



# **Raccolta e reporting dei dati di fatturazione AWS**

OnCommand Insight

NetApp  
October 24, 2024

# Sommario

- Raccolta e reporting dei dati di fatturazione AWS ..... 1
  - Preparazione di AWS per la raccolta di dati Insight ..... 1
  - Configurazione dell'origine dati dei costi di AWS Cloud ..... 2
  - Elaborazione dei dati dei costi di AWS Cloud in Insight ..... 3
  - Reporting sui dati dei costi del cloud in Insight ..... 3

# Raccolta e reporting dei dati di fatturazione AWS

L'origine dati dei costi Amazon AWS Cloud importa i dati di fatturazione generati da Amazon in Insight come dati di integrazione, rendendolo disponibile per il data warehouse per il reporting.

I dati di fatturazione del cloud sono disponibili per Insight in tre parti:

Verifica delle informazioni dell'account AWS.

Configurazione dell'origine dati dei costi AWS Cloud in Insight per la raccolta dei dati.

Invio dei dati al Data Warehouse tramite ETL per l'utilizzo nei report.

## Preparazione di AWS per la raccolta di dati Insight

L'account AWS deve essere configurato correttamente per consentire a Insight di raccogliere dati sui costi del cloud.

### A proposito di questa attività

I seguenti passaggi vengono eseguiti tramite l'account AWS. Per ulteriori informazioni, consulta la documentazione di Amazon: "<http://docs.aws.amazon.com>". Se non conosci la configurazione di un account cloud AWS, contatta il tuo cloud provider per ricevere assistenza.



Questi passaggi sono forniti qui a titolo di cortesia e sono ritenuti corretti al momento della pubblicazione. NetApp non garantisce la correttezza di questi passaggi. Per informazioni o assistenza sulla configurazione dell'account AWS, contattare il provider cloud o il titolare dell'account AWS.

Best practice: Insight consiglia di creare un utente IAM primario sullo stesso account proprietario del bucket S3 in cui vengono caricati i report di fatturazione e di utilizzarlo per configurare e raccogliere i dati di fatturazione AWS.

Per configurare l'account AWS in modo da consentire a Insight di raccogliere dati, attenersi alla seguente procedura:

### Fasi

1. Accedere al proprio account AWS come utente IAM (Identity Access Management). Per ottenere una raccolta corretta, accedere all'account IAM principale, invece di un account IAM di gruppo.
2. Vai su **Amazon S3** per creare il tuo bucket. Immettere un nome bucket univoco e verificare la regione corretta.
3. Attiva Amazon Cost and Usage Report. Vedere <https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/billing-reports-gettingstarted-turnonreports.html> per informazioni.
  - a. Vai alla sezione AWS **Billing and Cost Management Dashboard** e scegli **Report**.
  - b. Fare clic su **Create report** (Crea report) e immettere il nome del report. Per **unità di tempo**, scegliere giornaliera. Selezionare la casella per includere **ID risorsa**, quindi fare clic su **Avanti**.
  - c. Fare clic sul collegamento **Sample Policy** nella pagina Select delivery options. Copiare il testo della

policy di esempio nella casella negli Appunti. Fare clic su **Chiudi**.

- d. Tornare al bucket S3 creato, fare clic sulla scheda **Permissions** e selezionare il pulsante **Bucket Policy**.
  - e. Incollare il testo dalla policy di esempio e sostituirlo <bucketname> con il nome effettivo del bucket in ogni riga che contiene quanto segue: "Resource": "arn:aws:s3:: <bucketname>". **Salvare** la policy.
  - f. Tornare alla schermata Create Report (Crea report), inserire il bucket S3 e fare clic sul pulsante **Verify** (verifica). Fare clic su **Avanti**.
  - g. Verificare le informazioni e fare clic su **Rivedi e completa**.
4. Per consentire a Insight di raccogliere i dati da AWS, è necessario concedere le autorizzazioni. Il seguente collegamento fornisce informazioni dettagliate su come concedere le autorizzazioni a **Elenca tutti i bucket** (fase 4.1) e impostare le autorizzazioni sugli oggetti nella cartella (fase 5.2): <https://docs.aws.amazon.com/AmazonS3/latest/dev/walkthrough1.html>.
  5. Nella console IAM, selezionare **Policy** e fare clic su **Create policy**.
  6. Immettere un nome nel campo **Policy Name** (Nome policy) e fare clic su **Create policy** (Crea policy) in basso.
  7. Nella console di IAM, selezionare l'utente, quindi selezionare **Add Inline Policy** (Aggiungi policy in linea) nella parte inferiore della schermata.
  8. Fare clic su **Scegli un servizio** e selezionare S3.
  9. Selezionare la scheda **JSON**. Copiare il testo di esempio JSON dal punto 5.1.2.g della procedura dettagliata AWS nella casella JSON.
  10. Sostituire i campi *companybucket* e *Development* in JSON con le informazioni S3.
  11. Fare clic su **Review Policy** (esamina policy) per rivedere le impostazioni dei criteri.

## Configurazione dell'origine dati dei costi di AWS Cloud

Configuri l'origine dati dei costi di AWS Cloud come per qualsiasi origine dati Insight.

### Prima di iniziare

Devi avere il tuo account Amazon AWS già configurato e preparato per la raccolta dati Insight e avere a portata di mano le seguenti informazioni.

- Nome report
- Nome bucket S3
- Regione AWS in cui risiede il bucket S3.
- Prefisso del percorso del report

### A proposito di questa attività

Una volta che l'account AWS è pronto e sono state impostate le autorizzazioni appropriate, è possibile configurare OnCommand Insight per la raccolta dei dati dei report di fatturazione.



Sarà necessario aggiungere un'origine dati dei costi AWS Cloud separata per ciascun utente/account fatturabile da cui si desidera recuperare i dati di fatturazione.

## Fasi

1. Accedere a OnCommand Insight come amministratore.
2. Fare clic su **Admin > Data Sources** per aprire la pagina Insight Data Source.
3. Fare clic su **+Aggiungi** per aggiungere una nuova origine dati. Scegliere **Amazon** e selezionare **AWS Cloud Cost**.
4. Nella sezione **Configurazione**, compilare i campi *Nome report*, *Nome bucket S3*, *Regione S3* (deve essere la regione in cui si trova il bucket S3), *prefisso percorso report*, *ID chiave di accesso IAM AWS* e *chiave di accesso segreta IAM AWS*. In caso di dubbi, rivolgersi al proprio provider di servizi cloud o al titolare dell'account AWS.
5. Fare clic sulla casella di controllo per verificare che AWS fatturare le richieste API e i trasferimenti di dati effettuati dall'origine dati Insight.
6. In **Advanced Configuration** (Configurazione avanzata), inserire la connessione HTTP e il timeout socket. L'impostazione predefinita è 300 secondi.
7. Fare clic su **Save** (Salva).

## Elaborazione dei dati dei costi di AWS Cloud in Insight

Insight raccoglie i dati dal report di fatturazione AWS una volta al mese per il mese precedente e riflette il costo del cloud finalizzato per quel mese.

Dopo aver configurato le origini dati dei costi di AWS Cloud, se sono già stati generati report di fatturazione su S3, si otterranno fino a tre mesi di dati passati subito dopo il primo sondaggio dell'origine dati.

Insight raccoglie i dati "final" di AWS una volta al mese. Questa raccolta avviene alcuni giorni dopo la chiusura del mese precedente, consentendo ad AWS di finalizzare i dati effettivi.

I dati di fatturazione AWS vengono inviati al Data Warehouse di Insight per essere utilizzati nel reporting.

Tenere presente che ogni origine dati deve essere configurata per un singolo account/utente fatturabile.

## Reporting sui dati dei costi del cloud in Insight

I dati mensili sui costi del cloud raccolti in Insight vengono inviati al data warehouse ed è disponibile nel datamart dei costi del cloud per l'utilizzo nei report.

### Prima di iniziare

È necessario che le origini dati siano configurate per raccogliere i dati sui costi del cloud da AWS. Ogni utente/account fatturabile deve disporre di un'origine dati separata.

Consentire a Insight di iniziare la raccolta dei dati per almeno 36 ore.

Consentire l'esecuzione di ETL almeno una volta dopo tale periodo, per inviare i dati al data warehouse.

### A proposito di questa attività

Una volta raccolti e inviati i dati al data warehouse, è possibile visualizzarli in uno dei diversi report preconfigurati o creare report personalizzati. Insight memorizza i dati nel proprio datamart Cloud Cost.

Per visualizzare i dati sui costi del cloud in uno dei report preconfigurati:

## Fasi

1. Aprire Insight Reporting con uno dei seguenti metodi:
  - Fare clic sull'icona del portale di reporting  Nell'interfaccia utente Web di Insight Server o nell'interfaccia utente di Data Warehouse.
  - Avviare il reporting direttamente immettendo il seguente URL:  
`https://<dwh_server_name>:9300/p2pd/servlet/dispatch` oppure  
`https://<dwh_server_name>:9300/bi` (7.3.3 and later)
2. Una volta effettuato l'accesso a Reporting, fare clic su **cartelle pubbliche** e selezionare **costo cloud**.
3. È possibile visualizzare i dati di fatturazione di AWS nei report disponibili nella cartella **Cloud Cost** oppure creare un report personalizzato utilizzando il datamart \* Cloud Cost disponibile nella cartella **Packages**.

## Elevare il ruolo

Devi elevare il tuo ruolo ServiceNow a Security\_admin prima di poter integrare con Insight.

### Fasi

1. Accedere all'istanza di ServiceNow con le autorizzazioni di amministratore.
2. Nell'elenco a discesa **System Administrator** (Amministratore di sistema), selezionare **Elevate Roles** (Eleva ruoli) e elevare il proprio ruolo a Security\_admin. Fare clic su OK.

## Installare il set di aggiornamenti

Nell'ambito dell'integrazione tra ServiceNow e OnCommand Insight, è necessario installare un set di aggiornamenti, che carica i dati preconfigurati in ServiceNow per fornire al connettore campi e tabelle specifici per l'estrazione e il caricamento dei dati.

### Fasi

1. Accedere alla tabella dei set di aggiornamenti remoti in ServiceNow cercando "set di aggiornamenti recuperati".
2. Fare clic su **Importa set di aggiornamenti da XML**.
3. Il set di aggiornamenti si trova nel file .zip di Python Connector precedentemente scaricato sul disco locale (nel nostro esempio, il C:\OCI2SNOW) in \update\_sets sotto-cartella. Fare clic su **Choose file** (Scegli file) e selezionare il file .xml in questa cartella. Fare clic su **carica**.
4. Una volta caricato il set di aggiornamenti, aprirlo e fare clic su **Preview Update Set** (Anteprima set di aggiornamenti).

Se vengono rilevati errori, è necessario correggerli prima di poter eseguire il commit del set di aggiornamenti.

5. Se non si verificano errori, fare clic su **Commit Update Set** (Esegui commit Update Set).

Una volta eseguito il commit, il set di aggiornamenti viene visualizzato nella pagina **System Update Sets > Update Sources**.

## Integrazione di ServiceNow - impostazione dell'utente

Per consentire a Insight di connettersi e sincronizzare i dati, è necessario configurare un utente ServiceNow.

### A proposito di questa attività

#### Fasi

1. Creare un account di servizi in ServiceNow. Accedere a ServiceNow e accedere a **sicurezza del sistema > utenti e gruppi > utenti**. Fare clic su **nuovo**.
2. Immettere un nome utente. In questo esempio, useremo "OCI2SNOW" come utente dell'integrazione. Immettere una password per questo utente.



In questa procedura viene utilizzato un account utente dei servizi denominato "OCI2SNOW" nella documentazione. È possibile utilizzare un account di servizi diverso, ma assicurarsi che sia coerente con l'ambiente in uso.

3. Fare clic con il pulsante destro del mouse sulla barra dei menu e fare clic su **Save** (Salva). In questo modo, sarà possibile rimanere su questo utente per aggiungere ruoli.
4. Fare clic su **Edit** (Modifica) e aggiungere i seguenti ruoli a questo utente:
  - risorsa
  - importa\_trasformatore
  - servizio\_rest
5. Fare clic su **Save** (Salva).
6. Questo stesso utente deve essere aggiunto a OnCommand Insight. Accedere a Insight come utente con autorizzazioni di amministratore.
7. Accedere a **Admin > Setup** e fare clic sulla scheda **Users**.
8. Fare clic sul pulsante **azioni** e selezionare **Aggiungi utente**.
9. Per il nome, immettere "OCI2SNOW". Se si utilizza un nome utente diverso, immetterlo qui. Inserire la stessa password utilizzata per l'utente ServiceNow. È possibile lasciare vuoto il campo e-mail.
10. Assegnare a questo utente il ruolo **utente**. Fare clic su **Save** (Salva).

## Installare Python e le librerie

Python può essere installato sul server Insight o su un host o una macchina virtuale standalone.

#### Fasi

1. Sulla macchina virtuale o sull'host, scaricare Python 3.6 o versione successiva.
2. Scegliere l'installazione personalizzata e scegliere le seguenti opzioni. Questi sono necessari per il corretto funzionamento dello script del connettore o sono altamente consigliati.
  - Installare il programma di avvio per tutti gli utenti
  - Aggiungi Python al PERCORSO

- Installare pip (che consente a Python di installare altri pacchetti)
  - Installare tk/tcl e IDLE
  - Installare la suite di test Python
  - Installare py launcher per tutti gli utenti
  - Associare i file a Python
  - Creare collegamenti per le applicazioni installate
  - Aggiungere python alle variabili di ambiente
  - Precompilare la libreria standard
3. Dopo aver installato Python, installa le librerie Python “requests” e “psnow”. Eseguire il seguente comando:
- ```
python -m pip install requests pysnow
```

**NOTA:** questo comando potrebbe non riuscire quando si opera in un ambiente proxy. Per risolvere questo problema, è necessario scaricare manualmente ciascuna delle librerie Python ed eseguire le richieste di installazione una alla volta e nell’ordine corretto.

Il comando installerà diversi file.

4. Verificare che le librerie Python siano installate correttamente. Avviare Python utilizzando uno dei seguenti metodi:
- Aprire un prompt cmd e digitare `python`
  - In Windows, aprire **Start** e scegliere **Python > python-<version>.exe**
5. Al prompt di Python, digitare `modules`

Python ti chiederà di aspettare un attimo mentre raccoglie un elenco di moduli, che verrà visualizzato.

## Installazione del middleware Python

Ora che Python e le librerie necessarie sono installate, è possibile configurare il connettore middleware per comunicare con OnCommand Insight e ServiceNow.

### Fasi

1. Sull’host o sulla macchina virtuale in cui è stato scaricato il software Connector, aprire una finestra cmd come amministratore e passare a. `\OCI2SNOW\` cartella.
2. È necessario inizializzare lo script per generare un file **config.ini** vuoto. Eseguire il seguente comando:
 

```
oci_snow_sync.pyz init
```
3. Aprire **config.ini** file in un editor di testo ed apportare le seguenti modifiche nella sezione [OCI]:
  - Impostare **url** su `<a href="https://&lt;name.domain&gt" class="bare">https://&lt;name.domain&gt</a>` oppure `<a href="https://&lt;ip" class="bare">https://&lt;ip</a> address&gt;` Per l’istanza Insight.
  - Impostare **user** e **password** sull’utente Insight creato, ad esempio OCI2SNOW.
  - Impostare **include\_off\_vm** su **false**
4. Nella sezione [SNOW], apportare le seguenti modifiche:
  - Impostare **Instance** sull’FQDN o sull’indirizzo ip dell’istanza di ServiceNow

- Impostare **User** e **Password** sull'utente dell'account di servizio ServiceNow, ad esempio OCI2SNOW.
  - In **field for the OCI URL** (campo **URL OCI**), impostare il campo **url** su "u\_oci\_url". Questo campo viene creato come parte del set di aggiornamenti OCI del connettore. È possibile modificarlo nell'ambiente del cliente, ma in tal caso è necessario modificarlo qui e in ServiceNow. La Best practice consiste nell'abbandonare questo campo così com'è.
  - Impostare il campo **filter\_status** su "Installed, in Stock". Se si dispone di uno stato diverso, è necessario impostare questo stato qui per ottenere la corrispondenza di tutti i record con i record Insight prima di caricare nuovi record. Nella maggior parte dei casi, questo campo deve rimanere invariato.
  - Impostare **stale\_status** su "ritirata".
5. La sezione [Proxy] è necessaria solo se si utilizza un server proxy. Se è necessario utilizzare questa sezione, verificare le seguenti impostazioni:
- ;https = `http://<host>:<port>`
  - ;http = `http://<host>:<port>`
  - ;Include\_oci = vero
  - ;Include\_snow = vero
6. Modificare la sezione [Log] solo se sono necessarie informazioni di debug più dettagliate.
7. Per verificare il connettore, aprire un prompt dei comandi come amministratore e passare alla cartella OCI2SNOW. Eseguire il seguente comando: `oci_snow_sync.pyz test`

I dettagli sono disponibili nella `logs\` cartella.

## Sincronizzazione del connettore

Una volta configurati correttamente ServiceNow, Insight e il connettore, è possibile sincronizzare il connettore.

### Fasi

1. Aprire un prompt dei comandi e passare alla cartella OCI2SNOW.
2. Eseguire due volte il seguente comando. La prima sincronizzazione aggiorna gli elementi, la seconda aggiorna le relazioni: `oci_snow_sync.pyz sync`
3. Verificare che la tabella Storage Server nell'istanza di ServiceNow sia popolata. Aprire un server di storage e verificare che siano elencate le risorse correlate a tale storage.

## Pianificazione della sincronizzazione giornaliera

È possibile utilizzare il Task Scheduler di Windows per sincronizzare automaticamente il connettore ServiceNow.

### A proposito di questa attività

La sincronizzazione automatica garantisce che i dati Insight vengano regolarmente spostati in ServiceNow. È possibile utilizzare qualsiasi metodo per la pianificazione. La seguente procedura utilizza Task Scheduler di Windows per eseguire la sincronizzazione automatica.

## Fasi

1. Nella schermata di Windows, fare clic su **Start** e digitare **Esegui > Task Scheduler**.
2. Fare clic su **Crea attività di base...**
3. Immettere un nome significativo, ad esempio "OCI2SNOW Connector Sync". Inserire una descrizione dell'attività. Fare clic su **Avanti**.
4. Selezionare per eseguire l'attività **Daily**. Fare clic su **Avanti**.
5. Scegliere un'ora del giorno in cui eseguire l'attività. Fare clic su **Avanti**.
6. Per azione, selezionare **Avvia un programma**. Fare clic su **Avanti**.
7. Nel campo **Program/script**, immettere `C:\OCI2SNOW\oci_snow_sync_pyz`. Nel campo **argomenti**, immettere `sync`. Nel campo **Start in**, immettere `C:\OCI2SNOW`. Fare clic su **NEXT** (Avanti).
8. Esaminare i dettagli del riepilogo e fare clic su **fine**.

La sincronizzazione è ora pianificata per essere eseguita quotidianamente.

## Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

## Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.