

NUMERO DOCUMENTO: **C000CMP01STP01**

REVISIONE: **08.00**

DATA: **20/06/2025**

CAGE CODE: **A0069**

**Digital Security**

**Secure Cloud Management Platform**

**Secure Cloud Management Platform**

## Firme

Autore: <b>Product Owner IPT di Sviluppo</b> R. Cloud Product   Digital Systems & Engineering Technologies   Engineering	..... Carmelo Sciuto
Verifica: <b>PEM IPT di Prodotto</b> R. Digital Systems & Engineering Technologies   Engineering	..... Andrea Giorgio Busà
Verifica: <b>PAM IPT Sviluppo</b> Quality Cyber Security, Intelligence & Digital Solutions	..... Simonetta De Biase
Approvazione: <b>IPT Leader IPT di Sviluppo</b> R. Digital Platform   Digital Systems & Engineering Technologies   Engineering	..... Daniele Leone
Approvazione: <b>Technical Authority</b> Solution Architects   LoB Public Admin., Defence & Inter. Agencies	..... Susanna Fortunato
Autorizzazione: <b>Product Manager IPT Prodotto</b> Product Management Digital Trasformation   Product Management	..... Fabio Russo

## Contatti

Carmelo Sciuto <b>Product Owner IPT di Sviluppo</b> R. Cloud Product   Digital Systems & Engineering Technologies   Engineering	<b>Leonardo S.p.A.</b> Via A. Agosta SNC 95121 Catania
--	---

## Lista delle Revisioni

Rev.	Numero Modifiche	Data	Descrizione	Autore
01.00	-	24/01/2022	Prima emissione	D. Leone
02.00	DCN222372	29/07/2022	Integrazione Rilascio SCMP 2.0.0	D. Leone
03.00	DCN222981	20/12/2022	Integrazione Rilascio SCMP 3.0.0	D. Leone
04.00	DCN230550	30/06/2023	Integrazione Rilascio SCMP 4.0.0	D. Leone
05.00	DCN231199	22/12/2023	Integrazione Rilascio SCMP 5.0.0	D. Leone
06.00	DCN240480	28/07/2024	Integrazione Rilascio SCMP 6.0.0	D. Leone
07.00	DCN240891	20/12/2024	Integrazione Rilascio SCMP 7.0.0	D. Leone

# Documentazione Super Progetto

# 1 Documentazione per Sviluppatori

Questa sezione contiene la documentazione tecnica per gli sviluppatori.

## 1.1 Documentazione API

--8<-- "includes/developers/api.md"

## 1.2 Iniziare

Per iniziare a sviluppare con la nostra piattaforma, segui questi passaggi:

1. **Registrati** per un account sviluppatore
2. **Genera** le tue chiavi API
3. **Installa** i nostri SDK
4. **Costruisci** la tua prima integrazione

## 1.3 SDK e Librerie

Forniamo SDK ufficiali per diversi linguaggi di programmazione:

- **JavaScript/Node.js** - npm install @platform/sdk
- **Python** - pip install platform-sdk
- **Java** - Dipendenza Maven disponibile
- **PHP** - Pacchetto Composer disponibile

## 1.4 Esempi di Codice

### 1.4.1 Esempio di Autenticazione

```
const Platform = require('@platform/sdk');
```

```
const client = new Platform({  
  apiKey: 'your-api-key',  
  environment: 'production'  
});
```

```
// Autentica utente  
const user = await client.auth.login({  
  username: 'user@example.com',  
  password: 'password'  
});
```

## 1.5 Supporto

Per supporto tecnico:

- Consulta la nostra documentazione API
- Visita il nostro forum sviluppatori
- Contatta il supporto a [developers@example.com](mailto:developers@example.com)

## 2 Administration

La funzionalità di Administration è la base di partenza per poter utilizzare la SCMP.

I provider inseriti all'interno di questa funzionalità verranno utilizzati dal sistema per recuperare tutte le informazioni necessarie.

All'interno della funzionalità sarà possibile:

- Configurare i cloud provider che potranno essere utilizzati nel Tenant di riferimento.
- Configurare le folder dei vari provider.
- Configurare i cloud SIEM dei vari provider.
- Configurare i KeyVault dei vari provider.
- Configurare i CommVaults per il Backup e il Disaster & Recovery dei vari provider.
- Configurare i Confidential Computing per i vari provider.

### 2.0.1 provider/sottosistemi

#### 2.0.1.1 Lista dei sottosistemi

Per accedere alla funzionalità di Administration, in alto a sinistra cliccare sul pulsante **Administration**. Dopodiché, cliccare su **Administration**.

---

*Figura 1 – Accesso alla funzionalità di Administration*

A questo punto, l'utente si ritrova all'interno della pagina del tab **Cloud Systems**, dove possiamo visualizzare delle informazioni generali sui sottosistemi, ad esempio il provider di riferimento e la data di creazione del sottosistema e viene inoltre indicato con una spunta rossa se il sistema è di tipo On-Premise.

Possiamo notare che nella lista sono presenti delle "folder", dei contenitori di sottosistemi, cliccando in corrispondenza della "freccia" sulla riga della folder possiamo visualizzare i sottosistemi al suo interno e le loro informazioni.



Leonardo Cyber & Security Solutions

21 Oct 2025

08.00

Secure Cloud Management Platform

Name	Type	Creation Date	On-Premises	State
⌵ CMP Managed Folder	GOOGLE	16/12/2024 10:47:16	<input type="checkbox"/>	●
⌴ CMP Managed Azure Folder	AZURE	16/12/2024 10:48:00	<input type="checkbox"/>	●
MAE Digital Transformation	AZURE	16/12/2024 10:48:01	<input type="checkbox"/>	●
MAE CMP	AZURE	16/12/2024 10:48:02	<input type="checkbox"/>	●
MAE OSP 2030	AZURE	16/12/2024 10:48:02	<input type="checkbox"/>	●
MAE LAB	AZURE	16/12/2024 10:48:03	<input type="checkbox"/>	●
CMP-DEV3 CLUSTER	KUBERNETES	16/12/2024 11:03:34	<input type="checkbox"/>	●
Cluster 02	OPENSIFT	16/12/2024 11:10:56	<input type="checkbox"/>	●
vmware VMWareCMP	VMWARE	16/12/2024 11:11:39	<input checked="" type="checkbox"/>	●
SA CMP	REDHATEDGE	16/12/2024 13:00:37	<input checked="" type="checkbox"/>	●

Figura 2 – Lista dei sottosistemi e delle  
folder

Inoltre, per ogni sottosistema Ãˆ disponibile uno status, rappresentato da un "led" colorato:

- Verde: il funziona correttamente nella SCMP "status: ok".
- Rosso: il sottosistema non Ãˆ piÃ¹ utilizzabile dalla SCMP "status : failed".

La SCMP effettua periodicamente dei test di connessione su tutti i sottosistemi configurati, quando un sottosistema fallisce questo controllo, lo status del sottosistema viene aggiornato e vengono disabilitati tutti i processi di recupero delle informazioni (costi, inventario, monitoraggio, sicurezza).

Questo potrebbe accadere, ad esempio quando il secret o le password utilizzate per connettersi scadono e devono essere rinnovate. Andando a modificare il sottosistema Ãˆ possibile inserire i nuovi parametri di connessione per ristabilirne il corretto funzionamento, che verrÃ confermato dallo status "OK"

#### 2.0.1.1.1 INFORMAZIONI SUI CRON-JOB DEI SOTTOSISTEMI

Ogni tenant effettua, durante la giornata, diverse operazioni di recupero delle informazioni disponibili per tutti i sottosistemi configurati, cosÃ¬ da permettere all'utente di visualizzare tutti i dati necessari utilizzando la sola SCMP.

Per visualizzare l'esito di queste operazioni, cliccare sulla riga del sottosistema e all'interno della modale selezionare il pulsante "Show discovery info"



Oltre alle quantità di operazioni e il loro esito, scorrendo in basso, è possibile visualizzare la lista e i relativi dettagli cliccando la "freccia" in corrispondenza dell'operazione interessata.

---

*Figura 3 – Informazioni sui cron-job*

#### 2.0.1.1.2 VISUALIZZAZIONE, MODIFICA ED ELIMINAZIONE DI UN SOTTOSISTEMA

Per visualizzare i dati di un Cloud Provider, all'interno della lista, cliccare sul kebab menu in corrispondenza del Cloud Provider di interesse e cliccare su "Show".

---

*Figura 4 – Accesso al Cloud Provider in modalità visualizzazione*

In questa pagina è possibile visualizzare la configurazione del Provider

---

*Figura 5 – Sottosistema in modalità visualizzazione*

Se il provider è di tipo "ON-PREMISE" sotto la configurazione sarà visibile una tabella che riporta le capacità utilizzabili sul sistema e la lista delle risorse già presenti nel sottosistema

---

*Figura 6 – Lista macchine On-Premise*

Per tornare alla pagina dei Cloud Provider, in basso a sinistra, cliccare sul pulsante "Close".

Per modificare i dati di un Cloud Provider, all'interno della lista, cliccare sul kebab menu in corrispondenza di un Cloud Provider, e cliccare su "Edit".

---

*Figura 7 – Accesso al Cloud Provider in modalità edit*

Fatto ciò, l'utente si ritroverà all'interno della pagina del Cloud Provider in modalità "edit", modalità che consente di modificare i dati.

Per tornare alla pagina dei Cloud Provider, in basso a sinistra, cliccare sul pulsante "Save". A questo punto, l'utente si ritroverà all'interno della pagina dei Cloud Provider.

---

*Figura 8 – Avvio per l'eliminazione di un Cloud Provider*

Per eliminare un Cloud Provider, all'interno della lista, cliccare sul kebab menu in corrispondenza di un Cloud Provider, e cliccare su "Delete"

---

*Figura 9 – Conferma eliminazione del  
Cloud Provider*

Fatto ciò, apparirà una modale in cui è necessario cliccare sul pulsante "Remove"

A questo punto, il Cloud Provider non sarà più presente all'interno della lista e verrà lanciato il flusso di rimozione asset sul resource-manager.

#### 2.0.1.1.3 MODELLO DI COSTO PER I PROVIDER "ON-PREMISE"

Per gestire i costi dell'utilizzo delle risorse per i provider "On-Premise" viene data la possibilità di definire un modello di costo specifico per sottosistema.

Il modello di costo permette di configurare sia i costi "provider" cioè quelli realmente sostenuti e successivamente di applicare una percentuale di sconto o ricarico da applicare al cliente.

I provider che utilizzano questa funzionalità sono:

- VMware
- VCloud Director
- RedHat Edge
- OpenShift

Per poter modificare il modello cliccare il pulsante "tre punti" in corrispondenza di un sottosistema e selezionare la voce "Cost model".

---

*Figura 10 – Accesso al cost model del  
sottosistema*

Nella pagina del modello troviamo una prima sezione generica dove sarà possibile configurare i campi:

- Currency: la moneta di riferimento da utilizzare per il sottosistema.
- Discount/Surcharge: una percentuale di sconto o ricarico da applicare ai costi del cliente.



Leonardo Cyber & Security Solutions

21 Oct 2025

08.00

Secure Cloud Management Platform

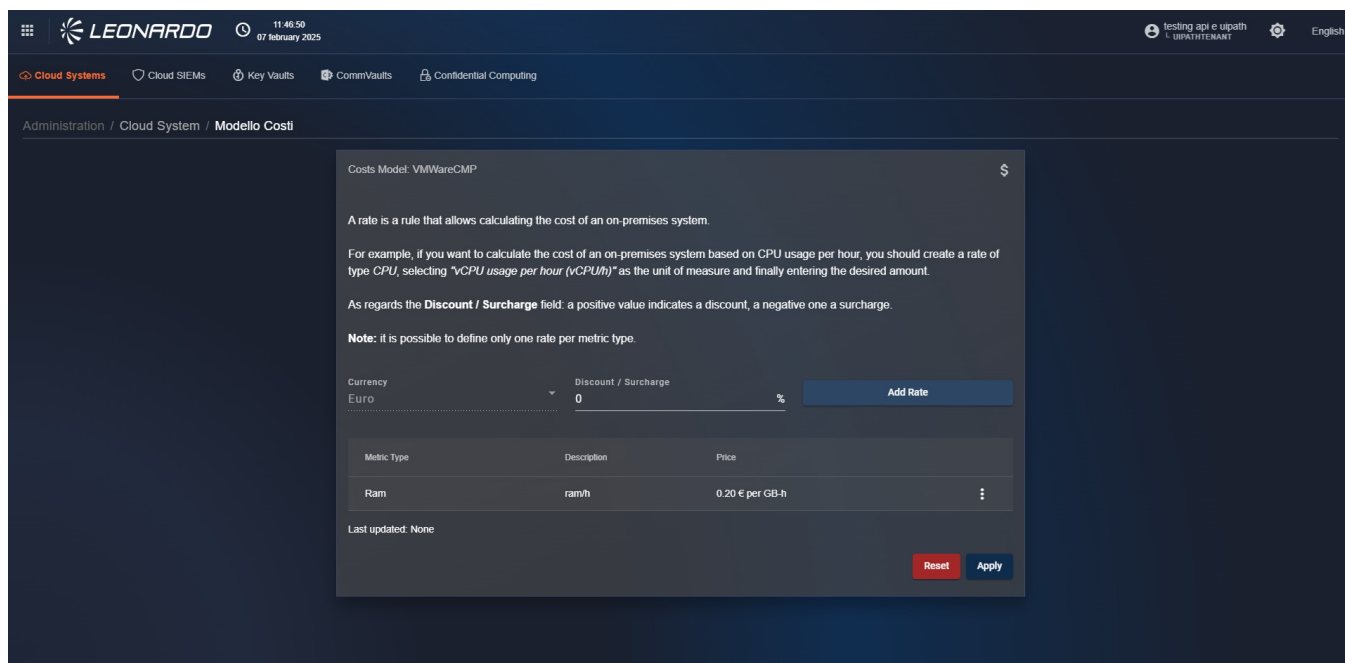


Figura 11 – Modello di costo

Successivamente cliccando il pulsante "Add rate" verrà aperta una modale nella quale, dopo aver scelto una metrica (specifica per il provider) e la relativa unità di misura da utilizzare, verrà inserito il prezzo da applicare a tutti gli elementi del sottosistema, infine cliccare il pulsante "Save" per confermare l'inserimento.

Figura 12 – Selezione della metrica da  
prezzare

Per confermare la modifica al modello dopo aver inserito tutte i costi per ogni tipologia di componente disponibile cliccare il pulsante "Apply" in basso.

Figura 13 – Modello dei costi completo

#### 2.0.1.1.4 AGGIORNAMENTO MANUALE DEI COSTI

Viene data la possibilità all'utente di effettuare un aggiornamento manuale dei costi in caso di necessità, questa operazione asincrona può essere richiesta singolarmente per sottosistema o globalmente su tutto il tenant, che viene propagato automaticamente su tutti i sottosistemi disponibili.

Per richiedere l'aggiornamento di un singolo sottosistema cliccare il pulsante "tre punti" sulla riga del sottosistema e selezionare la voce "Refresh Cost"

*Figura 14 – Aggiornamento manuale  
dei costi*

All'interno della modale possiamo indicare per quanti giorni, a partire dalla data odierna, devono essere riscalcati e riconfermati i costi del sottosistema selezionato. Dopo la conferma possiamo andare nella sezione "Info dei cron-job" per confermare le operazioni.

Inoltre è possibile richiedere l'aggiornamento dei costi per tutto il tenant: cliccando prima sul pulsante "hamburger menu" disponibile in alto a sinistra e selezionando la voce "refresh cost", l'attività sarà distribuita su tutti i sottosistemi disponibili nella pagina

*Figura 15 – Aggiornamento dei costi su  
tutto tenant*

Una volta selezionato un recupero costi è possibile indicare il numero dei giorni da recuperare e selezionando il box "Reset the cost" la SCMP effettuerà prima una pulizia dei dati (del relativo range selezionato) e successivamente effettua il refresh

*Figura 16 – Configurazione del refresh  
costi*

#### 2.0.1.1.5 PROCESSO DI RECUPERO E CALCOLO DEI COSTI

##### 2.0.1.1.5.1 Struttura del recupero costi

Il processo di recupero dei costi viene effettuato dal modulo "Abstraction Layer", questo modulo è composto da:

- Un sotto-modulo di ABS chiamato "layer" per ogni tipologia di provider (ad esempio "CMP-ABS-VMWare-layer")
- ABS Gateway: il sotto-modulo che si occupa di gestire la comunicazione e l'omologazione delle informazioni recuperate dai vari Layer dei diversi provider e le rende disponibili per gli altri moduli del sistema SCMP.

Il processo di recupero dei costi viene effettuato da un cron-job, che viene lanciato una volta per provider, automaticamente durante le ore notturne.

Per i provider di tipo ON-Premise vengono generati automaticamente dalla SCMP dei valori di usage basandosi sulla quantità risorse disponibili in inventario utilizzando gli stessi moduli "ABS". Successivamente, come per gli altri provider, i valori di usage verranno utilizzati per calcolare i costi tramite il modello di costo descritto nella sezione Administration.

In caso di fallimento il processo viene schedulato automaticamente fino al raggiungimento di 3 tentativi. Nel caso in cui il sistema non dovesse riuscire a risolvere in maniera automatica Ã¨ necessario lâ€™intervento manuale. Inoltre, Ã¨ possibile richiede un aggiornamento dei costi manuale utilizzando i pulsanti disponibili nella sezione Administration.

In basso i dettagli specifici per tipologia di sottosistema

#### 2.0.1.1.5.2 Recupero e calcolo costi cliente per il provider Azure

##### Modalit  di recupero:

- **Modello "standard":** Il modulo ABS richiede tramite le REST API messe a disposizione da Azure i costi per gli ultimi 2 giorni che vengono salvati all' interno del database SCMP.
- **Modello "Storage Account":** Il modulo ABS recupera un file che contiene le estrazioni dei costi effettuate suddivise per sottosistema,he vengono salvati all' interno del database SCMP.
- **Modello "Billing storage":** il modulo ABS recupera un file che contiene le estrazioni di tutte le sottoscrizioni disponibili nel "billing account", i risultati vengono divisi per sottosistema e salvati sul database

##### Calcolo dei costi per singola risorsa:

1. Il modulo ABS invia al modulo costi le informazioni di costo e le info sulla risorsa che li ha generati.
2. Il modulo costi verifica la configurazione del sottosistema per individuare la "tipologia di aggregazione", questo parametro indica quale catalogo utilizzare (RISORSE. o SKU) cos  da calcolarne correttamente il prezzo
3. Il modulo costi verifica se l'identificativo della risorsa(UUID) Ã¨ presente nel catalogo SCMP, se presente il sistema moltiplica lo usage per il costo di catalogo
4. Se la risorsa non Ã¨ presente a catalogo (quindi non rientra nello step precedente) la SCMP applicher  la percentuale di sconto/ricarico configurata nel sottosistema

#### 2.0.1.1.5.3 Recupero e calcolo costi cliente per il provider AWS

- **Modello "standard":** Il modulo ABS interroga le API di AWS Cost Explorer per ottenere i costi degli ultimi 2 giorni, salvando i dati all'interno del database SCMP.
- **Modello "ARN ROLE":** Il modulo ABS assume un ruolo IAM specifico ( ARN ROLE) per accedere ai dati di billing di AWS. I costi vengono estratti e suddivisi per sottosistema, quindi salvati nel database SCMP.

##### Calcolo dei costi per singola risorsa:

1. Il modulo ABS invia al modulo costi le informazioni di costo e le info sulla risorsa che li ha generati.
2. Il modulo costi verifica la configurazione del sottosistema per individuare la "tipologia di aggregazione", questo parametro indica quale catalogo utilizzare (RISORSE o SKU) cos  da calcolarne correttamente il prezzo
3. Il modulo costi verifica se l'identificativo della risorsa(UUID) Ã¨ presente nel catalogo SCMP, se presente il



Leonardo Cyber & Security Solutions

21 Oct 2025

08.00

Secure Cloud Management Platform

sistema moltiplica lo usage per il costo di catalogo.

4. Se la risorsa non Ã¨ presente a catalogo (quindi non rientra nello step precedente) la SCMP applicherÃ la percentuale di sconto/ricarico configurata nel sottosistema

#### 2.0.1.1.5.4 Recupero e calcolo costi cliente per il provider **Google**

- **Modello "standard"**: Il modulo ABS interroga le API di Google Cloud Billing per ottenere i costi degli ultimi 2 giorni, salvando i dati all'interno del database SCMP.
- **Modello "Dataset Export"**: Il modulo ABS accede ai dati di billing esportati da **BigQuery**. I costi vengono estratti, suddivisi per sottosistema e salvati nel database SCMP.

#### Calcolo dei costi per singola risorsa:

1. Il modulo ABS invia al modulo costi le informazioni di costo e le info sulla risorsa che li ha generati.
2. Il modulo costi verifica la configurazione del sottosistema per individuare la "tipologia di aggregazione", questo parametro indica quale catalogo utilizzare (RISORSE o SKU) cosÃ da calcolarne correttamente il prezzo
3. Se il campo "Cost from USD" Ã stato selezionato il sistema utilizzerÃ per il calcolo il prezzo in USD (restituito dal provider), al quale viene applicata una percentuale di sconto/ricarico definita nella sezione administration, altrimenti viene utilizzato il prezzo giÃ convertito in EUR.
4. Il modulo costi verifica se l'identificativo della risorsa (UUID) Ã presente nel catalogo SCMP, se presente il sistema moltiplica lo usage per il costo di catalogo.
5. Se la risorsa non Ã presente a catalogo (quindi non rientra nello step precedente) la SCMP applicherÃ la percentuale di sconto/ricarico configurata nel sottosistema

#### 2.0.1.1.5.5 Recupero e calcolo costi cliente per i provider **Oracle, OracleEXAcc**

- **Modello "standard"**: Il modulo ABS interroga le API ORACLE per ottenere i costi degli ultimi 2 giorni, salvando i dati all'interno del database SCMP.

#### Calcolo dei costi per singola risorsa:

1. Il modulo ABS invia al modulo costi le informazioni di costo e le info sulla risorsa che li ha generati.
2. Il modulo costi verifica la configurazione del sottosistema per individuare la "tipologia di aggregazione", questo parametro indica quale catalogo utilizzare (RISORSE o SKU) cosÃ da calcolarne correttamente il prezzo
3. Se il campo "Cost from USD" Ã stato selezionato il sistema utilizzerÃ per il calcolo il prezzo in USD (restituito dal provider), al quale viene applicata una percentuale di sconto/ricarico definita nella sezione administration, altrimenti viene utilizzato il prezzo giÃ convertito in EUR.
4. Il modulo costi verifica se l'identificativo della risorsa (UUID) Ã presente nel catalogo SCMP, se presente il sistema moltiplica lo usage per il costo di catalogo.

5. Se la risorsa non Ã¨ presente a catalogo (quindi non rientra nello step precedente) la SCMP applicherÃ la percentuale di sconto/ricarico configurata nel sottosistema

#### 2.0.1.1.5.6 Recupero e calcolo costi cliente per i provider *Kubernetes, OpenShift, vcloudDirector, VMWare, Red Hat Edge*

- *Modello "standard"*: Il modulo ABS genera dei dati di Usage su base di 24 ore per tutte le risorse disponibili nell'inventario, poichÃ© i provider sono On-premise e le risorse sono tutte allocate al cliente.

#### Calcolo dei costi per singola risorsa:

1. Il modulo ABS invia al modulo costi le informazioni di costo e le info sulla risorsa che li ha generati .
2. la SCMP applicherÃ la percentuale di sconto/ricarico configurata nel modello di costo

#### 2.0.1.2 Creazione nuovo sottosistema

Per inserire un nuovo sottosistema all'interno del portale bisogna cliccare sul "menu" disponibile in alto a destra e selezionare "Aggiungi nuovo cloud provider"

---

*Figura 17 – Aggiunta di un nuovo Cloud  
Provider*

L'utente visualizza i dati di base del sottosistema da inserire, spiegati in seguito.

#### 2.0.1.2.1 PARAMETRI CONDIVISI TRA I PROVIDER

All'interno della pagina di creazione possiamo notare 3 campi :

- Nome: indica il nome che verrÃ visualizzato per indicare il sottosistema.
- Tipo: indica la tipologia di cloud provider al quale appartiene il sottosistema.
- Versione: la versione relativa al provider del sottosistema da installare.

---

*Figura 18 – Parametri generali di un  
sottosistema*

Dopo aver selezionato la tipologia e la versione del sistema la maschera si aggiorna per visualizzare i parametri specifici in base al provider selezionato, visto che ognuno di loro gestisce l'autenticazione e le risorse in maniera differente.

Tutti i provider richiedono un'autenticazione, che puÃ² variare in base al sistema, per il recupero degli asset.

Queste informazioni sensibili, come password o certificati, vengono salvati in maniera sicura su un elemento infrastrutturale che si occupa della sicurezza dei dati <https://www.vaultproject.io/>.

#### 2.0.1.2.2 VERIFICA DELLA CONNESSIONE E SALVATAGGIO, CONDIVISO TRA I PROVIDER

Per tutti i sottosistemi sono disponibili in basso nella pagina 3 pulsanti

Il tasto “Chiudi” che permette di annullare l’inserimento di un nuovo sottosistema.

Il tasto “Test Connection” serve ad effettuare un test di connessione utilizzando i parametri inseriti, in caso di errori il sistema ritorna un messaggio di errore che indica “Error: Unauthorized system” e il pulsante diventa di colore rosso, in caso contrario il pulsante diventerà verde e sarà possibile salvare il sottosistema utilizzando il tasto “Salva”.

---

*Figura 19 – Pulsanti di connessione*

Al salvataggio, la SCMP comunicherà al modulo che gestisce quella tipologia di provider, di caricare all’interno del nostro bus (Kafka) tutti gli item relativi all’inventario, metriche, costi ed elementi di security.

Lo stesso modulo, si occuperà successivamente di schedulare dei job per l’aggiornamento periodico di tutti gli asset presenti.

Dopo aver salvato, apparirà una modale che informa l’utente che non è possibile eliminare un cloud provider prima delle 24 ore. Dalla modale, cliccare su “OK”. Dopo aver fatto ciò, l’utente si ritrova all’interno della pagina dei Cloud Provider.

#### 2.0.1.2.3 PARAMETRI AMAZON WEB SERVICES

Funzionalità abilitate:

- Recupero elementi di catalogo
- Recupero elementi di inventario
- Recupero delle metriche di utilizzo
- Recupero dei costi delle risorse
- Recupero delle informazioni di sicurezza
- Provisioning di risorse
- Provisioning di servizi
- Provisioning di blueprint complesse

I parametri specifici del sottosistema Amazon Web Services da inserire sono esposti nella tabella:

---

*Figura 20 – Maschera di configurazione  
Amazon Web Services*



Vengono indicati con \* i parametri obbligatori

Nome	Tipo	Descrizione	Esempio
AccessKey *	string	La chiave di accesso AWS Ã una stringa alfanumerica che identifica l'utente AWS.	ZYKZGVAKIS4YK5IX CAXB
SecretKey *	password	La chiave di accesso segreta AWS Ã una stringa alfanumerica che viene utilizzata per autenticare l'utente AWS	np6Kc_.xwsvhR8Q~r P05fCqYNXmbqfMG QLOEzfMt
use A role	Boolean	Specifica lâ€™utilizzo di uno o piÃ ruoli dâ€™amministrazione per lâ€™autenticazione su uno o piÃ account specifico/i dellâ€™organization del provider	true
Arn Role (solo se useArole Ã attivo)	string	Inserisci qui l'id Arn del ruolo associato ad un account specifico per lâ€™esecuzione della fase di discovery di monitoring e per il provisioning	arn:aws:iam:{account ID}:role/{roleName}
Audit Arn Role (solo se useArole Ã attivo)	string	Inserisci qui l'id Arn di Audit del ruolo associato ad un account specifico per lâ€™esecuzione della fase di discovery dâ€™inventario	arn:aws:iam:{account ID}:role/{roleName}
Aggregator Name	string	Inserisci qui il nome dellâ€™aggregator sulle risorse per lâ€™utilizzo del servizio AWS Config a supporto della fase di discovery dâ€™inventario	aws-{aggregatorNam e}
Cost Bucket Path	string	Inserisci qui il path del bucket di storage delle query sui costi	s3://{bucketPath}
Cost Export Dataset ID	string	Inserisci qui lâ€™ID del dataset dei costi sul quale eseguire le query	{databaseName}. {tabl eName}
usageAggregation	Boolean	Indica la tipologia di aggregazione utilizzata per il calcolo dei costi (true per le risorse, false per gli sku)	True
Rate Code Aggregation (solo se useAggregation Ã false)	Boolean	Indica se lâ€™aggregazione degli sku avviene per sku ID o per rate code.	true
catalogPriceDiscount	integer	Inserisci qui uno sconto/maggiorazione da applicare sui prezzi del catalogo per tutte le risorse che non hanno una relazione CMP	5
odlID	string	Inserisci qui l'id dell'ordine di lavoro che verrÃ associato al sottosistema e verrÃ inserito come tag su tutte le risorse del sottosistema	ODL001
dataFirstCostRecover	int	Inserire il numero di giorni precedenti alla data di creazione dei quali bisogna recuperare i costi al primo avvio del sottosistema	15



## ■ Configurazioni sul provider

### 1. Configurazione S3

- Accedere ad **Amazon S3**.
- Creare o utilizzare un bucket per i dati CUR.
- Abilitare il **Bucket Versioning**.

### 2. Definizione CUR

- Accedere ad **Billing and cost management**
- Andare nella sezione Data Exports
- Configurare un nuovo report CUR come segue
  - Export details:
    - **Standard data export**: formato standard d'esportazione
    - **Export name**: nome del report
  - Data table content settings:
    - Selezionare **CUR 2.0**
    - Selezionare come granularità **Hourly**
  - Data export delivery options
    - file format: **Parquet**
    - file versioning: **Overwrite existing data export file**
  - Data export storage settings
    - Configurare il puntamento al bucket S3 con quello creato inizialmente
    - Configurare il prefisso del bucket path con **data**

### 3. Creazione del ruolo IAM per Glue

- Accedere ad **IAM**.
- Creare un ruolo custom per la gestione di Amazon Glue.
- Assegnare le seguenti policy:
  - **AWSGlueServiceRole** (policy standard AWS)
  - Policy custom per accesso al bucket S3:



Leonardo Cyber & Security Solutions

21 Oct 2025

08.00

Secure Cloud Management Platform

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

#### 4. Creazione database Glue

- Accedere a **AWS Glue**.
- Creare il database.

#### 5. Configurazione del Crawler

- Creare un **crawler** in Glue:
  - Selezionare il ruolo custom precedentemente creato.
  - Definire il path S3 come `s3://{bucketPath}/data/`.
  - Impostare uno **scheduling** (es. ogni ora: `0 * * * * *`).

#### 6. Utilizzo in Athena

- Dopo la prima esecuzione del crawler, i dati saranno disponibili in **Athena** per le query.
- *Per dati storici passati, contattare il supporto AWS.*

### 1. Configurazione e Aggregatori AWS

#### a. Configurazione iniziale

- Accedere ad **AWS Config** e fare clic su **Get started**.
- Creare un bucket S3 per i dati aggregati.
- Abilitare l'override per risorse di tipo **IAM** e lasciare le restanti opzioni di default; AWS creerà automaticamente il ruolo necessario.

#### b. Aggregatore Config

- Creare un **aggregatore di risorse** nell'apposita sezione **Aggregators**.

- Includere tutte le regioni.

### 1. Creazione utente IAM

- Accedere ad **IAM** e andare nella sezione **Users**
- Creare un nuovo utente o selezionarne uno preesistente.
- Facoltativo: abilitare l'accesso a console per l'utente creato.

### 2. Policy da assegnare all'utente

- AmazonAthenaFullAccess
- AmazonS3FullAccess
- AWS\_ConfigRole
- AWSConfigUserAccess
- AmazonEC2ReadOnlyAccess
- CloudWatchReadOnlyAccess
- Aggiungere la seguente policy custom per la gestione del bucket dei CUR

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [ "s3:*" ],
      "Resource": [
        "arn:aws:s3:::{bucketPath}/",
        "arn:aws:s3:::{bucketPath}/*"
      ]
    }
  ]
}
```

### 3. Access Key

- Generare **Secret Credential**.
- Salvare la **Access Key** e **Secret Key** (non recuperabili in seguito). Per abilitare l'assunzione di ruoli tramite STS per servizi cross-account (es. AWS Config), associare la seguente policy all'utente creato:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": [
        "arn:aws:iam::{accountID}:role/{roleName}"
      ]
    }
  ]
}
```

#### 2.0.1.2.4 PARAMETRI AZURE

Funzionalità abilitate:

- Recupero elementi di catalogo
- Recupero elementi di inventario
- Recupero delle metriche di utilizzo
- Recupero dei costi delle risorse
- Recupero delle informazioni di sicurezza
- Provisioning di risorse
- Provisioning di servizi
- Provisioning di blueprint complesse

I parametri specifici del sottosistema Azure da inserire sono esposti nella tabella:

*Figura 21 – Maschera di configurazione  
Azure*

Vengono indicati con \* i parametri obbligatori

Nome	Tipo	Descrizione	Esempio
clientId *	string	L'ID univoco del client che si connette al sottosistema Azure Cloud. Questo ID viene utilizzato per identificare il client e per autorizzare l'accesso alle risorse del sottosistema.	5a85c16c6ad-49db-a58e-e209-ee11f5 3d6c6b

Nome	Tipo	Descrizione	Esempio
clientSecret *	password	La chiave segreta del client, utilizzata per autenticare il client con il sottosistema Azure Cloud. La chiave segreta deve essere tenuta segreta e non deve essere condivisa con nessuno.	np6Kc_.xwsvhR8Q~rP05fCqYNXmbqfMGQLOEzfMt
tenantId *	string	L'ID del tenant Azure a cui appartiene il sottosistema Azure Cloud. Il tenant Ã un'entitÃ organizzativa in Azure che rappresenta un'azienda o un'organizzazione.	884147733-ff13-4783-a765-834183773083
subscriptionId *	string	L'ID della sottoscrizione Azure utilizzata per accedere al sottosistema Azure Cloud. La sottoscrizione Ã un contratto per l'utilizzo dei servizi Azure.	884147733-ff13-4783-a765-834183773083
usageAggregation	boolean	Indica se l'aggregazione per "usage" Ã abilitata per la sottoscrizione. Quando questa spunta viene abilitata i costi del sottosistema verranno raggruppati per Tipologia risorsa	false
Storage account ID**	String	Inserire il percorso dove vengono effettuate le esportazioni dei costi	/subscriptions/{{sottoscrizione}}/resourceGroups/{{resourcegroup}}/providers/Microsoft.Storage/storageAccounts/{{storage account}}
Cost from Billing storage**	boolean	Selezionare questa casella per recuperare i costi in formato "billing Account"	true
catalogPriceDiscount	integer	Inserisci qui uno sconto/maggiorazione da applicare sui prezzi del catalogo per tutte le risorse che non hanno una relazione SCMP	5
odlID	string	Inserisci qui l'id dell'ordine di lavoro che verrÃ associato al sottosistema e verrÃ inserito come tag su tutte le risorse del sottosistema	ODL001
dataFirstCostRecover	int	Inserire il numero di giorni precedenti alla data di creazione dei quali bisogna recuperare i costi al primo avvio del sottosistema	15

#### ■ Variabili per il calcolo dei costi

Le variabili indicate con \*\* sono esclusive, quindi Ã possibile selezionarne solo una alla volta. Ogni variabile attiva un sistema diverso per il calcolo dei costi e, se ne vengono impostate piÃ¹ di una, verrÃ impedito il salvataggio del sottosistema. Nello specifico possiamo:

- Utilizzare il campo "Storage account ID" per recuperare i costi tramite le estrazioni automatiche effettuate singolarmente per sottosistema (solo se lo storage appartiene allo stesso tenant)
- Utilizzare il campo "Cost from Billing storage" per recuperare i costi a livello di billing account, quindi utilizzando un solo file per tutte le sottoscrizioni disponibili (Sono necessari i permessi di Contributor e Blob Contributor )
- Lasciando vuoto il campo "Cost from Billing storage" e il campo "Cost from billing storage" la SCMP recupererÃ i costi utilizzando le API Azure predisposte per i costi giornalieri.

Questa distinzione Ã necessaria per evitare che le API Azure rispondano con un errore 429 legato al grande numero di richieste effettuate, inoltre per utilizzare i metodi descritti precedentemente Ã necessario che il sistema Azure sia configurato correttamente e le utenze inserite abbiano tutti i permessi necessari

#### 2.0.1.2.5 PARAMETRI AZURESTACK

Funzionalità abilitate:

- Recupero elementi di catalogo
- Recupero elementi di inventario
- Recupero delle metriche di utilizzo
- Recupero dei costi delle risorse
- Recupero delle informazioni di sicurezza
- Provisioning di risorse
- Provisioning di servizi
- Provisioning di blueprint complesse

I parametri specifici del sottosistema AzureStack da inserire sono esposti nella tabella:

*Figura 22 – Maschera di configurazione  
AzureStack*

Vengono indicati con \* i parametri obbligatori

Nome	Tipo	Descrizione	Esempio
------	------	-------------	---------



Leonardo Cyber & Security Solutions

21 Oct 2025

08.00

Secure Cloud Management Platform

Nome	Tipo	Descrizione	Esempio
clientId *	string	L'ID univoco del client che si connette al sottosistema Azure Cloud. Questo ID viene utilizzato per identificare il client e per autorizzare l'accesso alle risorse del sottosistema.	5a85c16c6ad-49db -a58e-e209-ee11f5 3d6c6b
clientSecret *	password	La chiave segreta del client, utilizzata per autenticare il client con il sottosistema Azure Cloud. La chiave segreta deve essere tenuta segreta e non deve essere condivisa con nessuno.	np6Kc_.xwsvhR8Q ~rP05fCqYNXmbqf MGQLOEzfMt
tenantId *	string	L'ID del tenant Azure a cui appartiene il sottosistema Azure Cloud. Il tenant Ã un'entitÃ organizzativa in Azure che rappresenta un'azienda o un'organizzazione.	884147733-ff13-47 83-a765-83418377 3083
subscriptionId *	string	L'ID della sottoscrizione Azure utilizzata per accedere al sottosistema Azure Cloud. La sottoscrizione Ã un contratto per l'utilizzo dei servizi Azure.	884147733-ff13-47 83-a765-83418377 3083
usageAggregation	boolean	Indica se l'aggregazione per "usage" Ã abilitata per la sottoscrizione. Quando questa spunta viene abilitata i costi del sottosistema verranno raggruppati per Tipologia risorsa	false
catalogPriceDiscount	integer	Inserisci qui uno sconto/maggiorazione da applicare sui prezzi del catalogo per tutte le risorse che non hanno una relazione SCMP	5
odlId	string	Inserisci qui l'id dell'ordine di lavoro che verrÃ associato al sottosistema e verrÃ inserito come tag su tutte le risorse del sottosistema	ODL001
dataFirstCostRecover	int	Inserire il numero di giorni precedenti alla data di creazione dei quali bisogna recuperare i costi al primo avvio del sottosistema	15

Per i provider on Premise, in particolare, vengono richiesti dati sulla capacitÃ della infrastruttura, in modo tale che la SCMP possa effettuare dei calcoli preliminari in molteplici scenari.

Per esempio, durante il provisioning, in modo tale da non superare la capacitÃ massima consentita del provider.

#### 2.0.1.2.6 PARAMETRI AZURESTACK HCI

Funzionalità abilitate:

- Recupero elementi di catalogo
- Recupero elementi di inventario
- Recupero delle metriche di utilizzo



- Recupero dei costi delle risorse
- Recupero delle informazioni di sicurezza
- Provisioning di risorse
- Provisioning di servizi
- Provisioning di blueprint complesse

I parametri specifici del sottosistema AzureStack HCI da inserire sono esposti nella tabella:

*Figura 23 – Maschera di configurazione  
AzureStack HCI*

Vengono indicati con \* i parametri obbligatori

Nome	Tipo	Descrizione	Esempio
clientId *	string	L'ID univoco del client che si connette al sottosistema Azure Cloud. Questo ID viene utilizzato per identificare il client e per autorizzare l'accesso alle risorse del sottosistema.	5a85c16c6ad-49db -a58e-e209-ee11f5 3d6c6b
clientSecret *	password	La chiave segreta del client, utilizzata per autenticare il client con il sottosistema Azure Cloud. La chiave segreta deve essere tenuta segreta e non deve essere condivisa con nessuno.	np6Kc_.xwsvhR8Q ~rP05fCqYNXmbqf MGQLOEzfMt
tenantId *	string	L'ID del tenant Azure a cui appartiene il sottosistema Azure Cloud. Il tenant Ã un'entitÃ organizzativa in Azure che rappresenta un'azienda o un'organizzazione.	884147733-ff13-47 83-a765-83418377 3083
subscriptionId *	string	L'ID della sottoscrizione Azure utilizzata per accedere al sottosistema Azure Cloud. La sottoscrizione Ã un contratto per l'utilizzo dei servizi Azure.	884147733-ff13-47 83-a765-83418377 3083
usageAggregation	boolean	Indica se l'aggregazione per "usage" Ã abilitata per la sottoscrizione. Quando questa spunta viene abilitata i costi del sottosistema verranno raggruppati per Tipologia risorsa	false
catalogPriceDiscount	integer	Inserisci qui uno sconto/maggiorazione da applicare sui prezzi del catalogo per tutte le risorse che non hanno una relazione SCMP	5
odlId	string	Inserisci qui l'id dell'ordine di lavoro che verrÃ associato al sottosistema e verrÃ inserito come tag su tutte le risorse del sottosistema	ODL001
dataFirstCostRecover	int	Inserire il numero di giorni precedenti alla data di creazione dei quali bisogna recuperare i costi al primo avvio del sottosistema	15

Per i provider on Premise, in particolare, vengono richiesti dati sulla capacità della infrastruttura, in modo tale che la SCMP possa effettuare dei calcoli preliminari in molteplici scenari.

Per esempio, durante il provisioning, in modo tale da non superare la capacità massima consentita del provider.

#### 2.0.1.2.7 PARAMETRI AZURESTACK HYBRID CLOUD

Funzionalità abilitate:

- Recupero elementi di catalogo
- Recupero elementi di inventario
- Recupero delle metriche di utilizzo
- Provisioning di risorse
- Provisioning di servizi
- Provisioning di blueprint complesse

I parametri specifici del sottosistema AzureStack Hybrid cloud da inserire sono esposti nella tabella:

*Figura 24 – Maschera di configurazione  
AzureStack Hybrid cloud*

Vengono indicati con \* i parametri obbligatori

Nome	Tipo	Descrizione	Esempio
clientId *	string	L'ID univoco del client che si connette al sottosistema Azure Cloud. Questo ID viene utilizzato per identificare il client e per autorizzare l'accesso alle risorse del sottosistema.	5a85c16c6ad-49db -a58e-e209-ee11f5 3d6c6b
clientSecret *	password	La chiave segreta del client, utilizzata per autenticare il client con il sottosistema Azure Cloud. La chiave segreta deve essere tenuta segreta e non deve essere condivisa con nessuno.	np6Kc_.xwsvhR8Q ~rP05fCqYNXmbqf MGQLOEzfMt
tenantId *	string	L'ID del tenant Azure a cui appartiene il sottosistema Azure Cloud. Il tenant è un'entità organizzativa in Azure che rappresenta un'azienda o un'organizzazione.	884147733-ff13-47 83-a765-83418377 3083
subscriptionId *	string	L'ID della sottoscrizione Azure utilizzata per accedere al sottosistema Azure Cloud. La sottoscrizione è un contratto per l'utilizzo dei servizi Azure.	884147733-ff13-47 83-a765-83418377 3083

Nome	Tipo	Descrizione	Esempio
usageAggregation	boolean	Indica se l'aggregazione per "usage" Ã abilitata per la sottoscrizione. Quando questa spunta viene abilitata i costi del sottosistema verranno raggruppati per Tipologia risorsa	false
catalogPriceDiscount	integer	Inserisci qui uno sconto/maggiorazione da applicare sui prezzi del catalogo per tutte le risorse che non hanno una relazione SCMP	5
odlID	string	Inserisci qui l'id dell'ordine di lavoro che verrÃ associato al sottosistema e verrÃ inserito come tag su tutte le risorse del sottosistema	ODL001
dataFirstCostRecover	int	Inserire il numero di giorni precedenti alla data di creazione dei quali bisogna recuperare i costi al primo avvio del sottosistema	15

Per i provider on Premise, in particolare, vengono richiesti dati sulla capacitÃ della infrastruttura, in modo tale che la SCMP possa effettuare dei calcoli preliminari in molteplici scenari.

Per esempio, durante il provisioning, in modo tale da non superare la capacitÃ massima consentita del provider.

#### 2.0.1.2.8 PARAMETRI DISPOSITIVI REDHAT EDGE

FunzionalitÃ abilitate:

- Recupero elementi di catalogo
- Recupero elementi di inventario
- Recupero delle metriche di utilizzo
- Recupero dei costi delle risorse
- Recupero delle informazioni di sicurezza
- Provisioning di risorse
- Provisioning di servizi
- Provisioning di blueprint complesse

I parametri specifici del sottosistema Google Cloud da inserire sono esposti nella tabella.

*Figura 25 – Maschera di configurazione  
Edge*

Vengono indicati con \* i parametri obbligatori

Nome	Tipo	Descrizione	Esempio



Leonardo Cyber & Security Solutions

21 Oct 2025

08.00

Secure Cloud Management Platform

Nome	Tipo	Descrizione	Esempio
client_id *	string		104822473261 100667392
clientSecret *	string	Secret del cliente utilizzato per la connessione	82hg7ds1h0sd s7392
odlID	string	Inserisci qui l'id dell'ordine di lavoro che verr� associato al sottosistema e verr� inserito come tag su tutte le risorse del sottosistema	ODL001
catalogPriceDiscount	integer	Inserisci qui uno sconto/maggiorazione da applicare sui prezzi del catalogo per tutte le risorse che non hanno una relazione SCMP	10
dataFirstCostRecover	int	Inserire il numero di giorni precedenti alla data di creazione dei quali bisogna recuperare i costi al primo avvio del sottosistema	15

## ■ Configurazione lato PROVIDER

Per poter inserire il sistema nella SCMP sono necessarie alcune configurazioni da effettuare sul portale del provider.

Nello specifico :

- Creare un service account
  - a. Accedi a <https://console.redhat.com>
  - b. In alto a destra fai clic sull'icona "Settings" "Service Accounts" "Create service account."
  - c. Inserisci Nome e Descrizione "Create."
  - d. Copia subito Client ID e Client Secret (il secret non verrà più mostrato) .
- assegnare i permessi
  - a. Andare su Settings "User Access" "Groups"
  - b. Creare un gruppo che contenga i seguenti permessi/ruoli:

Servizio	Ruolo consigliato
Edge Management (fleet, update)	<b>Edge Management Administrator</b> o <b>User</b>
Image Builder	<b>Image Builder Administrator</b> o <b>User</b>
Insights Inventory (lettura host)	<b>Insights Inventory Viewer</b>

- Nella scheda Service accounts del gruppo "Add service account" seleziona l'account appena creato
- Rotazione e revoca permessi
  - a. Portale "Service Accounts" menu (â€œ)
  - b. Seleziona **Reset credentials** per rigenera solo il Client Secret.
  - c. Seleziona **Delete service account** per dismettere definitivamente l'automazione.

Con questa configurazione puoi orchestrare in modo sicuro tutto il ciclo di vita edge "dalla generazione delle immagini al rollout degli aggiornamenti" senza mai usare credenziali personali.

### 2.0.1.2.9 PARAMETRI GOOGLE CLOUD

Funzionalità abilitate:

## Recupero elementi di catalogo

- Recupero elementi di inventario
- Recupero delle metriche di utilizzo
- Recupero dei costi delle risorse
- Recupero delle informazioni di sicurezza
- Provisioning di risorse
- Provisioning di servizi
- Provisioning di blueprint complesse

I parametri specifici del sottosistema Google Cloud da inserire sono esposti nella tabella, il campo "Service account" essere inserito sia automaticamente che manualmente come descritto nel paragrafo.

Figura 26 – Maschera di configurazione  
Google

Vengono indicati con \* i parametri obbligatori (disponibili in basso sotto la sezione relativa al service account).

Nome	Tipo	Descrizione	Esempio
serviceAccount *	object	File di connessione generato dalla console Google	service_account.json
discoveryProjectId *	string	Identificativo del progetto di cui si effettuerà il discovery	Theproject-547280
costExportProjectId	string	Dataset id del service account di esportazione costi se il dataset è differente dal ProjectID	test-customer.test_customer.gcp_billing_export_resource_v1_01527DF_51B683_EB2A9
usageAggregation	boolean	Indica se l'aggregazione per "usage" è abilitata per la sottoscrizione. Quando questa spunta viene abilitata i costi del sottosistema verranno raggruppati per Tipologia risorsa	false
Cost from USD Currency	boolean	Indica se il costo finale è calcolato dal prezzo in USD o EUR	true
providerPriceDiscount ** (solo se costFromUSDCurrency è true)	integer	Inserisci qui uno sconto/maggiorazione da applicare sui prezzi in USD del provider per tutte le risorse	30



Leonardo Cyber & Security Solutions

21 Oct 2025

08.00

Secure Cloud Management Platform

Nome	Tipo	Descrizione	Esempio
catalogPriceDiscount **	integer	Inserisci qui uno sconto/maggiorazione da applicare sui prezzi del catalogo per tutte le risorse che non hanno una relazione SCMP	-5
odlID	string	Inserisci qui l'id dell'ordine di lavoro che verr� associato al sottosistema e verr� inserito come tag su tutte le risorse del sottosistema	ODL001
dataFirstCostRecover	int	Inserire il numero di giorni precedenti alla data di creazione dei quali bisogna recuperare i costi al primo avvio del sottosistema	15

#### ■ Variabili per il calcolo dei costi

Le variabili indicate con \*\* Vengono utilizzate in maniera differente, per il calcolo del costo "cliente" a seconda della presenza del campo "Cost from USD Currency". Nello specifico :

- Se il campo   disattivato il valore inserito in "catalogPriceDiscount"v viene utilizzato come percentuale aggiunta al prezzo recuperato dal provider(o scontata se il valore   negativo) come per gli altri provider
- Se il campo   attivato il valore inserito in "catalogPriceDiscount" e il valore di "providerPriceDiscount" viene utilizzato come coefficiente moltiplicato per il costo in USD recuperato dal provider

Questa distinzione   necessaria per evitare che le API Azure rispondano con un errore 429 legato al grande numero di richieste effettuate, inoltre per utilizzare i metodi descritti precedentemente   necessario che il sistema Azure sia configurato correttamente e le utenze inserite abbiano tutti i permessi necessari

Figura 27 – Caricamento del file di configurazione

Effettuando lâ€™upload del file il form viene completato automaticamente con i parametri necessari, ma   possibile anche inserirli manualmente (riquadro giallo presente nellâ€™immagine), seguendo la tabella, tutti i campi sono obbligatori:

Nome	Tipo	Descrizione	Esempio
Type	string	Inserire il nome della tipologia di autenticazione configurata	service_account
project_id *	string	Inserisci qui l'id univoco del progetto associato al service account	Theproject-367810

Nome	Tipo	Descrizione	Esempio
private_key_id *	string	Inserisci qui l'id univoco della chiave privata del service account	55cb5cf903ee93ea1e9c294a07e46e0af0633e6
private_key *	password	Contiene la chiave privata del service account in formato PEM. È fondamentale per l'autenticazione del service account alle API di Google Cloud	-----BEGIN PRIVATE KEY-----MIJQgIBADANBâ€¦
client_email *	string	L'indirizzo e-mail univoco del service account. È utilizzato per identificare il service account quando si autentica alle API di Google Cloud	user@dominio.com
client_id *	string	L'ID client del service account. È un identificatore univoco utilizzato per identificare il service account in Google Cloud	104822473261100667392
auth_uri *	string	L'URI utilizzato per l'autenticazione del service account alle API di Google Cloud	https://accounts.google.com/o/oauth2/auth
token_uri *	string	L'URI utilizzato per ottenere un token di accesso per il service account	https://oauth2.googleapis.com/token
auth_provider_x509_cert_url*	string	L'URL del certificato X.509 utilizzato per l'autenticazione del service account	https://www.googleapis.com/oauth2/v1/certs
client_x509_cert_url *	string	L'URL del certificato X.509 nel client	https://www.googleapis.com/robot/v1/metadata/f543/myserviceaccount%40projectName.gserviceaccount.com





Leonardo Cyber & Security Solutions

21 Oct 2025

08.00

Secure Cloud Management Platform

## ■ Configurazione sul provider

### 1. Accesso a GCP Console

- Vai su <https://console.cloud.google.com/>
- Effettua il login con il tuo account Google Cloud.

### 2. Creare o identificare il Service Account (SA) Dalla console, seleziona in alto il progetto nel quale voler aggiungere (o Ã` giÃ` presente) il service account Dalla console, per creare il service account, vai su IAM and admin > Service accounts. Clicca su Create service account. Assegna id (es: my-service-account), nome e descrizione ed infine Create. Nella pagina dell'account di servizio, vai alla sezione Keys Clicca su Add key e seleziona Create new key Scegli il formato json e clicca su Create Scarica e conserva il file JSON in un luogo sicuro.

### 3. Associare i permessi al Service Account

Nella stessa pagina degli account di servizio, trova l'account appena creato e clicca sul suo nome. Vai alla sezione Permissions e nella tabella in basso, in corrispondenza del service account, nella colonna Inheritance clicca su Edit principal. Nel menÃ¹ a comparsa, seleziona i ruoli appropriati per l'account di servizio. Di seguito l'elenco minimale dei ruoli per la SCMP: - App Engine Admin - BigQuery Data Transfer Service Agent - Cloud OS Config Service Agent - Compute Admin - Kubernetes Engine Service Agent - OS Inventroy Viewer - Security Centre Service Agent Clicca su Save e aggiungi i permessi al service account.

### 4. Abilitazione Service APIs

Torna alla home della console Seleziona in alto il progetto nel quale Ã` presente il service account Vai su APIs and services In alto cliccare su + Enable APIs and services Cerca nella barra di ricerca i servizi API da abilitare e clicca sul loro nome Una volta dentro il servizio API, seleziona Enable per abilitarlo; di seguito i servizi API per la SCMP: - Cloud Monitoring API - Compute Engine API - Cloud Asset API - BigQuery API - Cloud Resource Manager API - OS Config API - Security Command Center API - Cloud Billing API - Service Usage API - Cloud Dataplex API

### 5. Dataset dei costi

Se il dataset dei costi Ã` situato in un service account diverso da quello da voler integrare, specificare nella casella di testo Cost Export Dataset ID (nel modulo di creazione sottosistema presente in administration della SCMP) la completa stringa di connessione al relativo dataset (es: projectId.datasetName.tableName)

## 2.0.1.2.10 PARAMETRI KUBERNETES

Funzionalità abilitate:

- Recupero elementi di catalogo
- Recupero elementi di inventario

- Recupero delle metriche di utilizzo
- Recupero dei costi delle risorse
- Recupero delle informazioni di sicurezza
- Provisioning di risorse
- Provisioning di servizi
- Provisioning di blueprint complesse

I parametri specifici del sottosistema Kubernetes da inserire sono esposti nella tabella

*Figura 28 – Maschera di configurazione  
Kubernetes*

Vengono indicati con \* i parametri obbligatori

Nome	Tipo	Descrizione	Esempio
Certificate authority data *	string	Inserire i dati relativi al certificato utilizzato dall'utenza utilizzata per la connessione	Sgeijesf90434n7u3h97ef
Kubernetes API server URI *	string	Inserire l'URL del server al quale connettersi	https://www.google.com/infos
User certificate Data *	String	Inserire il certificato relativo all'utenza utilizzata per la connessione	---begin private key-- - fnbsujffsoije â€
User key Data *	String	Inserire la key relativa all'utenza utilizzata per la connessione	Sf8j9jts4ewht7h3wfwj908w
User token *	String	Token segreto relativo all'utenza utilizzata per la connessione al provider	Sf8eufce9sfber4543jh8dds fh89r43
User name *	String	Inserire l'username utilizzato per l'autenticazione	administrator
Label selector	string	Inserisci qui un selettore per filtrare le risorse recuperate dalla SCMP	Name=rossi
catalogPriceDiscount	integer	Inserisci qui uno sconto/maggiorazione da applicare sui prezzi del catalogo per tutte le risorse che non hanno una relazione SCMP	-10
odlID	string	Inserisci qui l'id dell'ordine di lavoro che verrà associato al sottosistema e verrà inserito come tag su tutte le risorse del sottosistema	ODL001

#### ■ Configurazione sul provider

il metodo standard di autenticazione Ãˆ tramite i parametri contenuti nel file kubeconfig. Il kubeconfig definisce:  
Endpoint API server (server) Metodo di autenticazione (certificati client, token, oidc, ecc.) Namespace di default  
Contesto Autenticazione: Tramite certificati client (client-certificate-data e client-key-data)

Oppure tramite token (token nel contesto dell'utente)

Esempio minimale di kubeconfig:

```
apiVersion: v1 kind: Config clusters: - cluster: certificate-authority-data: server: https:// name: my-cluster contexts: -  
context: cluster: my-cluster user: my-user name: my-context current-context: my-context users: - name: my-user  
user: token:
```

#### 2.0.1.2.11 PARAMETRI OPENSIFT

Funzionalità abilitate:

- Recupero elementi di catalogo
- Recupero elementi di inventario
- Recupero delle metriche di utilizzo
- Recupero dei costi delle risorse
- Recupero delle informazioni di sicurezza
- Provisioning di risorse
- Provisioning di servizi
- Provisioning di blueprint complesse

I parametri specifici del sottosistema OpenShift da inserire sono esposti nella tabella:

*Figura 29 – Maschera di configurazione  
OpenShift*

Vengono indicati con \* i parametri obbligatori

Nome	Tipo	Descrizione	Esempio
Username *	string	L'username dell' utenza OpenShift che verrÃ utilizzata per la connessione al provider	nome.cog nome@m ail.com

Nome	Tipo	Descrizione	Esempio
Password *	password	La password del client, utilizzata per autenticare il client con il sottosistema. La chiave segreta deve essere tenuta segreta e non deve essere condivisa con nessuno.	np6KcXm bqfMGQL OEzfMt
API server port *	integer	La porta sulla quale sono in ascolto le API OpenShift	8090
API url *	string	L'url OpenShift sul quale effettuare le richieste	www.google.com
discover all Namespaces	boolean	Se l'utenza possiede permessi di amministratore su tutti i "progetti" di OpenShift verranno recuperati tutti i namespaces	false
Namespace selector (visibile solo se attivo "discover all namespaces")	selection	Se l'utente utilizzato ha visibilit� di un numero limitato di namespace � necessario inserire qui la lista dei namespaces abilitati	demo,info s,production
odlID	string	Inserisci qui l'id dell'ordine di lavoro che verr� associato al sottosistema e verr� inserito come tag su tutte le risorse del sottosistema	ODL001
dataFirstCostRecover	int	Inserire il numero di giorni precedenti alla data di creazione dei quali bisogna recuperare i costi al primo avvio del sottosistema	15

#### ■ Autorizzazioni utente

Se lasciamo attivo il campo "Discover all namespaces" selezionato   necessario che l'utenza abbia i permessi di amministrazione su **TUTTI** i namespaces, altrimenti non sar  possibile l'inserimento del sistema.

Questa distinzione   necessaria perch  il sistema OpenShift blocca automaticamente le richieste non autorizzate correttamente.

#### ■ Configurazione sul provider

Per connettere un sistema cluster OpenShift, Ã sufficiente disporre di un'utenza nominale o impersonale che abbia i privilegi adeguati (ad es. cluster-admin o comunque sufficienti per l'uso previsto) sul cluster.

Autenticazione:

Username e Password

Note:

In OpenShift Ã molto comune usare ServiceAccount appositamente create, con relative RoleBinding o ClusterRoleBinding.

Le utenze possono essere sia umane (nominali) che tecniche (impersonali).

#### 2.0.1.2.12 PARAMETRI ORACLE

Funzionalità abilitate:

- Recupero elementi di catalogo
- Recupero elementi di inventario
- Recupero dei costi delle risorse
- Recupero delle informazioni di sicurezza

I parametri specifici del sottosistema Oracle da inserire sono esposti nella tabella:

*Figura 30 – Maschera di configurazione  
Oracle*

Vengono indicati con \* i parametri obbligatori

Nome	Tipo	Descrizione	Esempio
username *	string	Il nome utente utilizzato per l'autenticazione con OCI.	ocid5.user.oc77.aaabnbthaj6pn vsb2gqnaaaaait3mqzekefmlhwk ige2wxna6hfaj3f6njma
fingerprint *	string	Ã un valore univoco che identifica il dispositivo, utilizzato per l'autenticazione con OCI.	6a:f4:6e:9a:73:95:27:d5:64:8d1 1:a3:f5:0e:fb:f4:



Leonardo Cyber & Security Solutions

21 Oct 2025

08.00

Secure Cloud Management Platform

Nome	Tipo	Descrizione	Esempio
tenantId *	string	L'ID del tenant OCI a cui ci si vuole connettere	ocid5.tenancy.oc77...aaabnbtha j6pnvsb2gqnaaaait3mqzekefm lhwkige2wxna6hfaj3f6njma
region *	string	La regione Ã" la posizione geografica specifica in cui si trovano le risorse OCI.	eu-dcc-rome-1
Realm	string	Il nome del contenitore logico che raggruppa le risorse OCI e i relativi costi.	personal-realm.it
keyFile *	password	un file PEM che contiene la chiave pubblica e privata utilizzata per l'autenticazione.	"-----BEGIN PRIVATE KEY----- MIJQgIBADANBâ€¦"
usageAggregation	boolean	Indica se l'aggregazione per "usage" Ã" abilitata per la sottoscrizione. Quando questa spunta viene abilitata i costi del sottosistema verranno raggruppati per Tipologia risorsa	false
catalogPriceDiscount	integer	Inserisci qui uno sconto/maggiorazione da applicare sui prezzi del catalogo per tutte le risorse che non hanno una relazione SCMP	-10
odlId	string	Inserisci qui l'id dell'ordine di lavoro che verrÃ associato al sottosistema e verrÃ inserito come tag su tutte le risorse del sottosistema	ODL001
dataFirstCostRecover	int	Inserire il numero di giorni precedenti alla data di creazione dei quali bisogna recuperare i costi al primo avvio del sottosistema	15

## ■ Configurazione sul provider

Procedura per creare i parametri per integrazione esterna in Oracle Cloud Infrastructure (OCI): 1. Accesso a OCI Console

Vai su <https://cloud.oracle.com/>  
Effettua il login con il tuo account Oracle Cloud.

### 1. Creare o identificare lâ€™Utente IAM

Nel menu principale della console, vai su Identity & Security > Users. Seleziona un utente esistente oppure crea un nuovo utente per lâ€™integrazione: Clicca su Create User se devi crearne uno. Assegna un nome e unâ€™email. Salva.

### 2. Associare allâ€™utente un gruppo con permessi adeguati



Dopo aver creato l'utente, devi associarlo a un gruppo che ha i permessi per le risorse che vuoi gestire via API. Vai su Identity > Groups. Seleziona un gruppo (es. Administrators o crea un gruppo personalizzato). Clicca su Add User to Group e aggiungi l'utente appena creato.

### 3. Generare la chiave API (Key File)

Torna alla pagina utente (Identity > Users > seleziona l'utente). Vai nella scheda API Keys. Clicca su Add API Key. Hai due opzioni: Carica una chiave pubblica esistente (pubblica RSA). Oppure genera una nuova chiave pubblica e privata da console (scarica la chiave privata). Seleziona "Generate API Key Pair" per generare localmente la chiave: Scarica la chiave privata (.pem) e salvala con sicurezza (il tuo Key File). La chiave pubblica sarà associata automaticamente all'utente.

### 4. Ottenere i parametri richiesti

Ocid Utente (User OCID): Vai su Identity > Users > seleziona utente. Trovi l'OCID utente nella pagina utente (formato ocid1.user.oc1..aaaaaaa...). Fingerprint: il fingerprint della chiave pubblica API che hai aggiunto (visualizzato nella sezione API Keys). Ocid Tenant (Tenant OCID / Compartment OCID principale): Vai su Identity > Tenancy (clicca sul nome tenancy in alto a sinistra). Trovi l'OCID tenancy (il tenant principale, es. ocid1.tenancy.oc1..aaaaaaa...). Regione: Scegli la regione del tuo OCI (es. eu-frankfurt-1, us-ashburn-1, etc). Lo trovi nella parte superiore destra della console o in Governance & Administration > Regions. Realm: Di solito oc1 per la maggior parte dei tenant pubblici OCI. Puoi verificarlo nella documentazione o da CLI se necessario.

Riassunto dei parametri e dove reperirli

Parametro Dove trovarlo / come ottenerlo Ocid Utente Identity > Users > seleziona utente > OCID Fingerprint Identity > Users > API Keys > fingerprint Ocid Tenant Identity > Tenancy > OCID Regione In alto a destra della console (es. eu-frankfurt-1) Realm Generalmente oc1 (standard OCI realm) Key File Chiave privata .pem generata al momento dell'API Key

#### 2.0.1.2.13 PARAMETRI ORACLEEXACC

Funzionalità abilitate:

- Recupero elementi di catalogo
- Recupero elementi di inventario
- Recupero dei costi delle risorse
- Recupero delle informazioni di sicurezza

I parametri specifici del sottosistema OracleExAcc da inserire sono esposti nella tabella:

Figura 31 – Maschera di configurazione

OracleExAcc

Vengono indicati con \* i parametri obbligatori

Nome	Tipo	Descrizione	Esempio
username *	string	Il nome utente utilizzato per l'autenticazione con OCI.	ocid5.user.oc77.aaabnbthaj6pnvsb2g qnaaaait3mqzekefmlhwkige2wxna6h faj3f6njma
fingerprint *	string	È un valore univoco che identifica il dispositivo, utilizzato per l'autenticazione con OCI.	6a:f4:6e:9a:73:95:27:d5:64:8d11:a3:f5 :0e:fb:f4:
tenantId *	string	L'ID del tenant OCI a cui ci si vuole connettere	ocid5.tenancy.oc77...aaabnbthaj6pnvs b2gqnaaaait3mqzekefmlhwkige2wxn a6hfaj3f6njma
region *	string	La regione È la posizione geografica specifica in cui si trovano le risorse OCI.	eu-dcc-rome-1
Private key *	password	un file PEM che contiene la chiave pubblica e privata utilizzata per l'autenticazione.	" -----BEGIN PRIVATE KEY-----MIIJQ gIBADANBâ€¦"
catalogPriceDiscount	integer	Inserisci qui uno sconto/maggiorazione da applicare sui prezzi del catalogo per tutte le risorse che non hanno una relazione SCMP	-10
odlId	string	Inserisci qui l'id dell'ordine di lavoro che verrà associato al sottosistema e verrà inserito come tag su tutte le risorse del sottosistema	ODL001
dataFirstCostRecover	int	Inserire il numero di giorni precedenti alla data di creazione dei quali bisogna recuperare i costi al primo avvio del sottosistema	15

#### 2.0.1.2.14 PARAMETRI VCLOUD

Funzionalità abilitate:

- Recupero elementi di catalogo
- Recupero elementi di inventario
- Recupero delle metriche di utilizzo
- Recupero dei costi delle risorse
- Recupero delle informazioni di sicurezza



I parametri specifici del sottosistema VCloudDirector da inserire sono esposti nella tabella

Figura 32 – Maschera di configurazione  
VCloudDirector

Vengono indicati con \* i parametri obbligatori

Nome	Tipo	Descrizione	Esempio
url *	string	l'indirizzo del server VCloudDirector a cui ci si vuole connettere	https://url.westeurope.com/tenant/org-zzg-435832
tenantId *	string	L'ID del tenant del VCloudDirector Ã l'identificatore univoco del tenant a cui ci si vuole connettere.	org-zzg-435832
Use providerPermission	boolean	Da attivare se l'utenza ha tutte le autorizzazioni a livello provider , non attivandola non vengono recuperate tutte le informazioni ma delle sole organization abilitate	true
token *	password	Il token di autenticazione per il VCloudDirector Ã una stringa segreta che viene utilizzata per autenticare l'utente con il VCloudDirector	aesZo6LextKTQx92VoRpyzaesZo6LextKT
Location	String	Inserire la regione di appartenenza delle risorse VCloudDirector	Eu west
Location	string	inserire la posizione geografica del sistema	OnPremise
catalogPriceDiscount	integer	Inserisci qui uno sconto/maggiorazione da applicare sui prezzi del catalogo per tutte le risorse che non hanno una relazione SCMP	5
odlId	string	Inserisci qui l'id dell'ordine di lavoro che verrÃ associato al sottosistema e verrÃ inserito come tag su tutte le risorse del sottosistema	ODL001

#### 2.0.1.2.15 PARAMETRI VMWARE

Funzionalità abilitate:

- Recupero elementi di catalogo
- Recupero elementi di inventario
- Recupero delle metriche di utilizzo
- Recupero dei costi delle risorse
- Recupero delle informazioni di sicurezza

- Provisioning di risorse
- Provisioning di servizi
- Provisioning di blueprint complesse

I parametri specifici del sottosistema VMWare da inserire sono esposti nella tabella:

*Figura 33 – Maschera di configurazione  
VMWare*

Vengono indicati con \* i parametri obbligatori

Nome	Tipo	Descrizione	Esempio
clientId *	string	L'ID univoco del client che si connette al sottosistema Azure Cloud. Questo ID viene utilizzato per identificare il client e per autorizzare l'accesso alle risorse del sottosistema.	5a85c16c6ad-49db -a58e-e209-ee11f5 3d6c6b
clientSecret *	password	La chiave segreta del client, utilizzata per autenticare il client con il sottosistema Azure Cloud. La chiave segreta deve essere tenuta segreta e non deve essere condivisa con nessuno.	np6Kc_.xwsvhR8Q ~rP05fCqYNXmbqf MGQLOEzfMt
tenantId *	string	L'ID del tenant Azure a cui appartiene il sottosistema Azure Cloud. Il tenant Ã un'entitÃ organizzativa in Azure che rappresenta un'azienda o un'organizzazione.	884147733-ff13-47 83-a765-83418377 3083
subscriptionId *	string	L'ID della sottoscrizione Azure utilizzata per accedere al sottosistema Azure Cloud. La sottoscrizione Ã un contratto per l'utilizzo dei servizi Azure.	884147733-ff13-47 83-a765-83418377 3083
usageAggregation	boolean	Indica se l'aggregazione per "usage" Ã abilitata per la sottoscrizione. Quando questa spunta viene abilitata i costi del sottosistema verranno raggruppati per Tipologia risorsa	false
catalogPriceDiscount	integer	Inserisci qui uno sconto/maggiorazione da applicare sui prezzi del catalogo per tutte le risorse che non hanno una relazione SCMP	5
odlId	string	Inserisci qui l'id dell'ordine di lavoro che verrÃ associato al sottosistema e verrÃ inserito come tag su tutte le risorse del sottosistema	ODL001
daysFirstCostRecover	int	Inserire il numero di giorni precedenti alla data di creazione dei quali bisogna recuperare i costi al primo avvio del sottosistema	15

Per i provider on Premise, in particolare, vengono richiesti dati sulla capacitÃ della infrastruttura, in modo tale che la SCMP possa effettuare dei calcoli preliminari in molteplici scenari.

Per esempio, durante il provisioning, in modo tale da non superare la capacità massima consentita del provider.

### 2.0.1.3 Folders

#### 2.0.1.3.1 AZURE FOLDER

Per consentire alla SCMP di sfruttare tutte le potenzialità offerte dal provider "Azure" stata inserita la possibilità di configurare delle "Folders"

Durante la creazione di un provider selezionando la tipologia "Azure" possiamo notare la presenza di un campo esclusivo per il provider :

- Un box di conferma per indicare alla SCMP se il provider in inserimento "una "Folder".

Figura 34 – Opzione folder Azure

I parametri specifici del sottosistema Azure da inserire sono esposti nella tabella seguente:

Figura 35 – Maschera di configurazione  
Azure Folder

Vengono indicati con \* i parametri obbligatori

Nome	Tipo	Descrizione	Esempio
clientId *	string	L'ID univoco del client che si connette al sottosistema Azure Cloud. Questo ID viene utilizzato per identificare il client e per autorizzare l'accesso alle risorse del sottosistema.	5a85c16c6ad-49db -a58e-e209-ee11f5 3d6c6b
clientSecret *	password	La chiave segreta del client, utilizzata per autenticare il client con il sottosistema Azure Cloud. La chiave segreta deve essere tenuta segreta e non deve essere condivisa con nessuno.	np6Kc_.xwsvhR8Q ~rP05fCqYNXmbqf MGQLOEzfMt
tenantId *	string	L'ID del tenant Azure a cui appartiene il sottosistema Azure Cloud. Il tenant "un'entità organizzativa in Azure che rappresenta un'azienda o un'organizzazione.	884147733-ff13-47 83-a765-83418377 3083
usageAggregation	boolean	Indica se l'aggregazione per "usage" è abilitata per la sottoscrizione. Quando questa spunta viene abilitata i costi del sottosistema verranno raggruppati per Tipologia risorsa	false
catalogPriceDiscount	integer	Inserisci qui uno sconto/maggiorazione da applicare sui prezzi del catalogo per tutte le risorse che non hanno una relazione SCMP	5

Nome	Tipo	Descrizione	Esempio
odlID	string	Inserisci qui l'id dell'ordine di lavoro che verr� associato al sottosistema e verr� inserito come tag su tutte le risorse del sottosistema	ODL001
daysFirstCostRecover	int	Inserire il numero di giorni precedenti alla data di creazione dei quali bisogna recuperare i costi al primo avvio del sottosistema	15

#### 2.0.1.3.2 GOOGLE CLOUD FOLDERS

Per consentire alla SCMP di sfruttare tutte le potenzialit  offerte dal provider "Google Cloud"   stata inserita la possibilit  di configurare delle "Folders" e la possibilit  di importare il file generato dalla console del provider cos  da semplificare l'inserimento dello stesso.

Durante la creazione di un provider selezionando la tipologia "Google Cloud" possiamo notare la presenza di 2 campi esclusivi per il provider:

1. Un box di conferma per indicare alla SCMP se il provider in inserimento   una "Folder".
2. Un box dove, cliccando all'interno sar  possibile, tramite la finestra di selezione file di windows inserire il file di tipo "JSON" esportato direttamente dalla console Google.

Figura 36 – Parametri specifici di  
Google Cloud

I parametri specifici della Google Folder da inserire sono esposti nella tabella:

Nome	Tipo	Descrizione	Esempio
serviceAccount	object	File di connessione generato dalla console Google	service_account.json
costExportDatasetID	string	Inserire l'id del dataset da utilizzare per il recupero delle informazioni	ProjectId.dataset.table
usageAggregation	boolean	Indica se l'aggregazione per "usage" � abilitata per la sottoscrizione. Quando questa spunta viene abilitata i costi del sottosistema verranno raggruppati per Tipologia risorsa	false
Cost from USD Currency	Boolean	Indica se il costo finale � calcolato dal prezzo in USD o EUR	true
providerPriceDiscount (solo se costFromUSDCurrency � true)	integer	Inserisci qui uno sconto/maggiorazione da applicare sui prezzi in USD del provider per tutte le risorse	30



Leonardo Cyber & Security Solutions

21 Oct 2025

08.00

Secure Cloud Management Platform

Nome	Tipo	Descrizione	Esempio
Cost cross project	Boolean	Indica se recuperare i costi di tutti i progetti dell'account di fatturazione o solamente del progetto corrente	true
catalogPriceDiscount	integer	Inserisci qui uno sconto/maggiorazione da applicare sui prezzi del catalogo per tutte le risorse che non hanno una relazione SCMP	-20
odlID	string	Inserisci qui l'id dell'ordine di lavoro che verrà associato al sottosistema e verrà inserito come tag su tutte le risorse del sottosistema	ODL001
daysFirstCostRecover	int	Inserire il numero di giorni precedenti alla data di creazione dei quali bisogna recuperare i costi al primo avvio del sottosistema	15

#### ■ Abilitazioni obbligatorie

I seguenti servizi devono essere abilitati sul service account utilizzato:

- bigquery.googleapis.com
- cloudresourcemanager.googleapis.com
- cloudasset.googleapis.com
- cloudbilling.googleapis.com
- compute.googleapis.com
- container.googleapis.com
- monitoring.googleapis.com

Il campo "ServiceAccount" può essere inserito automaticamente effettuando l'upload del file o manualmente inserendo i campi disponibili nel form.

Dopo aver configurato un sistema di tipo "Folder" esso verrà visualizzato sia nella lista dei cloud provider, sia nella pagina delle folder.

Figura 37 – Visualizzazione delle folder

Dalla pagina di "Cloud System" del modulo di "Administration" cliccare in alto a destra il tab "Folders" dove verrà visualizzata la lista delle folder configurate nel tenant.

All'interno della pagina è possibile effettuare le stesse operazioni di visualizzazione modifica e eliminazione delle folder effettuate sulla pagina dei "Cloud Provider".

Figura 38 – Accesso a Folders

Accedendo ad una “Folder” in modalità “View” scorrendo in basso nella pagina possiamo visualizzare la lista dei sottosistemi presenti nel provider e le relative informazioni sullo status:

- In verde possiamo notare un sottosistema configurato correttamente nel provider e che la SCMP provvede ad inserire automaticamente nel sistema e sarà visibile nella sezione “Cloud Providers” e in tutte le funzionalità della SCMP.
- In rosso possiamo notare un sottosistema configurato in maniera errata che, dopo le opportune modifiche dalla console di “Google Cloud”, potrà essere accettato dalla SCMP.

Figura 39 – Visualizzazione  
sottosistemi della Folder

## 2.0.2 SIEM

L’utente può creare un provider di tipo SIEM, cliccando sul tab che raffigura uno scudo, posizionato nella barra in alto, dopo aver effettuato l’accesso alla pagina “Cloud SIEMs”, in alto a destra, cliccare sull’hamburger menu e poi cliccare su “Attach a SIEM”

Figura 40 – Creazione di un cloud  
provider SIEM

All’interno della pagina “Add SIEM”, compilare tutti i campi della sezione “General properties”. Dopo aver fatto questo, compilare tutti i campi della sezione “SIEM’s properties” seguendo la tabella:

Figura 41 – Compilazione del form per  
la creazione di un provider SIEM

Vengono indicati con \* i parametri obbligatori

Nome	Tipo	Descrizione	Esempio
clientId *	string	Identificativo univoco del SIEM al quale connettersi, Fornito dal SIEM durante la registrazione dell'applicazione	1b16698f-2df5-ed44-86b9e-d-4b42c 1fe7ad9
clientSecret *	password	Il secret da utilizzare per la connessione, fornito dal SIEM durante la registrazione dell'applicazione	1b16698f-2df5-ed44-86b9e-d-4b42c 1fe7ad9
resourceGroup *	string	Il gruppo di risorse Azure in cui è ospitato il SIEM	myGroup

Nome	Tipo	Descrizione	Esempio
subscriptionId *	string	L'ID sottoscrizione Azure associata al SIEM	1b16698f-2df5-ed44-86b9e d-4b42c 1fe7ad9
tenantId *	string	L'ID tenant Azure associato al SIEM	1b16698f-2df5-ed44-86b9e d-4b42c 1fe7ad9
workspaceID*	string	L'ID dell'area di lavoro Log Analytics associata al SIEM	1b16698f-2df5-ed44-86b9e d-4b42c 1fe7ad9
workspaceName*	string	Il nome dell'area di lavoro Log Analytics associata al SIEM	theWorkspaceName

Infine, in basso a destra, cliccare sul pulsante "Save". Dopodich , in basso appare un popup di avvenuta creazione del SIEM e l'utente viene reindirizzato all'interno della lista dei SIEM.

#### 2.0.2.1 Visualizzazione, modifica ed eliminazione

Per visualizzare un SIEM, in corrispondenza di un suddetto, cliccare sul kebab menu e poi cliccare su "Show". A questo punto, l'utente si ritrova all'interno della pagina "Show SIEM" in cui   possibile visualizzare ma non modificare i dati. Dopo aver visualizzato i dati, in basso a destra, cliccare sul pulsante "Close". Fatto questo, l'utente si ritrova all'interno della lista dei SIEM.

Figura 42 – Accesso al SIEM in  
modalit  visualizzazione

Figura 43 – SIEM in modalit   
visualizzazione

Per modificare un SIEM, in corrispondenza di un suddetto, cliccare sul kebab menu e poi cliccare su "Edit". A questo punto, ci si ritrova all'interno della pagina "Edit SIEM" in cui   possibile modificare i campi.

Dopo aver modificato i campi di interesse, in basso a destra, cliccare sul pulsante "Update". Fatto ci , in basso appare un popup di avvenuta modifica del SIEM e l'utente si ritrova all'interno della lista dei SIEM.

Figura 44 – Accesso al SIEM in  
modalit  edit

Figura 45 – SIEM in modalit  edit

Per eliminare un SIEM, in corrispondenza di un suddetto, cliccare sul kebab menu e poi cliccare su *Delete*. A questo punto appare una modale in cui è necessario cliccare sul pulsante *Remove*. Fatto questo, il SIEM non è più presente all'interno della lista.

*Figura 46 – Opzione per eliminare un SIEM "Delete"*

*Figura 47 – Conferma per eliminare un SIEM*

## 2.0.3 Secrets Managers

L'utente può creare un secret manager cliccando sul tab che raffigura un lucchetto, posizionato nella barra in alto, come mostrato in figura

Dopo aver effettuato l'accesso alla pagina *Secret manager*, in alto a destra, cliccare sull'hamburger menu e poi cliccare su *Add a secret manager*

*Figura 48 – Aggiunta di un nuovo Secret Manager*

Qui un esempio di form nel caso di aggiunta di un Secret manager dal provider di tipo Azure (selezionabile dal dropdown *Type* in alto nella pagina).

Dopo aver inserito tutti i parametri richiesti, in basso, cliccare il tasto *Save* per concludere l'inserimento e l'utente viene reindirizzato alla lista dei *Secret manager* dove è possibile visualizzare il componente appena creato.

### 2.0.3.1 Azure key vault

I parametri specifici per un Azure key vault da inserire sono esposti nella tabella:

*Figura 49 – Maschera di configurazione Azure key vault*

Vengono indicati con \* i parametri obbligatori

Nome	Tipo	Descrizione	Esempio
clientId *	string	Identificativo univoco del key vault	09f8985-9f89d0-4623-98982-5a510fd3d2



Nome	Tipo	Descrizione	Esempio
clientSecret *	password	Una chiave segreta utilizzata per autenticare l'applicazione con il Key Vault	np6Kc_xwsvhR8Q~rP05fCqYNXmbqfMGQLOEzfMt
resourceGroup *	string	Il gruppo di risorse Azure in cui Ã ospitato il Key Vault	resoruceGroupName
subscriptionId *	string	L'ID sottoscrizione Azure associata al Key Vault	09f8985-9f89d0-4623-98982-5a510fd3d2
tenantId	string	L'ID tenant Azure associato al Key Vault	09f8985-9f89d0-4623-98982-5a510fd3d2
privateUrl	string	URL privato di accesso al key Vault	https://vault.azure.net/vault

Tabella 25 – Campi specifici Azure key vault

### 2.0.3.2 Google Secret Manager

I parametri specifici del Google Secret Manager da inserire sono esposti nella tabella seguente:

*Figura 50 – Maschera di configurazione  
Google Secret Manager*

Vengono indicati con \* i parametri obbligatori

Nome	Tipo	Descrizione	Esempio
kmsProjectId *	string	l'ID del progetto Google Cloud Platform (GCP) associato al servizio Google Cloud Key Management Service (KMS).	5a85c16c6ad-49db-a58e-e209-ee11f53d6c6b
serviceAccount *	object	File di connessione generato dalla console Google	service_account.json

Ã possibile inserire manualmente sul form visualizzato i parametri presenti nel file æservice\_account.jsonæ se non si vuole effettuare l'upload, tutti i parametri sono obbligatori:

Nome	Tipo	Descrizione	Esempio
Type	string	Inserire il nome della tipologia di autenticazione configurata	service_account
project_id *	string	Inserisci qui l'id univoco del progetto associato al service account	Theproject-367810

Nome	Tipo	Descrizione	Esempio
private_key_id *	string	Inserisci qui l'id univoco della chiave privata del service account	55cb5cf903ee93ea1e9c294a07e46e0af0633e6
private_key *	password	Contiene la chiave privata del service account in formato PEM. È fondamentale per l'autenticazione del service account alle API di Google Cloud	-----BEGIN PRIVATE KEY-----MIJQgIBADANBâ€¦
client_email *	string	L'indirizzo email univoco del service account. È utilizzato per identificare il service account quando si autentica alle API di Google Cloud	user@dominio.com
client_id *	string	L'ID client del service account. È un identificatore univoco utilizzato per identificare il service account in Google Cloud	104822473261100667392
auth_uri *	string	L'URI utilizzato per l'autenticazione del service account alle API di Google Cloud	https://accounts.google.com/o/oauth2/auth
token_uri *	string	L'URI utilizzato per ottenere un token di accesso per il service account	https://oauth2.googleapis.com/token
auth_provider_x509_cert_url*	string	L'URL del certificato X.509 utilizzato per l'autenticazione del service account	https://www.googleapis.com/oauth2/v1/certs
client_x509_cert_url *	string	L'URL del certificato X.509 nel client	https://www.googleapis.com/robot/v1/metadata/f543/myserviceaccount%40projectName.gserviceaccount.com

### 2.0.3.3 Visualizzazione, modifica ed eliminazione di un sistema

È possibile visualizzare i dati di un Secret manager, all'interno della lista, cliccando sul kebab menu in corrispondenza di un manager, e successivamente su "Show".

*Figura 51 – Accesso al manager in modalità visualizzazione*

In questa pagina è possibile visualizzare la configurazione del Provider.

*Figura 52 – manager in modalità visualizzazione*

Per tornare alla pagina dei Secret manager, in basso a sinistra, cliccare sul pulsante "Close".

A questo punto, l'utente si ritroverà all'interno della pagina dei Secret manager.

Per modificare i dati di un Secret manager all'interno della lista, cliccare sul kebab menu in corrispondenza di un Cloud Provider, e cliccare su "Edit".

---

*Figura 53 – Accesso al manager in  
modalità edit*

Fatto ciò, l'utente si ritroverà all'interno della pagina del Cloud Provider in modalità edit in cui è possibile modificare i dati. Per tornare alla pagina dei Cloud Provider, in basso a sinistra, cliccare sul pulsante "Save". A questo punto, l'utente si ritroverà all'interno della pagina dei Cloud Provider.

Per eliminare un "Secret manager", all'interno della lista, cliccare sul kebab menu in corrispondenza di un Secret manager, e cliccare su "Delete".

---

*Figura 54 – Avvio per l'eliminazione di  
un Secret manager*

Fatto ciò, apparirà una modale in cui è necessario cliccare sul pulsante "Remove".

---

*Figura 55 – Conferma eliminazione del  
Secret manager*

A questo punto, il Secret manager non sarà più presente all'interno della lista e verrà lanciato il flusso di rimozione asset sul resource-manager.

## 2.0.4 Backup

Viene data la possibilità all'utente di inserire all'interno della SCMP una connessione con un CommVault per permettere successivamente il recupero e la visualizzazione delle informazioni relative ai backup e alle operazioni effettuate dal Vault.

Per accedere a questa funzionalità è necessario selezionare il tab "CommVault" disponibile in alto nella funzionalità "Administration".

Verremo riportati alla pagina che contiene la lista di tutti i "CommVault" configurati e cliccando sul menù<sup>1</sup> presente sulla destra sarà possibile aggiungere un nuovo CommVault

*Figura 56 – Accesso a CommVault*

In questa pagina , dopo aver inserito le credenziali di accesso (indirizzo ip, utenza e password) possiamo cliccare sul pulsante “Test connection” per confermare il corretto inserimento dei dati e successivamente confermare l’inserimento tramite il pulsante “Save”.

---

*Figura 57 – Creazione della  
connessione ad un CommVault*

## 2.0.5 Confidential computing

Nella sezione di Confidential Computing viene data la possibilità all’utente di inserire all’interno della SCMP una connessione ad un servizio di “Remote Attestation” per il controllo e la visualizzazione delle informazioni relative allo stato di confidenzialità delle macchine gestite dal servizio

Per accedere a questa funzionalità è necessario selezionare il tab “Confidential computing” disponibile in alto nella funzionalità “Administration” .

Verremo riportati alla pagina che contiene la lista di tutti i servizi di “Remote attestation” configurati e cliccando sul menù<sup>1</sup> presente sulla destra sarà possibile aggiungere una nuova connessione .

---

*Figura 58 – Accesso a Confidential  
Computing*

In questa pagina , dopo aver inserito le credenziali di accesso (indirizzo ip, utenza e password) possiamo cliccare sul pulsante “Test connection” per confermare il corretto inserimento dei dati e successivamente confermare l’inserimento tramite il pulsante “Save”.

---

*Figura 59 – Creazione della  
connessione ad un servizio  
“Remote Attestation”*