>sts.amazonaws.com</code> agli elenchi di domini che richiedono o l'accesso in uscita. Per ulteriori informazioni, consulta Configurare il firewall per l'accesso in uscita ai domini AWS .	20 giugno 2024
Per separare l'accesso, crea e usa account AWS separati.	Per ulteriori informazioni, consulta Azioni, risorse e chiavi di condizione per AWS Application Discovery Service .	5 aprile 2024

[Presentazione del database Agentless Collector e del modulo di raccolta dei 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 metriche delle prestazioni dal database e dai server di analisi locali. Per ulteriori informazioni, consulta 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 agentless sull'ambiente locale per aiutarti a pianificare in modo efficace la migrazione verso. Cloud AWS Per ulteriori informazioni, vedere [Agentless Collector](#).

16 agosto 2022

[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'identità. Per ulteriori informazioni, vedere [Concessione delle autorizzazioni](#) per l'utilizzo del diagramma reticolare.

24 maggio 2022

[Presentazione della regione d'origine](#)

La home region di Migration Hub offre un unico archivio di informazioni sulla scoperta e sulla pianificazione della migrazione per l'intero portafoglio e un'unica visualizzazione delle migrazioni verso più AWS regioni.

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, incluse 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](#).

18 gennaio 2019

La tabella seguente descrive le versioni della documentazione per l'Application Discovery Service User Guide prima del 18 gennaio 2019:

Modifica	Descrizione	Data
Nuova caratteristica	Documenti aggiornati per supportare l'esplorazione dei dati in Amazon Athena e aggiunto il capitolo 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 Console di gestione AWS stato aggiunto.	19 dicembre 2016
Rilevamento senza agente	In questa release viene descritto come impostare e configurare il rilevamento senza agente.	28 luglio 2016
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	Questa è la prima versione della Application Discovery Service User Guide.	12 maggio 2016

AWS Glossario

Per la AWS terminologia più recente, consultate il [AWS glossario](#) nella sezione Reference. Glossario AWS

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.