Leonardo Cyber & Security Solutions

NUMERO DOCUMENTO: **C000CMP01STP01**

REVISIONE: **08.00**

DATA: **20/06/2025**

CAGE CODE: **A0069**

Digital Security

Secure Cloud Management Platform

Secure Cloud Management Platform

Leonardo Cyber & Security Solutions

3 Nov 2025

08.00

Secure Cloud Management Platform

Firme

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

Contatti

Carmelo Sciuto **Product Owner IPT di Sviluppo** R. Cloud Product | Digital Systems & Engineering Technologies | Engineering	**Leonardo S.p.A.** Via A. Agosta SNC 95121 Catania

Leonardo Cyber & Security Solutions

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

Leonardo Cyber & Security Solutions

3 Nov 2025

08.00

Secure Cloud Management Platform

Super Project Documentation (EN)

.

1 Developer Documentation

This section contains technical documentation for developers.

1.1 API Documentation

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

♪ Start

To start developing with our platform, follow these steps:

1. **Register*** for a developer account
2. **Genera**** your API keys
3. **Install*** our SDK
4. **Building***** your first integration

1.2 SDK and Librerie

We provide official SDKs for different programming languages:

- **JavaScript/Node.js** - npm install @platform/sdk
- **Python** - pip install platform-sdk
- **Java*** - Maven employee available
- **PHP*** - Composer package available

1.3 Examples of Code

1.3.1 Authentication Example

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

const client = new Platform({ apiKey: 'your-api-key', environment: 'production' ?

// User Authentication const user = await client.auth.login({ username: 'user@example.com', password: 'password' ?
``

1.4 Support

For technical support:

- See our API Documentation
- Visit our forum developers
- Contact support at developers@example.com

2 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.

2.1 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

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.

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"

2.1.0.0.0.1 * Information on subsystem cron-jobs**

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 – Information on cron-job

2.1.0.0.0.2 # Displaying, modifying and deleting 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 viewing 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 machines

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 – Access to the Cloud Provider 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 – Starting for the Elimination of 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 – Confirm deletion of the Cloud Provider

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.

2.1.0.0.0.3 ## *Cost model for On-Premise providers**

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 the 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 – Price 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 prepared

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

Figura 13 – Full cost model

2.1.0.0.0.4 # *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 – Updating 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

*##

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,he 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 checks the subsystem configuration to identify the "aggregation typology", this parameter indicates which catalog to use (RISORSE. o SKU) so as to correctly calculate the price
3. The cost module checks whether the resource identifier(UUID) is present in the SCMP catalog, if present the system multiplies usage for the catalog cost
4. 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

♪ 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 (ARN 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 (RISORSE o SKU) so as to correctly calculate the price
3. The cost module checks whether the resource identifier(UUID) is present in the SCMP catalog, 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 (RISORSE 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 catalog, 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

♪ 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 (RISORSE 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 catalog, 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/reload 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

2.1.0.0.1 NEW SUBSYSTEM CREATION

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 – Add a new Cloud Provider

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

2.1.0.0.1.1

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 plates

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.

2.1.0.0.1.2

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 – Mask of configuration
Amazon Web Services

The mandatory parameters are indicated with *

♪ | AccessKey * | string | The AWS access key is an alphanumeric string that identifies the AWS user. | ZYKZGVAKIS4YK5IXCAXB | | SecretKey * | password | The secret access key AWS is an alphanumeric string that is used to authenticate user AWS | np6Kc_.xwsvhR8Q~rP05fCqYNXmbqfMGQLOEzfMt | | use A role | Boolean | Specifies the use of one or more administration roles for authentication on one or more specific accounts(s) of the organization of the | true | | Arn Role (only if useArole is active) | string | Enter here the id Arn of the role associated with a specific account for running the monitoring discovery phase and provisioning | arn:aws:iam: {accountID}:role/{roleName} | | Audit Arn Role (only if useArole is active) | string | Enter the Audit Arn of the role associated with a specific account for the execution of the inventory discovery stage | arn:aws:iam: {accountID}:role/{roleName} | | Aggregator Name | string | Enter here the name of the resource aggregator for the use of the AWS Config service to support the inventory discovery stage aws-{aggregatorName} | | Cost Bucket Path | string | Enter here the query storage bucket path | s3://{bucketPath} | | Cost Export Dataset ID | string | Enter here the cost dataset ID on which to query | {databaseName}.{tableName} | | usageAggregation | Boolean | Indicates the type of aggregation used for calculating costs (true for resources, false for sku) | True | | Rate Code Aggregation (only if useAggregation is false) | Boolean | Indica se l'aggregazione degli sku si è per sku ID o per rate code. | true | CatalogPriceDiscount | integer | Enter here a discount/mage to be applied on catalog prices for all resources that do not have a CMP | 5 | report | odlID | string | Enter here the work order id that will be associated with the subsystem and will be inserted as tag on all subsystem resources | ODL001 | | dataFirstCostRecover | int | Enter the number of days prior to the date of creation of which the costs must be recovered at the first start of the subsystem | 15 |

Configurations on the provider

1. Configuration S3
2. Access **Amazon S3***.
3. Create or use a bucket for CUR data.
4. Enable **Bucket Versioning**.
5. Definition CUR
6. Access to **Billing and cost management**
7. Go to Data Exports section
8. Configure a new CUR report as follows
9. Export details:
10. **Standard export date**: standard export format
11. **Export name***: report name
12. Data table content settings:
13. Select **CUR 2.0**

14. Select as granularity **Hourly**
15. Data export options
16. format file: **Parquet**
17. file versioning: **Overwrite existing data export file**
18. Data export storage settings
19. Configure the pointing to the S3 bucket with the one created initially
20. Configure the prefix of the bucket path with * *data*
21. Creation of the IAM role for Glue
22. Access **IAM**.
23. Create a custom role for managing Amazon Glue.
24. Assign the following policies:
25. `AWSGlueServiceRole' (standard AWSpolicy)
26. Custom policy for access to the S3 bucket: ♪ (') "Version": "2012-10-17", "Statement": ♪ (') "Effect": "Allow," "Action": ♪ "s3:GetObject", "s3:PutObject"] "Resource": ♪ "arn:aws:s3::{bucketPath}/" ♪ ? ♪ ? ``
27. Glue database creation
28. Access **AWS Glue**.
29. Create the database.
30. Crawler Configuration
31. Create a **crawler** in Glue:
32. Select the custom role previously created.
33. Define the path S3 as s3://{bucketPath}/data/ .
34. Set a **scheduling** (e.g. every hour: 0 * * * **).
35. Use in Athena
36. After the first crawler execution, the data will be available in **Athena** for queries.

37. 2.2 . *For past historical data, contact AWS support.*

38. Configuration and AWS Aggregates
39. Initial configuration
40. Access **AWS Config** *and click Get started***.

41. Create a S3 bucket for aggregate data.
42. Enable the **IAM**** override and leave the remaining default options; AWS will automatically create the necessary role.
43. Aggregate Config
44. Create a ** Resource aggregator **in the** Aggregators* section.

45. 2.3 Include all regions.

46. User creation IAM
47. Access **IAM** *and go to Users*****
48. Create a new user or select an existing user.
49. Optional: Enable console access for the created user.
50. Policy to be assigned to the user
51. AmazonAthenaFullAccess
52. AmazonS3FullAccess
53. 'AWS_ConfigRole'
54. AWSConfigUserAccess
55. 'AmazonEC2ReadOnlyAccess'
56. 'CloudWatchReadOnlyAccess'
57. Add the following custom policy to manage the CUR bucket ♪ (') "Version": "2012-10-17", "Statement": ♪ (') "Sid": "VisualEditor0", "Effect": "Allow," "Action": [S3:*] "Resource": ♪ "arn:aws:s3::{bucketPath}/", "arn:aws:s3::{bucketPath}/" ♪ ? ♪ ? ``
58. Access Key
59. Generate Secret Credential**.
60. 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: ♪ (') "Version": "2012-10-17", "Statement": ♪ (') "Effect": "Allow," "Action": "sts:AssumeRole", "Resource": ♪ "arn:aws:iam::{accountIamID}:role/{roleName}" ♪ ? ♪ ? ``

♪

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 *

♪ | clientId * | string | The unique client ID connecting to the Azure Cloud subsystem. This ID is used to identify the client and to authorize access to subsystem resources. | 5a85c16c6ad-49db-a58e-e209-ee11f53d6c6b | clientSecret * | password | The client's secret key, used to authenticate the client with the Azure Cloud subsystem. The secret key must be kept secret and should not be shared with anyone. ♪ | tenantId * | string | Tenant Azure ID to which the Azure Cloud subsystem belongs. The tenant is an organizational entity in Azure that represents a company or organization. | 884147733-ff13-4783-a765-834183773083 | subscriptionId * | string | The Azure subscription ID used to access the Azure Cloud subsystem. Subscription is a contract for the use of Azure services. | 884147733-ff13-4783-a765-834183773083 | usageAggregation | boolean | Indica se l'aggregazione per "usage" is enabled for subscription. When this check is enabled the subsystem costs will be grouped by resource type | false | | Storage account ID*** | String | Enter the route where the cost export | /subscriptions/{subscription}}/resourceGroups/{{{{resourcegroup}}/providers/Microsoft.Storage/storageAccounts/{{{{stc account}} | | Cost from Billing Storage** | boolean | Select this box to recover costs in "billing Account" format | true | | CatalogPriceDiscount | integer | Enter here a discount/mayor to be applied on catalog prices for all resources that do not have a SCMP | 5 | report | odlID | string | Enter here the work order id that will be associated with the subsystem and will be inserted as tag on all subsystem resources | ODL001 | | dataFirstCostRecover | int | Enter the number of days prior to the date of creation of which the costs must be recovered at the first start of the subsystem | 15 |

Available for cost calculation

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 (Contributionor and Blob Contributor permissions are required)
- Leaving the "Cost from Billing storage" field and 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

♪

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 *

♪ | clientId ***** | string | The unique client ID connecting to the Azure Cloud subsystem. This ID is used to identify the client and to authorize access to subsystem resources. | 5a85c16c6ad-49db-a58e-e209-ee11f53d6c6b | clientSecret * | password | The client's secret key, used to authenticate the client with the Azure Cloud subsystem. The secret key must be kept secret and should not be shared with anyone. ♪ | tenantId * | string | Tenant Azure ID to which the Azure Cloud subsystem belongs. The tenant is an organizational entity in Azure that represents a company or organization. | 884147733-ff13-4783-a765-834183773083 | subscriptionId * | string | The Azure subscription ID used to access the Azure Cloud subsystem. Subscription is a contract for the use of Azure services. | 884147733-ff13-4783-a765-834183773083 | usageAggregation | boolean | Indica se l'aggregazione per "usage" is enabled for subscription. When this check is enabled the subsystem costs will be grouped by resource type | false | | CatalogPriceDiscount | integer | Enter here a discount/mayor to be applied on catalog prices for all resources that do not have a SCMP | 5 | report | odlID | string | Enter here the work order id that will be associated with the subsystem and will be inserted as tag on all subsystem resources | ODL001 | | dataFirstCostRecover | int | Enter the number of days prior to the date of creation of which the costs must be recovered at the first start of the subsystem | 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.

2.3.0.0.1.3

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 HCI subsystem to be inserted are shown in the table:

Figura 23 – Configuration mask
AzureStack HCI

The mandatory parameters are indicated with *

♪ | clientId ***** | string | The unique client ID connecting to the Azure Cloud subsystem. This ID is used to identify the client and to authorize access to subsystem resources. | 5a85c16c6ad-49db-a58e-e209-ee11f53d6c6b | clientSecret * | password | The client's secret key, used to authenticate the client with the Azure Cloud subsystem. The secret key must be kept secret and should not be shared with anyone. ♪ | tenantId * | string | Tenant Azure ID to which the Azure Cloud subsystem belongs. The tenant is an organizational entity in Azure that represents a company or organization. | 884147733-ff13-4783-a765-834183773083 | subscriptionId * | string | The Azure subscription ID used to access the Azure Cloud subsystem. Subscription is a contract for the use of Azure services. | 884147733-ff13-4783-a765-834183773083 | usageAggregation | boolean | Indica se l'aggregazione per "usage" is enabled for subscription. When this check is enabled the subsystem costs will be grouped by resource type | false | | CatalogPriceDiscount | integer | Enter here a discount/mayor to be applied on catalog prices for all resources that do not have a SCMP | 5 | report | odlID | string | Enter here the work order id that will be associated with the subsystem and will be inserted as tag on all subsystem resources | ODL001 | | dataFirstCostRecover | int | Enter the number of days prior to the date of creation of which the costs must be recovered at the first start of the subsystem | 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.

–

Enabled features:

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

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

Figura 24 – Configuration mask
AzureStack Hybrid Cloud

The mandatory parameters are indicated with *

♪ | clientId ***** | string | The unique client ID connecting to the Azure Cloud subsystem. This ID is used to identify the client and to authorize access to subsystem resources. | 5a85c16c6ad-49db-a58e-e209-ee11f53d6c6b | clientSecret * | password | The client's secret key, used to authenticate the client with the Azure Cloud subsystem. The secret key must be kept secret and should not be shared with anyone. ♪ | tenantId * | string | Tenant Azure ID to which the Azure Cloud subsystem belongs. The tenant is an organizational entity in Azure that represents a company or organization. | 884147733-ff13-4783-a765-834183773083 | subscriptionId * | string | The Azure subscription ID used to access the Azure Cloud subsystem. Subscription is a contract for the use of Azure services. | 884147733-ff13-4783-a765-834183773083 | usageAggregation | boolean | Indica se l'aggregazione per "usage" is enabled for subscription. When this check is enabled the subsystem costs will be grouped by resource type | false | | CatalogPriceDiscount | integer | Enter here a discount/mayor to be applied on catalog prices for all resources that do not have a SCMP | 5 | report | odlID | string | Enter here the work order id that will be associated with the subsystem and will be inserted as tag on all subsystem resources | ODL001 | | dataFirstCostRecover | int | Enter the number of days prior to the date of creation of which the costs must be recovered at the first start of the subsystem | 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.

2.3.0.0.1.4

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 *

♪ | client_id* | string | | 104822473261100667392 | | clientSecret * | string | Secret of the customer used for connection | 82hg7ds1h0sds7392 | | odlID | string | Enter here the work order id that will be associated with the subsystem and will be inserted as tag on all subsystem resources | ODL001 | | CatalogPriceDiscount | integer | Enter here a discount/mage to be applied on catalog prices for all resources that do not have a SCMP | 10 | report | dataFirstCostRecover | int | Enter the number of days prior to the date of creation of which the costs must be recovered at the first start of the subsystem | 15 |

Configuration side PROVIDER

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

Specifically:

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

Service Recommended role
Edge Management (fleet, update)
Image Builder
Insights Inventory (host reading)

- In the Service Accounts tab of the ⇢ Add service account ⇢ the account you have just created
- Rotation and revocation permissions
- Portal ⇢ Service Accounts → menu ())
- Select **Reset credentials*** to regenerate only the Secret Client.
- 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.

2.3.0.0.1.5

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).

♪ | serviceAccount * | object | Connection file generated by the Google console | service_account.json | | discoveryProjectId * | string | Identification of the project of discovery | Theproject-547280 | | costExportProjectId | string | Dataset id of the export service account costs if the dataset is different from the ProjectID | test-customer.test_customer.gcp_billing_export_resource_v1_01527DF_51B683_EB2A9 | | usageAggregation | boolean | Indica se l'aggregazione per "usage" is enabled for subscription. When this check is enabled the subsystem costs will be grouped by resource type | false | | Cost from USD Currency | boolean | Indica if the final cost is calculated by the price in USD or EUR | true | | ProviderPriceDiscount ** (only if costFromUSDCurrency is true) | integer | Enter here a discount/mage to be applied on the provider's USD prices for all | 30 | resources | CatalogPriceDiscount ** | integer | Enter here a discount/mayor to be applied on catalog prices for all resources that do not have a SCMP | -5 | report | odlID | string | Enter here the work order id that will be associated with the subsystem and will be inserted as tag on all subsystem resources | ODL001 | | dataFirstCostRecover | int | Enter the number of days prior to the date of creation of which the costs must be recovered at the first start of the subsystem | 15 |

Available for cost calculation

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 – Configuration file loading

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:

♪ ♪ Type | string | Enter the name of the type of authentication configured | service_account | | project_id * | string | Enter here the unique project id associated with the service account | Theproject-367810 | | private_key_id * | string | Enter here the unique id of the private key of the service account | 55cb5cf903e93ea1e9c294a07e46e0af0633e6 | | private_key * | password | Contains the private key of the service account in PEM format. It is essential for authentication of the service account to Google Cloud APIs | -----BEGIN PRIVATE KEY-----MIIJQgIBADANB... | | client_e-mail * | string | The unique email address of the service account. It is used to identify the service account when authenticating to Google Cloud API | user@dominio.com | | client_id * | string | The service account client ID. Is a unique identifier used to identify the service account in Google Cloud | 104822473261100667392 | | auth_uri * | string | The URL used for authentication of service account to Google Cloud API |https://accounts.google.com/oauth2/auth> | | token_uri* | string | The URL used to obtain an access token for the service account | https://oauth2.googleapis.com/token | | auth_provider_x509_cert_url* | string | The URL of the X.509 certificate used for authentication of the service account https://www.googleapis.com/oauth2/v1/certs | | client_x509_cert_url* | string | The URL of the X.509 certificate in the | |https://www.googleapis.com/robot/v1/metadata/f543/myserviceaccount%40projectName.gserviceaccount.com> |

Configuration on the provider

1. Access to GCP Console
2. Go to https://console.cloud.google.com/
3. Login with your Google Cloud account.

4. 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.
5. 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 Inventroy Viewer - Security Centre Service Agent Click Save and add permissions to the service account.

1. 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

1. 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)

2.3.0.0.1.6

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 – Configuration mask
Kubernetes

The mandatory parameters are indicated with *

♪ | Certificate authority data * | string | Enter the certificate data used by the user used for connection | Sgeijesf90434n7u3h97ef | | Kubernetes API server URI* | string | Enter the server URL to which to connect | https://www.google.com/infos | ♪ User certified Data * | String | Enter the user certificate used for connection | --- begin private key--- fnbsujffsfoije ... | | User key Data * | String | Enter the user key used for connection | Sf8j9jts4ewht7h3wfwj908w | ♪ User token * | String | Token secret relative to the user used for connection to the provider | Sf8eufce9sfber4543jh8ddsfh89r43 | ♪ User name * | String | Enter the username used for authentication | administrator | | Label selector | string | Enter a selector to filter the recovered resources from the SCMP | Name=red | | CatalogPriceDiscount | integer | Enter here a discount/mage to be applied on catalog prices for all resources that do not have a SCMP | -10 | report | odlID | string | Enter here the work order id that will be associated with the subsystem and will be inserted as tag on all subsystem resources | ODL001 |

Configuration on the 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:

2.3.0.0.1.7

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 *

♪ ♪ Username ***** | string | The username of the OpenShift user that will be used for connection to the | provider name.cognome@mail.com | | Password * | password | Client password, used to authenticate the client with the subsystem. The secret key must be kept secret and should not be shared with anyone. ♪ | API server port * | integer | The port on which the API OpenShift | 8090 | | API url * | string | The url OpenShift on which to make requests | www.google.com | | discover all Namespaces | boolean | If the user has administrator permissions on all OpenShift "projects" will be recovered all fake namespaces | | Namespace selector (visible only if active "discover all namespaces) | selection | If the user has visibility of a limited number of namespaces it is necessary to enter here the list of enabled namespaces | demo,infos,production | | odlID | string | Enter here the work order id that will be associated with the subsystem and will be inserted as tag on all subsystem resources | ODL001 | | dataFirstCostRecover | int | Enter the number of days prior to the date of creation of which the costs must be recovered at the first start of the subsystem | 15 |

User permissions

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.

Configuration on the 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).

2.3.0.0.1.8

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 *

♪ | username * | string | The username used for authentication with OCI. ♪ | fingerprint * | string | is a unique value that identifies the device, used for authentication with OCI. == sync, corrected by elderman == @elder_man | tenantId * | string | The ID of the OCI tenant to which you want to connect | ocid5.tenancy. ♪ | region * | string | The region is the specific geographical location in which the OCI resources are located. | eu-dcc-rome-1 | Realm | string | The name of the logical container that groups the OCI resources and their costs. | personal-realm.it | keyFile * | password | a PEM file containing the public and private key used for authentication. | " -----BEGIN PRIVATE KEY---MIIJQgIBADANB..." | | usageAggregation | boolean | Indica se l'aggregazione per "usage" is enabled for subscription. When this check is enabled the subsystem costs will be grouped by resource type | false | | CatalogPriceDiscount | integer | Enter here a discount/mage to be applied on catalog prices for all resources that do not have a SCMP | -10 | report | odlID | string | Enter here the work order id that will be associated with the subsystem and will be inserted as tag on all subsystem resources | ODL001 | | dataFirstCostRecover | int | Enter the number of days prior to the date of creation of which the costs must be recovered at the first start of the subsystem | 15 |

Configuration on the 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.

1. 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.

1. 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.

1. 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.

1. 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..aaaaaaa.. .). 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

2.3.0.0.1.9

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 – Configuration mask
OracleExAcc

The mandatory parameters are indicated with *

♪ | username * | string | The username used for authentication with OCI. ♪ | fingerprint * | string | is a unique value that identifies the device, used for authentication with OCI. == sync, corrected by elderman == @elder_man | tenantId * | string | The ID of the OCI tenant to which you want to connect | ocid5.tenancy. ♪ | region * | string | The region is the specific geographical location in which the OCI resources are located. | eu-dcc-rome-1 | Private key * | password | a PEM file containing the public and private key used for authentication. | " -----BEGIN PRIVATE KEY---- MIIJQgIBADANB..." | | CatalogPriceDiscount | integer | Enter here a discount/mage to be applied on catalog prices for all resources that do not have a SCMP | -10 | report | odlID | string | Enter here the work order id that will be associated with the subsystem and will be inserted as tag on all subsystem resources | ODL001 | | dataFirstCostRecover | int | Enter the number of days prior to the date of creation of which the costs must be recovered at the first start of the subsystem | 15 |

2.3.0.0.1.10

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 *

♪ | url * | string | the address of the VCloudDirector server to which you want to connect | https://url.westeurope.com/tenant/org-zzg-435832 | | tenantId * | string | The VCloudDirector tenant ID is the unique tenant identifier you want to connect to. | org-zzg-435832 ♪ Use providerPermission | boolean | To activate if the user has all the permissions at the provider level, not activating it is not retrieved all the information but only the organization enabled | true | | token * | password | Authentication token for VCloudDirector is a secret string that is used to authenticate the user with the VCloudDirector | aesZo6LextKTQx92VoRpyzaesZo6LextKT | | Location | String | Enter the resource region VCloudDirector | Eu west | | Location | string | insert the geographical position of the system | OnPremise | | CatalogPriceDiscount | integer | Enter here a discount/mayor to be applied on catalog prices for all resources that do not have a SCMP | 5 | report | odlID | string | Enter here the work order id that will be associated with the subsystem and will be inserted as tag on all subsystem resources | ODL001 |

2.3.0.0.1.11

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 – Configuration mask
VMWare

The mandatory parameters are indicated with *

♪ | clientId ***** | string | The unique client ID connecting to the Azure Cloud subsystem. This ID is used to identify the client and to authorize access to subsystem resources. | 5a85c16c6ad-49db-a58e-e209-ee11f53d6c6b | clientSecret * | password | The client's secret key, used to authenticate the client with the Azure Cloud subsystem. The secret key must be kept secret and should not be shared with anyone. ♪ | tenantId * | string | Tenant Azure ID to which the Azure Cloud subsystem belongs. The tenant is an organizational entity in Azure that represents a company or organization. | 884147733-ff13-4783-a765-834183773083 | subscriptionId * | string | The Azure subscription ID used to access the Azure Cloud subsystem. Subscription is a contract for the use of Azure services. | 884147733-ff13-4783-a765-834183773083 | usageAggregation | boolean | Indica se l'aggregazione per "usage" is enabled for subscription. When this check is enabled the subsystem costs will be grouped by resource type | false | | CatalogPriceDiscount | integer | Enter here a discount/mayor to be applied on catalog prices for all resources that do not have a SCMP | 5 | report | odlID | string | Enter here the work order id that will be associated with the subsystem and will be inserted as tag on all subsystem resources | ODL001 | | datsFirstCostRecover | int | Enter the number of days prior to the date of creation of which the costs must be recovered at the first start of the subsystem | 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 – Option folder Azure

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

Figura 35 – Configuration mask Azure Folder

The mandatory parameters are indicated with *

♪ | clientId ***** | string | The unique client ID connecting to the Azure Cloud subsystem. This ID is used to identify the client and to authorize access to subsystem resources. | 5a85c16c6ad-49db-a58e-e209-ee11f53d6c6b | clientSecret * | password | The client's secret key, used to authenticate the client with the Azure Cloud subsystem. The secret key must be kept secret and should not be shared with anyone. ♪ | tenantId * | string | Tenant Azure ID to which the Azure Cloud subsystem belongs. The tenant is an organizational entity in Azure that represents a company or organization. | 884147733-ff13-4783-a765-834183773083 | usageAggregation | boolean | Indica se l'aggregazione per "usage" is enabled for subscription. When this check is enabled the subsystem costs will be grouped by resource type | false | | CatalogPriceDiscount | integer | Enter here a discount/mayor to be applied on catalog prices for all resources that do not have a SCMP | 5 | report | odlID | string | Enter here the work order id that will be associated with the subsystem and will be inserted as tag on all subsystem resources | ODL001 | | datsFirstCostRecover | int | Enter the number of days prior to the date of creation of which the costs must be recovered at the first start of the subsystem | 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:

♪ | serviceAccount | object | Connection file generated by the Google console | service_account.json | | costExportDatasetID | string | Enter the dataset id to be used for data recovery | Projectid.dataset.table | | usageAggregation | boolean | Indica se l'aggregazione per "usage" is enabled for subscription. When this check is enabled the subsystem costs will be grouped by resource type | false | | Cost from USD Currency | Boolean | Indica if the final cost is calculated by the price in USD or EUR | true | | ProviderPriceDiscount (only if costFromUSDCurrency is true) | integer | Enter here a discount/mage to apply on the provider's USD prices for all resources | 30 | ♪ Cost cross project | Boolean | Indica if you recover the costs of all billing account projects or just the current project | true | | CatalogPriceDiscount | integer | Enter here a discount/mage to be applied on catalog prices for all resources that do not have a SCMP | -20 | report | odlID | string | Enter here the work order id that will be associated with the subsystem and will be inserted as tag on all subsystem resources | ODL001 | | datsFirstCostRecover | int | Enter the number of days prior to the date of creation of which the costs must be recovered at the first start of the subsystem | 15 |

Abilitation mandatory

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 – See 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 – See subsystems of Folder

♪

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 – Creation of a 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 – Compilation of the form to create a SIEM provider

The mandatory parameters are indicated with *

♪ | clientId * | string | Unique SIEM identifier to which to connect , Provided by SIEM during application registration | 1b16698f-2df5-ed44-86b9ed-4b42c 1fe7ad9 | | clientSecret * | password | The secret to use for connection, provided by SIEM during application registration | 1b16698f-2df5-ed44-86b9ed-4b42c 1fe7ad9 | | resourceGroup * | string | The Azure resource group in which the SIEM | myGroup | | subscriptionId * | string | ID subscription Azure associated with SIEM | 1b16698f-2df5-ed44-86b9ed-4b42c 1fe7ad9 | | tenantId * | string | ID tenant Azure associated with SIEM | 1b16698f-2df5-ed44-86b9ed-4b42c 1fe7ad9 | | workspaceID* | string | Workspace ID Log Analytics associated with SIEM | 1b16698f-2df5-ed44-86b9ed-4b42c 1fe7ad9 | | workspaceName* | string | The name of the working area Log Analytics associated with 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.

2.3.0.0.2 DISPLAY, 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 visual 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 44 – Access to SIEM in edit mode

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 46 – Option to delete a SIEM "Delete"

Figura 47 – Confirm to delete a SIEM

♪ 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”

Figura 48 – Add a new 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:

Figura 49 – Configuration mask Azure key vault

The mandatory parameters are indicated with *

♪ | clientId * | string | Unique key vault identifier | 09f8985-9f89d0-4623-98982-5a510fd3d2 | | clientSecret * | password | A secret key used to authenticate the application with the Key Vault | np6Kc_.xwsvhR8Q~rP05fCqYNXmbqfMGQLOEzfMt | | resourceGroup * | string | The Azure resource group in which the Key Vault | resoruceGroupName | | subscriptionId * | string | ID subscription Azure associated with Key Vault | 09f8985-9f89d0-4623-98982-5a510fd3d2 | | tenantId | string | The ID tenant Azure associated with the Key Vault | 09f8985-9f89d0-4623-98982-5a510fd3d2 | | privateUrl | string | private URL access to the 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:

Figura 50 – Google Secret Manager configuration mask

The mandatory parameters are indicated with *

♪ | kmsProjectId ***** | string | project ID Google Cloud Platform (GCP) associated with the Google Cloud Key Management Service (KMS). | 5a85c16c6ad-49db-a58e-e209-ee11f53d6c6b | serviceAccount * | object | Connection file generated by the Google console | 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:

♪ ♪ Type | string | Enter the name of the type of authentication configured | service_account | | project_id * | string | Enter here the unique project id associated with the service account | Theproject-367810 | | private_key_id * | string | Enter here the unique id of the private key of the service account | 55cb5cf903e93ea1e9c294a07e46e0af0633e6 | | private_key * | password | Contains the private key of the service account in PEM format. It is essential for authentication of the service account to Google Cloud APIs | -----BEGIN PRIVATE KEY-----MIIJQgIBADANB... | | client_e-mail * | string | The unique email address of the service account. It is used to identify the service account when authenticating to Google Cloud API | user@dominio.com | | client_id * | string | The service account client ID. Is a unique identifier used to identify the service account in Google Cloud | 104822473261100667392 | | auth_uri * | string | The URL used for authentication of service account to Google Cloud API |https://accounts.google.com/oauth2/auth> | | token_uri* | string | The URL used to obtain an access token for the service account | https://oauth2.googleapis.com/token | | auth_provider_x509_cert_url* | string | The URL of the X.509 certificate used for authentication of the service account https://www.googleapis.com/oauth2/v1/certs | | client_x509_cert_url* | string | The URL of the X.509 certificate in the | |https://www.googleapis.com/robot/v1/metadata/f543/myserviceaccount%40projectName.gserviceaccount.com> |

2.3.0.0.3 DISPLAYING, 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 to the 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 – Starting for the Elimination of a Secret Manager

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

---

Figura 55 – Confirm deletion 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.

♪ 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 – Accesso a 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 – Creation of connection to a CommVault

♪ 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 – Accesso a 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 service "Remote Attestation"