

14 Oct 2025

08.00

Secure Cloud Management Platform

NON CLASSIFICATO Company internal

Informazioni a diffusione esclusiva

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

## Contatti

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

**Lista delle Revisioni**

| <b>Rev.</b> | <b>Numero Modifiche</b> | <b>Data</b> | <b>Descrizione</b>               | <b>Autore</b> |
|-------------|-------------------------|-------------|----------------------------------|---------------|
| 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      |

14 Oct 2025

08.00

Secure Cloud Management Platform

NON CLASSIFICATO Company internal

Informazioni a diffusione esclusiva

Table of Contents

## 1 Welcome to the Documentation

This is the home page of the English documentation.

### 1.1 Getting Started

Welcome to our comprehensive documentation. This guide will help you get started with our platform and understand its key features.

### 1.2 Quick Navigation

- [Developer Documentation](#) - Technical guides and API documentation
- [Support Resources](#) - Links to help and support

### 1.3 Features

Our platform offers a wide range of features designed to help you succeed:

- **Easy Integration** - Simple APIs and SDKs
- **Scalable Architecture** - Built to grow with your needs
- **Comprehensive Documentation** - Everything you need to know
- **24/7 Support** - We're here to help

### 1.4 What's New

Stay up to date with the latest features and improvements to our platform.

For more information, please refer to our [developer documentation](#) or visit our [support portal](#).

### 3 Administration

The Administration feature is the basis for using the SCMP.

The providers included within this feature will be used by the system to retrieve all necessary information.

Within the functionality will be possible:

- Configure the cloud providers that can be used in the Reference Tenant.
- Configure the folders of the various providers.
- Configure SIEM Clouds from various providers.
- Configure the KeyVaults of the various providers.
- Configure the CommVaults for Backup and Disaster & Recovery of the various providers.
- Confidential Computing for the various providers.

#### 3.0.1 provider/subsystems

##### List of subsystems

To access the Administration feature, at the top left click on the bento button. After that, click on "Administration"

□

*Figura 1 – Access to Administration functionality*

At this point, the user finds himself within the tab page "Cloud Systems", where we can view general information about subsystems, such as the reference provider and the date of creation of the subsystem and is also indicated with a red check if the system is on-premise type. 2 We can note that in the list there are "folders", subsystem containers, clicking at the "fresh" on the folder line we can view the subsystems inside and their information

□

*Figura 2 – List of subsystems and folders*

In addition, for each subsystem a status is available, represented by a colored "led":

- Green: it works correctly in the SCMP "status: ok".
- Red: the subsystem is no longer usable by the SCMP "status : failed".

The SCMP periodically performs connection tests on all configured subsystems, when a subsystem fails this control, the status of the subsystem is updated and all data recovery processes are disabled (costs, inventory, monitoring, security).

This may happen, for example when the secret or passwords used to connect expire and must be renewed. Going to change the subsystem you can insert the new connection parameters to restore the correct functioning, which will be confirmed by the status "OK"

##### \*\* INFORMATION ON SUBSYSTEM CRON-JOB\*\*

Each tenant performs, during the day, several information recovery operations available for all configured subsystems, so that the user can view all the necessary data using the SCMP only.

To view the outcome of these operations, click on the subsystem line and inside the modal select the "Show discovery info" button

In addition to the amount of operations and their outcome, scrolling down you can view the list and its details by clicking the "cold" at the time of the operation concerned.

□

*Figura 3 – About cron-job*

##### VIEW, EDIT AND DELETE A SUBSYSTEM

To view the data of a Cloud Provider, within the list, click on the kebab menu at the Cloud Provider of Interest and click on "Show".

□

*Figura 4 – Access to the Cloud Provider in display mode*

On this page you can view the configuration of the Provider

□

*Figura 5 – Subsystem in display mode*

If the provider is of "ON-PREMISE" type under the configuration will be visible a table showing the usable capabilities on the system and the list of resources already present in the subsystem

□

*Figura 6 – On-Premise machine list*

To return to the Cloud Provider page, click on the "Close" button.

To change the data of a Cloud Provider, within the list, click on the kebab menu at a Cloud Provider, and click on "Edit"

□

*Figura 7 – Cloud Provider access in edit mode*

This is done, the user will find himself inside the Cloud Provider page in "edit" mode, which allows you to change the data.

To return to the Cloud Provider page, click on the "Save" button on the left. At this point, you will find yourself on the Cloud Provider page.

□

*Figura 8 – Start for deleting a Cloud Provider*

To delete a Cloud Provider, within the list, click on the kebab menu at a Cloud Provider, and click on "Delete"

□

*Figura 9 – Cloud Provider Deletion Confirmation*

## Secure Cloud Management Platform

## NON CLASSIFICATO Company internal

## Informazioni a diffusione esclusiva

Done that, a modal will appear where you need to click on the "Remove" button

At this point, the Cloud Provider will no longer be present within the list and the asset removal flow will be launched on the resource-manager.

#### ON-PREMISE PROVIDER COST MODEL

To manage the costs of using resources for the "On-Premise" providers, you can define a specific cost model by subsystem.

The cost model allows you to configure both the costs "provider" i.e. the ones actually incurred and then apply a discount or reload percentage to be applied to the customer.

Providers using this feature are:

- VMWare
- VCloud Director
- RedHat Edge
- OpenShift

To change the model, click the "three points" button at a subsystem and select the "Cost model" item.

□

*Figura 10 – Access to subsystem cost model*

On the model page we find a first generic section where you can configure the fields:

- Currency: the reference currency to be used for the subsystem.
- Discount/Surcharge: a discount or recharge rate to be applied to customer costs.

□

*Figura 11 – Cost model*

After clicking the "Add rate" button will open a modal in which, after choosing a metric (specific for the provider) and the relative unit of measurement to be used, the price will be inserted to all the elements of the subsystem, finally click the "Save" button to confirm the insertion.

□

*Figura 12 – Selection of the metric to be presed*

To confirm the change to the model after entering all costs for each type of component available, click the "Apply" button below.

□

*Figura 13 – Complete cost model*

#### MANUAL COST UPDATE

The user is given the possibility to carry out a manual updating of the costs in case of necessity, this asynchronous operation can be requested individually by subsystem or globally on the whole tenant, which is automatically propagated on all available subsystems.

To request the update of a single subsystem click the "three points" button on the subsystem line and select the "Refresh Cost" entry

□

*Figura 14 – Manual cost update*

Within the modal we can indicate for how many days, starting from today's date, the costs of the selected subsystem must be repaid and confirmed. After confirming, we can go to the "cron-job info" section to confirm the operations.

You can also request the upgrade of costs for the whole tenant: by clicking first on the "hamburger menu" button available on the top left and selecting the "refresh cost", the activity will be distributed on all subsystems available on the page

□

*Figura 15 – Update of costs on all tenant*

Once you select a cost recovery you can indicate the number of days to recover and selecting the box "Reset the cost" the SCMP will first perform a data cleaning (of its selected range) and then refresh

□

*Figura 16 – Configuration of refresh costs*

#### COST RECOVERY AND CALCULATION PROCESS

##### Cost recovery structure

The cost recovery process is carried out by the "Abstraction Layer" module, this module consists of:

- An ABS sub-module called "layer" for each type of provider (e.g. "CMP-ABS-VMWare-layer")
- ABS Gateway: is the sub-module that manages the communication and homologation of the information recovered from the various Layers of the different providers and makes them available for the other modules of the SCMP system.

The cost recovery process is carried out by a cron-job, which is launched once per provider, automatically during night hours.

For ON-Premise providers are automatically generated by the SCMP of usage values based on the amount of resources available in inventory using the same "ABS" modules. Subsequently, as with high providers, usage values will be used to calculate costs through the cost model described in the Administration section.

In the event of failure, the process is automatically unscheduled until 3 attempts are reached. If the system fails to resolve automatically, manual intervention is required. In addition, you can request a manual cost update using the buttons available in the Administration section.

Below the specific details for subsystem type

##### Recovery and calculation of customer costs for the Azure provider

##### Recovery mode:

- **Standard model:** The ABS module requires the REST APIs made available by Azure for the last 2 days that are saved within the SCMP database.

- **Storage Account template:** The ABS module recovers a file that contains the cost extracts made divided by subsystem, they are saved inside the SCMP database.
- **Billing storage model:** the ABS module recovers a file that contains the extracts of all subscriptions available in the "billing account", the results are divided by subsystem and saved on the database

\*\* Cost calculation per resource:\*\*\*

1. The ABS module sends the cost information to the module and the information about the resource that generated them.
2. The cost module verifies the subsystem configuration to identify the "aggregation typology", this parameter indicates which catalog to use ( RESOURCES. o SKU:) so as to correctly calculate the price
3. The cost module checks whether the resource identifier (UUID) is present in the SCMP catalogue, if present the system multiplies usage by the catalog cost
4. If the resource is not listed (then it does not fall within the previous step) the SCMP will apply the percentage of discount/restrict configured in the subsystem

**Recovery and calculation of customer costs for the AWS provider**

- **Standard model:** The ABS module interrogates AWS Cost Explorer APIs to get the costs of the last 2 days, saving data within the SCMP database.
- **\*\* Model "ARN ROLE":** The ABS module assumes a specific IAM role ( #)) to access AWS billing data. The costs are extracted and subdivided by subsystem, then saved in the SCMP database.

\*\* Cost calculation per resource:\*\*\*

1. The ABS module sends the cost information to the module and the information about the resource that generated them.
2. The cost module verifies the subsystem configuration to identify the "aggregation typology", this parameter indicates which catalog to use ( RESOURCES o SKU:) so as to correctly calculate the price
3. The cost module checks whether the resource identifier (UUID) is present in the SCMP catalogue, if present the system multiplies usage for the catalog cost.
4. If the resource is not listed (then it does not fall within the previous step) the SCMP will apply the percentage of discount/restrict configured in the subsystem

**Recovery and calculation of customer costs for the Google provider**

- **Standard model:** The ABS module questions Google Cloud Billing APIs to get the costs of the last 2 days, saving data within the SCMP database.
- **Dataset Export model:** The ABS module accesses billing data exported by **BigQuery**. Costs are extracted, subdivided by subsystem and saved in the SCMP database.

\*\* Cost calculation per resource:\*\*\*

1. The ABS module sends the cost information to the module and the information about the resource that generated them.
2. The cost module verifies the subsystem configuration to identify the "aggregation typology", this parameter indicates which catalog to use ( RESOURCES o SKU:) so as to correctly calculate the price
3. If the "Cost from USD" field has been selected, the system will use for calculating the price in USD (refunded by the provider), to which a discount/recharge rate defined in the administration section, otherwise the price already converted to EUR is used.
4. The cost module checks whether the resource identifier (UUID) is present in the SCMP catalogue, if present the system multiplies usage for the catalog cost.
5. If the resource is not listed (then it does not fall within the previous step) the SCMP will apply the percentage of discount/restrict configured in the subsystem

**Recovery and calculation of customer costs for Oracle, OracleEXAcc providers**

- **Standard model:** The ABS module questions the ORACLE API to get the costs of the last 2 days, saving the data within the SCMP database.

\*\* Cost calculation per resource:\*\*\*

1. The ABS module sends the cost information to the module and the information about the resource that generated them.
2. The cost module verifies the subsystem configuration to identify the "aggregation typology", this parameter indicates which catalog to use ( RESOURCES o SKU:) so as to correctly calculate the price
3. If the "Cost from USD" field has been selected, the system will use for calculating the price in USD (refunded by the provider), to which a discount/recharge rate defined in the administration section, otherwise the price already converted to EUR is used.
4. The cost module checks whether the resource identifier (UUID) is present in the SCMP catalogue, if present the system multiplies usage for the catalog cost.
5. If the resource is not listed (therefore it does not fall within the previous step) the SCMP will apply the percentage of discount/recharge configured in the subsystem

**Customer cost recovery and calculation for Kubernetes, OpenShift, vcloudDirector, VMWare, Red Hat Edge providers**

- **Standard model:** The ABS module generates 24-hour Usage data for all available resources in the inventory, as providers are On-Premise and resources are all allocated to the customer.

\*\* Cost calculation per resource:\*\*\*

1. The ABS module sends the cost information to the module and the information about the resource that generated them.
2. the SCMP will apply the percentage of discount/recharge configured in the cost model

#### Creating new subsystem

To insert a new subsystem inside the portal, click on the "menu" available at the top right and select "+ Add new cloud provider"

□

*Figura 17 – Adding a new Cloud Provider*

The user displays the basic data of the subsystem to be entered, explained below.

#### \*PARAMETERS SHARED BETWEEN PROVIDERS

Within the creation page we can see 3 fields:

- Name: indicates the name that will be displayed to indicate the subsystem.
- Type: indicates the type of cloud provider to which the subsystem belongs.
- Version: the subsystem provider version to install.

□



Figura 18 – General parameters of a subsystem

After selecting the type and version of the system, the mask is updated to display the specific parameters according to the selected provider, since each of them manages authentication and resources differently.

All providers require authentication, which can vary according to the system, for asset recovery.

This sensitive information, such as passwords or certificates, is securely saved on an infrastructure element that deals with data security <https://www.vaultproject.io/>.

**VERIFICATION OF CONNECTION AND RESCUE, SHARED BETWEEN PROVIDERS**

For all subsystems are available at the bottom of page 3 buttons

The “Close” button that allows to cancel the insertion of a new subsystem.

The “Test Connection” key serves to carry out a connection test using the parameters inserted, in case of errors the system returns an error message that indicates “Error: Unauthorized system” and the button becomes red, otherwise the button will become green and you can save the subsystem using the “Save” button.

Figura 19 – Connection buttons

On the rescue, the SCMP will communicate to the module that manages that type of provider, to load inside our bus (Kafka) all items related to inventory, metrics, costs and security elements.

The same module, it will then scan jobs for the periodic update of all the assets present.

After saving, a modal will appear that informs the user that you cannot delete a cloud provider before 24 hours. From the modal, click on “OK”. After doing so, the user finds himself on the Cloud Provider page.

**\*AMAZON WEB SERVICES**

Enabled features:

- Catalogue element recovery
- Recovery of inventory items
- Recovery of use metrics
- Recovery of resources costs
- Recovery of security information
- Provisioning resources
- Provisioning services
- Provisioning complex blueprints

The specific parameters of the Amazon Web Services subsystem are shown in the table:

Figura 20 – Amazon Web Services configuration mask

The mandatory parameters are indicated with \*

| Nome   | Tipo     | Descrizione   | Esempio                                 |
|--|----------|---|---|
| AccessKey *  | string   | La chiave di accesso AWS è una stringa alfanumerica che identifica l'utente AWS.  | ZYKZGVAKIS4YK5IXCAXB                    |
| SecretKey *  | password | La chiave di accesso segreta AWS è una stringa alfanumerica che viene utilizzata per autenticare l'utente AWS                                   | np6Kc_xwsvhR8Q~rP05fCqYNXmbqfMGQLOEzfmT |
| use A role   | Boolean  | Specifica l'utilizzo di uno o più ruoli d'amministrazione per l'autenticazione su uno o più account specifico/i dell'organization del provider  | true                                    |
| Arn Role (solo se useArole è attivo)                   | string   | Inserisci qui l'id Arn del ruolo associato ad un account specifico per l'esecuzione della fase di discovery di monitoring e per il provisioning | arn:aws:iam:{accountID}:role/{roleName} |
| Audit Arn Role (solo se useArole è attivo)             | string   | Inserisci qui l'id Arn di Audit del ruolo associato ad un account specifico per l'esecuzione della fase di discovery d'inventario               | arn:aws:iam:{accountID}:role/{roleName} |
| Aggregator Name  | string   | Inserisci qui il nome dell' aggregator sulle risorse per l'utilizzo del servizio AWS Config a supporto della fase di discovery d'inventario     | aws-{aggregatorName}                    |
| 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 l'ID del dataset dei costi sul quale eseguire le query  | {databaseName}.{tableName}              |
| 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 è false) | Boolean  | Indica se l'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 verrà associato al sottosistema e verrà inserito come tag su tutte le risorse del sottosistema     | ODL001                                  |

| Nome                 | Tipo | Descrizione   | Esempio |
|----------------------|------|---|---------|
| 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:

```
{
  "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.

Template:DEV183-T-IT-S  
rev.02 it

© Copyright Leonardo S.p.a. – Tutti i diritti  
riservati

Pagina 10 di  
27

NON CLASSIFICATO

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 to be assigned to the user \_ \_ \_ \_ \_

- Add the following custom policy to manage the CUR bucket \_

3. Access Key

- Generate Secret Credential\*\*.
- Save the **Access Key and Secret Key (not recoverable later)**. To enable \* intake of roles via STS for cross-account services (e.g. AWS Config), associate the following policy with the user created: \_

\*\* AZURE PARAMETERS\*\*

Enabled features:

- Catalogue element recovery
- Recovery of inventory items
- Recovery of use metrics
- Recovery of resources costs
- Recovery of security information
- Provisioning resources
- Provisioning services
- Provisioning complex blueprints

The specific parameters of the Azure subsystem to be inserted are shown in the table:

Figura 21 – Azure configuration mask

The mandatory parameters are indicated with \*

| 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-ee11f53d6c6b  |
| 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 è un'entità organizzativa in Azure che rappresenta un'azienda o un'organizzazione.                          | 884147733-f113-4783-a765-834183773083  |
| 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-f113-4783-a765-834183773083  |
| 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  |
| Storage account ID** | String   | Inserire il percorso dove vengono effettuate le esportazioni dei costi  | /subscriptions/{{sottoscrizione}}/resourceGroups/{{resourcegroup}}/providers/Microsoft.Storage/storageAccounts/{{storage account}} |

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

**Variabili per il calcolo dei costi**

The variables indicated with \*\* are exclusive, so you can select only one at a time. Each variable activates a different system for calculating costs and, if more than one is set, the rescue of the subsystem will be prevented. Specifically we can:

- Use the "Storage account ID" field to recover costs through automatic extractions performed individually by subsystem (only if the storage belongs to the same tenant)
- Use the "Cost from Billing Storage" field to recover billing account costs, then using only one file for all available subscriptions (Contributor and Blob Contributor permissions are required)
- Leaving the "Cost from billing storage" field SCMP will recover costs using APIs Azure prepared for daily costs.

This distinction is necessary to prevent APIs Azure respond with a 429 error related to the large number of requests made, in addition to using the methods described above, it is necessary that the Azure system be correctly configured and the utilities inserted have all the necessary permits

**\*\* AZURESTACK PARAMETERS\*\***

Enabled features:

- Catalogue element recovery
- Recovery of inventory items
- Recovery of use metrics
- Recovery of resources costs
- Recovery of security information
- Provisioning resources
- Provisioning services
- Provisioning complex blueprints

The specific parameters of the AzureStack subsystem to be inserted are shown in the table:

Figura 22 – AzureStack configuration mask

The mandatory parameters are indicated with \*

| 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-ee11f53d6c6b |
| 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 è un'entità organizzativa in Azure che rappresenta un'azienda o un'organizzazione.                          | 884147733-f113-4783-a765-834183773083   |
| 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-f113-4783-a765-834183773083   |
| 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                                       |



The mandatory parameters are indicated with \*

| 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-ee11f53d6c6b |
| 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 è un'entità 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 è un contratto per l'utilizzo dei servizi Azure.                                   | 884147733-ff13-4783-a765-834183773083   |
| 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                                       |
| 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                                      |

For on Premise providers, in particular, data on infrastructure capacity is required, so that SCMP can perform preliminary calculations in multiple scenarios.

For example, during provisioning, so as not to exceed the maximum permitted capacity of the provider.

REDHAT EDGE DEVICE PARAMETERS

Enabled features:

- Catalogue element recovery
- Recovery of inventory items
- Recovery of use metrics
- Recovery of resources costs
- Recovery of security information
- Provisioning resources
- Provisioning services
- Provisioning complex blueprints

The specific parameters of the Google Cloud subsystem to be inserted are displayed in the table.

□

Figura 25 – Edge configuration mask

The mandatory parameters are indicated with \*

| Nome                 | Tipo    | Descrizione   | Esempio               |
|----------------------|---------|---|-----------------------|
| client_id *          | string  |   | 104822473261100667392 |
| clientSecret *       | string  | Secret del cliente utilizzato per la connessione  | 82hg7ds1h0sds7392     |
| 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                |
| 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

In order to insert the system into the SCMP, some configurations are required on the provider's portal.

Specifically:

- Create a service account
  - a. Login to <https://console.redhat.com>
  - b. On the top right click the ' Settings → Service Accounts → Create service account.
  - c. Enter Name and Description → Create.
  - d. Copy Client ID and Client Secret (the secret will no longer be shown).
- assign permissions
  - a. Go to Settings → User Access → Groups
  - b. Create a group containing the following permissions/roles:

| Servizio                          | Ruolo consigliato                    |
|-----------------------------------|--------------------------------------|
| Edge Management (fleet, update)   | Edge Management Administrator o User |
| Image Builder                     | Image Builder Administrator o User   |
| Insights Inventory (lettura host) | Insights Inventory Viewer            |

- In the Service Accounts tab of the → Add service account → the account you have just created
- Rotation and revocation permissions
  - a. Portal → Service Accounts → menu ()
  - b. Select **Reset credentials\*** to regenerate only the Secret Client.
  - c. Select **Delete service account\*** to permanently unsubscribe automation.

With this configuration you can safely orchestrate the entire edge life cycle – from image generation to rollout updates – without ever using personal credentials.

PARAMETERS GOOGLE CLOUD

Enabled features:

Recovery of catalog items

- Recovery of inventory items
- Recovery of use metrics
- Recovery of resources costs
- Recovery of security information
- Provisioning resources
- Provisioning services
- Provisioning complex blueprints

The specific parameters of the Google Cloud subsystem to be inserted are displayed in the table, the "Service account" field can be inserted both automatically and manually as described in the paragraph.

□

Figura 26 – Google configuration mask

The mandatory parameters (available below the service account section).

| 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 **<br>(solo se costFromUSDCurrency è true) | integer | Inserisci qui uno sconto/maggiorazione da applicare sui prezzi in USD del provider per tutte le risorse  | 30  |

| 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 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      |



Variabili per il calcolo dei costi

The variables indicated with \*\* are used differently, for the calculation of the "client" cost depending on the presence of the "Cost from USD Currency" field. Specifically:

- If the field is disabled the value inserted in "PriceDiscount"vcatalog is used as a percentage added to the price recovered by the provider (or discounted if the value is negative) as for other providers
- If the field is activated the value inserted in "PriceDiscount" catalog and the value of "PriceDiscount" is used as a coefficient multiplied by the cost in USD recovered by the provider

This distinction is necessary to prevent APIs Azure respond with a 429 error related to the large number of requests made, in addition to using the methods described above, it is necessary that the Azure system be correctly configured and the utilities inserted have all the necessary permits

Figura 27 – Uploading the configuration file

By uploading the file the form is automatically completed with the necessary parameters, but it is also possible to insert them manually (yellow panel present in the image), following the table, all fields are mandatory:

| 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  |
| 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-----MIJQglBADANB...   |
| client_e-mail *              | 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/#543/myserviceaccount%40projectName.gserviceaccount.com |

Configurazione sul provider

1. Access to GCP Console

Go to <https://console.cloud.google.com/>

Login with your Google Cloud account.

2. Create or identify the Service Account (SA)

From the console, select the project in which you want to add (or already present) the service account From the console, to create the service account, go to IAM and admin > Service accounts. Click on Create service account. Assign id (e.g. my-service-account), name and description and finally Create. On the service account page, go to the Keys section Click Add key and select Create new key Choose json format and click Create Download and store the JSON file in a safe place.

3. Associate permissions to the Service Account

On the same page of the service accounts, find the account you just created and click on your name. Go to the Permissions section and the table below, at the service account, in the Inheritance column click Edit principal. In the pop-up menu, select the appropriate roles for the service account. Below is the minimal list of roles for SCMP: - App Engine Admin - BigQuery Data Transfer Agent - Cloud OS Config Service Agent - Compute Admin - Kubernetes Engine Agent - OS Inventory Viewer - Security Centre Service Agent Click Save and add permissions to the service account.

4. Service APIs Enable

Back to the console home Select the project in which the service account is present Go to APIs and services Top click on + Enable APIs and services Search API services in the search bar to enable and click on their name Once inside the API service, select Enable to enable it; below the API services for 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 of costs

If the dataset of costs is located in a service account other than the one you want to integrate, specify in the text box Cost Export Dataset ID (mel subsystem creation module present in SCMP administration) the complete connection string to the related dataset (e.g. projectId.datasetName.tableName)

PARAMETERS KUBERNETES

Enabled features:

- Catalogue element recovery
- Recovery of inventory items
- Recovery of use metrics
- Recovery of resources costs
- Recovery of security information
- Provisioning resources
- Provisioning services
- Provisioning complex blueprints

The specific parameters of the Kubernetes subsystem to be inserted are shown in the table

Figura 28 – Kubernetes configuration mask

The mandatory parameters are indicated with \*

| Nome                         | Tipo    | Descrizione   | Esempio   |
|------------------------------|---------|---|---|
| Certificate authority data * | string  | Inserire i dati relativi al certificato utilizzato dall' utenza utilizzata per la connessione   | Sgeijest90434n7u3h97ef  |
| Kubernetes API server URI *  | string  | Inserire l' URL del server al quale connettersi   | <a href="https://www.google.com/infos">https://www.google.com/infos</a> |
| User certificate Data *      | String  | Inserire il certificato relativo all' utenza utilizzata per la connessione  | ---begin private key--- fmbujffsfoije ...                               |
| 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  | Sf8eufce9sfber4543jh8ddsfh89r43   |
| 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

the standard authentication method is through the parameters contained in the kubeconfig file. The kubeconfig defines: Endpoint API server (server) Authentication method (client certificates, tokens, oidc, etc.) Namespace by default Background Authentication: Through client certificates (client-certificate-data and client-key-data)

Or through tokens (tokens within the user context)

Minimal example of kubeconfig:

apiVersion: v1 kind: Config clusters: - cluster: certified-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:

\*\* OPENSIFT\*

Enabled features:

- Catalogue element recovery
- Recovery of inventory items
- Recovery of use metrics
- Recovery of resources costs
- Recovery of security information
- Provisioning resources
- Provisioning services
- Provisioning complex blueprints

The specific parameters of the OpenShift subsystem to be inserted are shown in the table:

Figura 29 – OpenShift configuration mask

The mandatory parameters are indicated with \*

| Nome  | Tipo      | Descrizione   | Esempio               |
|---|-----------|---|-----------------------|
| Username *  | string    | L'username dell' utenza OpenShift che verrà utilizzata per la connessione al provider   | nome.cognome@mail.com |
| 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. | np6KcXmbqIMGQLOEzfmT  |
| 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 visibilità di un numero limitato di namespace è necessario inserire qui la lista dei namespaces abilitati                                     | demo,infos,production |
| 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                    |

Autorizzazioni utente

If we leave the "Discover all namespaces" field active, it is necessary that the user has administrative permissions on **TUTTI** the namespaces, otherwise it will not be possible to insert the system.

This distinction is necessary because the OpenShift system automatically blocks unauthorized requests correctly.

Configurazione sul provider

To connect an OpenShift cluster system, you simply have a nominal or impersonal user that has the appropriate privileges (e.g. cluster-admin or otherwise sufficient for the intended use) on the cluster.

Authentication:

Username and Password

Notes:

In OpenShift it is very common to use ServiceAccount specially created, with related RoleBinding or ClusterRoleBinding.

Users can be both human (nominal) and technical (impersonal).

ORAGUE PARAMETERS

Enabled features:

- Catalogue element recovery
- Recovery of inventory items
- Recovery of resources costs
- Recovery of security information

The specific parameters of the Oracle subsystem to be inserted are shown in the table:

Figura 30 – Oracle configuration mask

The mandatory parameters are indicated with \*

| Nome                 | Tipo     | Descrizione  | Esempio  |
|----------------------|----------|--|--|
| username *           | string   | Il nome utente utilizzato per l'autenticazione con OCI.  | ocid5.user.oc77.aaabnbthaj6prnvsb2gqnaaaaait3mqzekefmlhwkige2wxna6hfaj3f6njma      |
| 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...aaabnbthaj6prnvsb2gqnaaaaait3mqzekefmlhwkige2wxna6hfaj3f6njma |
| region *             | string   | La regione è 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-----MIJQglBADANB..."                                      |
| 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  | -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   |

Configurazione sul provider

Procedure to create parameters for external integration in Oracle Cloud Infrastructure (OCI): 1. Access to OCI Console

Go to <https://cloud.oracle.com/>  
Login with your Oracle Cloud account.

- Create or identify IAM User

In the main console menu, go to Identity & Security > Users. Select an existing user or create a new user for integration: Click Create User if you need to create one. Assign a name and an email. Save.
- Associate a group with appropriate permissions

After creating the user, you must associate it with a group that has the permissions for the resources you want to manage via API. Go to Identity > Groups. Select a group (e.g. Administrators or create a custom group). Click Add User to Group and add the newly created user.
- Generate API key (Key File)

Return to user page (Identity > Users > select user). Go to the API Keys tab. Click Add API Key. You have two options: Upload an existing public key (public RSA). Or generate a new public and private console key (download the private key). Select "Generate API Key Pair" to locally generate the key: Download the private key (.pem) and save it safely (it is your Key File). The public key will be automatically associated with the user.
- Get the required parameters

Ocid User (User OCID): Go to Identity > Users > select user. Find the user OCID on the user page (formato ocid1.user.oc1..aaaaaa... ). Fingerprint: It is the fingerprint of the public API key you added (viewed in the API Keys section). OcId Tenant (Tenant OCID / Compartment OCID Main): Go to Identity > Tenancy (click on the tenancy name on the top left). Find the OCID tenancy (it is the main tenant, e.g. ocid1.tenancy.oc1..aaaaaa... ). Region: Choose the region of your OCI (e.g. eu-frankfurt-1, us-ashburn-1, etc). You can find it at the top right of the console or in Governance & Administration > Regions. Realm: It is usually oc1 for most OCI public tenants. You can verify it in the documentation or from CLI if necessary.

Summary of parameters and where to find them

Parameter Where to find it / how to get it OcId User Identity > Users > user select > OCID Fingerprint Identity > Users OcId Tenant Identity Region Top right of the console (e.g. eu-frankfurt-1) Realm Generally oc1 (OCI realm standard) Key File Private Key .pem generated at the time of the API Key

ORACLEEXACC PARAMETERS

## Secure Cloud Management Platform

NON CLASSIFICATO Company internal

Informazioni a diffusione esclusiva

Enabled features:

- Catalogue element recovery
- Recovery of inventory items
- Recovery of resources costs
- Recovery of security information

The specific parameters of the OracleExAcc subsystem to be inserted are shown in the table:

Figura 31 – OracleExAcc configuration mask

The mandatory parameters are indicated with \*

| Nome                 | Tipo     | Descrizione   | Esempio  |
|----------------------|----------|---|--|
| username *           | string   | Il nome utente utilizzato per l'autenticazione con OCI.   | ocid5.user.oc77.aaabnbthaj6pnvsb2gqnaaaait3mqzekefmlhwkige2wxna6hfaj3f6njma      |
| 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...aaabnbthaj6pnvsb2gqnaaaait3mqzekefmlhwkige2wxna6hfaj3f6njma |
| 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-----MIJQglBADANB..."                                     |
| 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   |

\*\* VCLoud DIRECTOR PARAMETERS \*\*

Enabled features:

- Catalogue element recovery
- Recovery of inventory items
- Recovery of use metrics
- Recovery of resources costs
- Recovery of security information

The specific parameters of the VCloudDirector subsystem to be inserted are shown in the table

Figura 32 – VCloudDirector configuration mask

The mandatory parameters are indicated with \*

| 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 è 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 è 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  |

## Secure Cloud Management Platform

NON CLASSIFICATO Company internal

Informazioni a diffusione esclusiva

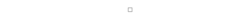
| Nome  | Tipo   | Descrizione   | Esempio |
|-------|--------|---|---------|
| odlID | string | Inserisci qui l'id dell'ordine di lavoro che verrà associato al sottosistema e verrà inserito come tag su tutte le risorse del sottosistema | ODL001  |

**\*\* VMWARE PARAMETERS\*\***

Enabled features:

- Catalogue element recovery
- Recovery of inventory items
- Recovery of use metrics
- Recovery of resources costs
- Recovery of security information
- Provisioning resources
- Provisioning services
- Provisioning complex blueprints

The specific parameters of the VMWare subsystem to be inserted are shown in the table:

  
Figura 33 – VMWare configuration mask

The mandatory parameters are indicated with \*

| 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-ee11f53d6c6b |
| 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~rP05fCqYNxbqfMGQLOEzIMt  |
| 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-f113-4783-a765-834183773083   |
| 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-f113-4783-a765-834183773083   |
| 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                                       |
| 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                                      |

For on Premise providers, in particular, data on infrastructure capacity is required, so that SCMP can perform preliminary calculations in multiple scenarios.

For example, during provisioning, so as not to exceed the maximum permitted capacity of the provider.

**Folders****AZURE FOLDER**

To allow the SCMP to exploit all the potential offered by the provider "Azure" the possibility of setting up "Folders" has been inserted

During the creation of a provider by selecting the type "Azure" we can notice the presence of an exclusive field for the provider:

- A confirmation box to indicate to the SCMP if the provider is a "Folder".

  
Figura 34 – Folder option Azure

The specific parameters of the Azure subsystem to be inserted are shown in the following table:

  
Figura 35 – Azure Folder configuration mask

The mandatory parameters are indicated with \*

| 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-ee11f53d6c6b |

## Secure Cloud Management Platform

NON CLASSIFICATO Company internal

Informazioni a diffusione esclusiva

| 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 è un'entità organizzativa in Azure che rappresenta un'azienda o un'organizzazione.                          | 884147733-ff13-4783-a765-834183773083   |
| 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                                       |
| 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                                      |

## GOOGLE CLOUD FOLDERS

To allow the SCMP to take advantage of all the potential offered by the provider "Google Cloud" the possibility to configure "Folders" and the ability to import the file generated by the provider's console so as to simplify the insertion of the same.

During the creation of a provider by selecting the type "Google Cloud" we can notice the presence of 2 exclusive fields for the provider:

1. A confirmation box to indicate to the SCMP if the provider is a "Folder".
2. A box where, by clicking inside it will be possible, through the windows file selection window insert the "JSON" type file exported directly from the Google console.

Figura 36 – Specific parameters of Google Cloud

The specific parameters of the Google Folder to be inserted are displayed in the table:

| 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" 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                      |
| 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

The following services must be accessed on the service account used:

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

The "ServiceAccount" field can be inserted automatically by uploading the file or manually by entering the fields available in the form.

After setting up a "Folder" system it will be displayed both in the cloud provider list, and in the folder page.

Figura 37 – View folders

From the "Cloud System" page of the "Administration" module, click the tab "Folders" on the top right where the list of folders configured in the tenant will be displayed.

Within the page you can do the same editing and deletion of folders on the "Cloud Provider" page.

Figura 38 – Access to Folders

By accessing a "Folder" in "View" mode by scrolling down on the page we can view the list of subsystems in the provider and the related status information:

- In green we can see a properly configured subsystem in the provider and that the SCMP automatically inserts into the system and will be visible in the "Cloud Providers" section and in all SCMP features.
- In red we can see an incorrectly configured subsystem that, after the appropriate changes from the "Google Cloud" console, can be accepted by the SCMP.

Figura 39 – Subsystem View of Folder

3.0.2 SIEM

The user can create a SIEM-type provider, by clicking on the tab that depicts a shield, placed in the top bar, d0opo having logged in to the page "Cloud SIEMs", on the top right, click on the burger menu and then click on "Attach a SIEM"

Figura 40 – Creating to SIEM cloud provider

Within the "Add SIEM" page, fill out all fields of the "General properties" section. After doing this, fill out all fields of the section "SIEM's properties" following the table:

Figura 41 – Filling the form to create a SIEM provider

The mandatory parameters are indicated with \*

| Nome             | Tipo     | Descrizione  | Esempio                                |
|------------------|----------|--|--|
| clientId *       | string   | Identificativo univoco del SIEM al quale connettersi , Fornito dal SIEM durante la registrazione dell'applicazione | 1b16698f-2df5-ed44-86b9ed-4b42c1fe7ad9 |
| clientSecret *   | password | Il secret da utilizzare per la connessione, fornito dal SIEM durante la registrazione dell'applicazione            | 1b16698f-2df5-ed44-86b9ed-4b42c1fe7ad9 |
| resourceGroup *  | string   | Il gruppo di risorse Azure in cui è ospitato il SIEM   | myGroup                                |
| subscriptionId * | string   | L'ID sottoscrizione Azure associata al SIEM  | 1b16698f-2df5-ed44-86b9ed-4b42c1fe7ad9 |
| tenantId *       | string   | L'ID tenant Azure associato al SIEM  | 1b16698f-2df5-ed44-86b9ed-4b42c1fe7ad9 |
| workspaceId*     | string   | L'ID dell'area di lavoro Log Analytics associata al SIEM   | 1b16698f-2df5-ed44-86b9ed-4b42c1fe7ad9 |
| workspaceName*   | string   | Il nome dell'area di lavoro Log Analytics associata al SIEM  | theWorkspaceName                       |

Finally, at the bottom right, click on the "Save" button. After that, a popup of SIEM creation appears below and the user is redirected to the SIEM list.

View, edit and delete

To view a SIEM, at a said one, click on the kebab menu and then click on "Show" . At this point, the user finds himself within the "Show SIEM" page where you can view but do not change the data. After viewing the data, at the bottom right, click on the "Close" button. This is done, the user finds himself within the SIEM list.

Figura 42 – Access to SIEM in display mode

Figura 43 – SIEM in display mode



To change a SIEM, at a said one, click on the kebab menu and then click on "Edit" . At this point, you will find yourself inside the "Edit SIEM" page where you can change the fields.

After changing the fields of interest, at the bottom right, click on the "Update" button. This is done, a popup of the SIEM changed and the user is found in the SIEM list.



Figura 45 – SIEM in edit mode

To delete a SIEM, at a said one, click on the kebab menu and then click on "Delete" . At this point a modal appears where you need to click on the "Remove" button.



Figura 47 – Confirmation to eliminate to SIEM

3.0.3 Secrets Managers

The user can create a secret manager by clicking on the tab depicting a padlock, placed in the top bar, as shown in the figure

After accessing the "Secret Manager" page, at the top right, click on the burger menu and then click on "Add a secret manager"



Here is an example of form in the case of adding a Secret Manager from the Azure provider (selectable from the dropdown "Type" at the top of the page).

After entering all the parameters required, at the bottom, click the "Save" button to conclude the insertion and the user is redirected to the list of "Secret Managers" where you can view the newly created component.

Azure key vault

The specific parameters for an Azure key vault to be inserted are displayed in the table:

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

Table 25 – Specific fields Azure key vault

Google Secret Manager

The specific parameters of the Google Secret Manager to be inserted are displayed in the following table:



The mandatory parameters are indicated with \*

| 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                    |

You can manually insert the parameters in the "service\_account.json" file if you do not want to upload it, all parameters are mandatory:

| Nome | Tipo   | Descrizione  | Esempio         |
|------|--------|--|-----------------|
| Type | string | Inserire il nome della tipologia di autenticazione configurata | service_account |

| Nome                         | Tipo     | Descrizione   | Esempio  |
|------------------------------|----------|---|--|
| project_id *                 | string   | Inserisci qui l'id univoco del progetto associato al service account  | Theproject-367810  |
| 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-----MIJQgIBADANB...   |
| 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 |

Viewing, modifying and deleting a system

You can view the data of a Secret Manager, within the list, by clicking on the kebab menu at a manager, and then on "Show".

Figura 51 – Access to the manager in display mode

On this page you can view the configuration of the Provider .

Figura 52 – manager in display mode

To return to the Secret Manager page, on the bottom left, click on the "Close" button.

At this point, you will find yourself on the Secret Manager page.

To change the data of a Secret Manager within the list, click on the kebab menu at a Cloud Provider, and click on "Edit".

Figura 53 – Access manager in edit mode

This is done, you will find yourself within the Cloud Provider page in edit mode where you can change your data. To return to the Cloud Provider page, click on the "Save" button on the left. At this point, you will find yourself on the Cloud Provider page.

To delete a "Secret manager", within the list, click on the kebab menu at a Secret Manager, and click on "Delete" .

Figura 54 – Start for deletion of a Secret Manager

Done that, a modal will appear where you need to click on the "Remove" button

Figura 55 – Confirm elimination of the Secret Manager

At this point, the Secret Manager will no longer be present within the list and the asset removal flow will be launched on the resource-manager.

3.0.4 Backup

The user is given the possibility to connect a CommVault to the SCMP to allow the recovery and visualization of the backup information and operations carried out by Vault.

To access this feature you need to select the "CommVault" tab available at the top in the "Administration" feature.

We will return to the page that contains the list of all configured "CommVault" and clicking on the menu on the right you can add a new CommVault

□

*Figura 56 – Access to CommVault*

On this page, after entering the login credentials (ip address, user and password) we can click on the "Test connection" button to confirm the correct insertion of the data and then confirm insertion via the "Save" button.

□

*Figura 57 – Connecting to a CommVault*

### 3.0.5 Confidential computing

In the Confidential Computing section, the user can enter a connection to a "Remote Attestation" service to control and display information relating to the confidentiality status of machines managed by the service.

To access this feature you need to select the "Confidential computing" tab available at the top in the "Administration" feature.

We will return to the page that contains the list of all the services of "Remote attestation" configured and clicking on the menu on the right you can add a new connection .

□

*Figura 58 – Access to Confidential Computing*

On this page, after entering the login credentials (ip address, user and password) we can click on the "Test connection" button to confirm the correct insertion of the data and then confirm insertion via the "Save" button.

□

*Figura 59 – Creation of connection to a "Remote Attestation" service*