# Nivola Documentation

***Release 1.0.0***

**CSI Piemonte**

**Feb 04, 2021**

# CONTENTS

CHAPTER

ONE

# OVERVIEW

## 1.1 What is Nivola?

Nivola is a completely open source cloud computing platform that simplifies the use of services by public administration and enterprises. Nivola is implemented by CSI Piemonte and provides computing power, storage, network and database and much more. The aim is to offer each customer complete autonomy in creating their own information system and migrating applications, in complete security. The services are easily scalable, with no licence fees or hardware management costs. Each customer can therefore independently create their own information system, paying for it solely on the basis of usage, through systems that measure actual consumption.

### 1.1.1 100% Open Source

Nivola is an open source platform owned by the public administration, which controls its evolution and can plan future developments. This freedom from market technologies guarantees the stability needed to build a state-of-the-art IT system without incurring additional investment due to technological lock-ins. At the heart of Nivola's development is OpenStack, a set of open source software tools for creating and managing cloud computing services, according to the Infrastructure as a Service (IaaS) model. Born from a NASA and Rackspace project, OpenStack is now the result of the collaboration of thousands of developers. More than 60,000 members and over 600 companies from more than 180 countries participate in the community. Nivola extends the basic functionalities of OpenStack with specific services and processes for PA and enterprises and the code is released to the open source community under the GPL v3 licence, involving the research world and the administrations themselves interested in supporting its development.

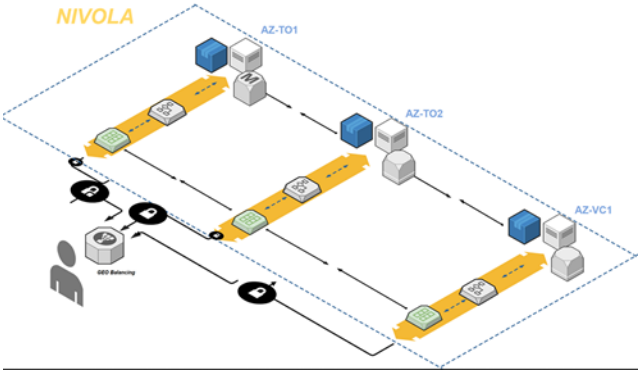
### 1.1.2 A world of simple and customisable services

Nivola simplifies the adoption, access and use of new application services in the cloud, regardless of the sourcing model chosen by the administration, be it internal development, acquisition from the market or reuse by another administration. The customer has at his disposal a wide catalogue of services easily adaptable to his needs, exposed through Application Program Interfaces (API), a uniform set of functionalities accessible via software.

## 1.2 Basic concepts

### 1.2.1 Availability zones

These are the geographical areas where the data centres of public cloud service providers reside. Corporate customers choose one or more Availability Zones for their services according to their business needs. Availability Zones are availability zones made up of independent, isolated infrastructures hosted within the CSI Piemonte data centres. When creating their services, it is possible to choose the Availability Zone according to specific geographic distribution needs while maintaining high reliability.



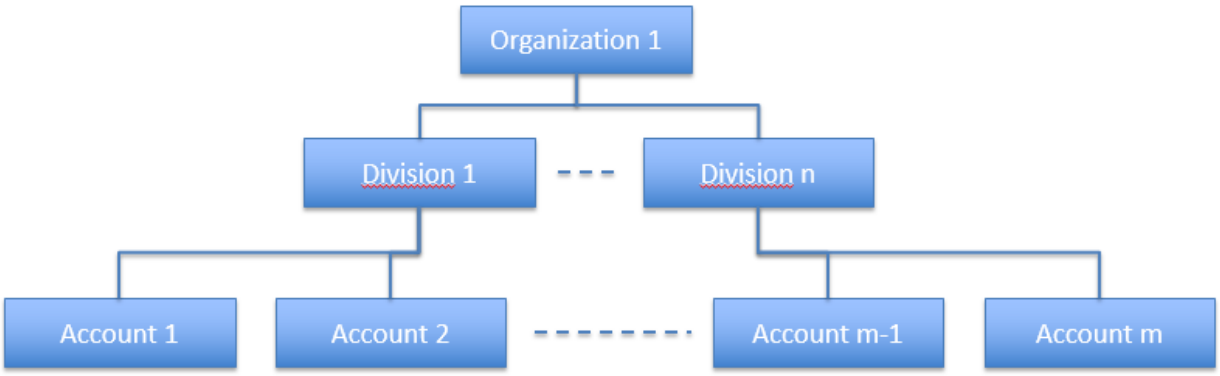

### 1.2.2 The organisational structure

Within Nivola it will be possible to model an organisational structure on three levels so as to allow the allocation of responsibilities and management of services according to a precise hierarchy. In the Account, the infrastructure will be set up to meet the necessary technological and security requirements. The Division is entrusted with the task of controlling the consumption of the resources of the Accounts, which it will be able to create autonomously. The top of the structure is the Organisation, which will have a complete vision of the use of the platform, with the possibility of adapting it to the Divisions and Accounts.

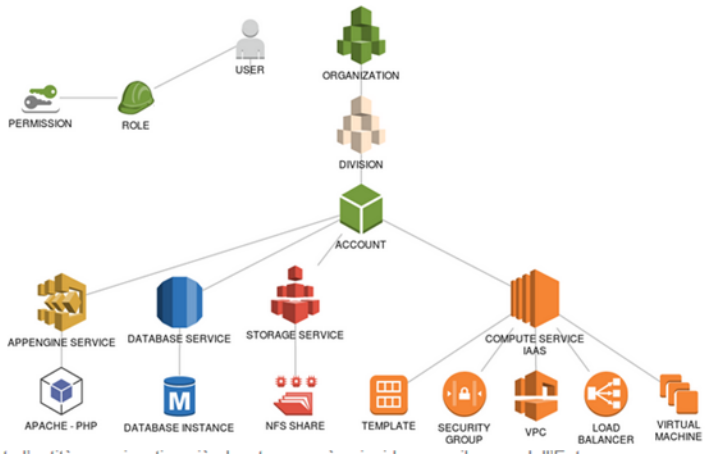
The organisational structure is the hierarchical subdivision that allows customisation of services, access or settings for different groups of users or devices. In the Nivola platform the organisational structure is divided into 3 levels:

- **Organisation**: it is hierarchically the highest organisational entity and may coincide with the name of the client e.g. “Regione Piemonte”, “Csi Piemonte” and so on. In the platform, resources are available to various organisations, which are however logically completely separate and independent;;
- **Division**: : is the second organisational level. An organisation may have several divisions. The concept of Division therefore represents a logical subdivision of the Organisation, and may therefore reflect a territorial, organisational or business type division; furthermore, each Division controls the resources and consumption of each Account within the Division”;
- **Account**: is the last organisational level and depends on the Division. A Division contains one or more Accounts. The Account is the organisational level within which the user can create, control and manage their

services. “It is possible to create multiple accounts for the purpose of separating different projects, or to distinguish development environments from production environments, or to divide consumption reporting.




Note that all resources and services can only be associated at Account level. It is not possible to associate services with Divisions or Organisations. The Account is therefore the container in which all user services are implemented and made available. The management of user resources will therefore take place at Account level with roles enabled to operate at this level.




### 1.2.3 Users, Roles and Account

Several roles can be distinguished within the platform, which are related to the defined organisational structure. Each role can correspond to at least one user, and therefore at least one natural person performing that function. A person registered on the system can be associated with several roles even on different organisational structures. For example, a user may have different roles on accounts in different divisions.

To date, the following user roles are implemented within the system.

**Organisation Master**: this role represents users who can carry out administrative functions within the organisation, such as the creation of divisions and accounts within the organisation; it can also profile users to make them operational within its structure and possibly register users not yet present on the platform. The Organisation Master can monitor the costs and status of resources at all levels of his organisation (divisions and accounts) and view the related reports. However, he does not have access to the management functions (create/edit/delete) of the resources associated with the accounts of his organisation.

**Division Master**: this role represents users who can perform administrative functions within the Division, such as the creation of accounts within their division; they can also profile users to make them operational within their structure

and possibly register users not yet present on the platform. The Organisation Master can monitor the costs and status of resources at all levels of his organisational structure (accounts) and view the related reports. However, he does not have access to the management functions (create/edit/delete) of the resources associated with the accounts of his division.

**Back Office Administrator**: user who, within the system, has privileges over BackOffice functions (registration of new Users, Accreditation, creation of organisational levels) and monitoring of costs and platform status. The BackOffice Administrator can profile users with roles at any level of the organisational structure. He can also access aggregated cost and consumption reports at any level. The role is usually associated to users of Csi Piemonte management and support groups.

**Account Master**: user who can manage all resources within the account, over which he therefore has maximum privileges. The Account Master can therefore create/delete/edit resources, he can also manage resources created by other users in the account. The account master can view and access cost and consumption reports for his account. The Account Master can register new users within his account and can profile or revoke users who have already been granted access.

**Account Viewer**: user who can view all resources within the Account, but does not have edit/delete privileges. The Account Viewer can therefore view the list of services active on the Account, and can view their details, but cannot activate new services or change their status. The Account Viewer can view and access reports of aggregate costs and consumption for the Account. The Account Viewer cannot register new users on the platform and cannot profile other users for access.

The phase of introducing a new user is as follows: a master, within the limits of the privileges of his hierarchical level, can accredit a user registered on the platform by assigning him a role, thereby granting him permissions to perform certain functions which will place the new user in a certain group.

The same operation can be carried out and delegated to the Backoffice operator.

To sum up:

- An Organisation Master may *accredit or revoke users* within its own divisions or accounts.
- A Division Master may *accredit or revoke users* within his own accounts and division.
- An Account Master can *accredit or revoke users* within their account.
- The Backoffice Administrator can *accredit or revoke users* at any level of the hierarchical structure

## 1.3 Certifications and Compliance

For us, Security and Privacy are fundamental and so important that the development of the Nivola platform was conducted with three key aspects in mind:

- **security**
- **organisation of the service**
- **reliability**

Starting from these pillars, we have identified services, processes, organisation and IT solutions that fully comply with Italian and international regulations, in particular for cloud computing services and the data centres that host the Nivola Availability Zones, including connectivity at the Turin and Vercelli data centres. By applying these constraints we have obtained the most important certifications in the Cloud field, which make us compliant with the highest standards of security and reliability.

**ISO 9001:2015**


Certification ensures that our system provides for the systematic management of risks and opportunities, the constant monitoring of business processes to ensure quality standards, and the adherence to service times and costs in the context of

- design, implementation, interconnection, maintenance, training, management and operational management of **automated information systems and of application, infrastructure and network information services**;
- design and delivery of **training interventions** and training on the ICT services provided.

**ISO 27001:2013**


**ISO/IEC 27001** is the only auditable and certifiable international standard that defines **the requirements for an ISMS** (Information Security Management System) and is designed to ensure the selection of appropriate and proportionate security controls. It is based on precise requirements to ensure security in the management of information and the handling of derived risks. The certification obtained by CSI Piemonte ensures that all cloud services available to customers are designed to guarantee maximum security in information management. The scope of certification includes the design, implementation, delivery and support of facility management services for Data Centres and cloud computing services.

**ISO 27017:2015**


**ISO/IEC 27017** series of standards and **defines advanced controls for both providers and customers of cloud services**. It clarifies the roles and responsibilities of the different actors in the cloud with the aim of ensuring that data stored in cloud computing is safe and secure. The integration with ISO 27017 is therefore aimed at **demonstrating CSI Piemonte's ability to ensure data protection**.

**ISO 27018:2014**


The Certification attests that the Nivola System complies with the directives on the protection of personal data and therefore the privacy of customers who entrust their information to a Cloud service.

**The Code of Conduct for the Protection of Personally Identifiable Information (PII) in Public Cloud Services for Cloud Providers** is a guideline for public cloud service providers who want to improve their management of personal data.

The **objective of this standard** is to provide a structured way, based on privacy by design, to address the main legal and contractual issues related to the management of personal data in distributed computing infrastructures following the public cloud model. The specific countermeasures introduced by ISO 27018 are based on defined international privacy principles. These principles have been used to guide the design, development, implementation, monitoring and measurement of privacy policies and privacy controls in the cloud computing services offered by CSI Piemonte.

Integration with ISO 27018 is intended to **demonstrate CSI Piemonte's ability to ensure data protection**.

**ISO 20000-1:2018**

The Certification demonstrates that CSI, as a Cloud Provider, implements all best practices to establish, implement, maintain and improve a service management system, a reference framework to support management in the lifecycle of cloud service delivery. The standard promotes the use of an integrated model of IT service management processes that corresponds to the ITIL® framework (IT Infrastructure Library), a standard adopted by CSI Piemonte since the early 2000s.

**ISO 22301:2012**

The Certification recognises the ability of CSI Piemonte in relation to the cloud services provided to put in place behaviours, recommendations, processes, technologies in order to ensure the resilience of the services provided in the face of events that may compromise customer services and the very ability to provide cloud services in continuity.

**ISO 50001:2011**

The Certification determines that our Energy Management System has been planned and implemented in compliance with energy legislation and is aimed at ensuring the energy efficiency of the production processes it promotes:

- energy saving and progressive reduction of waste;
- optimisation of current energy uses, in particular in the data centre and heating/air conditioning of buildings;
- evaluation of energy efficiency aspects in procurement processes

**ANSI TIA 942 2017 Rating III**


The ability of our Data Center to guarantee the continuity of the services provided is guaranteed by the certificate obtained. Rating III demonstrates that the Data Centres hosting Nivola's cloud services are equipped with highly reliable and resilient systems. All components are redundant, allowing any maintenance intervention without the need of service interruption. The minimum uptime guaranteed by Tier III is 99.98% on an annual basis.

**AGID CSP qualification - PA Cloud**

Accreditation as a Type C Cloud Service Provider qualified by **AGID** to provide cloud services to the Italian Public Administration allows customers to benefit from secure and reliable services. The qualification ensures that in providing our services we adopt all the standards required to offer digital services to the PA. Additional information can be viewed in the AGID Cloud Marketplace. https://cloud.italia.it/marketplace/service/12

CHAPTER

TWO

# HOW TO TAKE YOUR FIRST STEPS

This chapter describes the basic steps to start using the platform.

## 2.1 Necessary steps

In order to start using the Nivola platform, you need to follow the steps below.

1. *Accreditation Process*
2. *Completing the Organisational Levels*
3. *Activate Users*
4. *Check VPCs*
5. *Check Security Group*
6. *Creating Services*


1
Accreditamento
Per cominciare a utilizzare la piattaforma è necessario ricevere dal supporto la comunicazione via e-mail della prima credenziale associata ad un livello organizzativo
2
Completare Livelli Organizzativi
Verifica che la struttura organizzativa sia completa fino all'account. Nel caso non lo sia, aggiungere i livelli organizzativi necessari .
3
Attivazione utenti
Lctetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.
4
Verifica Security Group
Verificare che i Security Group necessari per segregare gli ambienti applicativi,web e storage siano definiti e completi delle regole necessarie. Apportare le eventuali modifiche
5
Creare Servizi
Creare ed utilizzare i servizi infrastrutturali che la piattaforma mette a disposizione.

## 2.2 Accreditation Process

In order to use the services exposed by the Nivola platform, it is necessary to be accredited according to the following process:

1. Contact your reference account or go to the Contacts section accessible from the site www.nivolapiemonte.it. Once the contract or the use of the service in "Demo" mode has been activated, the Nivola Support Team will contact the customer's reference account to proceed with the creation of the first access credentials.
2. After receiving the official registered offer, proceed with issuing an order to CSI-Piemonte.
3. Approve and commit the amount in the offer by means of a decision.
4. Please send the documentation by PEC to protocollo@cert.csi.it, indicating in the subject line of the email:

a) Activation of Nivola Services.

b) Protocol number on the offer.

c) Name of organisation.

5. Please indicate a contact person who will be contacted by our support service for technical details. If the person to be contacted in the event of a security incident is different from the person indicated above, a different contact person must be identified in accordance with the latest data breach regulations.

These aspects are set out in the service user manual and in the general terms and conditions, where you can find more details and information, including on the termination of the service. Should this occur the ISC undertakes to make its data available to the Customer and subsequently to delete them.


At the end of the application phase you will receive an e-mail from the Support Team informing you of your **first accreditation**. In this way the user will be able to check the organisational structure modelled by Support and grant further accreditations.

## 2.3 Completing the Organisational Levels

The platform consists of three organisational levels, the one hosting the services being the **account**. If the account has not been defined by the support, before creating it it will be necessary to identify or create a **Division** on which it depends. The presence of the **Organisation** and the Division are necessary conditions for the generation of the **account**.

## 2.4 Activate Users

After having set up the organisational structure, it will be possible to indicate to **Nivola** the **users** associated with **roles** which, at each level, will be able to act on the objects with specific tasks.

## 2.5 Check VPCs

After creating the account and associating the users with the correct organisational profile, the correct configuration of their **VPCs (Virtual Private Cludes)** must be checked. Within their VPCs, users can manage and configure their own resources. The **VPC** guarantees the necessary isolation between the various organisations.

## 2.6 Check Security Group

Nivola provides some pre-configured SGs, but it is possible to modify their rules or create new SGs according to specific needs. "It is therefore important to check them and eventually modify or integrate them before starting to create the Services. In any case, it will always be possible to modify the security rules even after the Services have been created, but it is not possible to move a Service from one SG to another after it has been created. In this case it will be necessary to destroy the Service and recreate it in the correct SG.

## 2.7 Creating Services

After completing the above steps, you can start creating services via the Service Portal menu. The creation process is always guided through a creation wizard. The process can always be interrupted before the final confirmation and you can directly access this guide for more information.

CHAPTER

THREE

# THE SERVICE PORTAL

- **What is SP**
- **Access to the Service**
- **User interface**

**What is SP**

The Nivola Service Portal (NSP) constitutes the Reserved Area for customers and integrates in a web interface all the functionalities offered by the platform. It provides the full range of functions designed to create, control and manage your own cloud services independently. Through a set of simple and intuitive graphical wizards, all the services offered by Nivola can be used by users, even those without specific technical skills. The user can constantly monitor the status of resources through integration with monitoring dashboards, information and reports on costs and consumption, can create new services and communicate with the *Nivola Support Center* using different communication channels.

**Access to the Service**

from the following authentication systems:

1. SPID
2. CIE - Electronic Identity Cards
3. TS-CNS - Health Card System
4. PSNet
5. Piedmont system

Regardless of the authentication system chosen by the user, the Nivola Service Portal will proceed to

1. redirect the user to the correct Identity Provider for verification of credentials
2. obtain the user's tax code
3. authorise access to the Nivola platform according to your profile

This is the window that is presented to the user when logging in:


Depending on the type of customer, the user can choose between

- Company
- PA, for Public Administration customers
- CSI Piedmont staff
- It is possible to access using SPID credentials or Piedmont system for public administration.


- PA. It can be accessed using SPID or RUPAR credentials.


**User interface**

After *l'autenticazione* user is presented with their own personalised Home Page. The content displayed depends on the user's role in the system.

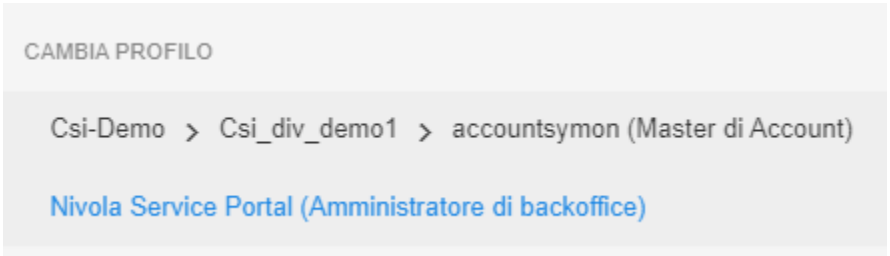
The User Home Page is divided into 3 distinct sections

**1 – Status bar**


It is located at the top of the system and indicates which user and which profile the user is logged into the system with.

If the user has other associated roles, he can change the profile under which he acts within the system. By pressing on


The "Change profile" menu is presented, with which the user can change his profile




 Allows the user to contact support via chat.

Press instead  to access Nivola's online documentation.

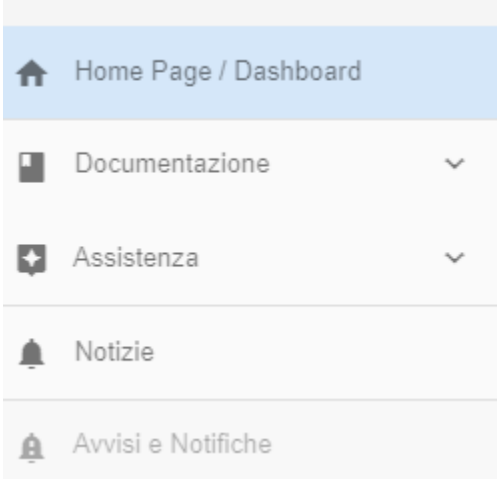
To exit the system and close the work session press the symbol 

**2- Menu navigation**

The left-hand side menu contains the list of services that the user can consult and use according to his profile.

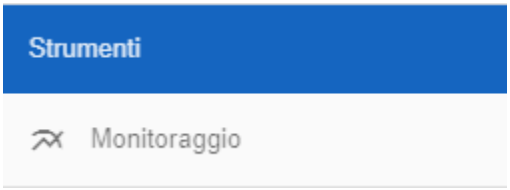
The navigation menu consists of several sections according to the type of services.

The first section



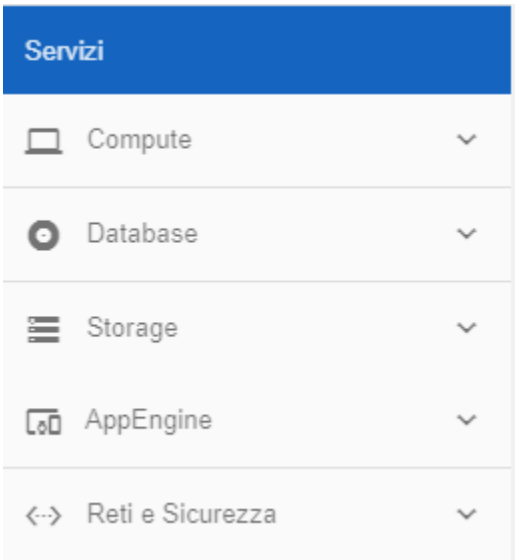

allows access to all the information material on Nivola via “Documentation”, allows contacting assistance via “Assistance” and to have the details of news and information on the platform via “News”.

The “Tools” section



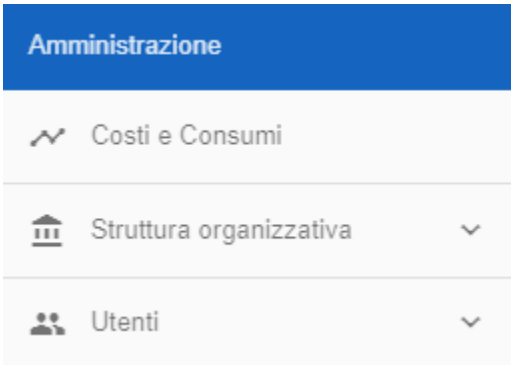

It contains the menu items for accessing the tools offered by the platform to its users. For example, the monitoring consoles or log display systems can be accessed from here.

The “Services” section is the menu of the services offered by the Nivola platform. In this item the user will find the list of all the services on which he can operate within Nivola to create his own Cloud resources.



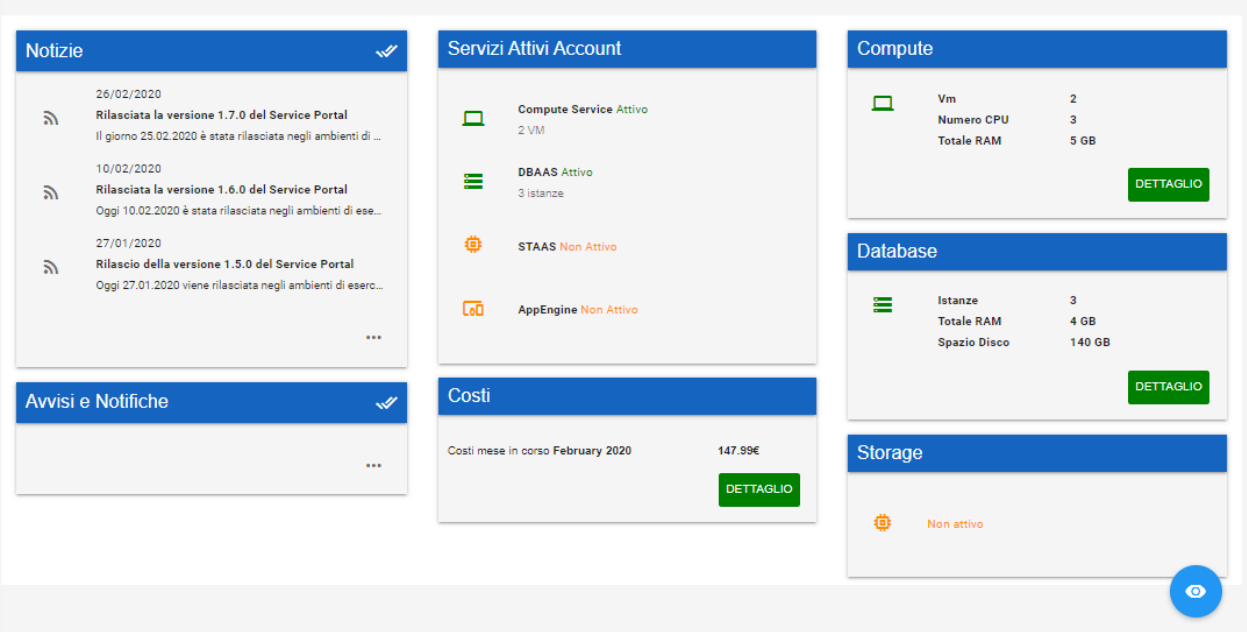

In the “Administration” section all those items are made available that allow the user to manage, according to his profile, user profiling and accreditation, or he can view the details of his organisational structure and access the pages

detailing the costs and consumption of his Cloud.




### 3 - Home Page

This is the initial page presented to the platform user. It is composed of a set of dynamic dashboards displayed by default according to the profile with which it is accessed. Through this home page the user can see a summary of consumption and the status of their services and consult the latest news published.

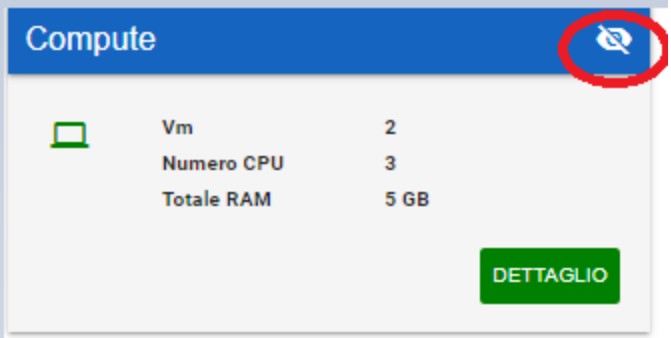



The Home Page is customisable by the user, who can set the display and layout of the dashboards according to his preferences or priorities.

To activate the Home Page edit mode, press

At this point it will be possible:

- Disabilitare la visualizzazione di una dashboard. Per fare questo premere il simbolo evidenziato presente nella dashboard che vi vuole non più visualizzare in quanto non di interesse




- Disable the display of a dashboard. To do this, press the highlighted symbol on the dashboard that you no longer wish to view as it is of no interest.
- Move the dashboard within the HomePage frame. To do this, hold down the mouse on the blue bar of the dashboard and move it within the workspace. Release the mouse once you have defined the new position.

To confirm changes to the layout and make the personalised home page effective, press

CHAPTER

FOUR

# HOW TO

In this section you will find a series of tutorials to get you started right away with the platform, through the portal.

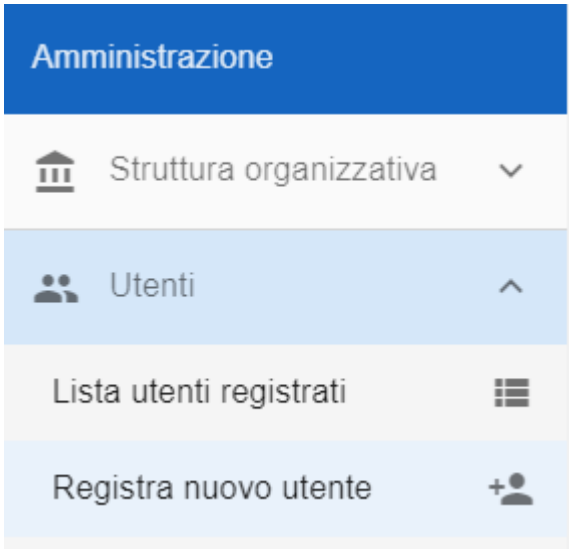
## 4.1 Managing a User

These are the functions for managing the user lifecycle in the Nivola Portal.

### 4.1.1 Create User

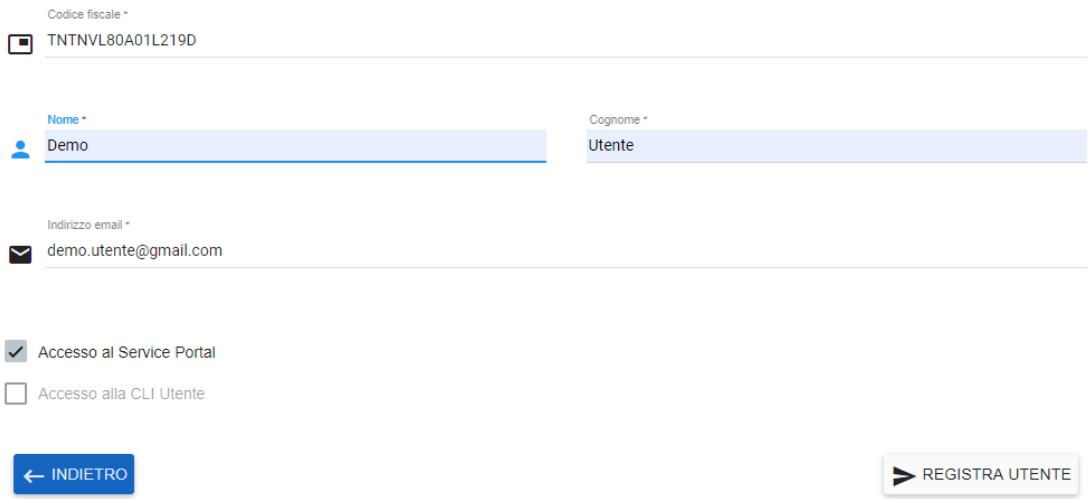
The **Create a User** function can be activated mainly in these two ways:

1. From the left-hand side of the screen, click on the label **Register New User** in the **Administration** group




2. From the **Registered Users** list, press the

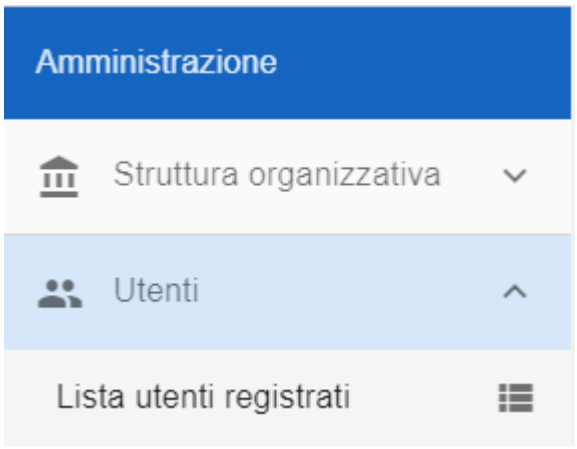
In both cases, after activating the function, fill in the form presented by the system indicating: *Fiscal Code, Name, Surname* and the *type of access* and then press the **REGISTER USER** button.



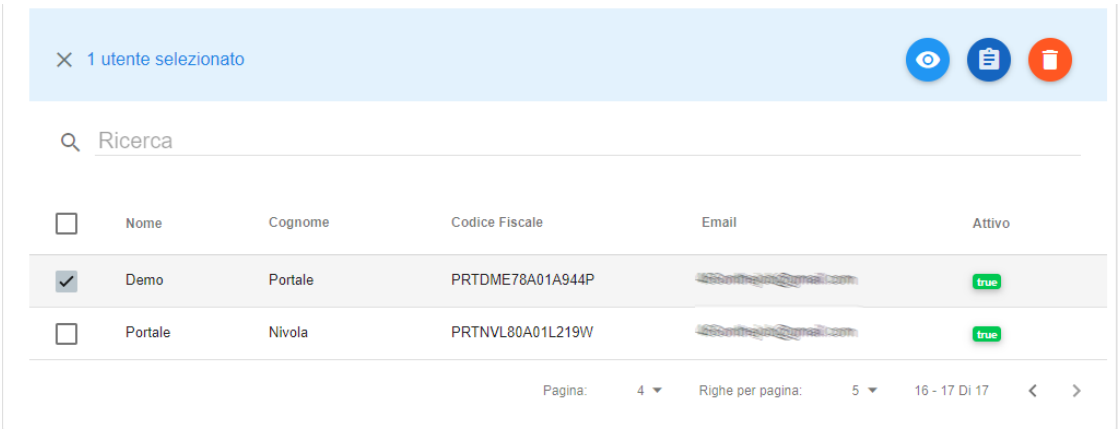

There is an option, exclusively for users of the csi domain, in which autoregistration is possible. The user, if the data entered is correct, will be generated and then available for l' *Accreditamento*

### 4.1.2 Accredit User

The **User Accreditation** function can be activated from the **Registered Users** list

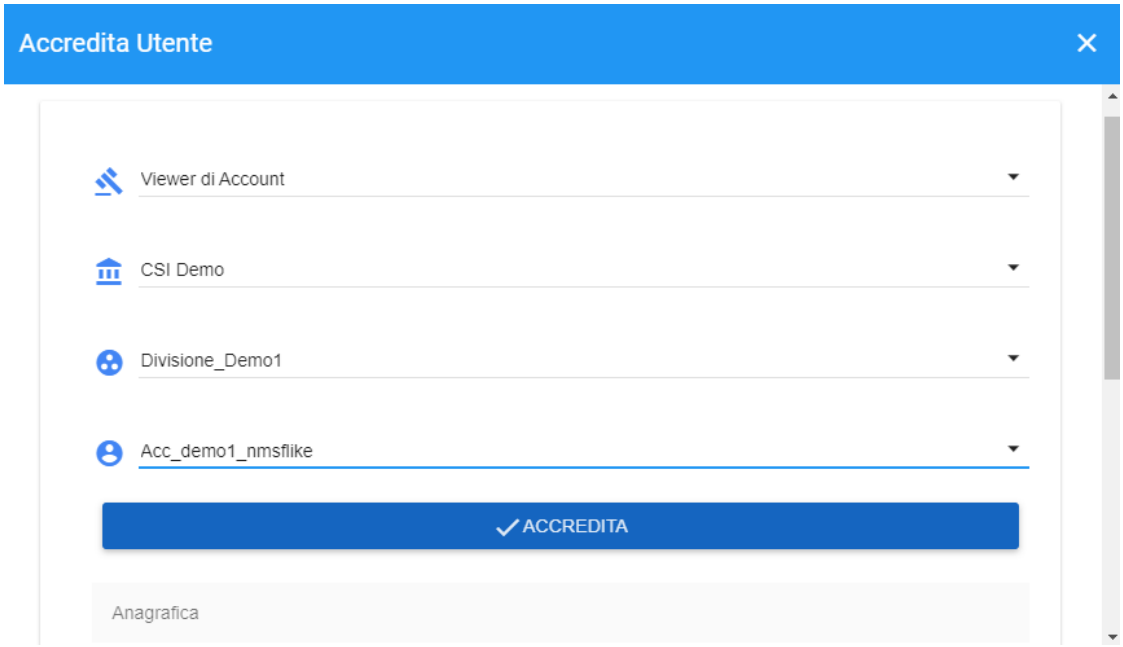



From the list, select the user to be credited by ticking the relevant checkbox.



Press the **Accredit User** button

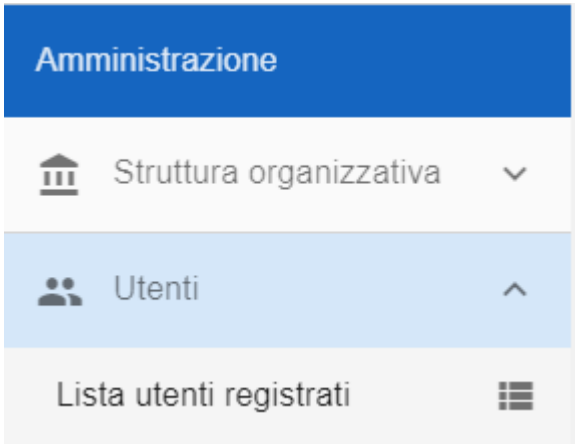
In the new form, using the Combo Boxes, indicate your **Role, Organisation, Division, Account** and press the **Accredit** button



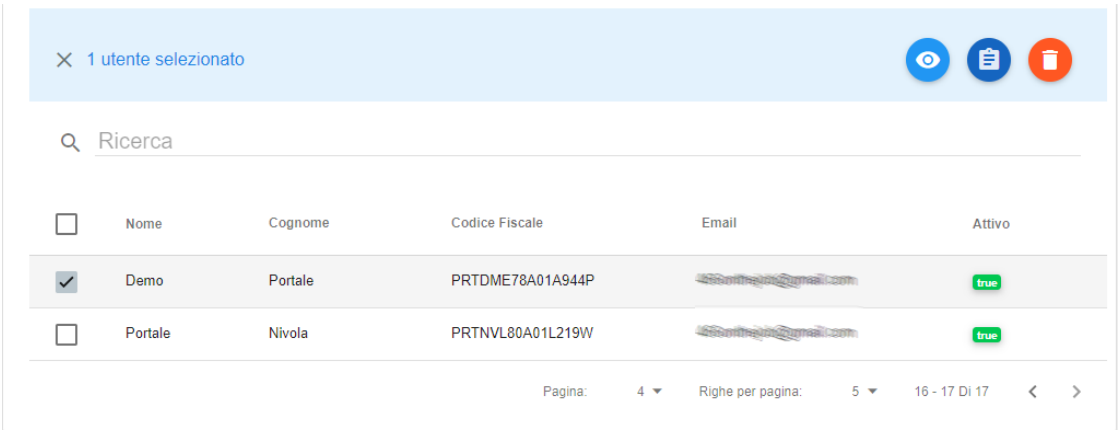

The user will be accredited in the organisational level and role indicated.

### 4.1.3 Verify User Credits

The function for the **User's Credit Check** can be activated from the **Registered Users List** button



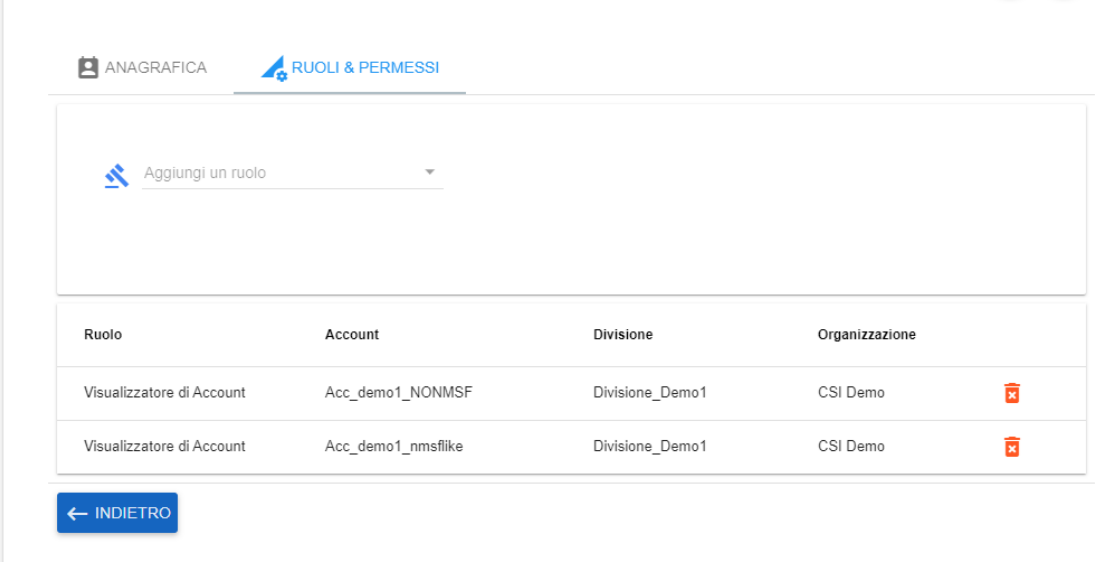

From the list, select the user whose details you wish to consult by ticking the relevant checkbox.




Press on the **View User Details** button

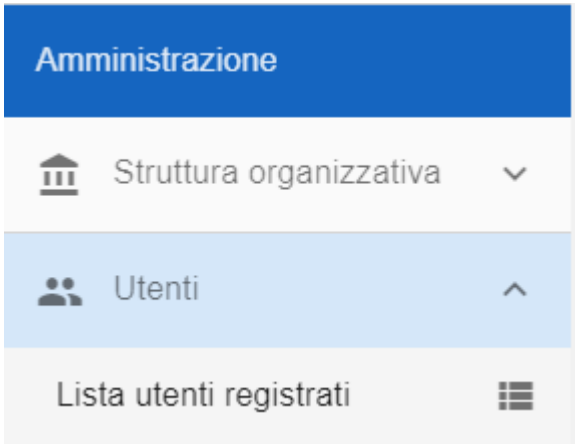
The first page displayed by the portal is the **Profile** page.


Using the tabstrip, the list of **Roles and Permissions** assigned to the user will be displayed.

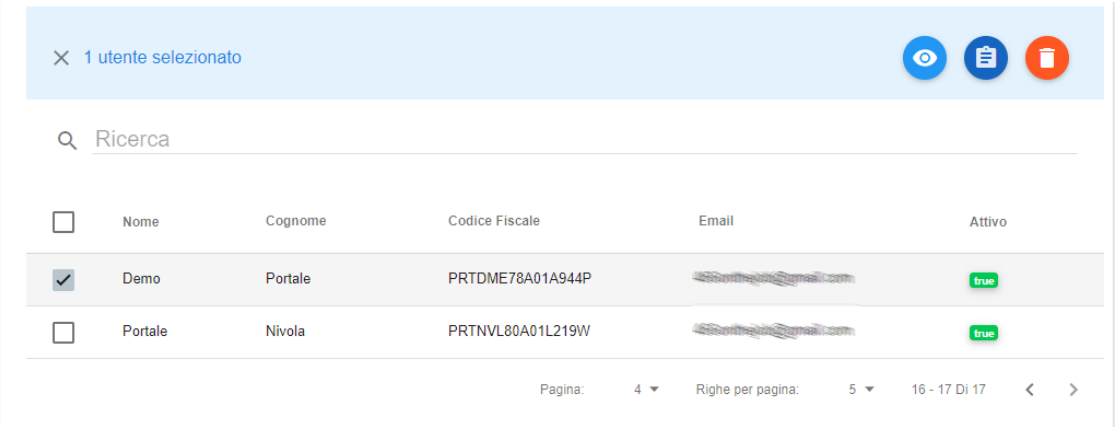



### 4.1.4 Revocare Utente

La funzione è attivabile dall'elenco **Utenti Registrati**




Dall'elenco selezionare l'utente da accreditare mettendo una spunta sulla Checkbox relativa




Premere sul pulsante **Accredita utente**

Dalla lista degli accreditamenti, individuare quello da revocare


Per completare l'operazione, cliccare il tasto **Revoca accreditamento**

## 4.2 Creare Account

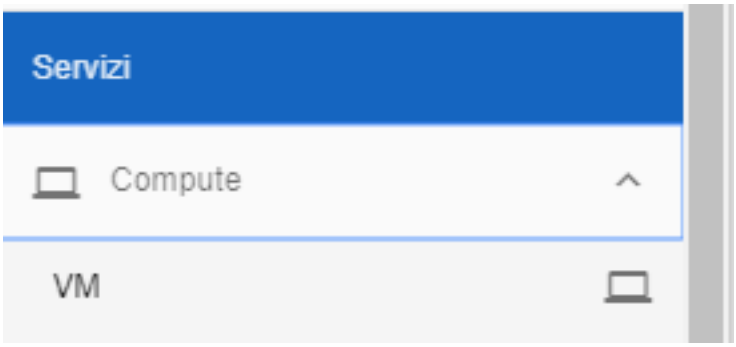
**TO DO**

## 4.3 Lavorare con Virtual Machine

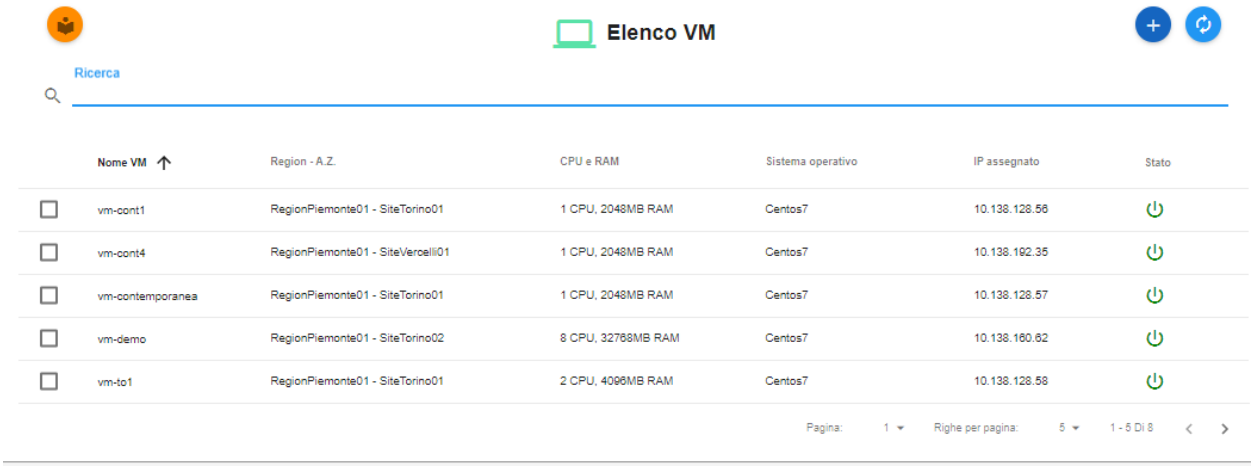
Tutte le funzioni per gestire il ciclo di vita delle Virtual Machine

### 4.3.1 Creare Virtual Machine

La funzione rientra nel **servizio compute**. La **creazione Vm** è attivabile dalla parte sinistra dello schermo, cliccando sulla label **VM** sotto **Compute**



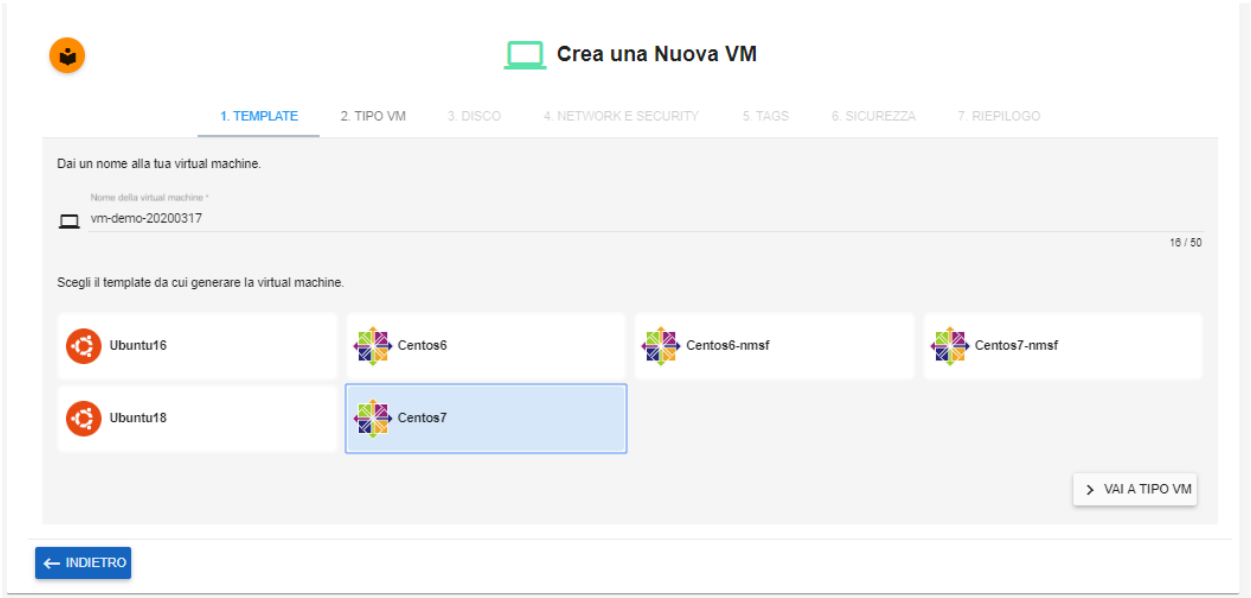

A seguito di un clic su **VM**, il sistema popolerà la parte destra del video con l'**Elenco delle VM**.



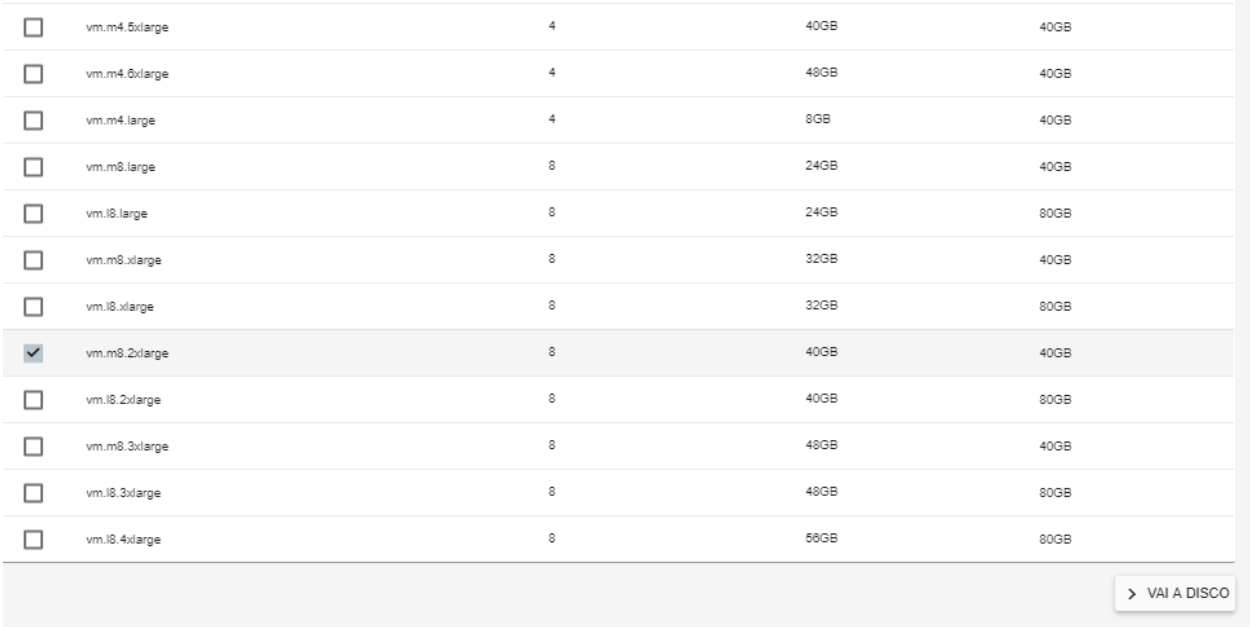

Per la creazione del server, dalla lista, procedere in questo modo:

1. Fare clic sul pulsante **"+"**:

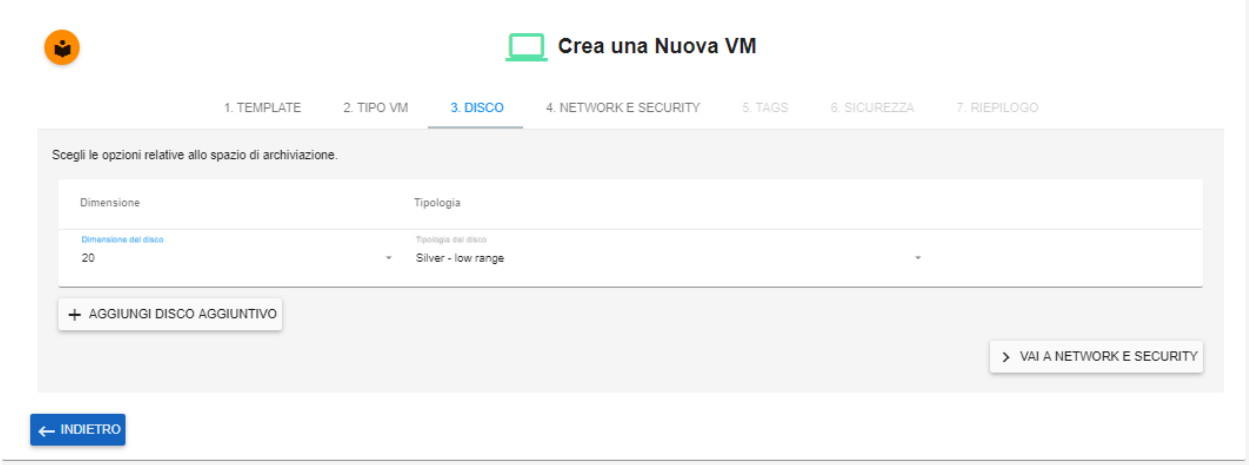
2. Inserire il **Nome della virtual machine** nella textbox e scegliere il **TEMPLATE** da cui generare la virtual machine. Per farlo baste un clic su uno degli OS proposti e in ultimo sul pulsante **VAI TIPO VM**;



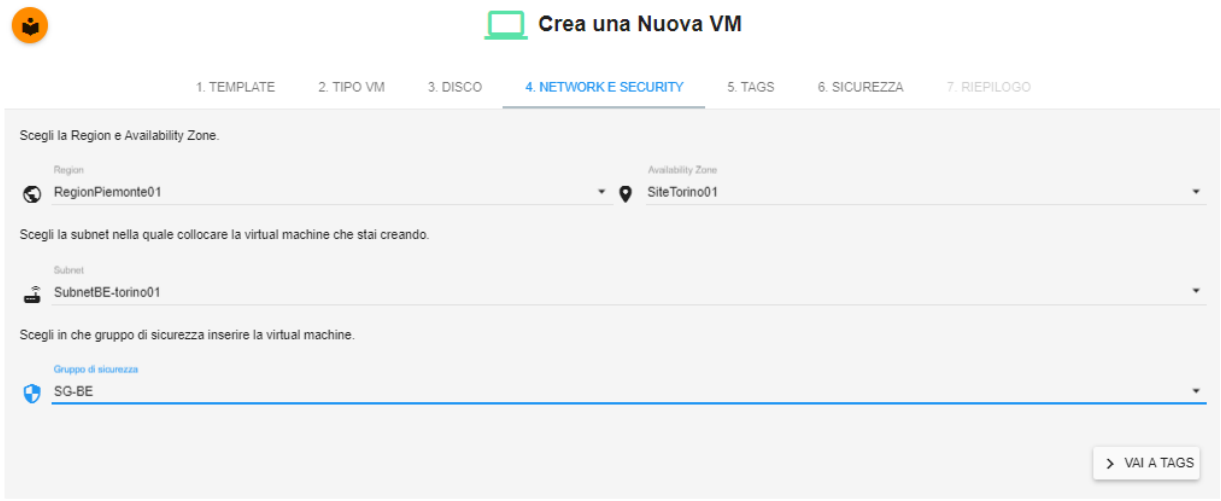

3. Specificare il type, la CPU, la RAM e il Disco sfruttando il **CheckBox** in testa ad ogni riga esposta dal portale e cliccare sul pulsante **VAI A DISCO**;



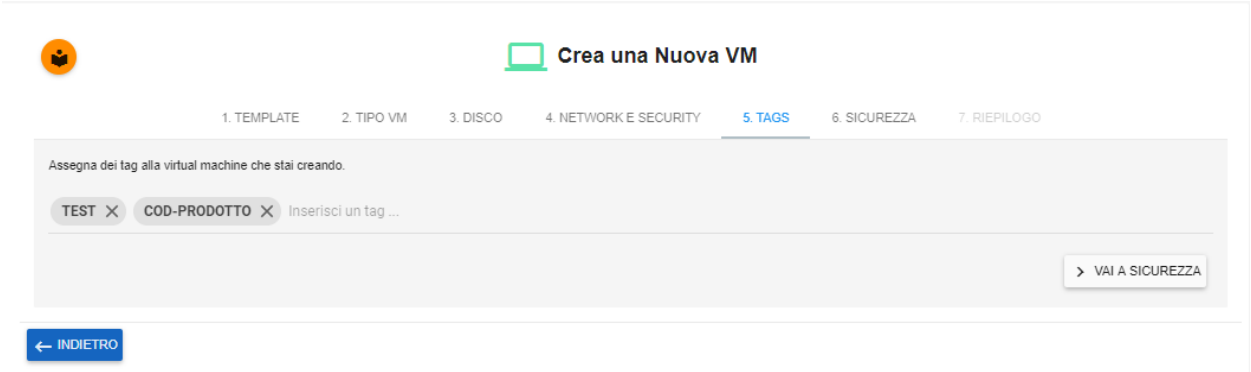

4. Indicare dimensione del disco ed eventualmente, aggiungere altri dischi, sfruttando il pulsante **AGGIUNGI DISCO AGGIUNTIVO**. Al termine, proseguire cliccando su **VAI A NETWORK E SECURITY**;




5. Sfruttando le combo box proposte, inserire: **Region, Availability Zone, Subnet e Gruppo di sicurezza**. Al termine cliccare su **VAI A TAGS**;



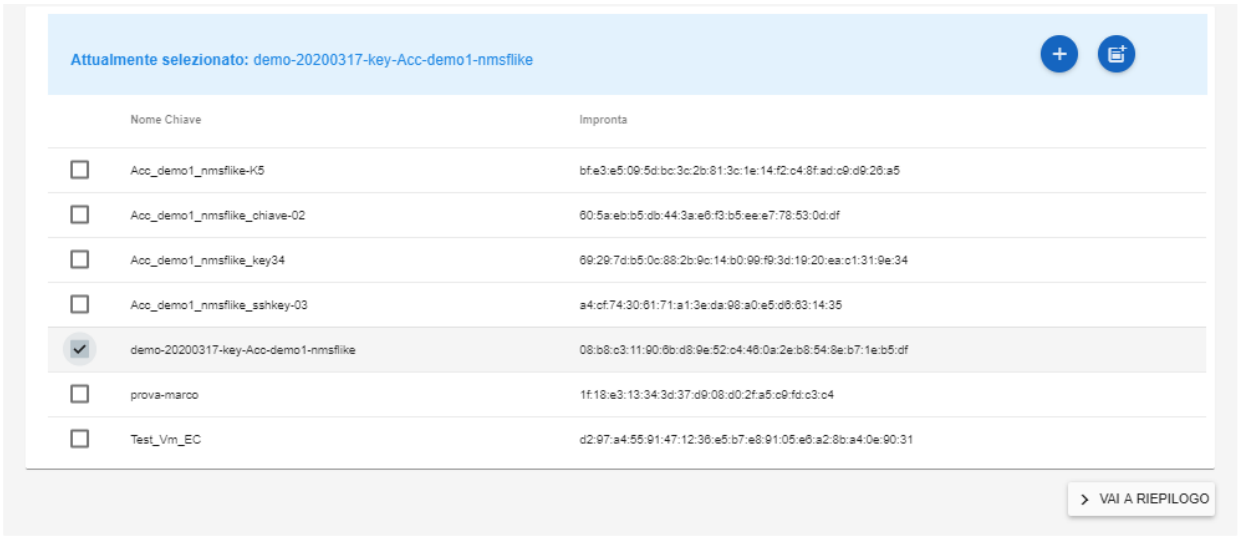

6. Nel caso servissero, è possibile assegnare dei tags alla virtual machine, scrivendoli nella casella di testo e premendo invio. E' possibile eliminare quanto inserito in precedenza, cliccando la **"X"** a fianco dei tags da cancellare. Alla fine, proseguire premendo **VAI A SICUREZZA**;




7. In questa fase è obbligatorio generare una **CHIAVE SSH** da associare alla virtual machine, per farlo, Nivola mette a disposizione 3 metodi distinti.

**SCEGLIENDO UNA DELLE CHIAVI DALLA LISTA**

Con questa soluzione il sistema propone una serie di **chiavi ssh** da cui scegliere. L'operatore potrà individuare la chiave sfruttando la checkbox e successivamente, concludere premendo **VAI A RIEPILOGO**;

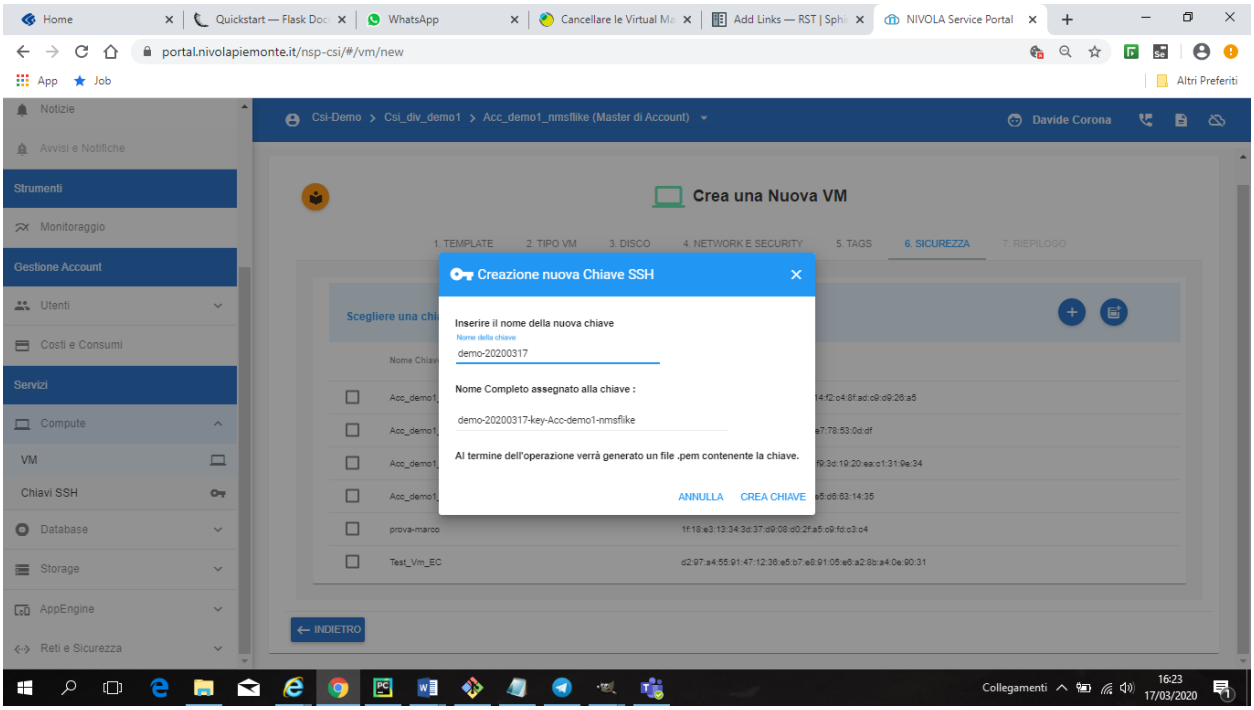



### CREANDO CHIAVE SSH EX NOVO

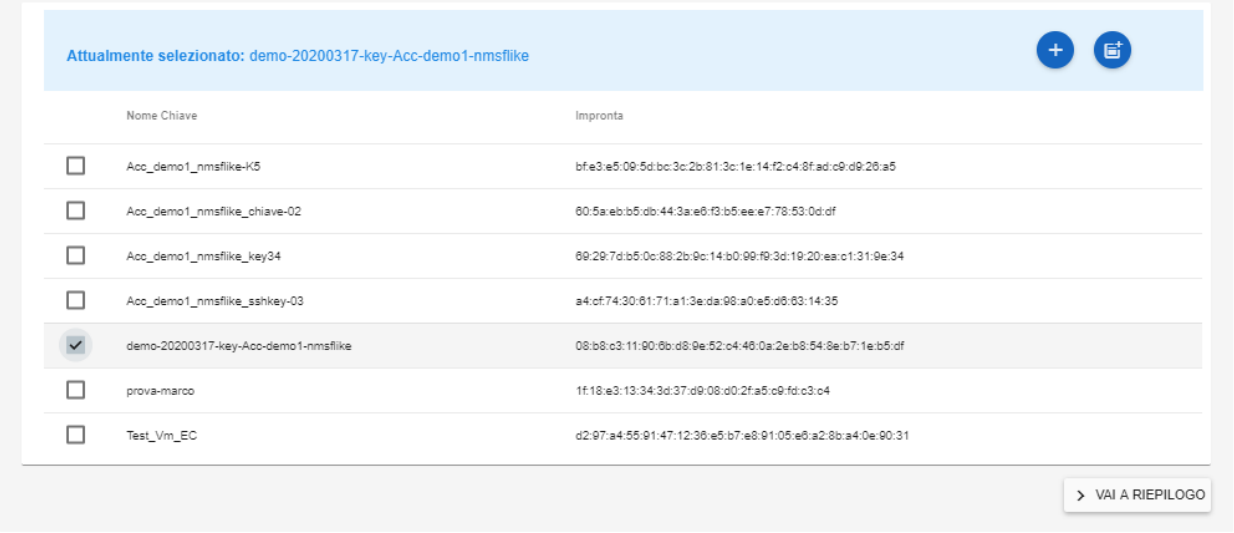
Con questo metodo si chiede al sistema di generare direttamente una nuova **chiave ssh**;

La funzione inizia premendo il tasto **"+"**

Nella casella di testo, **inserire nome della nuova chiave** dando modo al sistema di dare un nome alla chiave aggiungendo il suffisso "key", il nome dell'account al termine della stringa digitata. Terminare premendo **CREA CHIAVE**



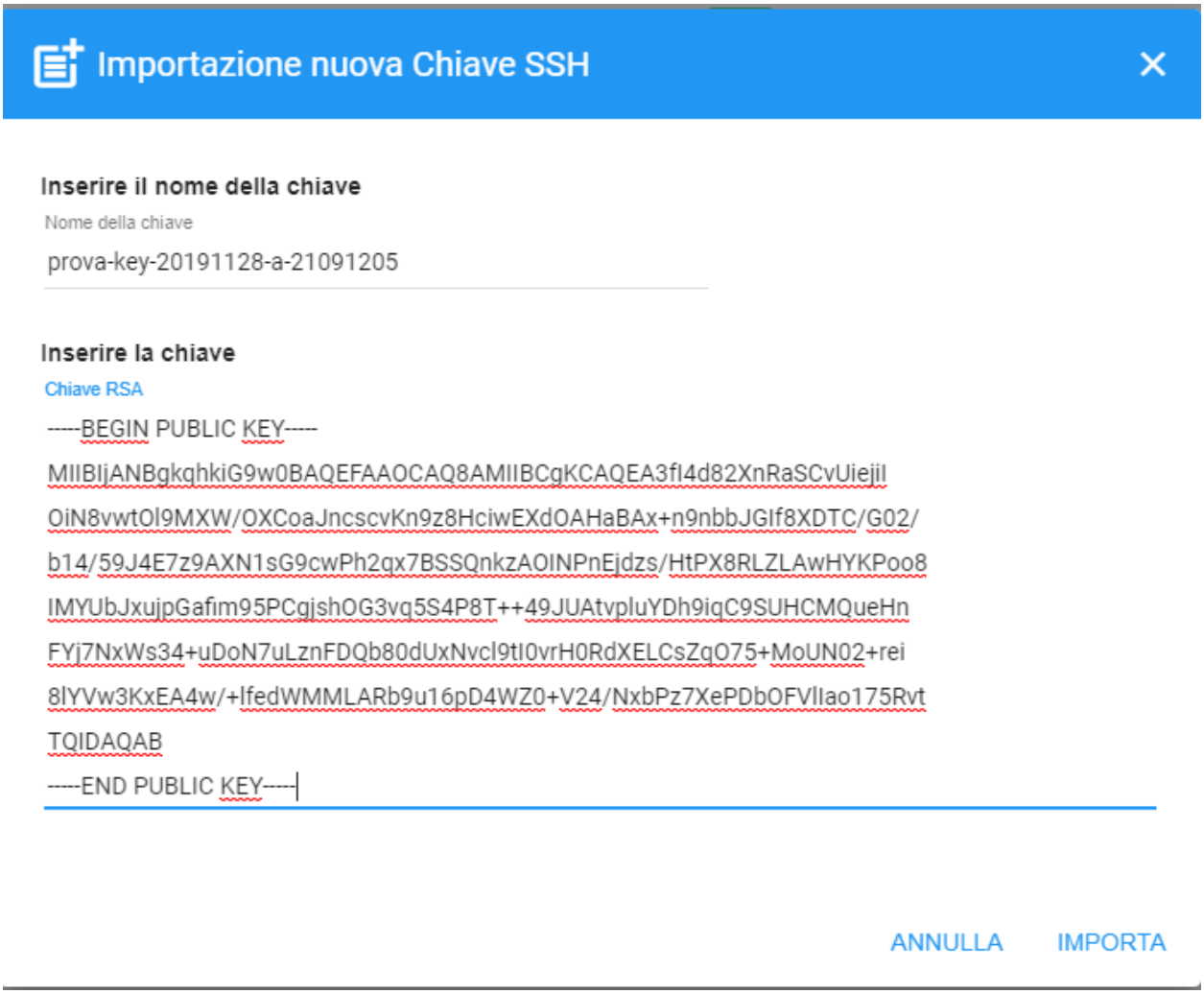
dopo di che distinguerla nella lista e premere **VAI A RIEPILOGO**;



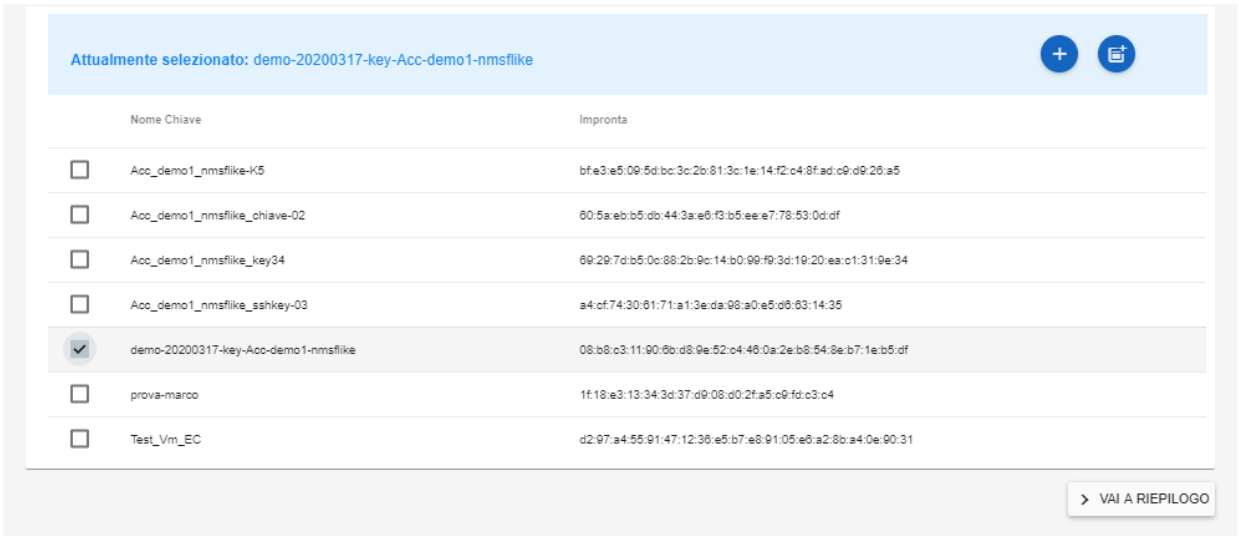

**IMPORTANDO LA CHIAVE SSH**

Premere il tasto per l' "importazione"

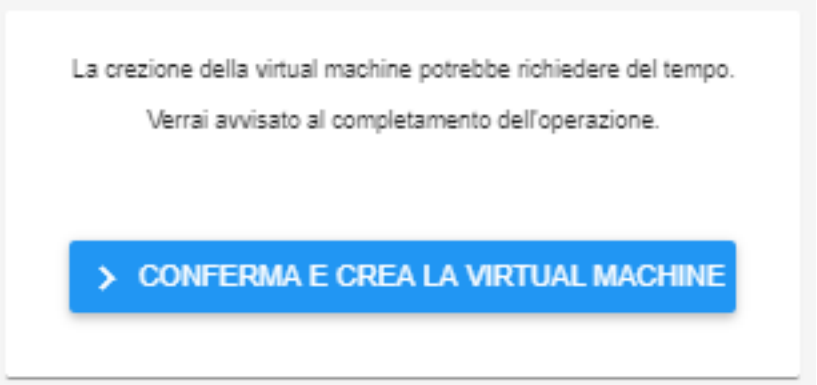
**Inserire il nome chiave**, immettere la chiave precedentemente generata da un sistema esterno a Nivola, nel campo di testo **Inserire la chiave** e premere **IMPORTA**;



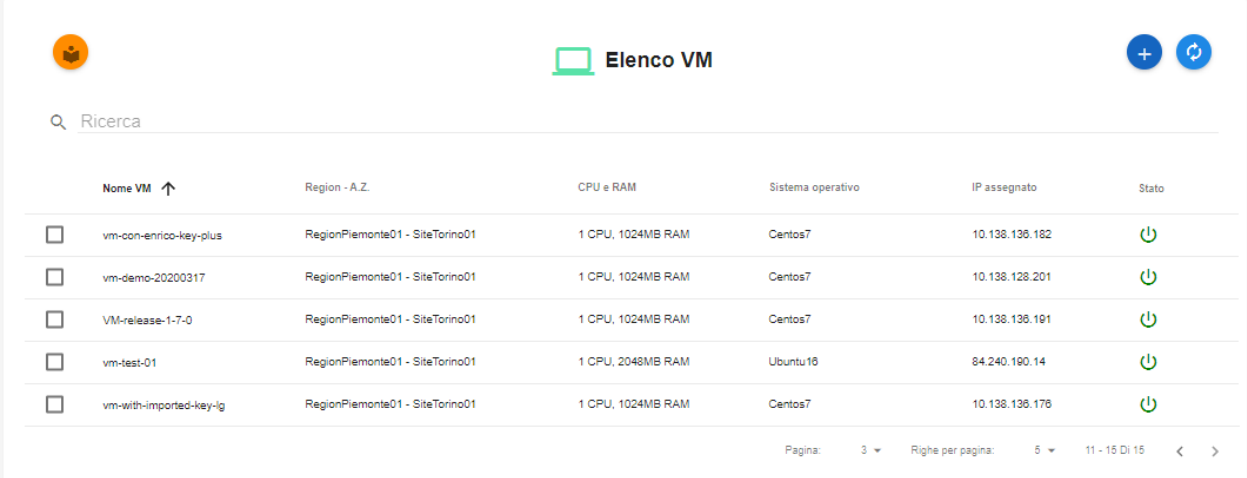

Conclusa la generazione della **chiave ssh**, utilizzare la checkbox per selezionarla dalla lista e premere **VAI A RIEPILOGO**;




8. Controllare gli attributi del server da creare e validarli premendo sul pulsante **CONFERMA E CREA LA VIRTUAL MACHINE**. Il portale procederà alla creazione della **VM** utilizzando i parametri inseriti dall'operatore;




9. Attendere qualche secondo e il server, comparirà nell'**ELENCO VM**. Lo stato iniziale della nuova **Virtual Machine** sarà **acceso** e quindi disponibile.



### 4.3.2 Accedere alla Virtual Machine

I requisiti necessari sono avere una **login** e una **password** forniti dal **Nivola Support Center**. Acclarata questa condizione, procedere come segue:

1) *Accedere alla Commad Line Interface*

2) *Raggiungere la VM seguendo quanto descritto nel paragrafo *Access your Virtual machine**

### 4.3.3 Gestire Virtual Machine

La gestione delle **Virtual Machine** è attivabile dalla voce **servizio compute** posta, nella parte sinistra dello schermo. Cliccando sulla freccia a destra della voce, apparirà **VM** e a seguito di un clic il sistema popolerà la parte centrale del video con l'**Elenco delle VM**.

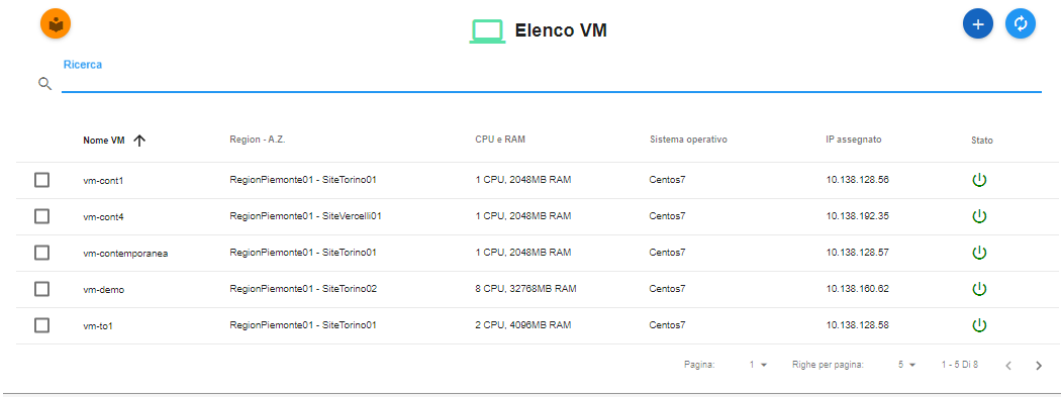
Per **gestione delle VM** si intendono tutte le operazioni che consentono l'uso sistemistico del server in precededenza *creato*. Appartengono a questo gruppo di operazioni:

1. *Cercare le Virtual Machine*
2. *Stoppare le Virtual Machine*
3. *Startare le Virtual Machine*

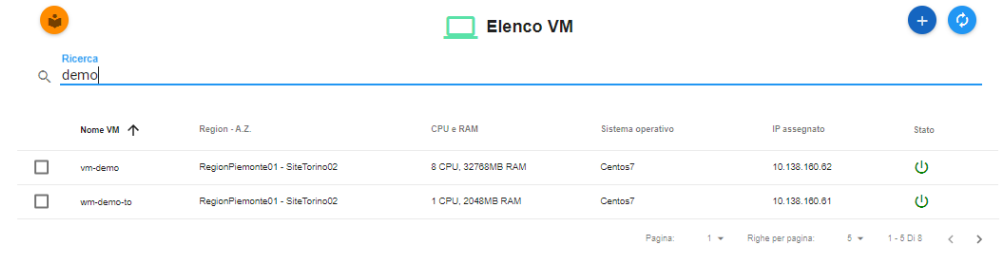
#### Cercare le Virtual Machine

All'interno di ciascun Account è possibile fare ricerche su tutte le istanze create. La ricerca è eseguita tramite una stringa inserita dall'operatore. Nivola ricerca il set di caratteri nelle colonne dove sono elencate le caratteristiche dei server. Per eseguire una ricerca è necessario procedere in questo modo:

1. Inserire la stringa da usare come chiave di ricerca, sotto la label **"Ricerca"** e premere invio;



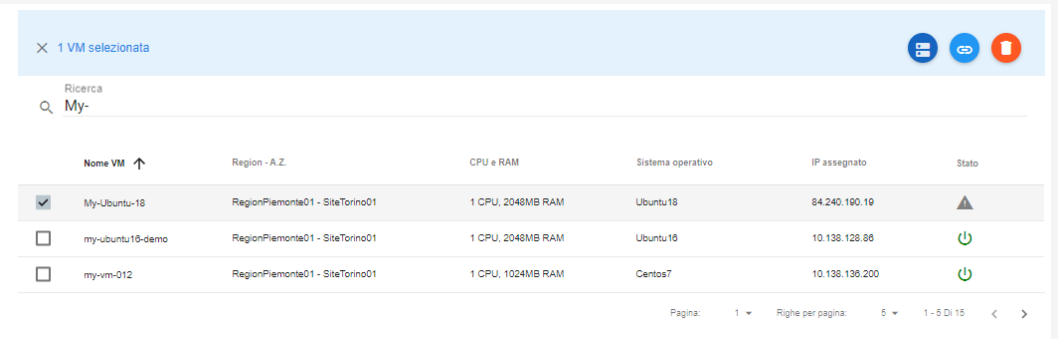

2. Il sistema popolerà lo schermo, con le VM che soddisfano il criterio di selezione;



### Stoppare le Virtual Machine

Per fermare l'attività della Virtual Machine, seguire i seguenti passaggi:

1. Selezionare la VM dall'**Elenco VM** e fare clic sul bottone **Pannello gestione VM**;



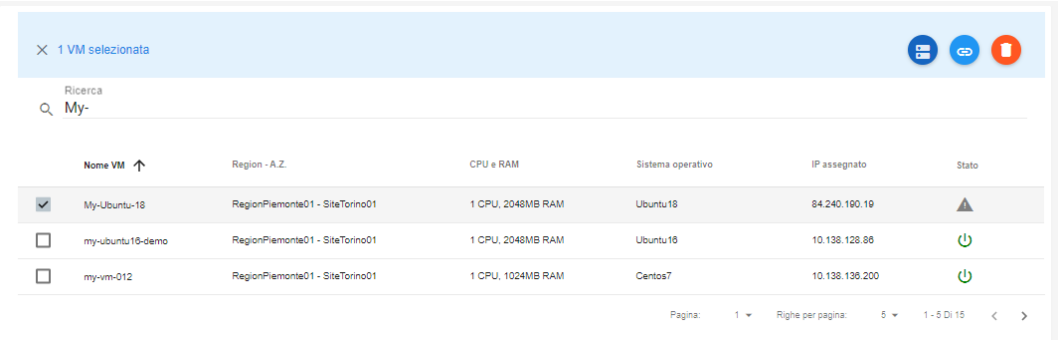

2. Cliccare su tasto **"Pannello gestione VM"**;

3. Cliccare su tasto **"START/STOP"**, successivamente su pulsante **"STOP"** e la VM verrà stoppata;


### Startare le Virtual Machine

Per effettuare lo **start** della Virtual Machine, procedere come segue:

1. Individuare il sever dall'**Elenco VM** e fare clic sul bottone **Pannello gestione VM**;



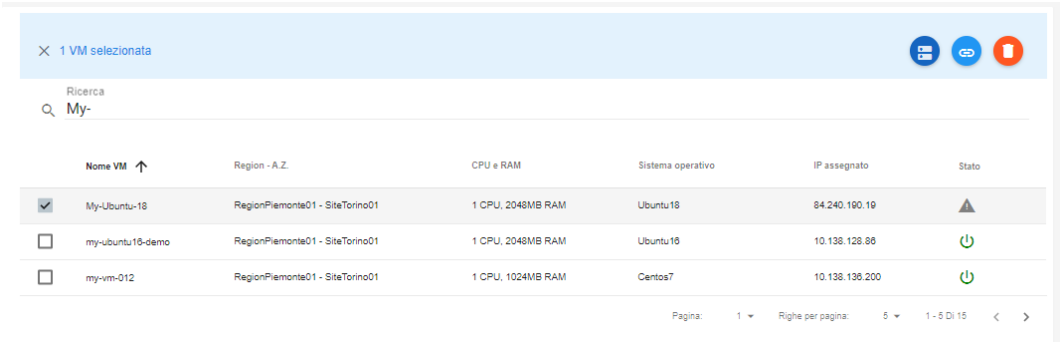

2. Premere il pulsante **"Pannello gestione VM"**;

3. Concludere con il tasto **"START/STOP"** e successivamente sul pulsante **"START"**;


### 4.3.4 Cancellare le Virtual Machine

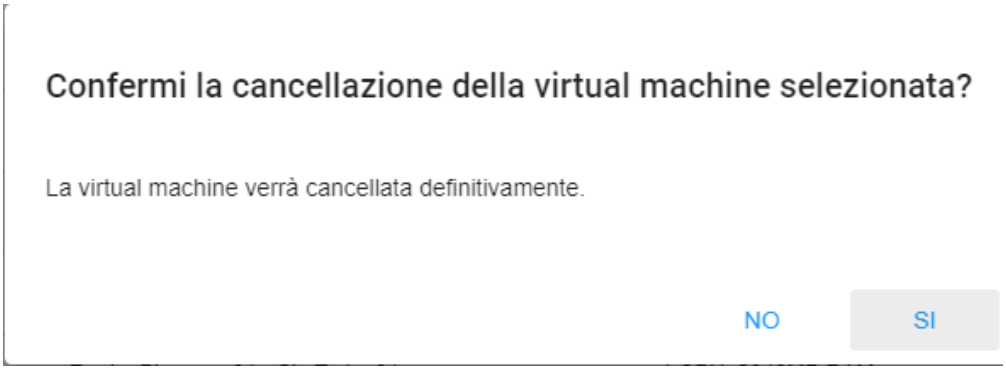
Per **cancellare** una Virtual Machine procedere con le seguenti operazioni:

1. Cercare e Selezionare, dall'**Elenco VM**, l'host da eliminare;

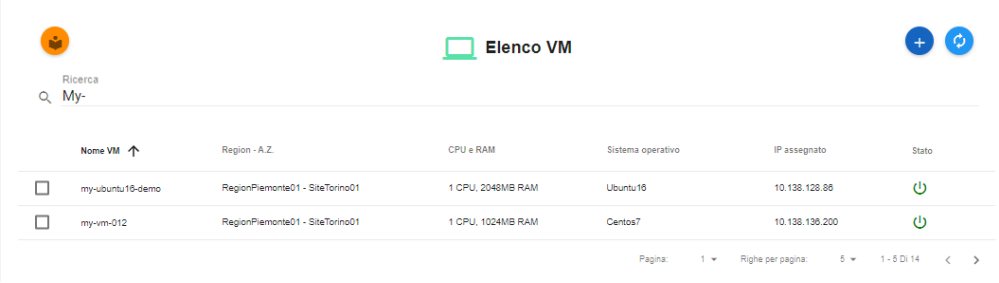



2. Cliccare su tasto **"Elimina VM"**;

3. Confermare l'operazione, sfruttando il pulsante **"SI"**;

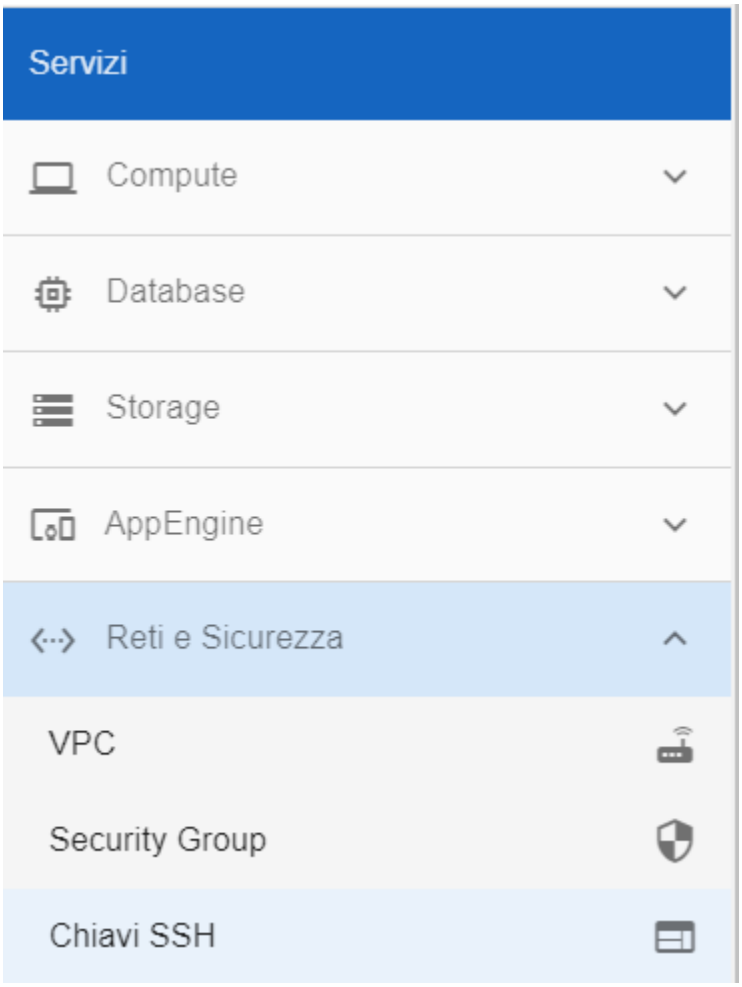



4. La VM sarà **eliminata definitivamente** scomparendo dall'elenco.




### 4.3.5 Creare o Cancellare chiavi SSH

La funzione è utilizzabile da **Reti e Sicurezza** cliccando sulla voce **Chiavi SSH**




E' possibile creare **chiavi ssh** attraverso 2 metodi[1][2] ma per entrambi è necessario rispettare questi vincoli:

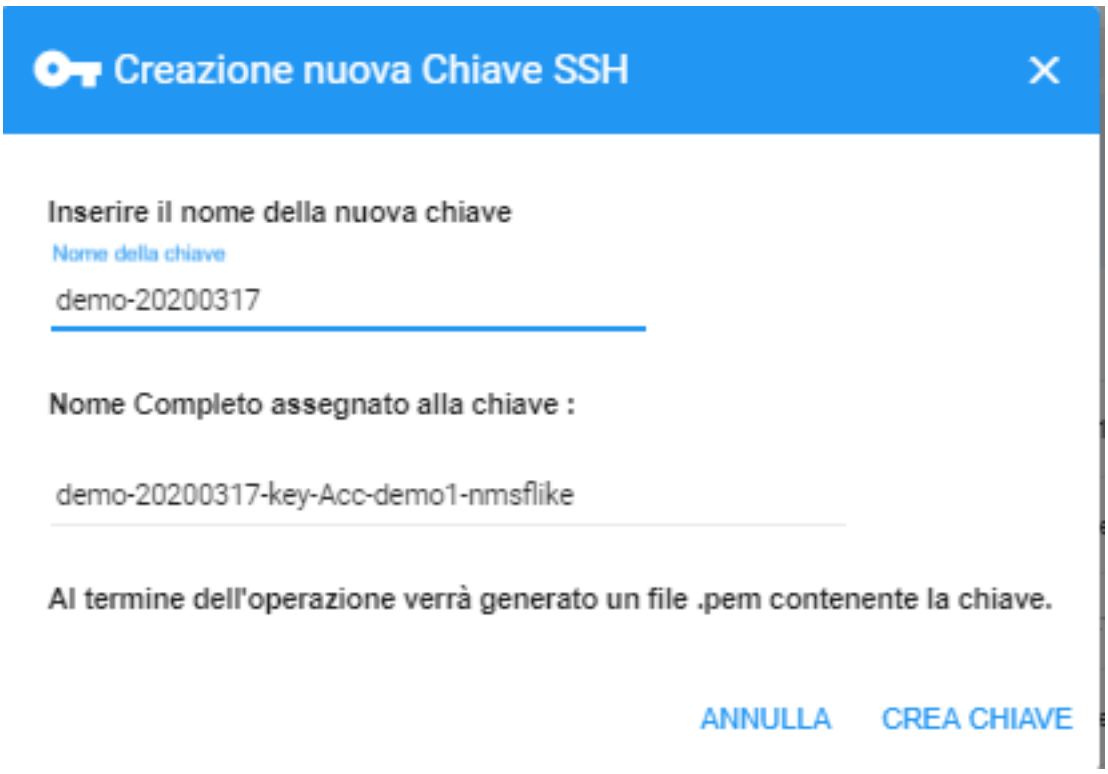
- Il **nome della chiave ssh** deve essre **univoco** in tutto il sistema.
- Il **nome della chiave ssh** non può superare i 40 caratteri
- Nel **nome della chiave ssh** oltre le lettere e i numeri gli unici caratteri particolari ammessi sono **"_"** e **"-"**

1
2

### Creazione direttamente da Nivola

Premere tasto **"+"**;

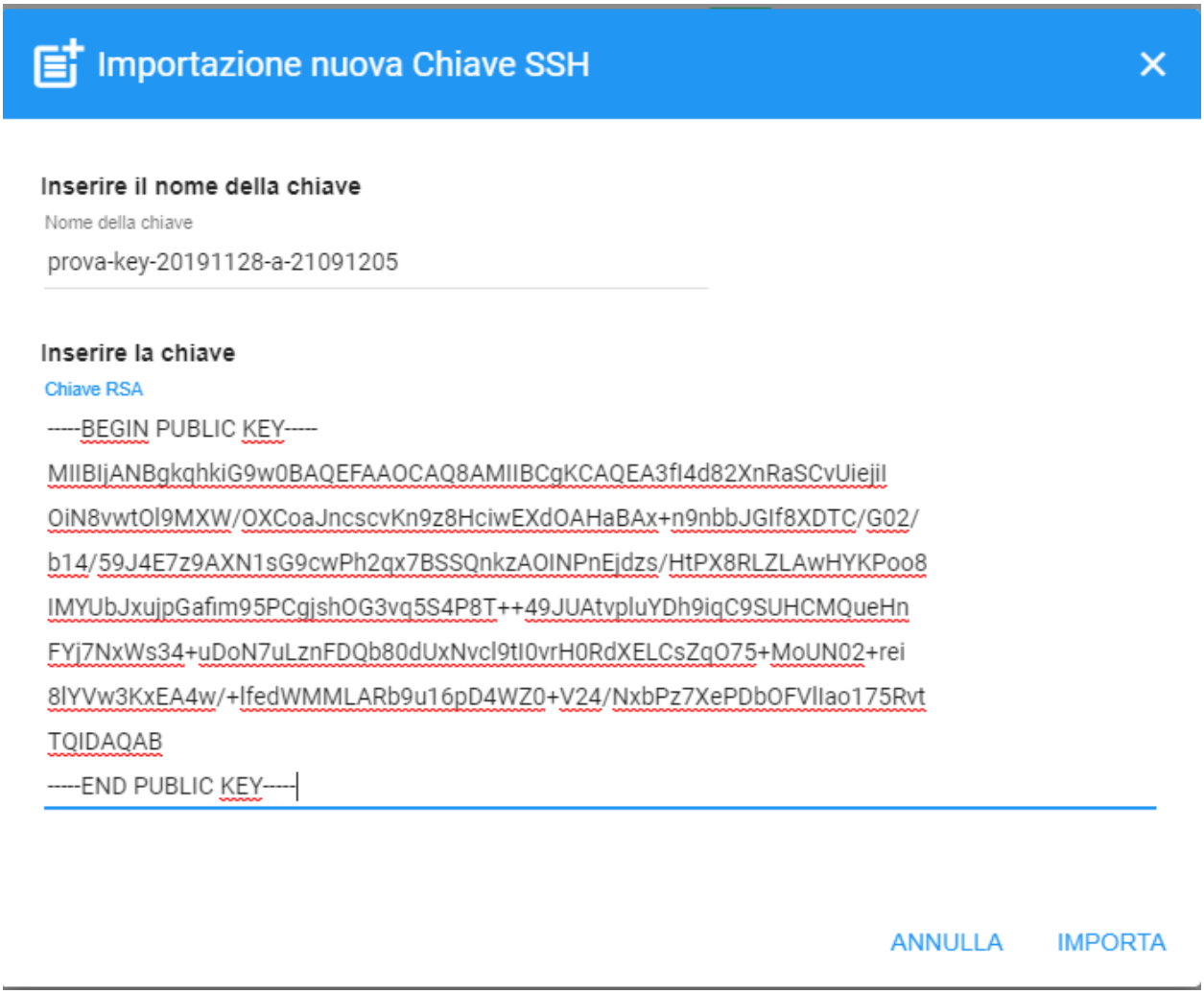
**Inserire nome della nuova chiave e attendere la produzione. Una volta** generata, selezionarla, premere **CREA CHIAVE** e attendere la risposta del sistema.




### Creazione attraverso l'import

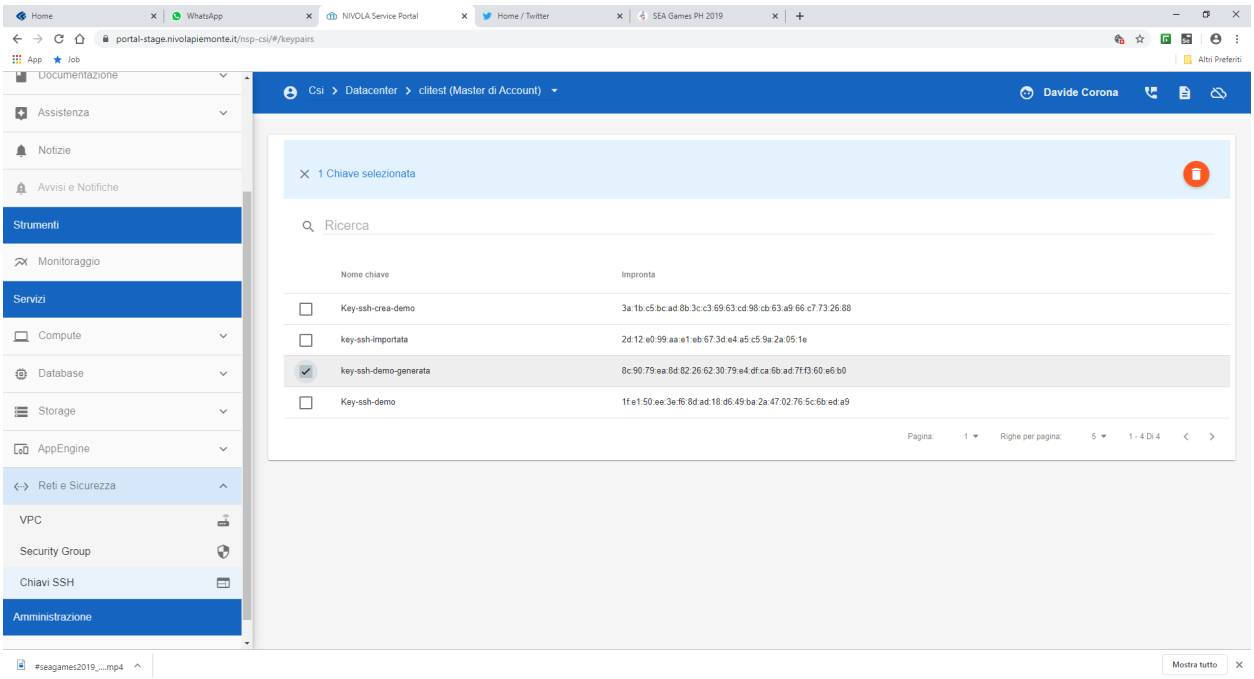
Premere il tasto **"+"**;

**Inserire il nome chiave**, digitare la chiave precedentemente generata nella casella **Inserire la chiave** premere **IMPORTA**.

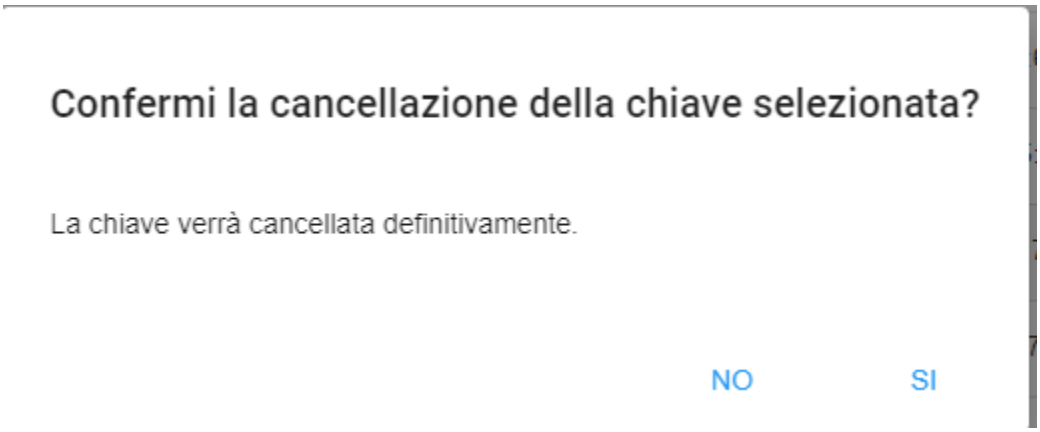



### Cancellare Chiave SSH

Selezionare la **chiave ssh** da cancellare e premere il tasto arancione con il simbolo del cestino.




Il sistema chiederà conferma dell'operazione:



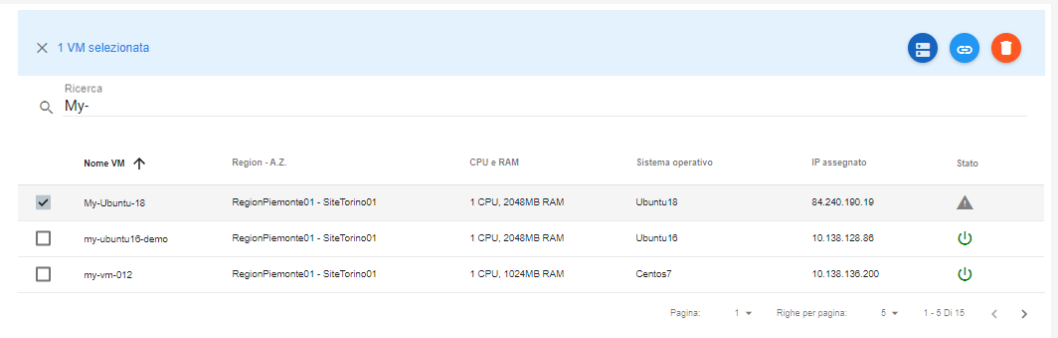

Confermare, cliccando su **"SI"** e la chiave verrà eliminata, scomparendo dall'elenco.

### 4.3.6 Modificare il tipo della Virtual Machine

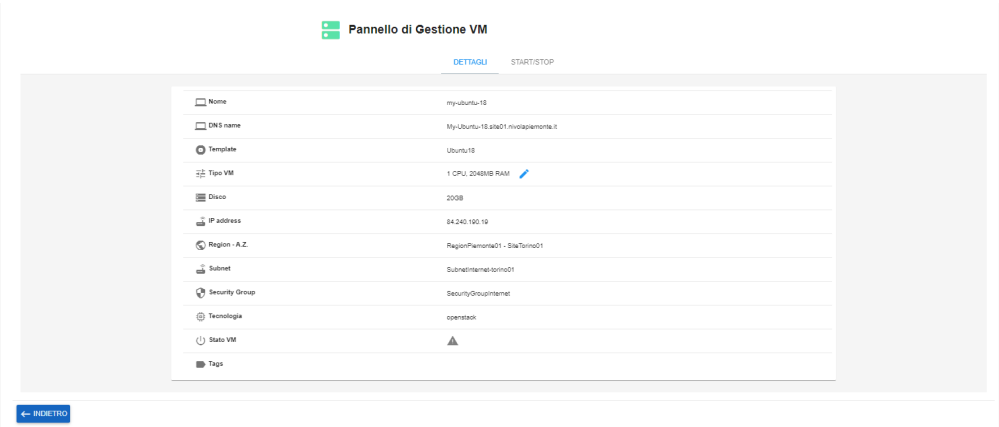
Il sistema consente, con la modifica del **tipo della Virtual Machine**, di sostituire la **CPU** e la **RAM** attribuiti al server in fase di creazione.

Per **modificare il tipo VM** è necessario procedere in questo modo:

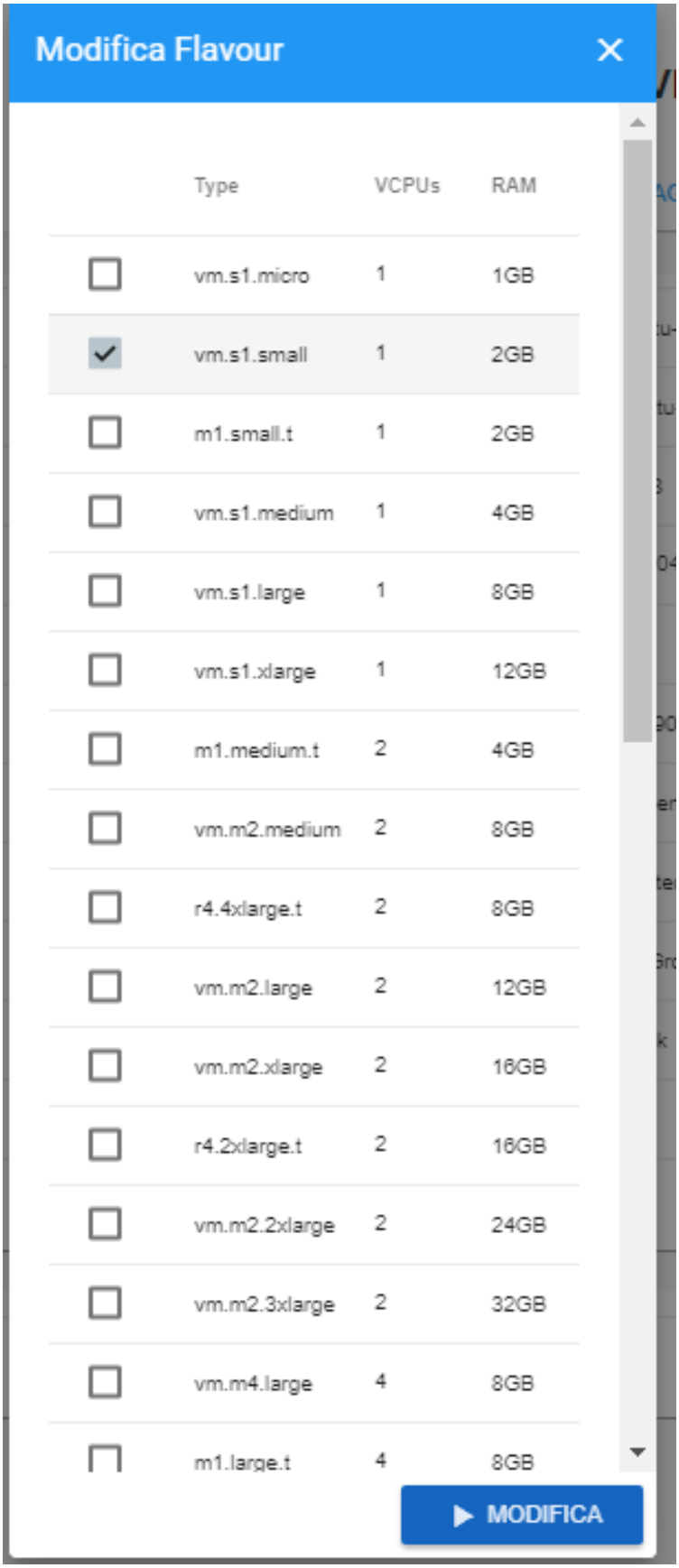
1. Selezionare il server dall'**Elenco VM** e fare clic sul bottone **Pannello gestione VM**;




2. Cliccare sul simobolo della matita a fianco del **Tipo VM**;



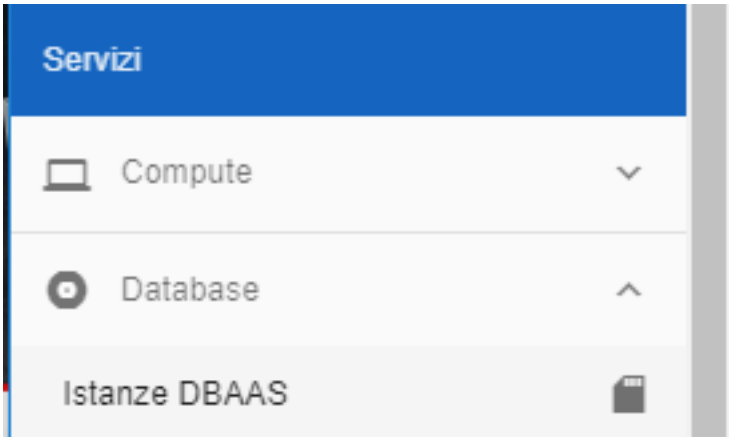

3. Utilizzare il check box a fianco del **flavour** necessario e premere il tasto **MODIFICA**;


Modifica Flavour
Type
VCPUs
RAM
vm.s1.micro 1 1GB
vm.s1.small 1 2GB
m1.small.t 1 2GB
vm.s1.medium 1 4GB
vm.s1.large 1 8GB
vm.s1.xlarge 1 12GB
m1.medium.t 2 4GB
vm.m2.medium 2 8GB
r4.4xlarge.t 2 8GB
vm.m2.large 2 12GB
vm.m2.xlarge 2 16GB
r4.2xlarge.t 2 16GB
vm.m2.2xlarge 2 24GB
vm.m2.3xlarge 2 32GB
vm.m4.large 4 8GB
m1.large.t 4 8GB
MODIFICA

4. Nivola apporterà la variazione richiesta al server;

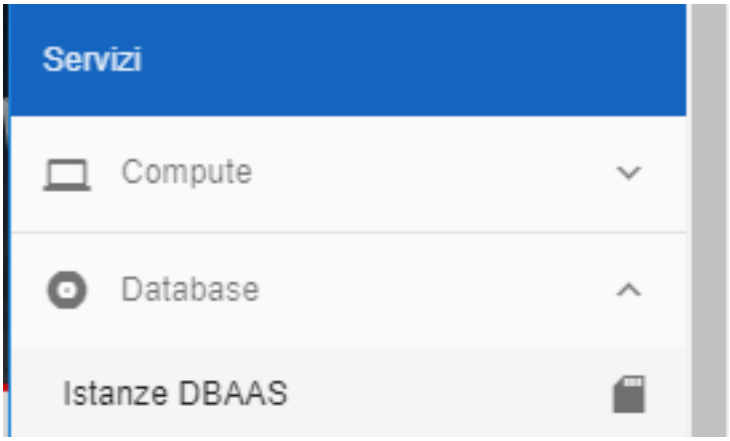
## 4.4 Lavorare con il Database as a Service

"Data Base as a Service" sono servizi gestiti, costituiti da ambienti virtuali dedicati in differenti configurazioni e tecnologie, con differenti livelli di affidabilità e ridondanza in funzione delle esigenze del Cliente. Sono inclusi i servizi di backup, restore, monitoraggio, aggiornamento e patching. Gli engine previsti sono **Mysql** e **Postgres**

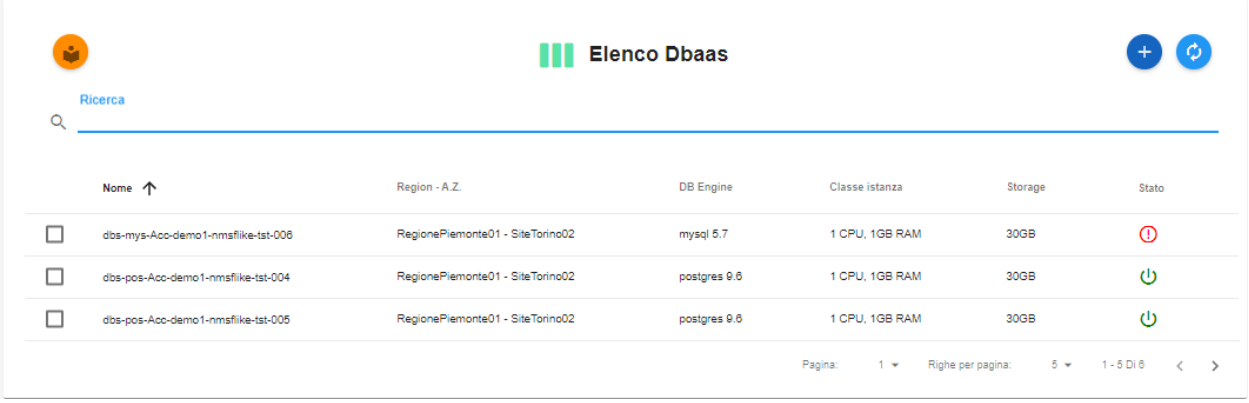



### 4.4.1 Creare istanze del Database as a Service

La funzione rientra nel **Database as Service**. La **creazione DBaaS** è utilizzabile dalla parte sinistra dello schermo, cliccando sulla pulsante **Istanze DBAAS** sotto la label **Database**




A seguito di un clic su **Istanze DBaaS**, il sistema, popolerà la parte destra del video con l'**Elenco Dbaas**.



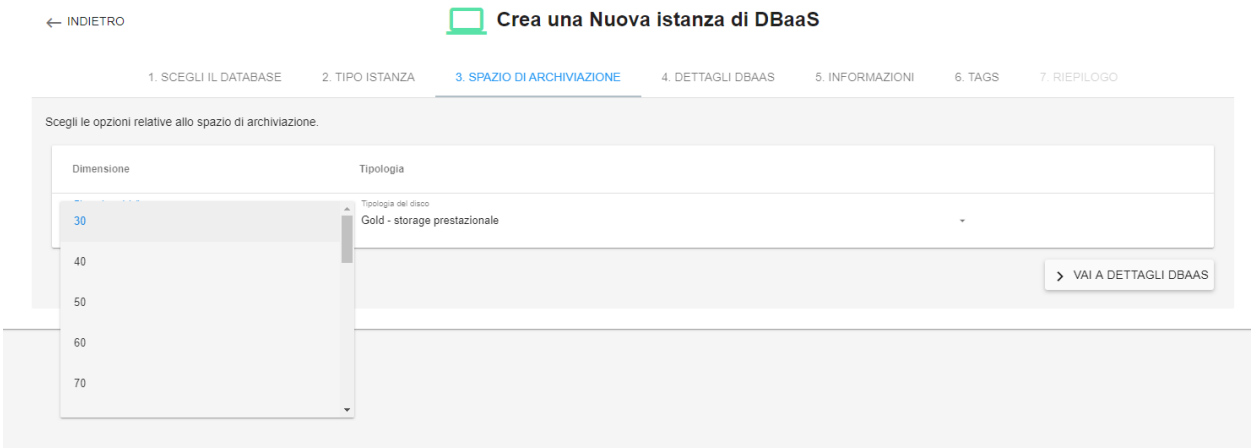

Per istanziare un DBAAS, procedere seguendo i passaggi elencati:

1. Fare clic sul pulsante **"+""**:

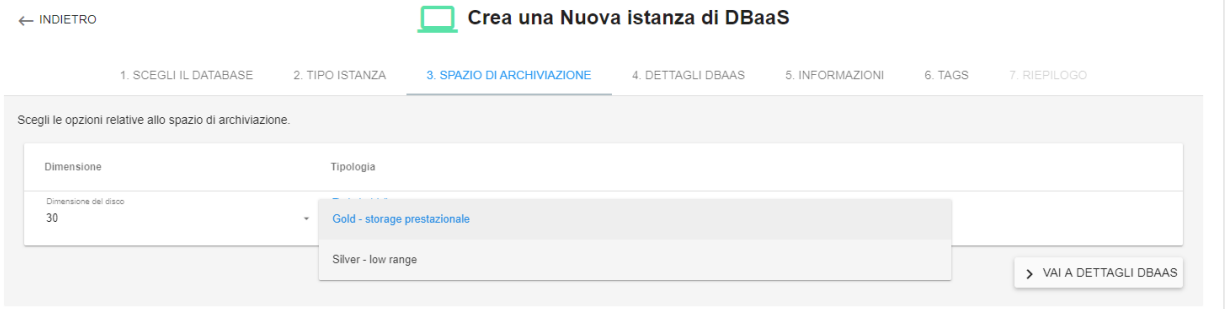
2. Specificare l'engine, selezionandolo tra le opzioni proposte dal portale e un codice progressivo di tre cifre nel formato. Nivola compilerà il campo nome dell'istanza in modo da evitare duplicati. Al termine premere **"VAI AL TIPO DI ISTANZA"**;


3. Scegliere la dimensione delle risorse da assegnare all'istanza di DBaaS mettendo un flag nella *check box* utile ed infine cliccare sul pulsante **VAI A SPAZIO DI ARCHIVIAZIONE**


4. Nella sezione **SPAZIO DI ARCHIVIAZIONE**, indicare la **dimensione** selezionandolo da uno dei valori proposti nella **combo box**

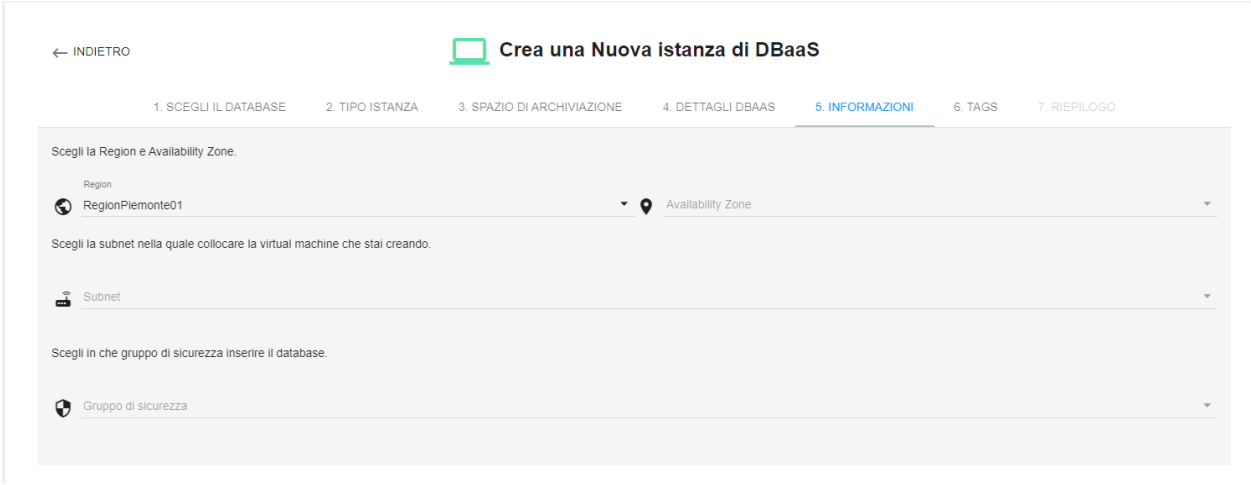



5. Nella stessa sezione, attraverso la **combo box**, precisare la **tipologia** dello spazio di archviazione e premere **"VAI A DETTAGLI DBAAS"**

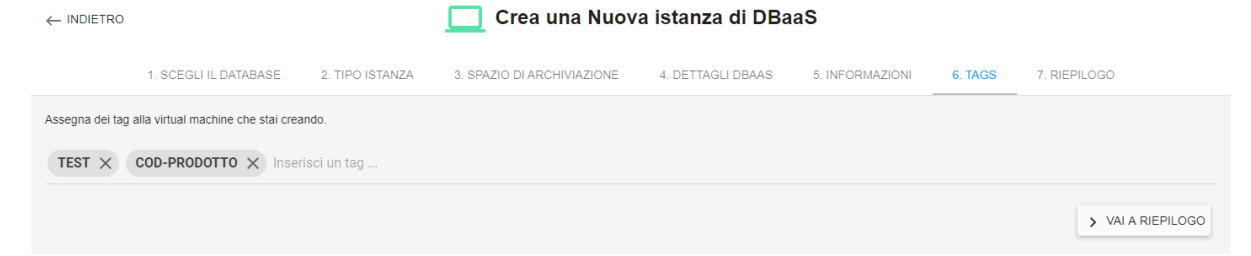



6. Assegnare al sistema la **porta di ascolto** convalidando il valore di default oppure sosituendolo con un valore nella casella di testo. Proseguire facendo un clic su **"VAI A INFORMAZIONI"**

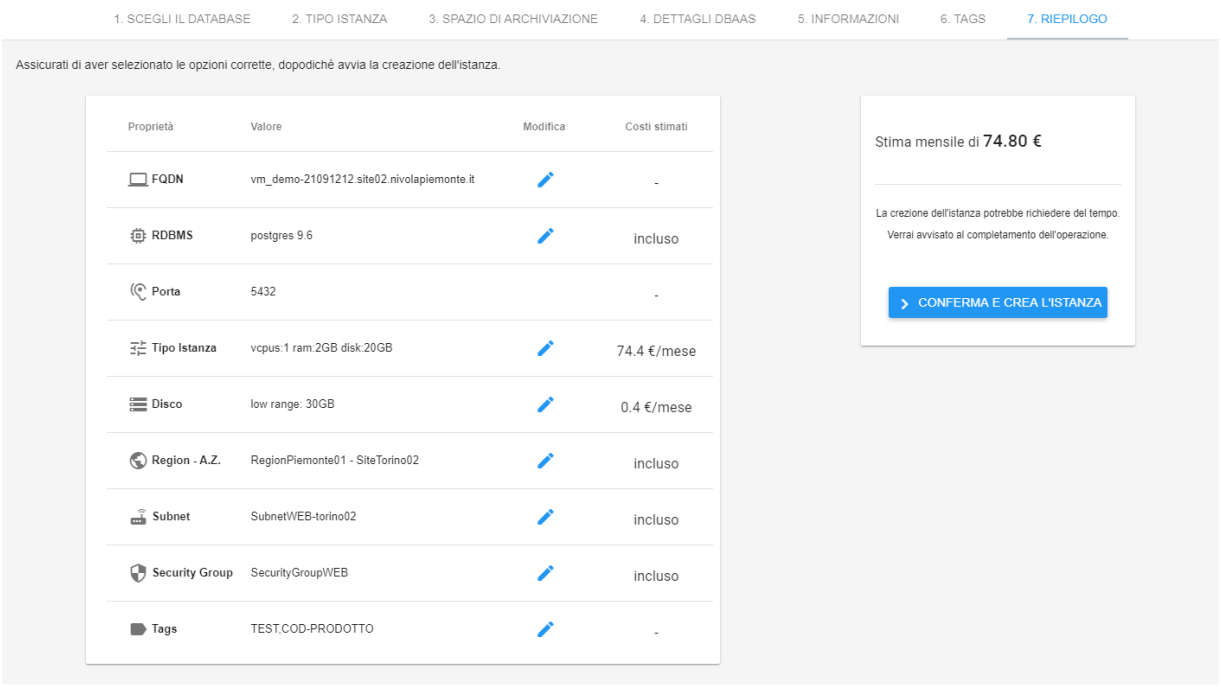

7. Attraverso le combo box, presenti nella pagina, specificare: **Region, Availability Zone, Subnet e Gruppo di sicurezza**. Al termine cliccare su **VAI A TAGS**.




8. Qualora servisse, assegnare dei tag all'istanza, scrivendo la stringa seguita da invio. Quanto inserito è possibile cancellarlo, utilizzando la **"X"** a fianco dei tags. Premere **VAI A RIEPILOGO** per proseguire.




9. Nel **riepilogo**, dopo aver controllato i parametri inseriti nel processo di creazione, cliccare su **"CONFERMA E CREA L'ISTANZA"** per materializzare la nuova istanza.




### 4.4.2 Gestire le istanze e utenti di un DBaaS

La gestione del **Data Base as Service** è attivabile da servizio **Database** nella parte sinistra dello schermo. Cliccando sulla freccia a destra della funzione, apparirà **Istanze DBAAS** e a seguito di un clic su quest'ultima opzione, il sistema popolerà la parte destra del video con l'**Elenco DBAAS** e i pulsanti da cui attivare le operazioni.

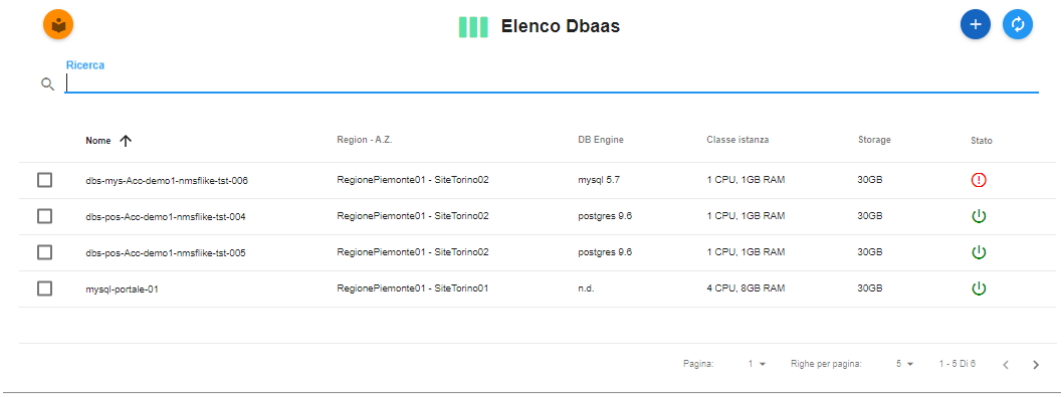
Per **gestione del DBAAS** si intendono tutte le funzioni per l'utilizzo dell'istanza DB in precedenza *creata* Appartengono a questo gruppo di operazioni:

1. *Cercare un istanza DbaaS*
2. *Connettersi ad un istanza DbaaS*
3. *Creazione utente*
4. *Cancellazione utente*

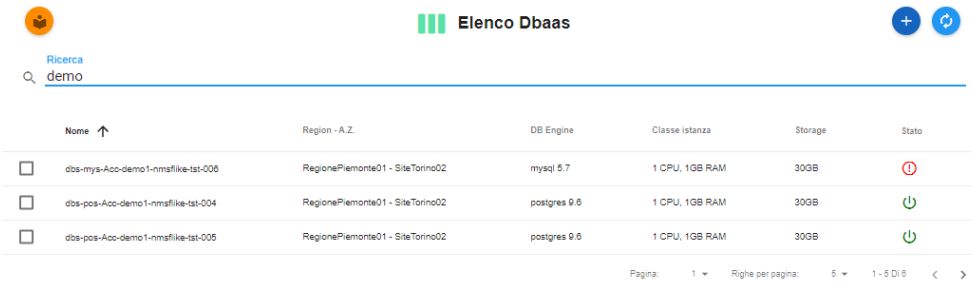
#### Cercare un istanza DbaaS

All'interno di ciascun Account è possibile fare ricerche su tutte le istanze create La ricerca è eseguita tramite una stringa inserita dall'operatore. Nivola ricerca il set di caratteri nelle colonne dove sono elencate le caratteristiche dei server. Per eseguire una ricerca è necessario procedere come segue:

1. Inserire stringa di ricerca sotto la label **"Ricerca"** e premere invio;



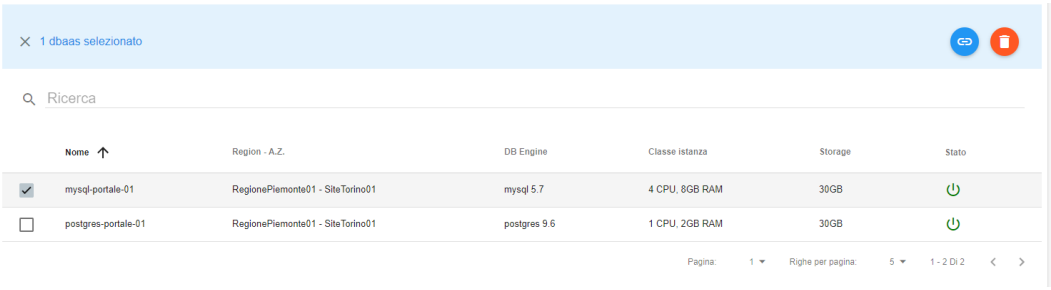

2. Attendere che il sistema popoli, con il risultato, la parte destra del video;




## Connettersi ad un istanza DbaaS

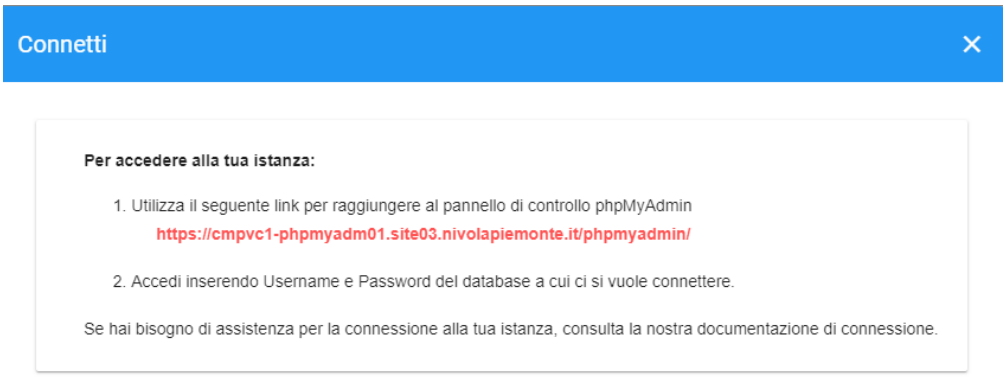
Per raggiungere un istanza del Database è necessario procedere nella maniera seguente:

1. Selezionare l'istanza;




2. Premere **pulsante connetti** ;

3. Attendere che il sistema esponga l'**url** del pannello di controllo;



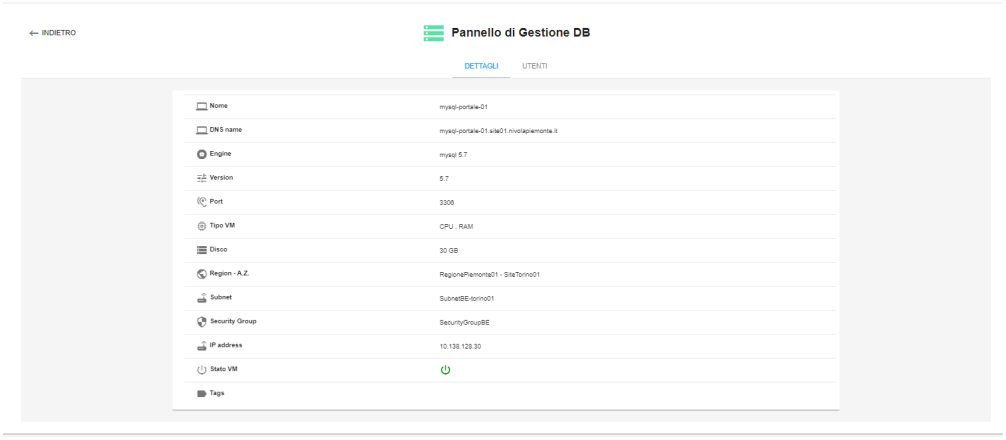

4. Dopo il clic sull'indirizzo, Nivola, metterà a disposizione dell'operatore il tool per l'amministrazione dell'istanza. Per completare il percorso, sarà necessario indicare **nome utente** e **Password**;

### Creazione utente

La funzione è fruibile attraverso il tasto **Pannello gestione Dbaas**:

Dop aver attivato la funzione, procedere attraverso i questi passaggi:

1. Scegliere il tabstrip **UTENTI**;



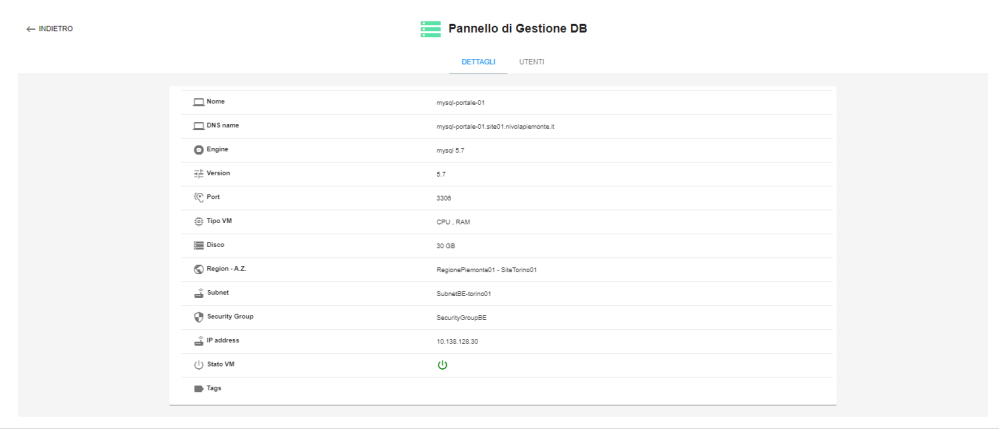

3. Indicare obbligatoriamente **nome utente**, **Tipologia** in via facoltativa le **note*** e concludere con il tasto **CREA UTENTE** ;


### Cancellazione utente

Per dismettere un utente è necessario utilizzare il tasto **Pannello gestione Dbaas**:

La cancellazione dell'utente è effettuata seguendo il metodo di seguito descritto:

1. Scegliere il tabstrip **UTENTI**;

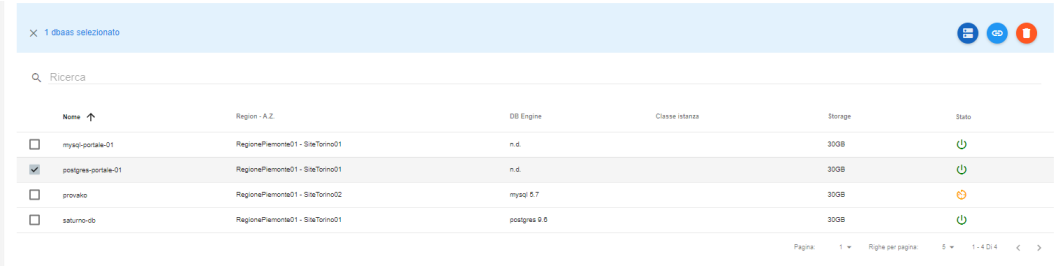



2. Selezionare l'utente da eliminare e premere il tasto **DISMETTI UTENTE** ;


### 4.4.3 Cancellare un'istanza Database as a Service

Per **cancellare** un **istanza DBAAS** seguire i seguenti passaggi:

1. Selezionare l'**istanza del dbaas** VM dall'Elenco dbaas e fare clic sul bottone **cancella**;

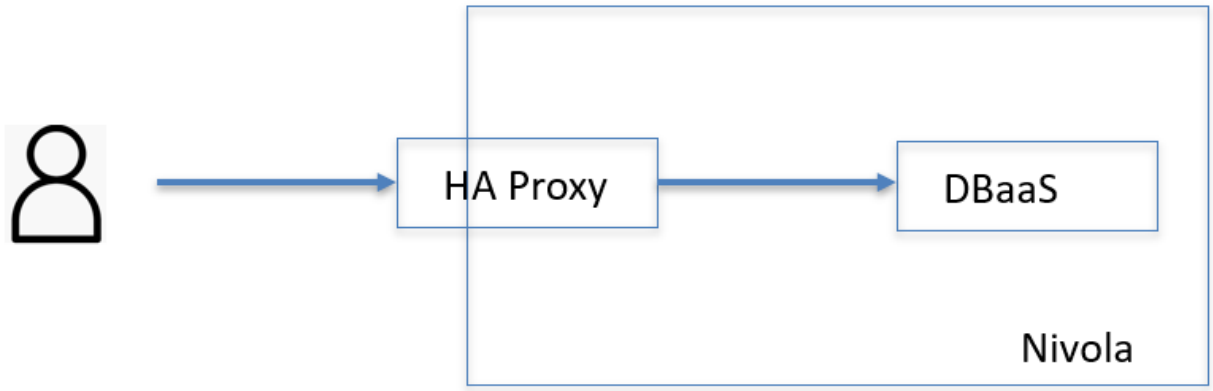



2. Cliccare su tasto **"Elimina"**;

3. Confermare con il tasto **"SI"** e l'istanza sarà cancellata;

### 4.4.4 Come accedere al Database as a Service

L'accesso alle base dati può essere oltre che applicativo anche a livello utente. Quest'ultimo accesso può avvenire da rete VPN o dalla propria postazione di lavoro, esso però, non è diretto. Infatti, l'accesso avviene tramite un haproxy, questa url viene fornita dal gruppo di supporto, quando si informano i richiedenti del provisioning. Per collegarsi al DB, ogni fruitore può utilizzare uno strumento a proprio piacere.



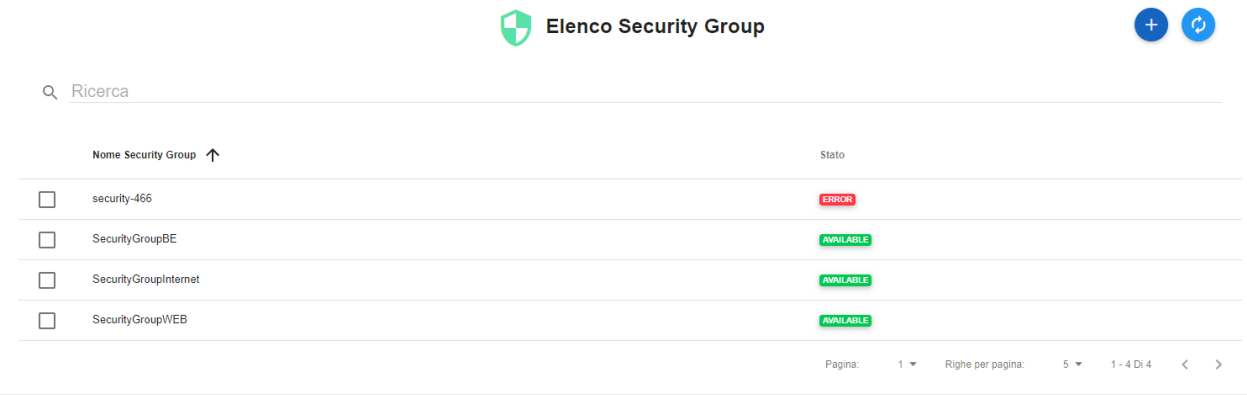

## 4.5 Servizi di rete

I vari segmenti di rete presenti all'interno della parte infrastrutturale di Nivola sono tutti protetti tramite firewall e le relative regole di sicurezza, che garantiscono il controllo degli accessi effettuati. Il controllo degli accessi e la configurazione delle regole a cui devono attenersi, sono il compito delle funzioni che i servizi di rete svolgono. Per la parte di account, le policies permettono la comunicazione a tutti i servizi presenti all'interno dello stesso perimetro di rete, bloccano gli accessi da e verso altri account e/o reti. Gli utenti possono procedere in autonomia per quanto riguarda la creazione di regole che permettono l'accesso da internet verso il proprio account o da rete di backend verso il proprio account.

### 4.5.1 Creare un Security Group

La funzione rientra in **Reti e Sicurezza**. La **creazione SG** è utilizzabile dalla parte sinistra dello schermo, cliccando la freccia a fianco di **Reti e Sicurezza** e successivamente su **Security Group** nel sottomenù.


A seguito di un clic su **Security Group**, il sistema, esporrà l'**Elenco dei Security Group** nella parte centrale dello schermo.

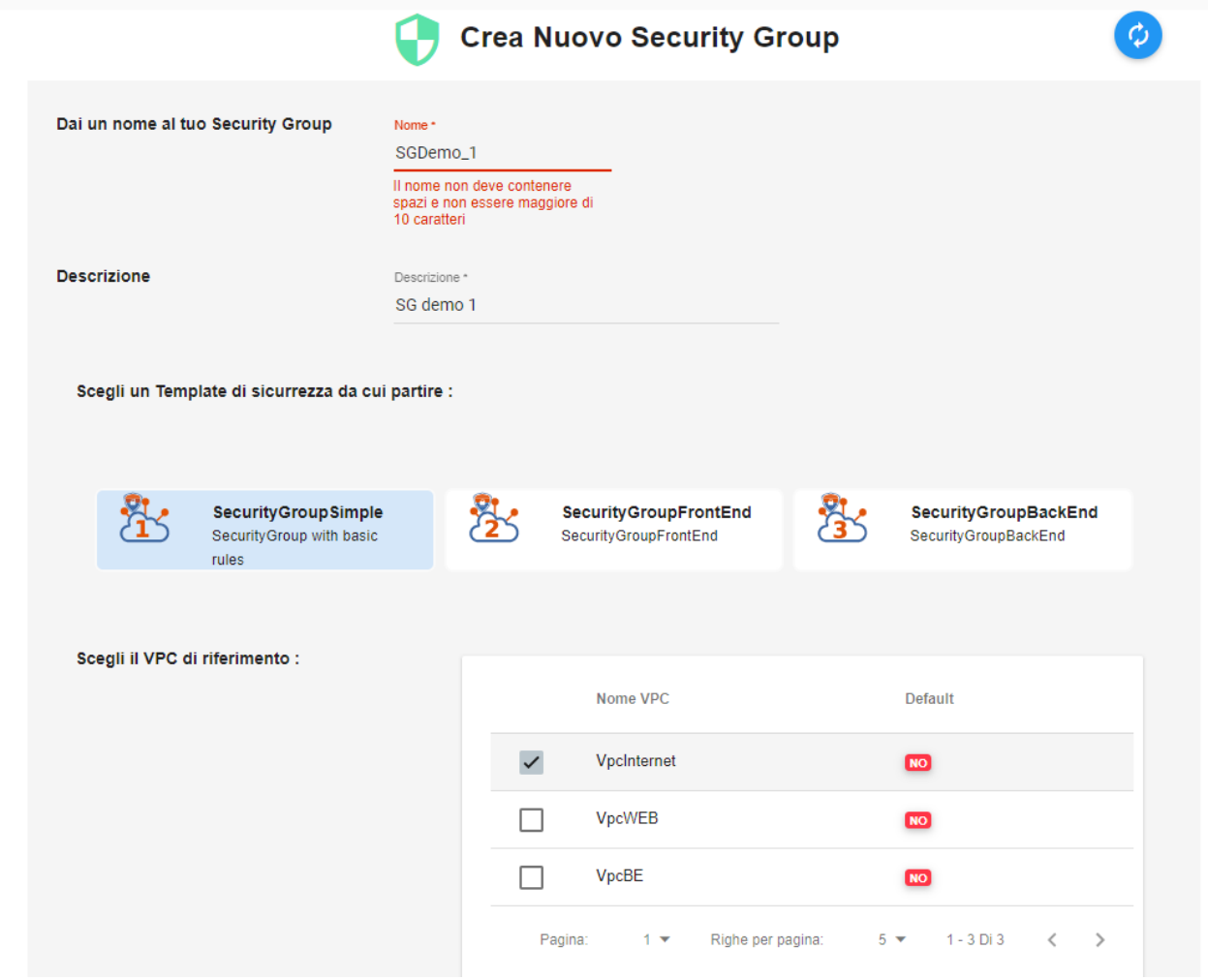



Per istanziare un Security Group, procedere seguendo i passaggi successivi:

1. Fare clic sul pulsante **"+"**:

2. Specificare i parametri necessari al sistema:

- Inserire **Nome del Security Group** nella textbox, rispettando la regola che non deve contenere spazi e non superare i 10 caratteri;
- Scrivere la **Descrizione** nella casella di testo;
- Optare per un *Template di Sicurezza* selezionandolo tra quelli proposti;
- Indicare il **VPC di riferimento** evidenziandolo dalla checkbox;




3. Terminare premendo su **CREA SECURITY GROUP**,


### 4.5.2 Gestire regole del Security Group

La funzione rientra in **Reti e Sicurezza**. *La creazione del Security Group* è utilizzabile dalla parte sinistra dello schermo, cliccando la freccia a fianco di **Reti e Sicurezza** e successivamente, su **Security Group** nel sottomenù.

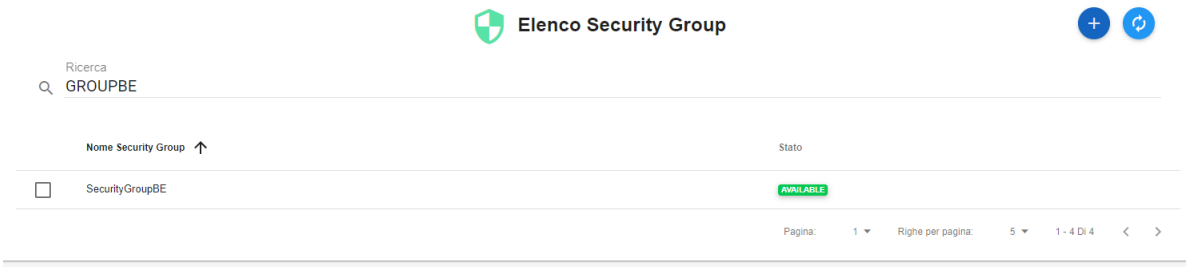

Costituiscono questo gruppo di operazioni:

1. *Cercare un Security Group*
2. *Visualizzare regole del Security Group*
3. *Aggiungere regole al Security Group*

### Cercare un Security Group

All'interno di ogni Account è possibile fare ricerche su tutte le sue istanze. La ricerca è eseguita tramite una stringa inserita dall'operatore. Nivola ricerca il set di caratteri nelle colonne dove sono elencate le caratteristiche dei SG. Per effettuare la ricerca è necessario procedere in questo modo:

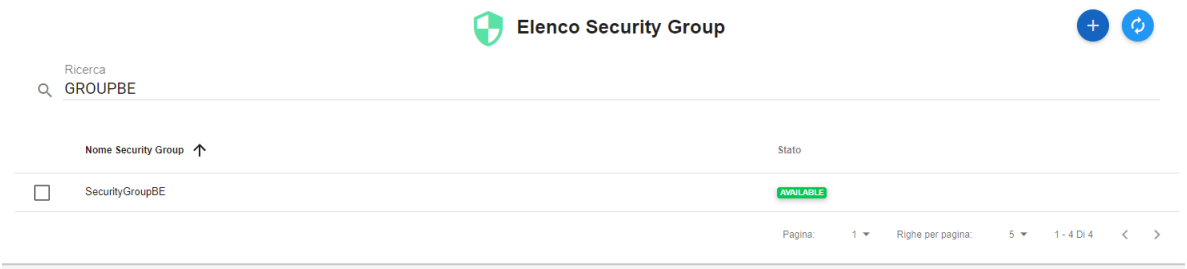
1. Inserire stringa di ricerca sotto la label **"Ricerca"** e premere invio;




### Visualizzare regole del Security Group

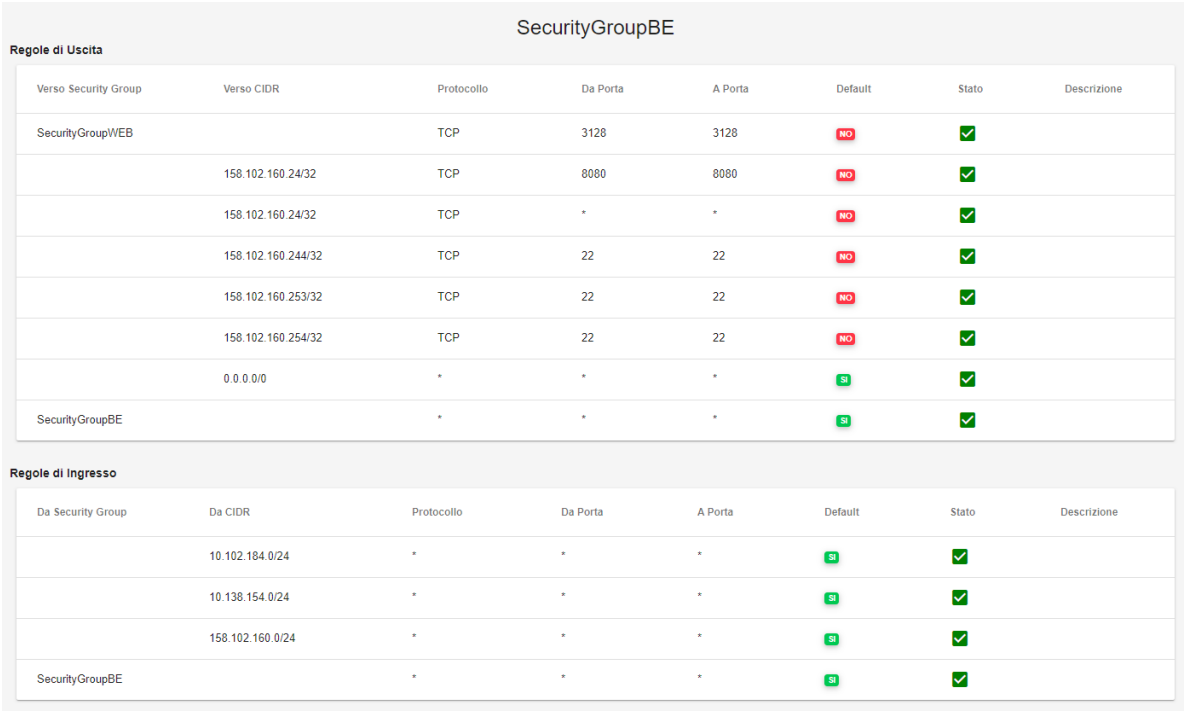
Le regole che caratterizzano un **Security Group** possono essere consultate nel dettaglio attraverso questi passaggi:

1. Inserire stringa di ricerca sotto la label **"Ricerca"** e premere invio;




2. Selezionare la regola e premere il pulsante **Visualizza Regole**;

3. Attendere che il sistema esponga l'elenco delle regole d'ingresso e di uscita del Security Group;




## Aggiungere regole al Security Group

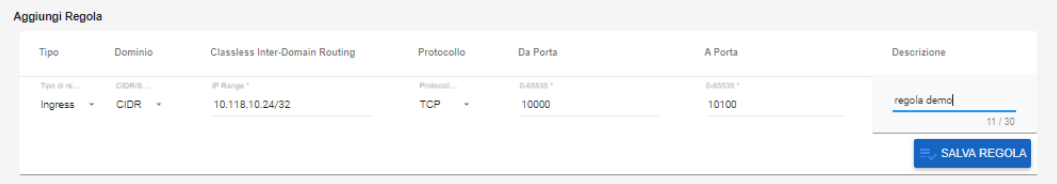
Per aggiungere una regola ad un **Security Group** si dovranno effettuare le seguenti operazioni:

1. Dopo aver individuato il SG, selezionarlo e premere pulsante **Modifica Security Group**;

2. Inserire i parametri necessari al sistema per definire la nuova regola:
   - **Tipo di regola** scegliendo uno dei valori presenti nella comboox;

- **Dominio** indicandolo tra quelli proposti;
- Il range degli IP scrivendolo sotto la label **Classless Inter-Domain Routing**;
- **Protocollo** indicandolo tra le opzioni possibili;
- Definire l'intervallo delle porte nei campi **Da Porta A Porta**;
- La **Descrizione** della regola è da inserire, scrivendola, nel textbox;

3. Al termine, per salvare la regola inserita, premere il pulsante **SALVA REGOLA**;




### 4.5.3 Template di Sicurezza

I template di Sicurezza sono utilizzati nella fase di *creazione del Security Group*.

Ogni template ha delle policies definite di default, che permettono la comunicazione tra server posti all'interno e all'esterno dello stesso SG.

Per acquisire familiarità con la tematica dei template è importante conoscere i **CIDR** (subnet, indirizzi IP) su cui si attestano gli host delle reti di Management e quelli di Gestione.

Per **rete di gestione** sono da interdersi tutte le reti su cui sono collocate le postazioni degli amministratori di sistema. Sulla **rete di management** invece, è dove sono connessi tutti gli host e/o server infrastrutturali, dedicati ai servizi.

La tabella riportata è lo schema a cui l'utente può fare riferimento.

| CIDR | DESCRIZIONE |
|---|---|
| 158.102.160.0/24 | **Classe di indirizzi IP** degli host attestati sulla rete di **Gestione** |
| 10.102.184.0/24 | **Classe di indirizzi IP** degli host attestati sulla rete di **Gestione** |
| 10.138.154.0/24 | **Classe di indirizzi IP** degli host attestati sulla rete di **Management** |
| 10.138.218.0/24 | **Classe di indirizzi IP** degli host attestati sulla rete di **Management** |

I modelli utilizzabili, in alternativa tra loro, sono:

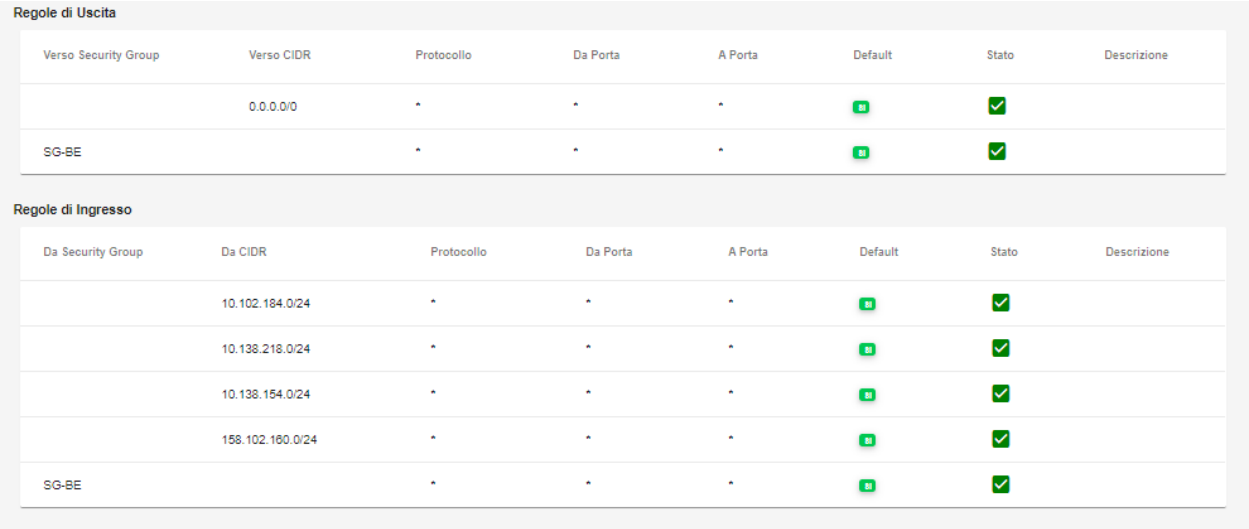
1. *Security Group BackEnd*
2. *Security Group FrontEnd*
3. *Security Group Simple*
4. *Security Group Isolated*
5. *Security Group Simple Private*

### Security Group BackEnd


I servizi che assumono questo modello consentono di uscire dal Security Group senza alcuna limitazione in quanto a IP e alle Porte.

Per gli Host collocati al suo interno, la comunicazione potrà avvenire senza filtri in grado di inibire porte ed IP.

Le uniche macchine in grado di accedere saranno soltanto quelle poste sulle reti di Management e di Gestione.



Regole di Uscita

| Verso Security Group | Verso CIDR | Protocollo | Da Porta | A Porta | Default | Stato | Descrizione |
|---|---|---|---|---|---|---|---|
| | 0.0.0.0/0 | * | * | * | | | |
| SG-BE | | * | * | * | | | |

Regole di Ingresso

| Da Security Group | Da CIDR | Protocollo | Da Porta | A Porta | Default | Stato | Descrizione |
|---|---|---|---|---|---|---|---|
| | 10.102.184.0/24 | * | * | * | | | |
| | 10.138.218.0/24 | * | * | * | | | |
| | 10.138.154.0/24 | * | * | * | | | |
| | 158.102.160.0/24 | * | * | * | | | |
| SG-BE | | * | * | * | | | |

### Security Group FrontEnd


I Security Group che usano questo template permettono di uscire senza alcun vincolo di Ip e di porte.

Dentro il perimetro del SG, le VM possono comunicare soltanto attraverso le **porte 80 e 443**.

Gli host che di default sono in grado raggiungere il SG, creato con questo template, sono quelli attestati sulla rete Management e su quella di Gestione.

Regole di Uscita

| Verso Security Group | Verso CIDR | Protocollo | Da Porta | A Porta | Default | Stato | Descrizione |
|---|---|---|---|---|---|---|---|
| | 0.0.0.0/0 | * | * | * | | | |
| SG-FE | | TCP | 443 | 443 | | | |
| SG-FE | | TCP | 80 | 80 | | | |

Regole di Ingresso

| Da Security Group | Da CIDR | Protocollo | Da Porta | A Porta | Default | Stato | Descrizione |
|---|---|---|---|---|---|---|---|
| | 10.102.184.0/24 | * | * | * | | | |
| | 10.138.218.0/24 | * | * | * | | | |
| | 10.138.154.0/24 | * | * | * | | | |
| | 158.102.160.0/24 | * | * | * | | | |
| SG-FE | | TCP | 443 | 443 | | | |
| SG-FE | | TCP | 80 | 80 | | | |

### Security Group Simple


E' un modello che impedisce ogni tipo di comunicazione da e verso l'esterno del Security Group che lo adotta. La trasmissione e la comunicazione è consentita unicamente tra gli host dello stesso SG.

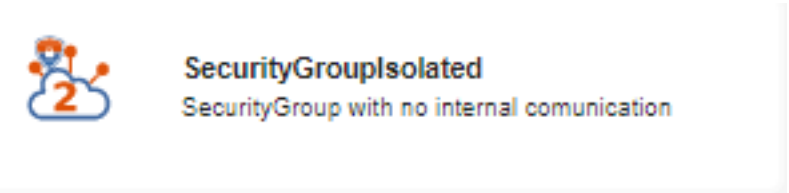
Regole di Uscita

| Verso Security Group | Verso CIDR | Protocollo | Da Porta | A Porta | Default | Stato | Descrizione |
|---|---|---|---|---|---|---|---|
| SG-SIMPLE | | * | * | * | | | |

Regole di Ingresso

| Da Security Group | Da CIDR | Protocollo | Da Porta | A Porta | Default | Stato | Descrizione |
|---|---|---|---|---|---|---|---|
| SG-SIMPLE | | * | * | * | | | |

### Security Group Isolated



Questo template caratterizza il SG che lo utilizza ad impedire agli host al suo interno di comunicare tra loro mentre l'uscita è priva di filtri. L'ingresso è consentito esclusivamente ai server delle reti di Management e di Gestione.

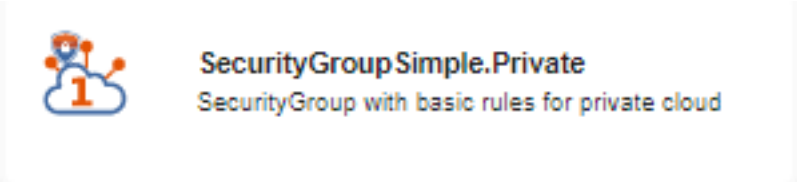
Regole di Uscita

| Verso Security Group | Verso CIDR | Protocollo | Da Porta | A Porta | Default | Stato | Descrizione |
|---|---|---|---|---|---|---|---|
| | 0.0.0.0/0 | * | * | * | ☑ | ☑ | |

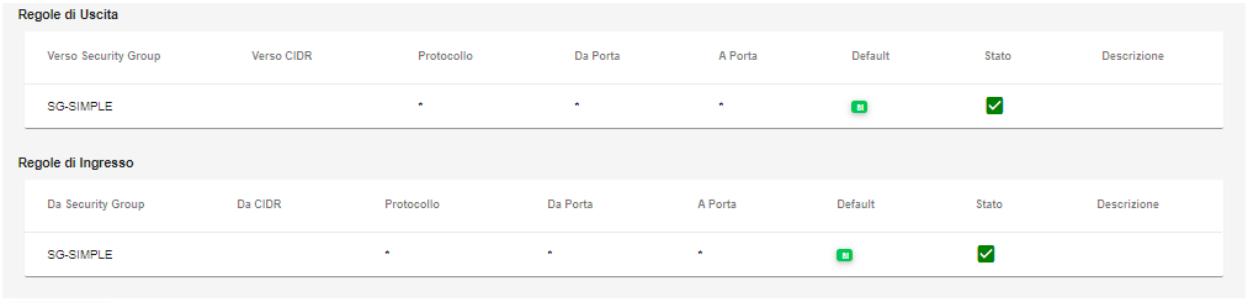
Regole di Ingresso

| Da Security Group | Da CIDR | Protocollo | Da Porta | A Porta | Default | Stato | Descrizione |
|---|---|---|---|---|---|---|---|
| | 10.102.184.0/24 | * | * | * | ☑ | ☑ | |
| | 10.138.218.0/24 | * | * | * | ☑ | ☑ | |
| | 10.138.154.0/24 | * | * | * | ☑ | ☑ | |
| | 158.102.160.0/24 | * | * | * | ☑ | ☑ | |

### Security Group Simple Private




Isola completamente il Security group che nasce assumendolo come template, quindi nessuno degli host è raggiungibile sia per ricevere e per comunicare. La comunicazione, tra gli host all'interno dello stesso SG, è priva di ogni restrizione in entrata ed in uscita.



Regole di Uscita

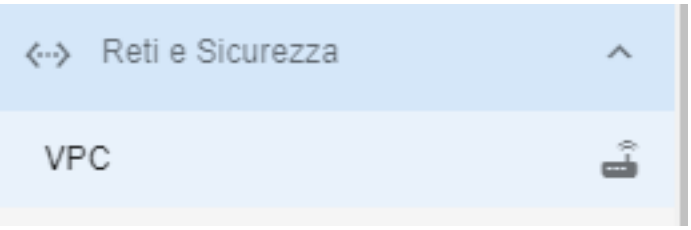
| Verso Security Group | Verso CIDR | Protocollo | Da Porta | A Porta | Default | Stato | Descrizione |
|---|---|---|---|---|---|---|---|
| SG-SIMPLE | | * | * | * | ☑ | ☑ | |

Regole di Ingresso

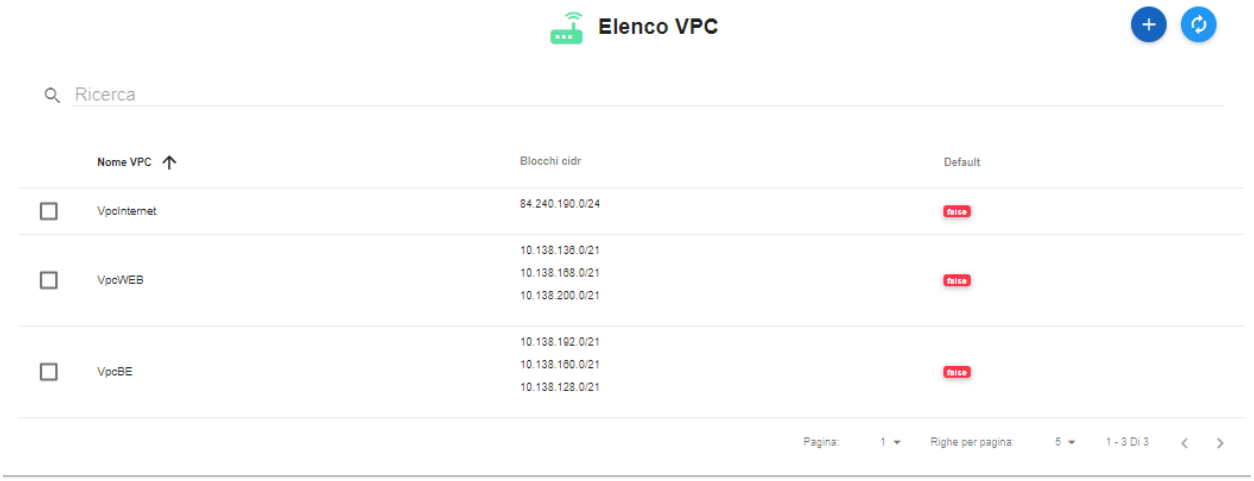
| Da Security Group | Da CIDR | Protocollo | Da Porta | A Porta | Default | Stato | Descrizione |
|---|---|---|---|---|---|---|---|
| SG-SIMPLE | | * | * | * | ☑ | ☑ | |

## 4.5.4 Creare un VPC

La funzione rientra in **Reti e Sicurezza**. La **creazione SG** è utilizzabile dalla parte sinistra dello schermo, cliccando la freccia a fianco di **Reti e Sicurezza** e successivamente su **VPC** nel sottomenù.



A seguito del clic su **VPC**, il sistema, esporrà l'**Elenco VPC** nella parte centrale dello schermo.

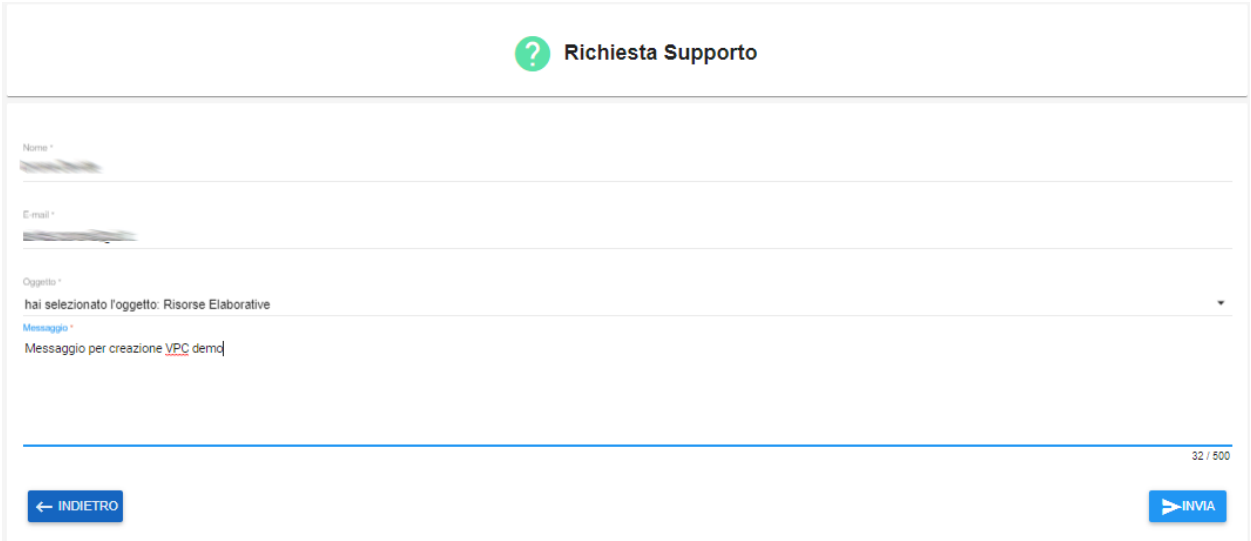



La creazione di un VPC avviene con una richiesta specifica al **Supporto del Csi-Piemonte**. Il provider, dopo aver preso in carico la richiesta, avviserà l'utente non appena conclusa l'attività prevista. L'istanza è effettuata via e-mail dal sistema dopo la compilazione di una form come spiegato nei passaggi successivamente descritti.

1. Fare clic sul pulsante **"+"**:

2. Specificare i parametri necessari al sistema:

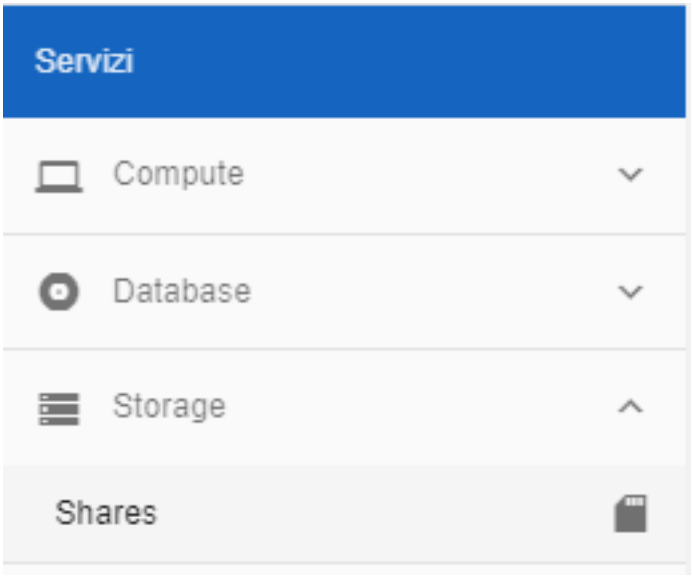
- Inserire **Nome** ed **e-mail** del richiedente;
- Indicare l'**Oggetto** selezionandolo tra quelli proposti nella combo;
- E' possibile accompagnare la richiesta, scrivendo un **Messaggio** nella textbox;




3. Terminare la richiesta, premendo il tasto **INVIA**;


## 4.6 Lavorare con lo Storage as Service

Il servizio per la creazione e gestione di spazio disco è attivabile dalla parte sinistra dello schermo, cliccando sulla label **Shares** sotto la funzione **Storage**.

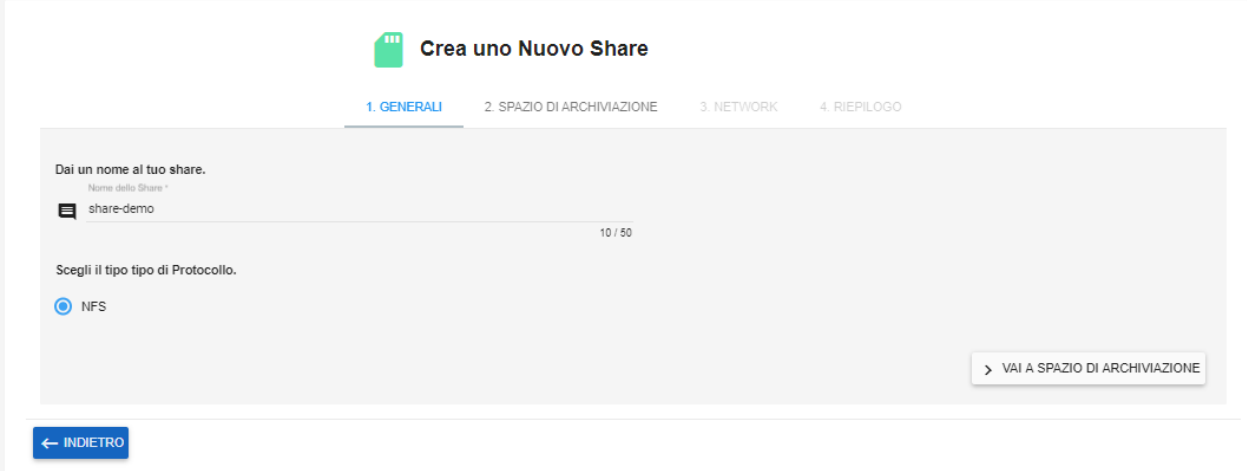



### 4.6.1 Creare lo Storage as Service

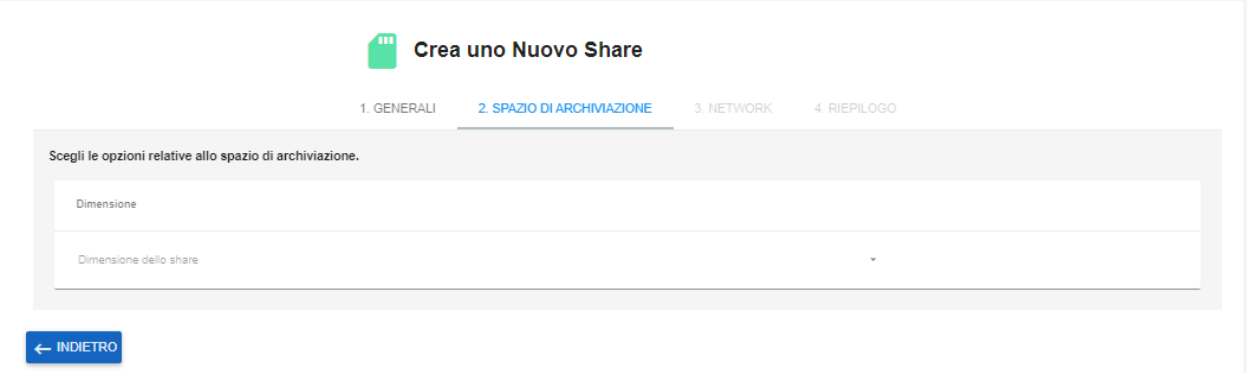
Per la creazione di share, procedere come segue:

1. Fare clic sul pulsante **"+""**:

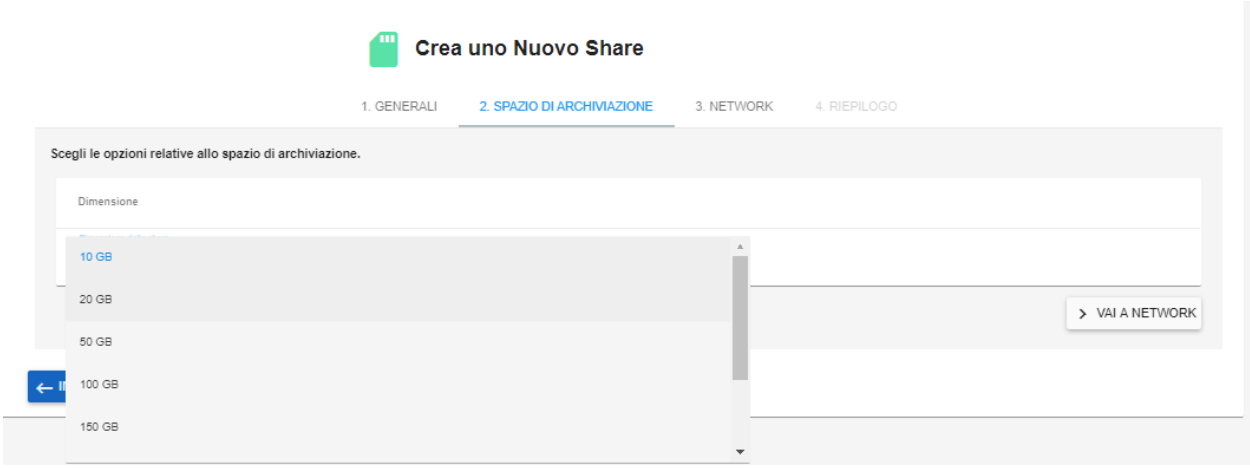
2. Inserire il **Nome dello share** nella textbox e cliccare il pulsante **VAI A SPAZIO DI ARCHIVIAZIONE**;



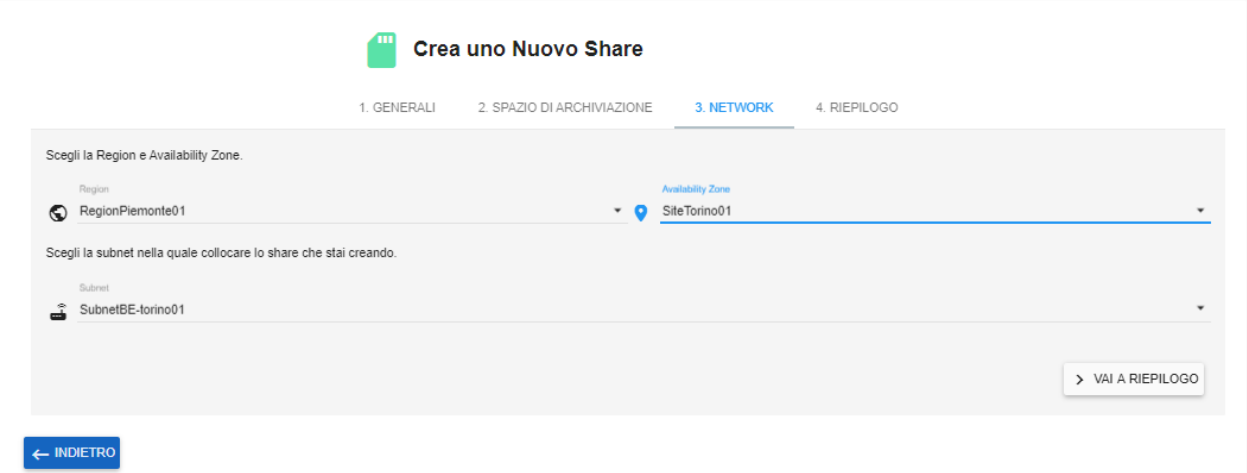

3. Premere **Dimensione dello share**;



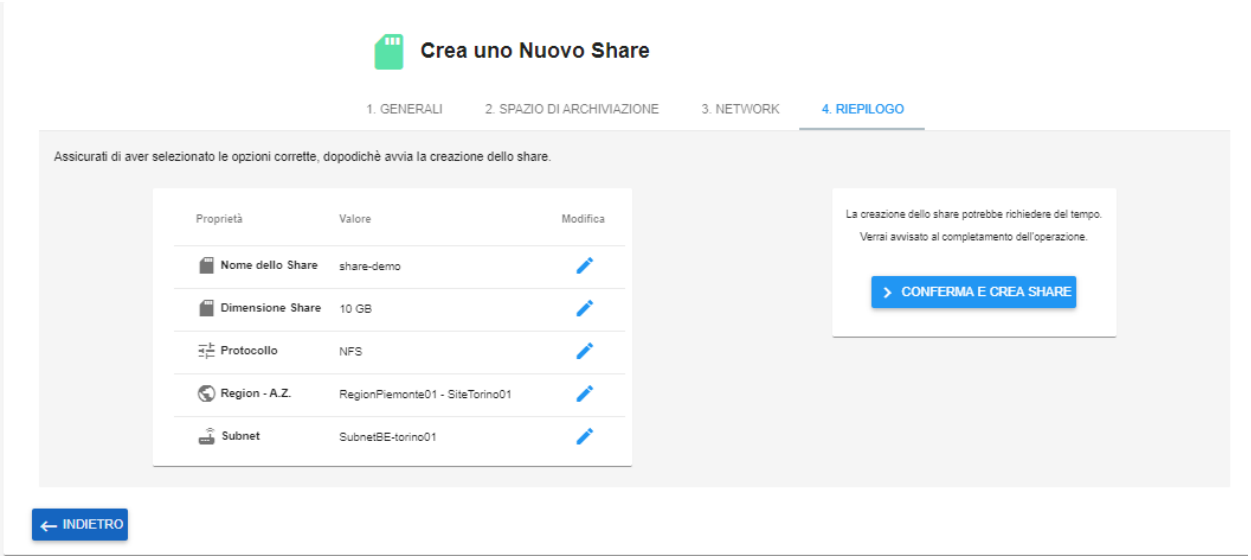

4. Specificare dimensione dello Share indicando uno dei valori presenti nella **combo box** e proseguire premendo il pulsante **VAI A NETWORK**;



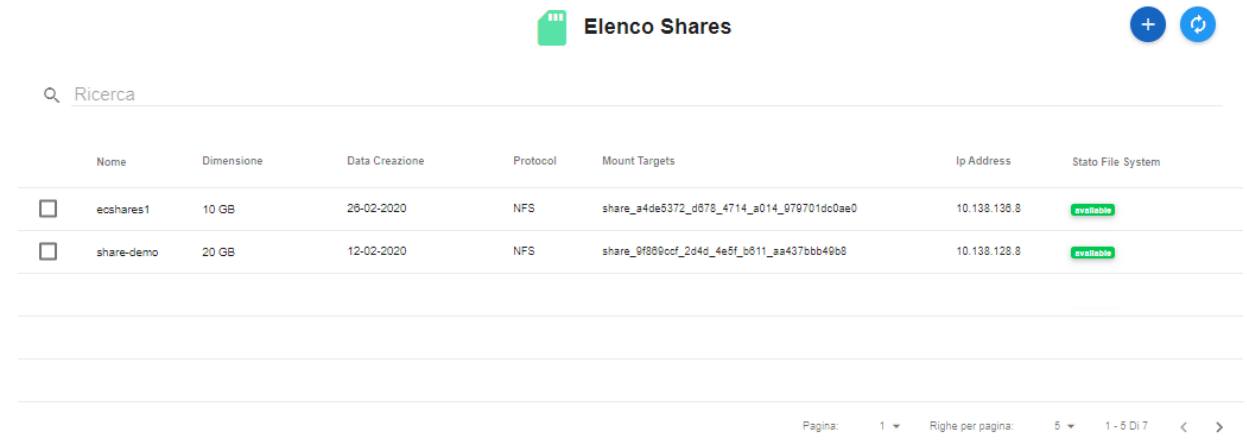

6. Sfruttando le combo box, proposte, inserire: **Region, Availability Zone, Subnet**. Al termine cliccare su **VAI A RIEPILOGO**;




7. Controllare i parametri inseriti e premere, **CONFERMA E CREA SHARE**;




8. Lo storage creato comparire nell'elenco;



### 4.6.2 Gestire lo Storage as Service

La gestione del servizio è attivabile dalla voce **Storage** posta, nella parte sinistra dello schermo. Cliccando su **Shares**, il sistema popolerà la parte centrale del video con il **Pannello di Gestione Share**.

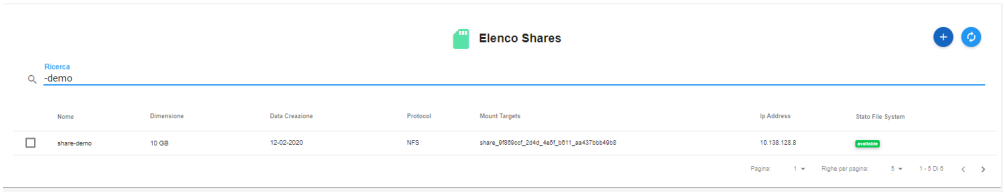
Per **gestione dello STAAS** si intendono tutte le operazioni che consentono l'uso sistemistico dello spazio disco *creato* in precedenza. Appartengono a questo gruppo di attività:

1. *Cercare uno Share*
2. *Modificare capacità dello Share*
3. *Condividere Share*
4. *Togliere l'autorizzazione*

#### Cercare uno Share

All'interno di ciascun Account è possibile fare ricerche su tutte le istanze create. La ricerca è eseguita tramite una stringa inserita dall'operatore. Nivola ricerca il set di caratteri nelle colonne dove sono elencate le caratteristiche dei server. Per eseguire una ricerca è necessario procedere come segue:

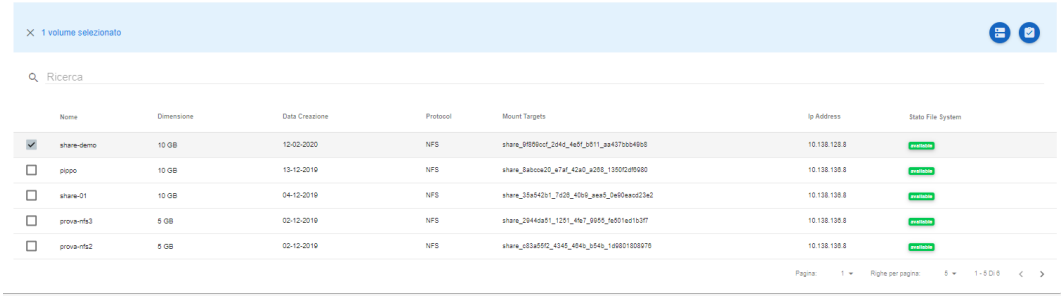
1. Inserire la stringa da usare come chiave di ricerca, sotto la label **"Ricerca"** e attendere che il sistema concluda la ricerca;




#### Modificare capacità dello Share

Per aumentare o diminuire la capienza del disco, seguire quanto riportato di seguito:

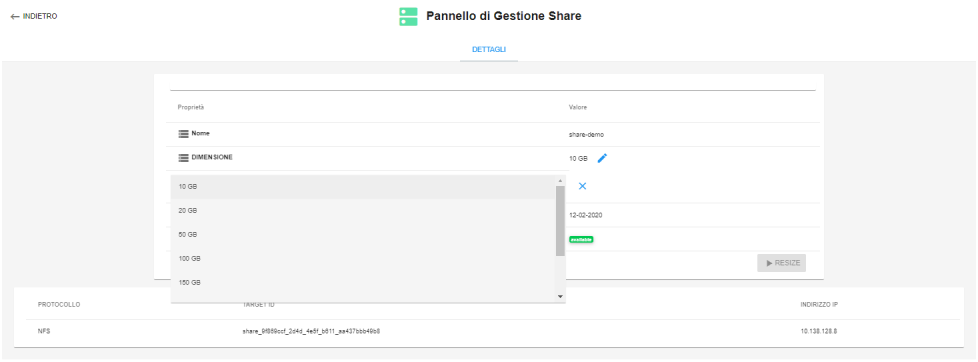
1. Selezionare lo storage dall'**Elenco Shares**;



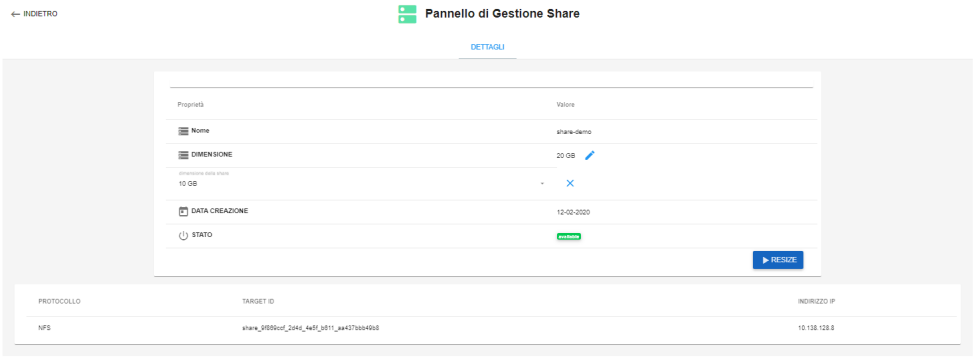

2. Premere il tasto **Pannello gestione Volume**;

3. Cliccare sul simbolo **modifica** a fianco alla dimensione;

4.Scegliere la nuova capacità dalla combo box proposta dal sistema;



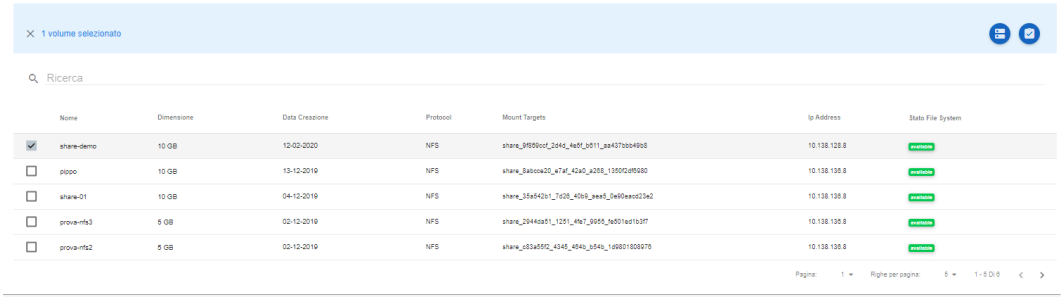

5. Agire con il mouse sul pulsante **RESIZE** e attendere che il sistema apporti la modifica;




## Condividere Share

Per permettere ad un host l'**autorizzazione** di accedere allo spazio di archiviazione, occorre procedere seguendo questi passi:

1. Individuare lo **Share** da condividere;

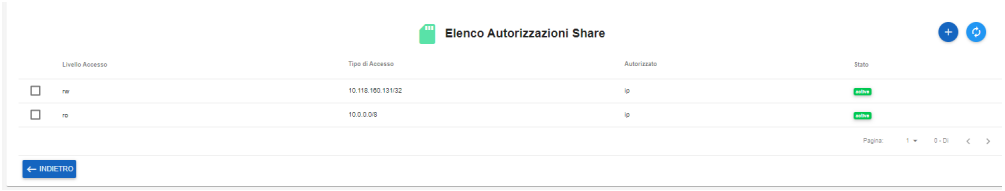



2. Cliccare su tasto **Autorizzazioni**;

3. Dall'**Elenco Autorizzazioni Share** premere il tasto **"+"**;

4. Sfruttando le combobox indicare al sistema **"Livello di accesso"", **Tipo di accesso** e in base a quest'ultimo parametro, gli apparati autorizzati ad usarlo. Al termine premere **CREA AUTORIZZAZIONE**.;

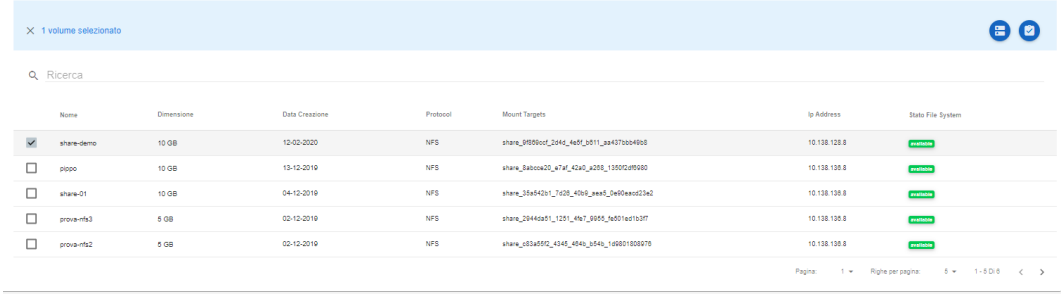

5. La nuova **autorizzazione** andrà a popolare l'**Elenco Autorizzazioni Share**.;




## Togliere l'autorizzazione

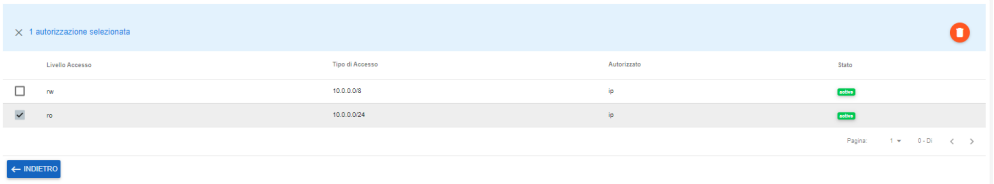
Per revocare un **autorizzazione** concessa in precedenza è necessario seguire queste operazioni:

1. Individuare lo **Shares** a cui è si riferisce l'autorizzazione da rimuovere;




2. Cliccare su tasto **Autorizzazioni**;

3. Selezionare la check box dell'autorizzazione da annullare;




4. Premere sul tasto **"cestino"**;

5. L'**autorizzazione** sarà cancellata dall'**Elenco Autorizzazioni Share**;

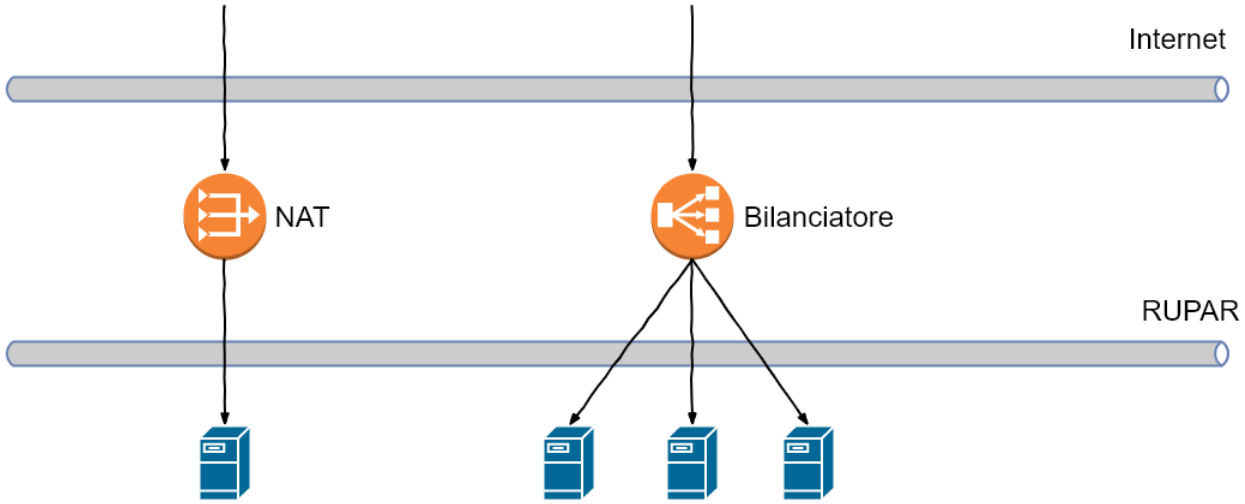

## 4.7 Come comunicare con internet

**I server non possono essere allocati direttamente sulla rete internet ed avere un IP pubblico, per esigenze di sicurezza la** comunicazione con strumenti e servizi esterni viene mediato. In particolare per comunicare verso l'esterno si deve utilizzare

il proxy del pod in cui si trovano i propri server:

1) http://podto1-proxy.site01.nivolapiemonte.it:3128/ per i server in pod1
2) http://podto2-proxy.site02.nivolapiemonte.it:3128/ per i server in pod2
3) http://podto3-proxy.site03.nivolapiemonte.it:3128/ per i server in pod3

invece, per essere contattati dall'esterno si deve utilizzare o un NAT dell'IP privato o il bilanciamento di carico in caso i server che erogano il servizio siano molteplici




## 4.8 Come abilitare la VPN

Gli ambienti creati su Nivola possono essere amministrati raggiungendo le VM tramite VPN, che possono essere abilitate dai referenti CSI utilizzando l'apposito processo previsto. Il **profilo VPN** da indicare in fase di richiesta è **5143_CUSTOM_Fornitori_Nivola_Default**. Contestualmente a questa attivazione, le utenze esterne al CSI saranno registrate come **nome.cognome@fornitori.nivola** e dovranno impostare la password attraverso la procedura descritta al seguente indirizzo: https://comunica.csi.it/cambia-password/index.html.

L'utente esterno, una volta abilitato il canale VPN, potrà accedere alla CLI autenticandosi utilizzando le credenziali nome.cognome@fornitori.nivola e password impostata.

La password ha una scadenza di tre mesi e deve essere rinnovata all'indirizzo https://comunica.csi.it/cambia-password/index.html.

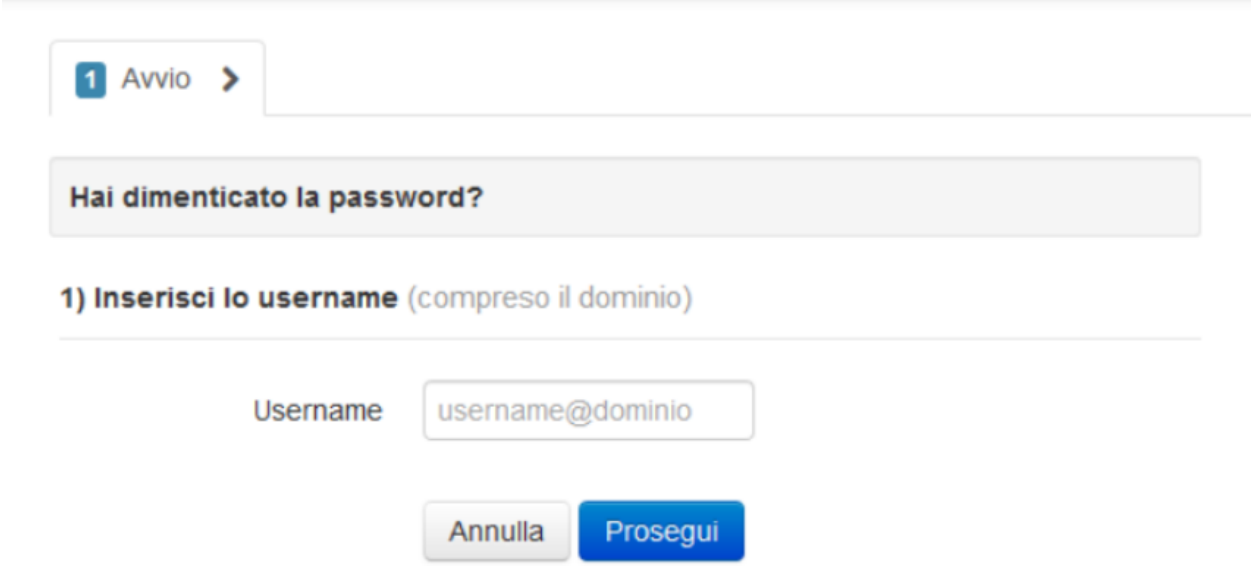
Nel caso in cui il richiedente esterno disponesse già di un accesso VPN con il CSI Piemonte, gli sarà associato anche il profilo di Nivola e gli saranno conferite, come descritto sopra, le credenziali per *accedere alla CLI*.

## 4.9 Gestione Password Fornitori Esterni

Operazione specifica per i fornitori esterni che non sono organici all'organizzazione csi e che accedono ad un utenza nome.cognome@fornitori.nivola e che hanno la necessità di cambiare o creare la password.

Collegarsi alla url https://sa.csi.it/nivola Nella pagina evidenziata, al punto 1, si trovano le indicazioni per gestire il cambio password e la creazione della prima password. Nello specifico si deve accedere alla url https://comunica.csi.it/cambia-password/index.html

In questa pagina si inserisce la user nome.cognome@fornitori.nivola e si segue la procedura che prevede una telefonata gratuita con il cellulare indicato in fase di attivazione.




## 4.10 Strumenti Monitoraggio e Log

### 4.10.1 Monitoraggio

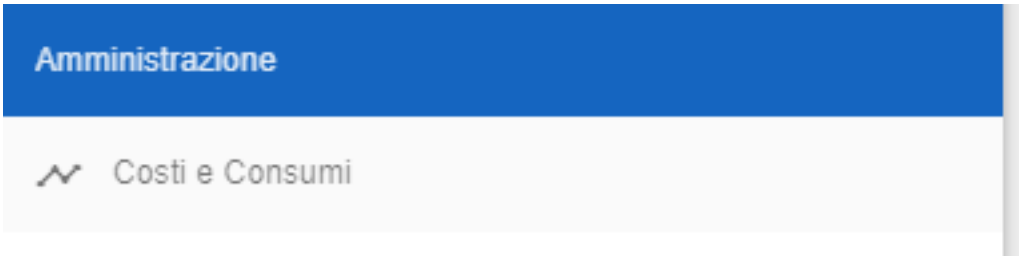
**TO DO**

### 4.10.2 Log

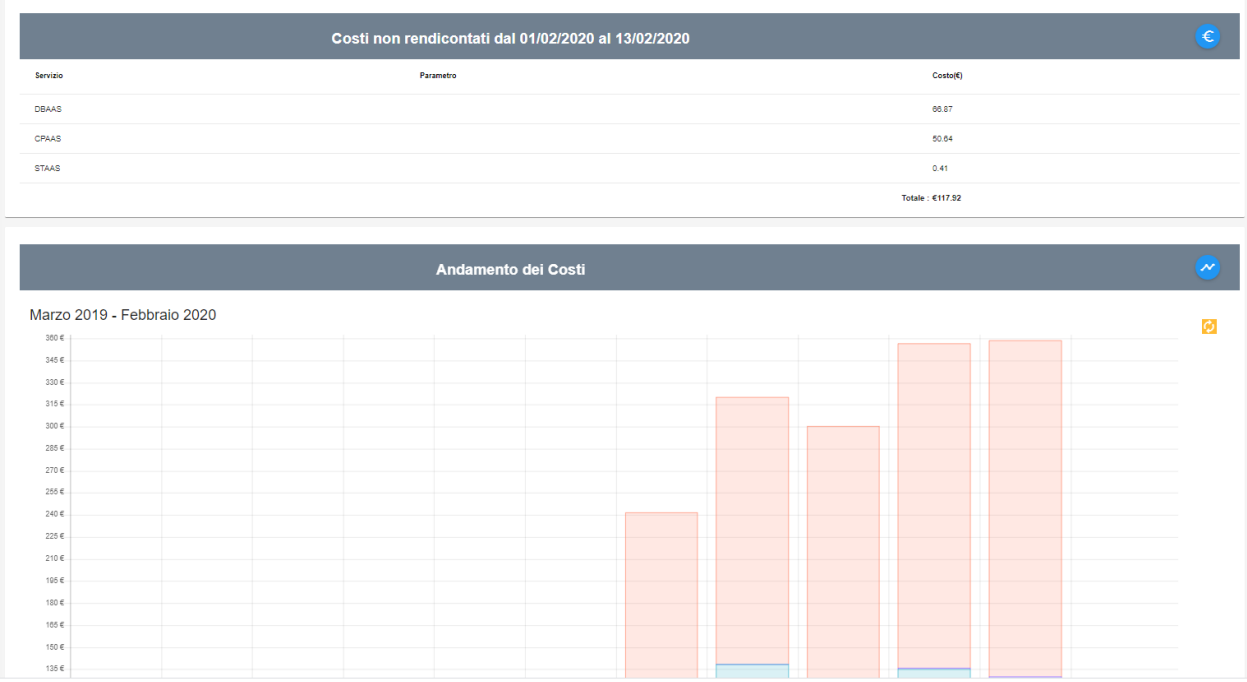
**TO DO**

## 4.11 Consultare costi e consumi

I **Costi e Consumi** sono visibili attraverso il menu posto alla sinistra dello schermo. Cliccando sulla label **Costi Consumi** sotto la label **Amministrazione**




A seguito del clic su **Costi e Consumi**, il sistema presenterà nella parte destra del video i **Costi non rendicontati** e l'**Andamento dei Costi**. Il grafico e la tabella, fanno riferimento al **Consumo** e al **Costo** dei servizi acquistati e istanziati nell'account.




## 4.12 Come attivare il Supporto

Le attività di assistenza relative al Service Portal Nivola e a tutti i servizi fruibili non possono prescindere dai livelli di servizio individuati nonché degli strumenti adottati per l'erogazione dei servizi di assistenza.

L'attività di assistenza all'interno del Team di Supporto Nivola è articolata su uno schema di supporto basato su tre livelli:

1. Developer: chat, compilazione form su SP
2. Standard: chat, compilazione form su SP, invio e-mail, contatto telefonico
3. Premium: chat, compilazione form su SP invio e-mail, contatto telefonico

Per quanto riguarda la copertura oraria e Livelli di Servizio fare riferimento all'Allegato tecnico del Catalogo Servizi Nivola.

Tutti i canali, ad eccezione della chat, sono presidiati dal **Centro Unico di Contatto (CUC)** nella fascia lavorativa dal lunedì al venerdì dalle 8 alle 18. Per le restanti fasce orarie è possibile avere un riscontro immediato solo attraverso il canale telefonico garantito dal gruppo Conduzione Operativa.

Il Centro Unico di Contatto inoltra la richiesta al **Nivola Support Center (NSC)** tramite lo strumento di ticketing. Nel caso in cui, la problematica non possa essere risolta da NSC viene inoltrata al gruppo di Ingegneria Nivola.

Durante l'orario presidiato dal gruppo **Assistenza Operativa**, nel caso non fossero in grado di risolvere la probletica evidenziata dall'utente, sarà chiamato il reperibile del gruppo di NSC o di Ingegneria.

L'utente ha a disposizione all'interno del Service Portal Nivola una sezione specifica dove può trovare le informazioni di base relative all'utilizzo della piattaforma.

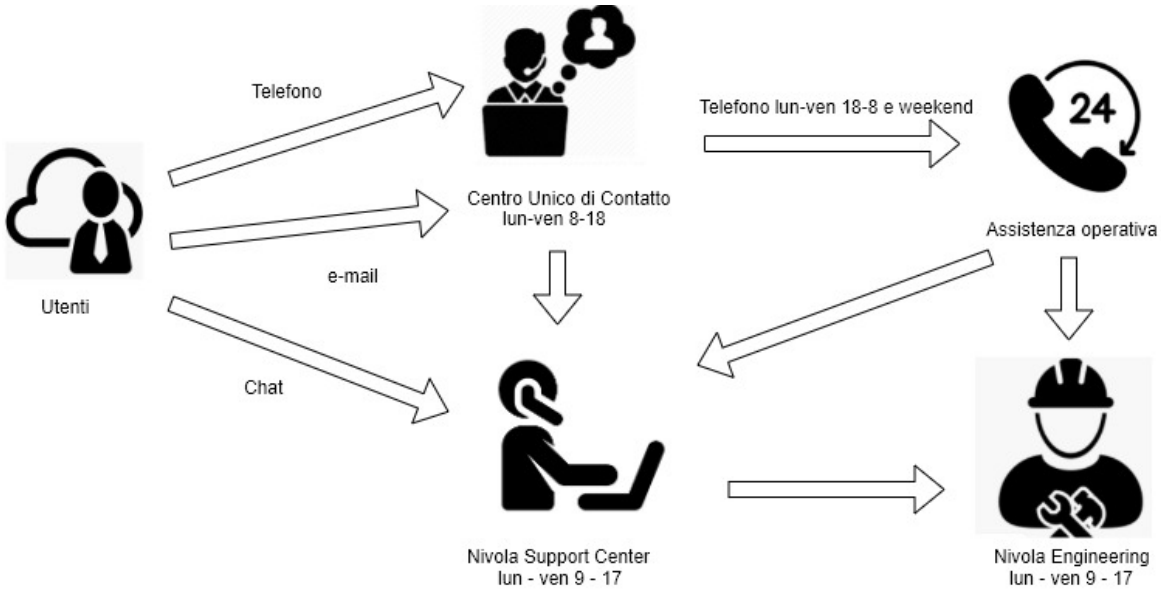
In particolare sono disponibili:

- manuali utente sull'utilizzo della piattaforma;
- eventuali video esplicativi per la verifica e l'utilizzo di funzionalità specifiche;

- FAQ per la risoluzione dei problemi più comuni.

Qualora l'utente/cliente, attraverso l'utilizzo di questi strumenti non trovasse la risposta alla sua problematica ha a disposizione alcuni strumenti interattivi che gli permettono di comunicare direttamente con il Team di Supporto Nivola:

- chat attivabile dal Service Portal
- compilazione form su Service Portal




L'accessibilità ai singoli strumenti di assistenza è diversa a seconda dei singoli livelli di servizio attivati dall'utente/cliente (cfr. tabella di seguito riportata):

| | Knowledge Base (manuali, faq, video) | Chat Service Portal | e-mail via form (Service Portal) | e-mail | telefono |
|---|---|---|---|---|---|
| Developer | ✓ | ✓ | ✓ | ✗ | ✗ |
| Standard | ✓ | ✓ | ✓ | ✓ | ✓ |
| Premium | ✓ | ✓ | ✓ | ✓ | ✓ |

Le 3 tipologie di supporto sono collegate all'istanza di servizio. Ad esempio il cliente può attivare 2 istanze di DBaaS richiedendo il supporto Developer sull'istanza di Test e un supporto Premium per l'istanza di produzione purchè appartenenti ad Account differenti.

**Riferimenti per il Supporto**

Il Supporto è attivabile dagli utenti esterni sui seguenti canali

Service Portal: chat, compilazione form su Service Portal

**E-mail** alla casella: hd_servizinivola@csi.it

**Telefono** Centro Unico di Contatto: +39 011 0824221

CHAPTER

FIVE

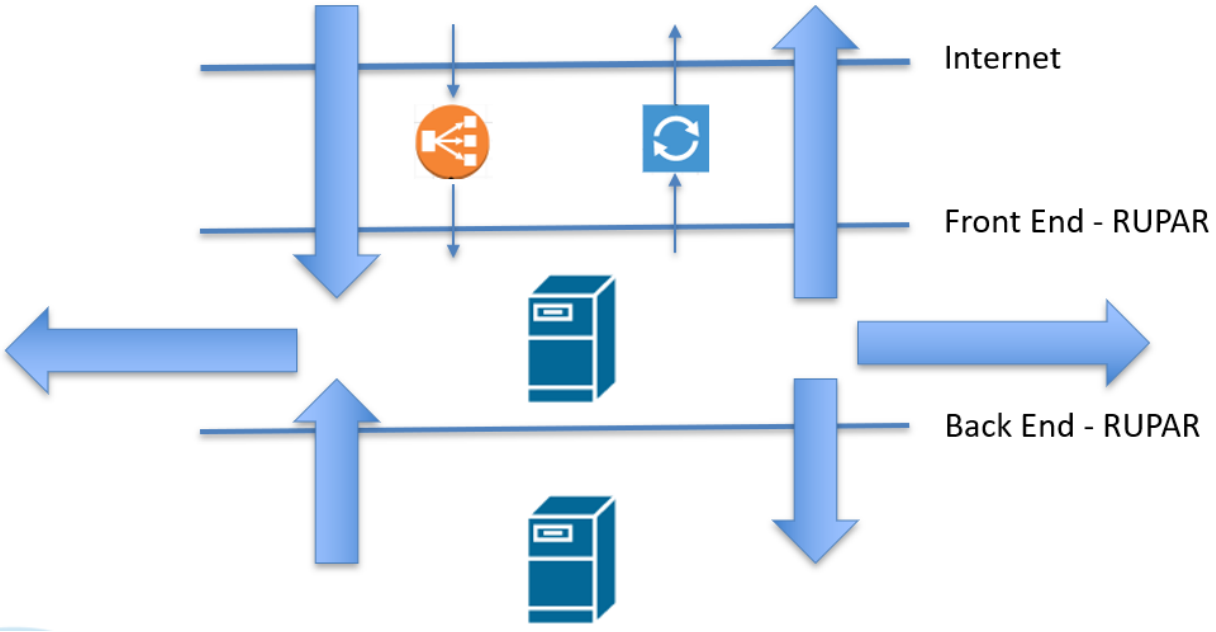
# LINEE GUIDA

## 5.1 Modelli di Rete

In tutti i modelli la rete internet non può ospitare dei server, la comunicazione avviene come descritto nella sezione “Come comunicare con Internet”.

### 5.1.1 RUPAR Cloud CSI.

Questo tipo di modello di rete è stato pensato per ospitare gli asset del CSI, utilizzati per erogare servizi per i propri clienti. L’immagine sottostante descrive le possibili comunicazioni di rete:

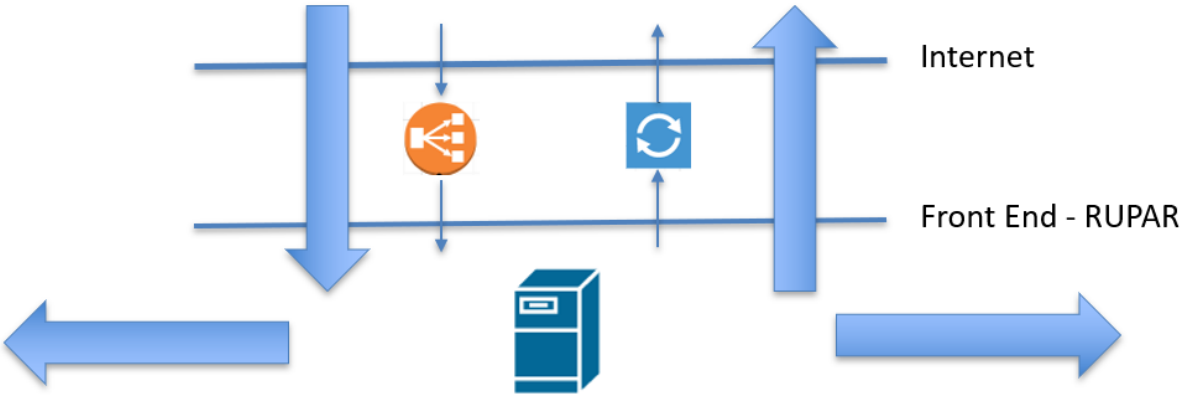



Sono presenti tre reti:

- **Internet**, si riferisce ad un piano di indirizzamento pubblico;
- **Front-end (RUPAR)**, si riferisce ad indirizzi della rete RUPAR per condividere ed accedere a sistemi e servizi con altri Enti della PA; questi sistemi possono essere raggiunti dalla rete internet tramite NAT e Bilanciatore;
- **Back-end (RUPAR)**, si riferisce ad indirizzi IP privati non raggiungibili tramite internet e che consentono la comunicazione solo con sistemi e servizi sulla stessa sotto ret o con la front-end corrispondente.

### 5.1.2 RUPAR Cloud ENTI.

Questo tipo di modello è stato ideato per ospitare i servizi degli Enti che intendono avvalersi del cloud del CSI. L'immagine sottostate descrive le possibili comunicazioni di rete:

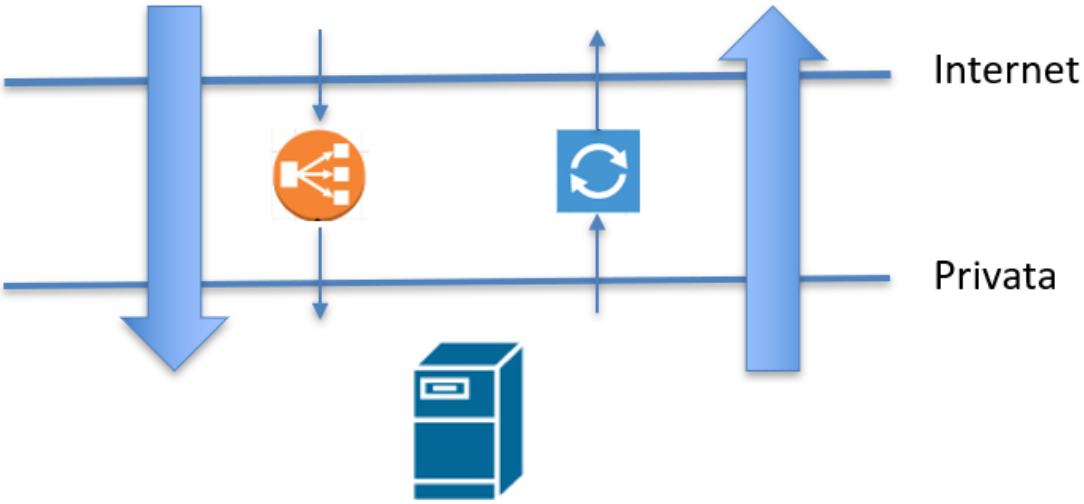



Sono presenti due reti:

- Internet, si riferisce ad un piano di indirizzamento pubblico;
- Front-end (RUPAR), si riferisce ad indirizzi della rete RUPAR per condividere ed accedere a sistemi e servizi con altri Enti della PA o del CSI; questi sistemi possono essere raggiunti dalla rete internet tramite NAT e Bilanciatore

### 5.1.3 Private Cluod – Internet.

Questo tipo di modello è idoneo per gli Enti non in RUPAR o per le aziende che intendono utilizzare il CSI come proprio Cloud Provider.

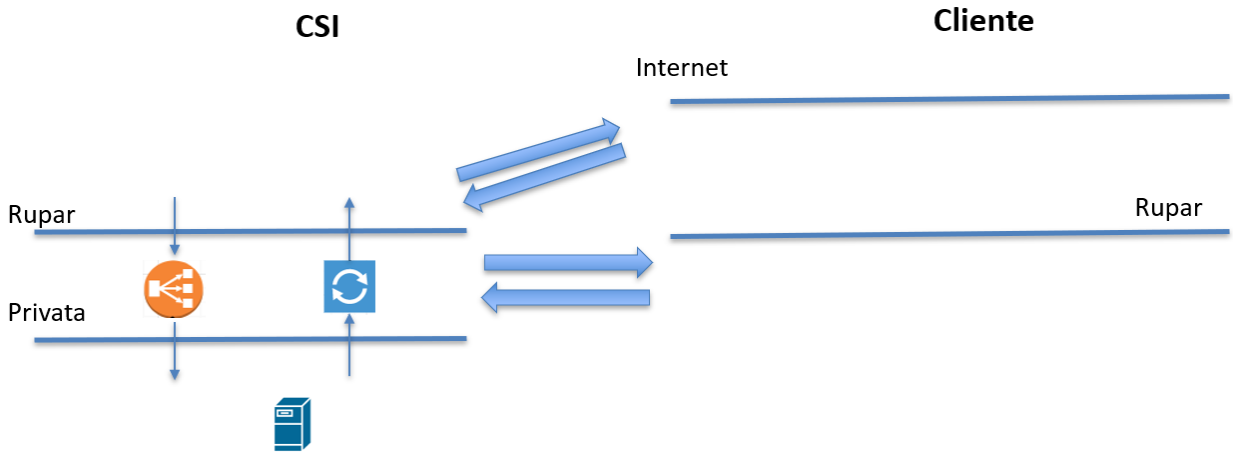



Sono presenti due reti: - Internet, si riferisce ad un piano di indirizzamento pubblico; - Privata, si riferisce ad indirizzi privati (non RUPAR) con i quali è possibile comunicare solo all'interno di questa sottorete o con Internet.

### 5.1.4 Private Cloud – RUPAR.

Questo tipo di modello è funzionale per gli Enti che sono in RUPAR, che hanno un proprio accesso verso Internet e che vogliono usarlo per i propri servizi ospitati sul Cloud del CSI.

L'immagine sottostante descrive questo scenario:




- RUPAR, si riferisce ad un piano di indirizzamento RUPAR dell'Ente;
- Privata, si riferisce ad indirizzi privati (non RUPAR) con i quali è possibile comunicare solo all'interno di questa sottorete o con la rete RUPAR dell'Ente.

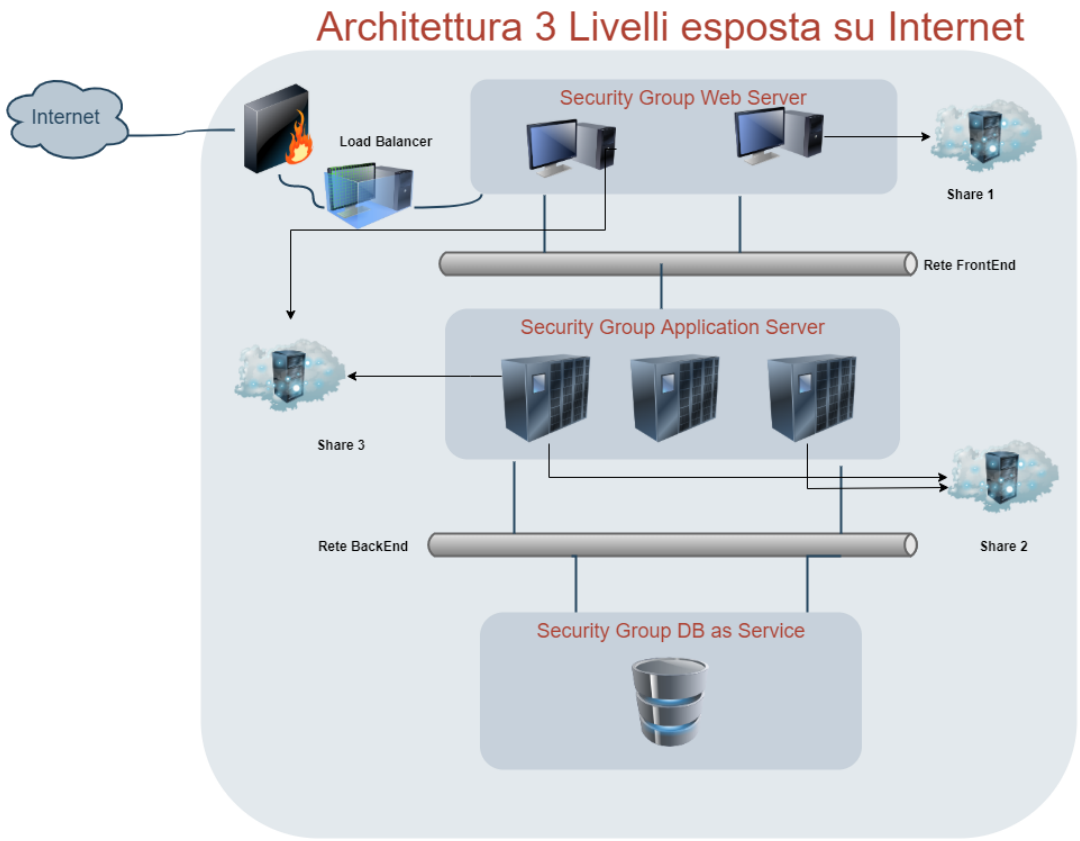
## 5.2 Modelli di Sicurezza

**Nivola** è una piattaforma completamente open source che semplifica l'utilizzo dei servizi cloud da parte della pubblica amministrazione. Nivola è realizzata dal **CSI Piemonte** e mette a disposizione potenza di calcolo, storage, rete e database e molto altro. Il risultato è quello di offrire a ogni amministrazione la completa autonomia nella creazione del proprio sistema informativo e nella migrazione delle applicazioni, in assoluta sicurezza. I servizi sono facilmente scalabili, senza spese di licenza e di gestione dell'hardware. Ogni ente può quindi creare in autonomia il proprio sistema informativo, pagando esclusivamente in base all'utilizzo, attraverso sistemi di rilevazione dei consumi .

## 5.3 Modello architetturale 3 livelli esposto su internet

La scelta dei 3 livelli rispetta la logica che i Web Server siano gli unici raggiungibili da Internet e dotati delle opportune protezioni. Gli Application Server, invece, sono da porre nella rete di Backend perchè devono essere connessi esclusivamente dai Web Server. Le istanze di Data Base as a Service (DBaaS) sono da collocare nella rete di backend, isolate e utilizzabili solo dagli Application Server.

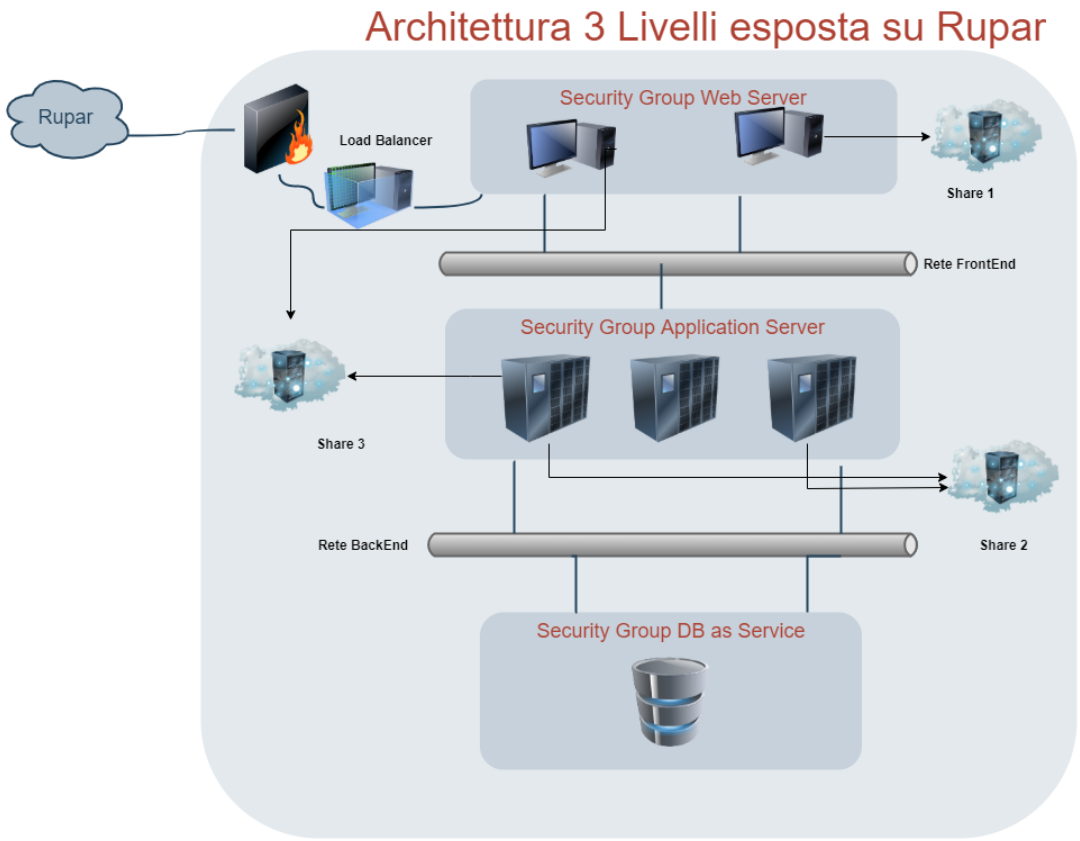
Il modello riportato nella figura sottostante, rappresenta un esempio di infrastruttura applicativa, disposta su 3 livelli e visibile da internet. Lo schema rappresenta il paradigma consigliabile a fronte di risorse da proteggere e in grado colloquiare attraverso reti diverse. Il disegno riporta, istanze create all'interno di **tre security group** distinti e attestati sulla rete di backend e su quella di frontend. Il Security Group dedicato ai **Web Server**, permette alle VM create al suo interno di essere raggiunte da **internet** sfruttando un **Load Balancer** che è protetto da un **firewall**. La **rete di backend** è condivisa dal Security group del **DB as a Service** e da quello degli **Application Server**. In questo modo, l'istanza DBaaS, è completamente separata e accessibile unicamente dalla rete di backend. A cavallo delle reti invece, possono essere generate istanze dello **Storage as Service**. Nello schema, sono stati collocati, share condivisi da macchine create su SG diversi o che rientrano nello stesso.




## 5.4 Modello architetturale 3 livelli su rete privata (RUPAR)

La scelta dei 3 livelli rispetta la logica che i Web Server siano gli unici raggiungibili da Rete privata (Rupar) e dotati delle opportune protezioni. Gli Application Server, invece, sono da porre nella rete di Backend perchè devono essere connessi esclusivamente dai Web Server. Le istanze di Data Base as a Service (DBaaS) sono da collocare nella rete di backend, isolate e utilizzabili solo dagli Application Server.

Il modello riportato nella figura sottostante, rappresenta un esempio di infrastruttura applicativa, disposta su 3 livelli e visibile da Rupar. Lo schema rappresenta il paradigma consigliabile a fronte di risorse da proteggere e in grado colloquiare attraverso reti diverse. Il disegno riporta, istanze create all'interno di **tre security group** distinti e attestati sulla rete di backend e su quella di frontend. Il Security Group dedicato ai **Web Server**, permette, alle VM create al suo interno, di essere raggiunte da **internet** sfruttando un **Load Balancer** che è protetto da un **firewall**. La **rete di backend** è condivisa dal Security group del **DB as a Service** e da quello degli **Application Server**. In questo modo, l'istanza DBaaS, è completamente separata e accessibile unicamente dalla rete di backend. A cavallo delle reti invece, possono essere generate istanze dello **Storage as Service**. Nello schema, sono stati collocati, share condivisi da macchine create su SG diversi o che rientrano nello stesso.


Architettura 3 Livelli esposta su Rupar
Rupar
Load Balancer
Security Group Web Server
Share 1
Rete FrontEnd
Security Group Application Server
Share 3
Rete BackEnd
Share 2
Security Group DB as Service

CHAPTER

SIX

# USARE LA COMMAND LINE INTERFACE (CLI)

In questa sezione si trovano una serie di tutorial per iniziare rapidamente ad interagire con la piattaforma, attraverso la Command Line Interface.

## 6.1 Access to CLI

The ways to access on Command Line Interface (CLI) are two. The first is using by the provider's users only:

```
ssh <login domnt>@cmpto1-cons02.site01.nivolapiemonte.it
```

The second, used by business user is:

```
ssh <login psnet>@cmpto2-cons02.site02.nivolapiemonte.it
```

The "login psnet" is provided by Nivola Support Center.

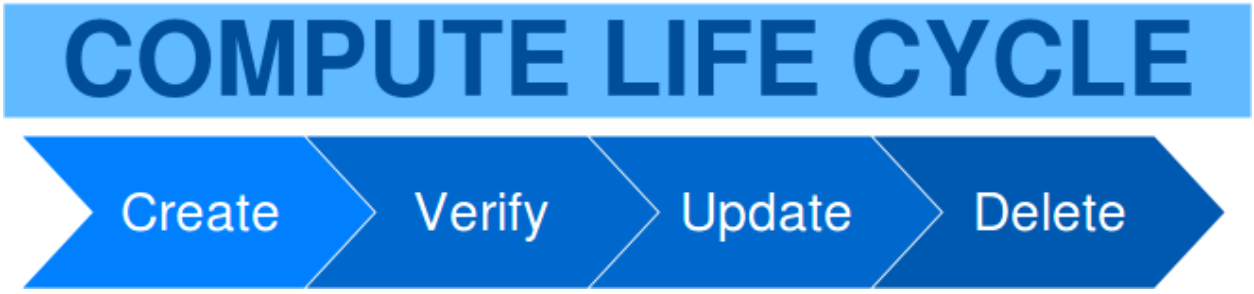
## 6.2 Manage Virtual Machine from CLI

It is the main service that you must have in your Account to use all the other following services. From CLI is possible to manage the Virtual Machines (VM). Generally the life cycle of the VM includes the following steps.

- [Create] your Virtual machine
- [Access] your Virtual machine
- [Verify] the virtual machine into account
- [Update] Virtual Machine
- [Stop] Virtual Machine
- [*Start* Virtual Machine
- [Delete] Virtual Machine

The steps creation and capabiity assign are mandatory for service use.

### 6.2.1 Life Cycle of Virtual Machine




#### How to Create Virtual Machine

**Add**:

Using add command you are going to create a virtual machine and all it needs for applications that you will runs above. It is necessary to have an Account and the role with privileges who permit to use add command. The way to use the command add is the following:

```
$ beehive bu cpaas vms add name=.. account=.. type=.. subnet=.. image=.. security-
↪group=.. key-name=.. [pwd=..] [main-disk=..] [disks=..] [hypervisor=..] [meta=..]␣
↪[options ...]

  Add Virtual Machine.

  Fields:
    name                    vm name
    account                 account id or composed name (org.div.account)
    type                    vm type
    subnet                  subnet id or name
    image                   image id or name
    security-group          security group id or name
    key-name                ssh key name
    pwd                     root password [optional]
    main-disk               optional main disk size configuration. Use <size>:<tag> to␣
↪set custom disk size and storage tag.
                            Ex. 5:oracle [optional]
    disks                   list of additional disk sizes comma separated. Use :<tag>␣
↪to set custom storage tag.
                            Ex. 5,10 or 5:oracle,10 [optional]
    hypervisor              set hypervisor. Can be: openstack or vsphere␣
↪[default=openstack]
    meta                    custom metadata [optional]

  optional arguments:
    -h, --help              show this help message and exit
    --debug                 toggle debug output
    --quiet                 suppress all output
    -o {json}               output handler
    -v, --version           show program's version number and exit
    -k KEY, --key KEY       Secret key file to use for encryption/decryption
    --vault VAULT           Ansible vault password to use for inventory decryption
    -e ENV, --env ENV       Execution environment
    -E ENVS, --envs ENVS    Comma separated execution environments
    -f FRMT, --frmt FRMT    response format
```

(continues on next page)

(continued from previous page)

```
    --color COLOR         response colered. Can be true or false. [default=true]
    --verbose VERBOSITY   ansible verbosity
    --cmds                list available commands
    --notruncate          disable long string truncation
    --truncate TRUNCATE   set max length of long string
    --curl                log curl request
    --fields FIELDS       response fields
```

**add example**:

The example we are going to use for explain how to create a Virtual Machine has like as goal the VM named **vm-demo** inside account Datacenter.account-demo. All variables used in this example are mandatories. There are three steps that you could use to create a usable VM:

- To get account id, type, subnet and image
- To use add comand for creating the VM
- To use the list command to verify that everything is OK

First Step

You are going to remember the Account id using list command

```
$ beehive bu accounts list

   Account list obtained

   id                                   name          division    contact    managed␣
↪     core services    base services  status    date
   ----------------------------------  ------------  ----------  ---------  --------
↪-  ---------------  ---------------  --------  --------------------
   930aa960-374a-427b-9a33-a7869251e14e  account-demo  Datacenter  -          True    ␣
↪                 0                0  ACTIVE    2019-02-20T08:49:15Z
```

List command help you to get from Nivola the Types that you can use within account-demo

```
$  beehive bu cpaas vms types list accounts=account-demo


   VM Types list obtained

   id                                   instance_type    desc                        ␣
↪status    active    creation              is_default
   ----------------------------------  ---------------  --------------------------  ␣
↪--------  --------  -------------------  ------------
   9bb61461-f6e6-4540-99ea-2de3c0eac140  vm.l8.4xlarge    vcpus:8 ram:56GB disk:80GB ␣
↪ACTIVE    True      2019-02-19T11:11:01Z  False
   d509186d-0b9a-45ad-8da4-64aa4a0b5282  vm.l8.3xlarge    vcpus:8 ram:48GB disk:80GB ␣
↪ACTIVE    True      2019-02-19T11:11:01Z  False
   76a9b1da-b118-40ad-b0f8-31450b696f33  vm.l8.2xlarge    vcpus:8 ram:40GB disk:80GB ␣
↪ACTIVE    True      2019-02-19T11:11:00Z  False
   e040ac12-86f5-41b1-a329-f3c3213b183x  vm.l8.xlarge     vcpus:8 ram:32GB disk:80GB ␣
↪ACTIVE    True      2019-02-19T11:10:59Z  False
   7ddd3c4c-0b32-401f-bf3b-e90519ef6a3z  vm.l8.large      vcpus:8 ram:24GB disk:80GB ␣
↪ACTIVE    True      2019-02-19T11:10:58Z  False
   8b8c93a2-376d-4a5b-94d0-48cc57003339  vm.m8.3xlarge    vcpus:8 ram:48GB disk:40GB ␣
↪ACTIVE    True      2019-02-19T11:10:57Z  False
   860e7430-5244-4179-9e09-d8d8e97fe57g  vm.m8.2xlarge    vcpus:8 ram:40GB disk:40GB ␣
↪ACTIVE    True      2019-02-19T11:10:57Z  False
```

(continues on next page)

(continued from previous page)

```
   6affa6af-5c6d-4725-8311-354837a6ed8h  vm.m8.xlarge     vcpus:8 ram:32GB disk:40GB ␣
↪ACTIVE    True      2019-02-19T11:10:56Z  False
   d15850cb-6ae7-4569-bdbb-27e8558c56f1  vm.m8.large      vcpus:8 ram:24GB disk:40GB ␣
↪ACTIVE    True      2019-02-19T11:10:55Z  False
   526ff3e0-ceb7-4f3c-9c35-ba2274b0f49a  vm.m4.6xlarge    vcpus:4 ram:48GB disk:40GB ␣
↪ACTIVE    True      2019-02-19T11:10:54Z  False
```

List command help you to get from Nivola the Subnets that you can use within account-demo

```
$  beehive bu cpaas subnets list accounts=account-demo

   Subnets list obtained

   id                                    name                    state      account ␣
↪  availabilityZone    vpc          cidr
   ------------------------------------  ----------------------  ---------  --------
↪  ------------------  -----------  ---------------
   015514b4-9533-4aa3-a449-91a02c45940x  SubnetInternet-torino01  available  gaetest ␣
↪  SiteTorino01        VpcInternet  84.240.190.0/24
   6f22eb27-3aea-40e2-be6b-af5ad1c4290x  SubnetWEB-vercelli01     available  gaetest ␣
↪  SiteVercelli01      VpcWEB       10.138.200.0/21
   85d9dc49-285e-426a-9bcb-ef56e90f498j  SubnetWEB-torino02       available  gaetest ␣
↪  SiteTorino02        VpcWEB       10.138.168.0/21
   8b64ee86-eda4-40d9-a206-e64c3aeba6a9  SubnetWEB-torino01       available  gaetest ␣
↪  SiteTorino01        VpcWEB       10.138.136.0/21
   09627b89-c342-4072-8f9f-2cf421e5393c  SubnetBE-vercelli01      available  gaetest ␣
↪  SiteVercelli01      VpcBE        10.138.192.0/21
   76cf51db-70d5-4084-a65e-61c4ab76aa7b  SubnetBE-torino02        available  gaetest ␣
↪  SiteTorino02        VpcBE        10.138.160.0/21
   2f8d7886-e08a-4512-a825-b7ac6bcfc3c6  SubnetBE-torino01        available  gaetest ␣
↪  SiteTorino01        VpcBE        10.138.128.0/21
   b07ef60a-4f64-4640-8d23-5a4e7b9d1920  SubnetInternet-torino01  available  clitest ␣
↪  SiteTorino01        VpcInternet  84.240.190.0/24
   e3cc531c-125f-40a2-8eb8-be3f81505369  SubnetWEB-vercelli01     available  clitest ␣
↪  SiteVercelli01      VpcWEB       10.138.200.0/21
```

List command help you to get from Nivola the Images that you can use within account-demo

```
$  beehive bu cpaas images list accounts=account-demo

   Images list obtained

   id                                    name          state      type     account   ␣
↪     platform
   ------------------------------------  ------------  ---------  -------  --------- ␣
↪     -------------
   dd07271b-410e-4162-82ec-572a9904b4b8  Centos7-nmsf  available  machine  test      ␣
↪     centos 7.6
   97ca993d-f2ff-46fb-81b6-0331e21b5575  Ubuntu16      available  machine  gaetest   ␣
↪     ubuntu 16
   36ba1d80-58f4-4f20-97c2-384cc0d73085  OracleLinux7  available  machine  gaetest   ␣
↪     OracleLinux 7
   ab343efb-a2fe-4e94-b293-5b037dbaeb0e  Centos6       available  machine  gaetest   ␣
↪     centos 6.9
   cfe3ffd2-0b1e-4279-b17d-6178a3adba31  Centos7       available  machine  gaetest   ␣
↪     centos 7.    5
   aaa8e2c7-7c73-47c3-9766-2dc2f3844949  Ubuntu16      available  machine  account-
↪demo     ubuntu 16
```

(continues on next page)

(continued from previous page)

```
   a5164e53-4e28-4f99-9c10-5c893fd9dadf  OracleLinux7  available  machine  account-
↪demo    OracleLinux 7
   66c4c569-8a22-4de1-ab9e-573e66706733  Centos6       available  machine  account-
↪demo    centos 6.9
   01fb2a8f-2d14-47c2-aa70-f780b1cf8a8f  Centos7       available  machine  account-
↪demo    centos 7.5
   38a085d0-491e-43ed-bc4b-04d57f81d4cf  Ubuntu16      available  machine  test
↪     ubuntu 16
```

At last you have to know the ssh key using the command ssh key list

```
$  beehive ssh keys list

   ssh keys list obtained

   id                                    name         desc    date
↪pub_key
   ------------------------------------  -----------  ------  --------------------  ---
↪-------------------------------------------------------------------------------
   f057bff8-4d62-40fe-9b77-73ccb1b8e6fx  sshkey-demo          2018-09-05T11:16:23Z
↪c3NoLXJzYSBBQUFBQjNOemFDMXljMkVBQUFBREFRQUJBQUFCQVFDbXQyTmU3TXlFYUJLQ1VKOXBJR3dM...
```

Step two

You can create a VM using the add command obtaining the id from Nivola

```
$ beehive business cpaas vms add name=vm-demo account=Datacenter.account-demo type=vm.
↪l8.large subnet=SubnetBE-torino02 image=Centos7 security-group=SecurityGroupBE key-
↪name=sshkey-gae

  The VM vm-demo is created and Nivola will show you his id using the message follow

  msg
  ------------------------------------------------------------
  Add virtual machine: b0633d20-399e-4168-9f13-60fba49a40fe
```

To see the VM is running use the list command with the following syntax

```
$ beehive business cpaas vms list account=account-demo

  id                                    name              type          state
↪launchTime            account    availabilityZone    privateIp      privateDnsName
↪                            image    subnet
  ------------------------------------  ----------------  ------------  -------  ------
↪--------------  ---------  ------------------  -------------  ----------------------
↪---------------------  -------  -------------------
  b0633d20-399e-4168-9f13-60fba49a40fe  vm-demo           vm.l8.large   running  2019-
↪02-27T09:44:34Z  account-demo  SiteTorino02     10.138.160.62  vm-demo.site02.
↪nivolapiemonte.it             Centos7  SubnetBE-torino02
```

### How to List Virtual Machine

The command below is used to acces on Virtual machine instantiated into your account.

**Access**:

```
$  beehive ssh nodes connect <node> [nodeuser=..] [options ...]

  <node> is node name or uuid or ipadress
  <nodeuser> is node user default is is root

    optional arguments:
    -h, --help            show this help message and exit
    --debug               toggle debug output
    --quiet               suppress all output
    -o {json}             output handler
    -v, --version         show program's version number and exit
    -k KEY, --key KEY     Secret key file to use for encryption/decryption
    --vault VAULT         Ansible vault password to use for inventory decryption
    -e ENV, --env ENV     Execution environment
    -E ENVS, --envs ENVS  Comma separated execution environments
    -f FRMT, --frmt FRMT  response format
    --color COLOR         response colered. Can be true or false. [default=true]
    --verbose VERBOSITY   ansible verbosity
    --cmds                list available commands
    --notruncate          disable long string truncation
    --truncate TRUNCATE   set max length of long string
    --curl                log curl request
    --fields FIELDS       response fields
    --afields AFIELDS     response additional fields
    -y, --assumeyes       Assume that the answer to any question which would be
                          asked is yes.
    -rt, --runtime        Enable command duration log.
```

### How to List Virtual Machine

The command below is used to ontain the list Virtual machine instantiated into your account.

**list**:

```
$ beehive business cpaas vms list account=account-demo

  id                                   name              type         state
↪launchTime            account    availabilityZone    privateIp      privateDnsName
↪                            image    subnet
  ------------------------------------  ----------------  -----------  -------  ------
↪--------------  ---------  ------------------  -------------  ----------------------
↪---------------------  -------  ------------------
  b0633d20-399e-4168-9f13-60fba49a40fe  vm-demo           vm.l8.large  running  2019-
↪02-27T09:44:34Z  account-demo  SiteTorino02     10.138.160.62  vm-demo.site02.
↪nivolapiemonte.it             Centos7  SubnetBE-torino02
```

### How to Update Virtual Machine

The commands below are used to update Virtual machine.

**update**:

The command is used to modify Virtual Machine attributes.

```
$ beehive bu cpaas vms update <vm> [field=..] [options ...]

  Update VM

  Fields:

    vm                    vm id
    type                  vm type

   optional arguments:    are the same described into add command
```

In this example we are going to change the type attribute.

```
$ beehive bu cpaas vms update b0633d20-399e-4168-9f13-60fba49a40fe type=vm.m8.xlarge

  update
```

This is the Nivola response when the type was changed

```
$ msg
  ------------------------------------------------------------
  Modify virtual machine b0633d20-399e-4168-9f13-60fba49a40fe
```

### How to Start Virtual Machine

If it is necessary to start the VM, you have to use next command from CLi:

```
$ beehive bu cpaas vms start <vm>

  <vm> is a vm's id

    optional arguments:
    -h, --help            show this help message and exit
    --debug               toggle debug output
    --quiet               suppress all output
    -o {json}             output handler
    -v, --version         show program's version number and exit
    -k KEY, --key KEY     Secret key file to use for encryption/decryption
    --vault VAULT         Ansible vault password to use for inventory decryption
    -e ENV, --env ENV     Execution environment
    -E ENVS, --envs ENVS  Comma separated execution environments
    -f FRMT, --frmt FRMT  response format
    --color COLOR         response colered. Can be true or false. [default=true]
    --verbose VERBOSITY   ansible verbosity
    --cmds                list available commands
    --notruncate          disable long string truncation
    --truncate TRUNCATE   set max length of long string
    --curl                log curl request
    --fields FIELDS       response fields
```

(continues on next page)

(continued from previous page)

```
    --afields AFIELDS     response additional fields
    -y, --assumeyes       Assume that the answer to any question which would be
                          asked is yes.
    -rt, --runtime        Enable command duration log.
```

### How to Stop Virtual Machine

If you need to stop the VM, you have to use next command:

```
$ beehive bu cpaas vms stop <vm>

  <vm> is a vm's id

    optional arguments:
    -h, --help            show this help message and exit
    --debug               toggle debug output
    --quiet               suppress all output
    -o {json}             output handler
    -v, --version         show program's version number and exit
    -k KEY, --key KEY     Secret key file to use for encryption/decryption
    --vault VAULT         Ansible vault password to use for inventory decryption
    -e ENV, --env ENV     Execution environment
    -E ENVS, --envs ENVS  Comma separated execution environments
    -f FRMT, --frmt FRMT  response format
    --color COLOR         response colered. Can be true or false. [default=true]
    --verbose VERBOSITY   ansible verbosity
    --cmds                list available commands
    --notruncate          disable long string truncation
    --truncate TRUNCATE   set max length of long string
    --curl                log curl request
    --fields FIELDS       response fields
    --afields AFIELDS     response additional fields
    -y, --assumeyes       Assume that the answer to any question which would be
                          asked is yes.
    -rt, --runtime        Enable command duration log.
```

### How to Delete Virtual Machine

The commands below are used to erase Virtual machine from Nivola.

**delete**:

The command is used to erase Virtual Machine from the cloud-system

```
$ beehive bu cpaas vms delete <vm> [options ...]


  Delete a Virtual Machine

  Fields:

    vm                  is the vm id


  optional arguments:     are the same described into add command
```

Next example show you how to use delete command

```
$ beehive bu cpaas vms delete 59e7e61c-665d-48a5-8ca3-a769e45f8e1b


  Delete VM
```

Below the nivola's response after VM was deleted

```
$ msg
  ------------------------------------------------------------
  Delete virtual machine 59e7e61c-665d-48a5-8ca3-a769e45f8e1b
```

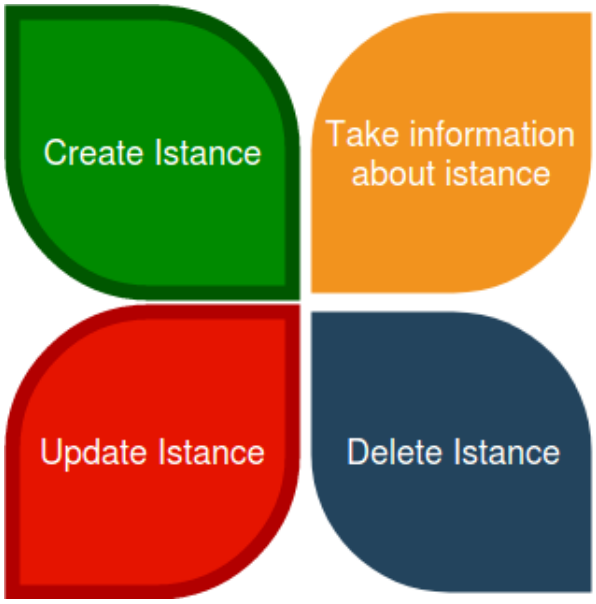
## 6.3 Manage Security Group from CLI

Security group acts as a firewall for Nivola instances, controlling both inbound and outbound traffic at the instance level. The life cycle of the security group includes the following steps.

- Obtain information on template of the Security Group and VPC
- Create Security Group
- Manage rules of Security Group
- Delete Security Group

For manage security groups we assume that you are familiar with **VPC**. VPC is an acronym for Virtual Private Cloud. VPC is a virtual network dedicated to the Nivola account. It is logically isolated from the other Nivola networks. It is possible to use the instance within your Vpc. It is possible to configure the Vpc by modifying the range of IP addresses, creating subnets, configuring route tables, network gateways and security settings. The VPC consists of one or more security group. For create a security group you need using a template.

### 6.3.1 Life Cycle of Security Group



### 6.3.2 Use case of Security Group

#### Obtain information about Security Group and VPC

**list security groups**:

The command list security group. The command list security group. The command is used to gather information on security groups that can be used by user.

```
$ beehive bu cpaas securitygroups list [field=..] [options ...]

  List all security groups

  fields:
     accounts              list of account name or uuid comma separated [optional]
     ids                   list of security group ids comma separated [optional]
     vpc-ids               list of vpc ids comma separated [optional]
     tags                  list of tags comma separated [optional]
     page                  list page [default=0]
     size                  list page size [default=10]


  optional arguments:
    -h, --help            show this help message and exit
    --debug               toggle debug output
    --quiet               suppress all output
    -o {json}             output handler
    -v, --version         show program's version number and exit
    -k KEY, --key KEY     Secret key file to use for encryption/decryption
    --vault VAULT         Ansible vault password to use for inventory decryption
    -e ENV, --env ENV     Execution environment
    -E ENVS, --envs ENVS  Comma separated execution environments
    -f FRMT, --frmt FRMT  response format
    --color COLOR         response colered. Can be true or false. [default=true]
    --verbose VERBOSITY   ansible verbosity
    --cmds                list available commands
    --notruncate          disable long string truncation
    --truncate TRUNCATE   set max length of long string
    --curl                log curl request
    --fields FIELDS       response fields
```

**list example**:

```
$ beehive business cpaas securitygroups list

   Security Group list obtained

   id                                   name                    state      account    ␣
↪vpc            egress_rules    ingress_rules
   ------------------------------------  ----------------------  ---------  ---------  ␣
↪-----------  --------------  ---------------
   bcdf974a-53bb-42dc-8c29-ea7c97843ca4  SecurityGroupBE         available  acc-demo   ␣
↪VpcBE                      2               4
   200775e3-9e08-4705-9b42-f417b7784788  SecurityGroupInternet   available  acc-demo1  ␣
↪VpcInternet                3               5
   e12492a0-7e97-4cf8-aa6d-9adbc8dea5cb  SecurityGroupWEB        available  acc-demo   ␣
↪VpcWEB                     3               5
   bf8cec43-9973-4cd1-a1e9-c2d31c9f6386  SecurityGroupInternet   available  acc-test   ␣
↪VpcInternet                3               5
```

(continues on next page)

(continued from previous page)

```
   74c12829-c1a6-4ba7-b103-2b7f187eefde  SecurityGroupWEB       available  acc-test1 ␣
↪VpcWEB                      3               6
   86a1554e-2e7c-401f-83af-0e2623c24c61  SecurityGroupBE        available  acc-test2 ␣
↪VpcBE                       8               4
```

**list security groups template**:

The commands below show as obtain a list of template usable for creating of the security group.

```
$ beehive bu cpaas securitygroups templates [template-id [options ...]

  List security group templates

  fields:
     template-id           template id [optional]

  optional arguments:     are the same described into first command explained in this␣
↪chapter
```

**list security groups template example**:

```
$ beehive business cpaas securitygroups templates

   Security Group template list obtained

   Page: 0
   Count: 3
   Total: 3
   Order: id DESC

   id                                    instance_type          desc                  ␣
↪          status    active    creation              is_default
   ------------------------------------  ---------------------  ----------------------
↪--------  --------  --------  --------------------  ------------
   d6c3c32b-8124-49c9-9e5d-598fec7f98b1  SecurityGroupSimple    SecurityGroup with␣
↪basic rules  ACTIVE    True      2019-01-03T14:03:28Z  False
   c59e58f2-14e0-493f-9851-35a840b708e7  SecurityGroupFrontEnd  SecurityGroupFrontEnd␣
↪          ACTIVE    True      2018-06-15T20:03:15Z  False
   e0fe7e7f-6fda-4931-bc9f-61d36503cex7  SecurityGroupBackEnd   SecurityGroupBackEnd  ␣
↪          ACTIVE    True      2018-06-15T20:03:14Z  True
```

It is necessary to know the VPC father

**list VPC**:

The commands below show as obtain a list of Virtual private Cloud usable for creating of the security group.

```
$ beehive bu cpaas vpcs list [field=..] [options ...]

  List all vpcs

  fields:
  accounts              list of account name or uuid comma separated [optional]
  ids                   list of vpc ids comma separated [optional]
  tags                  list of tags comma separated [optional]
  page                  list page [default=0]
  size                  list page size [default=10]
```

(continues on next page)

(continued from previous page)

```
  optional arguments:     are the same described into first command explained in this␣
↪chapter
```

**list vpcs example**:

In the next example will be possible to see how to use the list vpcs command utilizable for the account-demo.

```
$ beehive business cpaas vpcs list account=account-demo

  The list of all vpcs utilizable from account-demo

  Page: 0
  Count: 9
  Total: 9
  Order: id asc

  id                                   name          state      account         cidr
  -----------------------------------  ------------  ---------  ---------       -------
↪-----------------------------------------
  d810b85c-2214-4ca6-9c7f-2d33dac1dafe  VpcInternet   available  account-demo    84.240.
↪190.0/24
  1546f7a6-a789-4d74-8c65-2b30aaca9f2f  VpcWEB        available  account-demo    10.138.
↪136.0/21, 10.138.168.0/21, 10.138.200.0/21
  1b33e19a-fa1a-475e-be9c-3ec2fd1f99ad  VpcBE         available  account-demo    10.138.
↪128.0/21, 10.138.160.0/21, 10.138.192.0/21
  f71e9661-cde6-46b1-8c7d-8fefd13039c4  VpcInternet   available  clitest         84.240.
↪190.0/24
  a41e2be6-cc86-498b-b659-59ad56024eac  VpcWEB        available  clitest         10.138.
↪136.0/21, 10.138.168.0/21, 10.138.200.0/21
  69294068-e38b-4fc1-8e4b-b14bfbefcda9  VpcBE         available  clitest         10.138.
↪128.0/21, 10.138.160.0/21, 10.138.192.0/21
  d0801fdd-5686-4ff4-ad9d-bbf43236aad8  VpcInternet   available  test            84.240.
↪190.0/24, 84.240.191.0/24
  60766403-e50d-42d2-93bf-34e23183e389  VpcWEB        available  test            10.138.
↪136.0/21, 10.138.168.0/21, 10.138.200.0/21
  0fd1a70c-ef3a-4ba7-961c-15baee6962b5  VpcBE         available  test            10.138.
↪128.0/21, 10.138.160.0/21, 10.138.192.0/21
```

### Create Security Group

To create the security group it will use add command like showed follow

**Add security group**:

```
$  beehive bu cpaas securitygroups add <name> <vpc> [template=..] [options ...]

   Create a security group

   fields:
   name                  security group name
   vpc                   parent vpc
   template-id           template id [optional]

  optional arguments:     are the same described into first command explained in this␣
↪chapter
```

**Add security group example**:

In this example sec-group-demo is created using add command with a vpcBE and template The variables that Nivola need are indicated to Nivola using their id. When the creation process will end Nivola indicate the new security group into the list of them. Available will be the status of the new security group visible using command "securitygroup list"

```
$  beehive business cpaas securitygroups add sec-group-demo 1b33e19a-fa1a-475e-be9c-
↪3ec2fd1f99ad template=e0fe7e7f-6fda-4931-bc9f-61d36503ce67

   The Nivola reply will be

   msg
   ------------------------------------------------------
   Add securitygroup 0c35528a-6e43-45c3-8b41-d8265deeddf4
```

Next step we are going to see the new list of security groups

```
$ beehive business cpaas securitygroups list

  The CLI response after the list command confirming the creation of the sec-group-
↪demo and his state av

  id                                    name                    state      account
↪  vpc            egress_rules    ingress_rules
  ------------------------------------  ----------------------  ---------  ---------
↪  -----------  ---------------  ----------------
  0c35528a-6e43-45c3-8b41-d8265deeddf4  sec-group-demo          available  account-
↪demo  VpcBE                        0                0
```

### Update rules of the security group

**add-rule ingress/egress**:

The commands below are used to change ingress or egress rules.

```
$ beehive bu cpaas securitygroups add-rule <type> <securitygroup> <dest/source>␣
↪[proto=..] [port:..] [options ...]

  Add a security group rule.

   Fields:
   type                  egress or ingress. For egress group is the source and␣
↪specify the destination.
                         For ingress group is the destination and specify the source.
   securitygroup         securitygroup id
   proto                 can be tcp, udp, icmp or -1 for all. [default=-1]
   port                  can be an integer between 0 and 65535 or a range with start␣
↪and end in the same
                         interval. Range format is <start>-<end>. Use -1 for all␣
↪ports. [default=-1]
   dest/source           rule destination. Syntax <type>:<value>. Source and␣
↪destination type can be SG, CIDR.
                         For SG value must be <sg_id>. For CIDR value should like 10.
↪102.167.0/24.

  optional arguments:     are the same described into first command explained in this␣
↪chapter
```

In the next example a ingress rule is added to security group sec-group-demo.

**add-rule ingress**:

For the new ingress rule the variables used are tcp as protocol, 53 as a port and CIDR as source.

```
$ beehive business cpaas securitygroups add-rule ingress 0c35528a-6e43-45c3-8b41-
↪d8265deeddf4 CIDR:0.0.0.0/0 proto=tcp port=53
```

The nivola response after the command confirming the creation of ingress rule will be

```
$ msg
  ------------------------------
  Create securitygroup rule True
```

**security group get**:

If it need more information about security group it could be use the command get

```
$ beehive bu cpaas securitygroups get <securitygroup> [options ...]


   Get security group with rules

   fields:
   securitygroup         securitygroup id


    account               account name or uuid

  optional arguments:     are the same described into add command
```

Next example show how to use the command

```
$ beehive business cpaas securitygroups get 0c35528a-6e43-45c3-8b41-d8265deeddf4
```

The nivola response after the command showing the information that you need

```
$ id                                    name              desc                role
  ------------------------------------  ----------------  ------------------  ------
  c63f04c9-bde0-4ac3-8479-57a637049cd2  736@domnt.csi.it  Davide Gialli       master
  01ac26db-a213-4307-8dc9-d7ac45f2e3e3  187@domnt.csi.it  Gaetano Rossi       master

  attrib               value
  -------------------  ------------------------------------
  sgOwnerAlias         account-demo
  vpcId                1b33e19a-fa1a-475e-be9c-3ec2fd1f99ad
  groupDescription     sec-group-demo
  groupName            sec-group-demo
  state                available
  vpcName              VpcBE
  ownerId              30
  stateReason.message  None
  stateReason.code     None
  sgOwnerId            f6a6c1db-4a9f-4788-af9a-9bc92d4f487e
  groupId              0c35528a-6e43-45c3-8b41-d8265deeddf4
  Egress rules:
  toSecuritygroup                                              toCidr     protocol ␣
↪  fromPort    toPort    reserved    state
```

(continues on next page)

(continued from previous page)

```
  ------------------------------------------------------------  ---------  ----------
↪  ----------  --------  ----------  -------
                                                          0.0.0.0/0  *           *
↪       *         True        ACTIVE
  gaetest:sec-group-demo [0c35528a-6e43-45c3-8b41-d8265deeddf4]             *
↪  *           *         True        ACTIVE
  Ingress rules:
  fromSecuritygroup                                                  fromCidr
↪protocol    fromPort    toPort    reserved    state
  ------------------------------------------------------------  ----------------  ---
↪-------  ----------  --------  ----------  --------
                                                                   0.0.0.0/0
↪tcp         53          53        False       BUILDING
                                                                   10.102.184.0/24   *
↪         *           *         True        ACTIVE
                                                                   10.138.154.0/24   *
↪         *           *         True        ACTIVE
                                                                   158.102.160.0/24  *
↪         *           *         True        ACTIVE
  gaetest:sec-group-demo [0c35528a-6e43-45c3-8b41-d8265deeddf4]                    *
↪         *           *         True        ACTIVE
```

**del-rule ingress/egress**:

The commands below are used to delete ingress or egress rules from SG.

```
$ beehive bu cpaas securitygroups del-rule <type> <securitygroup> <dest/source>
↪[proto=..] [port:..] [options ...]

  Delete a security group rule.

    fields:
    type                      egress or ingress. For egress group is the source and
↪sp
↪      ecify the destination.
                              For ingress group is the destination and specify the
↪sou
↪       rce.
    securitygroup             securitygroup id
    proto                     can be tcp, udp, icmp or -1 for all. [default=-1]
    port                      can be an integer between 0 and 65535 or a range with
↪st
↪      art and end in the same
                              interval. Range format is <start>-<end>. Use -1 for all
↪
↪    ports. [default=-1]
    dest/source               rule destination. Syntax <type>:<value>. Source and
↪dest
↪        ination type can be SG, CIDR.
                              for SG value must be <sg_id>. For CIDR value should
↪like
↪         10.102.167.0/24.

    optional arguments:
        -h, --help            show this help message and exit
        --debug               toggle debug output
        --quiet               suppress all output
```

(continues on next page)

(continued from previous page)

```
        -o {json}             output handler
        -v, --version         show program's version number and exit
        -k KEY, --key KEY     Secret key file to use for encryption/decryption
        --vault VAULT         Ansible vault password to use for inventory decryption
        -e ENV, --env ENV     Execution environment
        -E ENVS, --envs ENVS  Comma separated execution environments
        -f FRMT, --frmt FRMT  response format
        --color COLOR         response colered. Can be true or false. [default=true]
        --verbose VERBOSITY   ansible verbosity
        --cmds                list available commands
        --notruncate          disable long string truncation
        --truncate TRUNCATE   set max length of long string
        --curl                log curl request
        --fields FIELDS       response fields
        --afields AFIELDS     response additional fields
        -y, --assumeyes       Assume that the answer to any question which would be
                              asked is yes.
        -rt, --runtime        Enable command duration log.
```

### Delete security group

If the life of security group into Nivola finish it necessary erase it from the Nivola system using delete command.

**delete securitygroup**:

The commands below is used to erase security group from Nivola.

```
$ beehive bu cpaas securitygroups delete <securitygroup> [options ...]

  Delete a security group

  fields:
    securitygroup         securitygroup id

  optional arguments:     are the same described into first command explained in this␣
↪chapter
```

Next example show how to use the command

```
$  beehive business cpaas securitygroups delete 0c35528a-6e43-45c3-8b41-d8265deeddf4
```

The nivola response after the command confirming security group was erased

```
msg
-------------------------
Delete securitygroup True
```

## 6.4 How to add disk to Virtual Machine

You can attach the volume to one of virtual machine who are into your account. The prerequisites you need are the id of [instance] and [volume]

The command you have to edit is

```
$  beehive provider instances volumes add <instance_id> <volume_id>

  Add provider compute instance volumes
  fields:
      id                    instance name or uuid
      volume                volume name or uuid
  optional arguments:
      -h, --help            show this help message and exit
      --debug               toggle debug output
      --quiet               suppress all output
      -o {json}             output handler
      -v, --version         show program's version number and exit
      -k KEY, --key KEY     Secret key file to use for encryption/decryption
      --vault VAULT         Ansible vault password to use for inventory decryption
      -e ENV, --env ENV     Execution environment
      -E ENVS, --envs ENVS  Comma separated execution environments
      -f FRMT, --frmt FRMT  response format
      --color COLOR         response colered. Can be true or false. [default=true]
      --verbose VERBOSITY   ansible verbosity
      --cmds                list available commands
      --notruncate          disable long string truncation
      --truncate TRUNCATE   set max length of long string
      --curl                log curl request
      --fields FIELDS       response fields
      --afields AFIELDS     response additional fields
      -y, --assumeyes       Assume that the answer to any question which would be
                            asked is yes.
      -rt, --runtime        Enable command duration log.
```

### 6.4.1 How to know instance id

To get the instance id it is necessary to type the command:

```
$  beehive provider instances list



  optional arguments:
      -h, --help            show this help message and exit
      --debug               toggle debug output
      --quiet               suppress all output
      -o {json}             output handler
      -v, --version         show program's version number and exit
      -k KEY, --key KEY     Secret key file to use for encryption/decryption
      --vault VAULT         Ansible vault password to use for inventory decryption
      -e ENV, --env ENV     Execution environment
      -E ENVS, --envs ENVS  Comma separated execution environments
      -f FRMT, --frmt FRMT  response format
      --color COLOR         response colered. Can be true or false. [default=true]
```

(continues on next page)

(continued from previous page)

```
      --verbose VERBOSITY   ansible verbosity
      --cmds                list available commands
      --notruncate          disable long string truncation
      --truncate TRUNCATE   set max length of long string
      --curl                log curl request
      --fields FIELDS       response fields
      --afields AFIELDS     response additional fields
      -y, --assumeyes       Assume that the answer to any question which would be
                            asked is yes.
      -rt, --runtime        Enable command duration log.
```

### 6.4.2 How to know volume id

To get the volume id you have to type the command:

```
$  beehive provider volumes list


  optional arguments:
      -h, --help            show this help message and exit
      --debug               toggle debug output
      --quiet               suppress all output
      -o {json}             output handler
      -v, --version         show program's version number and exit
      -k KEY, --key KEY     Secret key file to use for encryption/decryption
      --vault VAULT         Ansible vault password to use for inventory decryption
      -e ENV, --env ENV     Execution environment
      -E ENVS, --envs ENVS  Comma separated execution environments
      -f FRMT, --frmt FRMT  response format
      --color COLOR         response colered. Can be true or false. [default=true]
      --verbose VERBOSITY   ansible verbosity
      --cmds                list available commands
      --notruncate          disable long string truncation
      --truncate TRUNCATE   set max length of long string
      --curl                log curl request
      --fields FIELDS       response fields
      --afields AFIELDS     response additional fields
      -y, --assumeyes       Assume that the answer to any question which would be
                            asked is yes.
      -rt, --runtime        Enable command duration log.
```

## 6.5 To create a volume

You can create a volume that you can then attach to any Virtual Machine whithin the same account, compute zone and availability zone. For create a volume the [json] is required then you have to use the command below:

```
$  beehive provider volumes add <json file>


  Create volume

    volume:
```

(continues on next page)

(continued from previous page)

```
       container: ResourceProvider01
       name: demo-volume01
       desc: demo-volume01
       compute_zone: ComputeService-44ff4cf3
       availability_zone: SiteVercelli01
       size: 5
       type: openstack
       flavor: vol.default



optional arguments:
    -h, --help            show this help message and exit
    --debug               toggle debug output
    --quiet               suppress all output
    -o {json}             output handler
    -v, --version         show program's version number and exit
    -k KEY, --key KEY     Secret key file to use for encryption/decryption
    --vault VAULT         Ansible vault password to use for inventory decryption
    -e ENV, --env ENV     Execution environment
    -E ENVS, --envs ENVS  Comma separated execution environments
    -f FRMT, --frmt FRMT  response format
    --color COLOR         response colered. Can be true or false. [default=true]
    --verbose VERBOSITY   ansible verbosity
    --cmds                list available commands
    --notruncate          disable long string truncation
    --truncate TRUNCATE   set max length of long string
    --curl                log curl request
    --fields FIELDS       response fields
    --afields AFIELDS     response additional fields
    -y, --assumeyes       Assume that the answer to any question which would be
                          asked is yes.
    -rt, --runtime        Enable command duration log.
```

The last step is to create volume using

### 6.5.1 To create json

The requirements that you need for json are [flavors], [computezones] and [others]. You can generate a json file using this CLI's command:

```
[login@cmpto1-cons02 ~]$ more add-volume.json
{
"volume":{
"container": "ResourceProvider01",
"name":"dbs-tst-001-aefd07ad-volume-1",
"desc":"Disco-dati",
"compute_zone": "ComputeService-366929f1",
"availability_zone": "SiteTorino02",
"type":"vsphere",
"flavor": "vol.oracle.default",
"size": 200
}
}
```

### 6.5.2 To know flavors

The command to know a flavour is:

```
$  beehive provider volumeflavors list


  List provider items

  optional arguments:
      -h, --help            show this help message and exit
      --debug               toggle debug output
      --quiet               suppress all output
      -o {json}             output handler
      -v, --version         show program's version number and exit
      -k KEY, --key KEY     Secret key file to use for encryption/decryption
      --vault VAULT         Ansible vault password to use for inventory decryption
      -e ENV, --env ENV     Execution environment
      -E ENVS, --envs ENVS  Comma separated execution environments
      -f FRMT, --frmt FRMT  response format
      --color COLOR         response colered. Can be true or false. [default=true]
      --verbose VERBOSITY   ansible verbosity
      --cmds                list available commands
      --notruncate          disable long string truncation
      --truncate TRUNCATE   set max length of long string
      --curl                log curl request
      --fields FIELDS       response fields
      --afields AFIELDS     response additional fields
      -y, --assumeyes       Assume that the answer to any question which would be
                            asked is yes.
      -rt, --runtime        Enable command duration log.
```

### 6.5.3 To know compute zones

CLI is going to show you the compute zone using the command

```
$  beehive provider compute-zones list


  List compute-zones

  optional arguments:
      -h, --help            show this help message and exit
      --debug               toggle debug output
      --quiet               suppress all output
      -o {json}             output handler
      -v, --version         show program's version number and exit
      -k KEY, --key KEY     Secret key file to use for encryption/decryption
      --vault VAULT         Ansible vault password to use for inventory decryption
      -e ENV, --env ENV     Execution environment
      -E ENVS, --envs ENVS  Comma separated execution environments
      -f FRMT, --frmt FRMT  response format
      --color COLOR         response colered. Can be true or false. [default=true]
      --verbose VERBOSITY   ansible verbosity
      --cmds                list available commands
      --notruncate          disable long string truncation
```

(continues on next page)

(continued from previous page)

```
      --truncate TRUNCATE   set max length of long string
      --curl                log curl request
      --fields FIELDS       response fields
      --afields AFIELDS     response additional fields
      -y, --assumeyes       Assume that the answer to any question which would be
                            asked is yes.
      -rt, --runtime        Enable command duration log.
```

### 6.5.4 To know other information

The las info that you need for create a json are get using the command:

```
$  beehive provider volumes list


  List volumes

  optional arguments:
      -h, --help            show this help message and exit
      --debug               toggle debug output
      --quiet               suppress all output
      -o {json}             output handler
      -v, --version         show program's version number and exit
      -k KEY, --key KEY     Secret key file to use for encryption/decryption
      --vault VAULT         Ansible vault password to use for inventory decryption
      -e ENV, --env ENV     Execution environment
      -E ENVS, --envs ENVS  Comma separated execution environments
      -f FRMT, --frmt FRMT  response format
      --color COLOR         response colered. Can be true or false. [default=true]
      --verbose VERBOSITY   ansible verbosity
      --cmds                list available commands
      --notruncate          disable long string truncation
      --truncate TRUNCATE   set max length of long string
      --curl                log curl request
      --fields FIELDS       response fields
      --afields AFIELDS     response additional fields
      -y, --assumeyes       Assume that the answer to any question which would be
                            asked is yes.
      -rt, --runtime        Enable command duration log.
```

## 6.6 Copy file

There are two ways to make a copy of a file. [Get] to copy from remote VM to Server where you are using the CLI on contrary you need to use [put].

### 6.6.1 How to copy file using get

```
$  beehive ssh nodes files get <node> <local-file> <remote-file> [nodeuser=..]␣
↪[options ...]

  Copy file from node

    fields:
          node                  node name or uuid
          nodeuser              connection user [default=root]
          local-file            full path of local file to copy to node
          remote-file           full path of remote file

    optional arguments:
          -h, --help            show this help message and exit
          --debug               toggle debug output
          --quiet               suppress all output
          -o {json}             output handler
          -v, --version         show program's version number and exit
          -k KEY, --key KEY     Secret key file to use for encryption/decryption
          --vault VAULT         Ansible vault password to use for inventory decryption
          -e ENV, --env ENV     Execution environment
          -E ENVS, --envs ENVS  Comma separated execution environments
          -f FRMT, --frmt FRMT  response format
          --color COLOR         response colered. Can be true or false. [default=true]
          --verbose VERBOSITY   ansible verbosity
          --cmds                list available commands
          --notruncate          disable long string truncation
          --truncate TRUNCATE   set max length of long string
          --curl                log curl request
          --fields FIELDS       response fields
          --afields AFIELDS     response additional fields
          -y, --assumeyes       Assume that the answer to any question which would be
                                asked is yes.
          -rt, --runtime        Enable command duration log.
```

### 6.6.2 How to copy file using put

```
$  beehive ssh nodes files put <node> <local-file> <remote-file> [nodeuser=..]␣
↪[options ...]

  Copy file from node

    fields:
          node                  node name or uuid
          nodeuser              connection user [default=root]
          local-file            full path of local file to copy to node
          remote-file           full path of remote file
```

(continues on next page)

(continued from previous page)

```
optional arguments:
      -h, --help            show this help message and exit
      --debug               toggle debug output
      --quiet               suppress all output
      -o {json}             output handler
      -v, --version         show program's version number and exit
      -k KEY, --key KEY     Secret key file to use for encryption/decryption
      --vault VAULT         Ansible vault password to use for inventory decryption
      -e ENV, --env ENV     Execution environment
      -E ENVS, --envs ENVS  Comma separated execution environments
      -f FRMT, --frmt FRMT  response format
      --color COLOR         response colered. Can be true or false. [default=true]
      --verbose VERBOSITY   ansible verbosity
      --cmds                list available commands
      --notruncate          disable long string truncation
      --truncate TRUNCATE   set max length of long string
      --curl                log curl request
      --fields FIELDS       response fields
      --afields AFIELDS     response additional fields
      -y, --assumeyes       Assume that the answer to any question which would be
                            asked is yes.
      -rt, --runtime        Enable command duration log.
```

CHAPTER

SEVEN

# GLOSSARIO

In questa sezione si trovano una serie di tutorial per iniziare fin da subito ad interagire con la piattaforma, attraverso il portale.

## 7.1 Termini ed Acronimi usati da Nivola

Nella tabella seguente, raggruppati in ordine alfabetico, si riportano i termini e gli acronimi frequentemente utilizzati su Nivola, allo scopo di far acquisire familiarità con la piattaforma.

### 7.1.1 1.1 A

| Acronimo/Termine | Significato |
|---|---|
| ACCOUNT | Contenitore di istanze di servizio Per gli Account dell'Organizzazione CSI il nome con cui identificarlo è il **codice prodotto**. Per i prodotti del CSI è previsto un Account per l'ambiente di produzone ed un altro per gli altri denominato **preprod**. |
| API | Application Programming Interface (in italiano traducibile come Interfaccia di programmazione di un'applicazione), le API sono strumenti di programmazione messi a disposizione degli sviluppatori per facilitare il loro compito nella realizzazione di applicazioni integrate. |
| APP Engine | Template preconfigurato composto da risorse elaborative, database, storage, reti e sicurezza che implementa una particolare funzione |
| Availability Zone (AZ) | Aggregato di uno o più Site. L'AZ è caratterizzata da una sua completa autonomia infrastrutturale e indipendenza |

### 7.1.2 1.2 B

| Acronimo/Termine | Significato |
|---|---|
| BCK-aaS | Il servizio di backup as a service è un'opzione attivabile dall'utente per il backup delle macchine virtuali attivate in Nivola. Il Cliente può scegliere se attivare il backup sulle risorse selezionate e scegliere i livelli di retention più appropriati per il proprio servizio.<br>Il servizio viene erogato attraverso piattaforme che permettono una notevole affidabilità infrastrutturale, e attraverso la funzione di "deduplica dei dati", per il raggiungimento di una elevata efficienza. I backup sono depositati su apparati storage differenti da quelli che ospitano dati e servizi . |

### 7.1.3 1.3 C

| Acronimo/Termine | Significato |
|---|---|
| Capability | Attributo essenziale dell'account per istanziare i servizi. E' assegnato all'account in fase di creazione. A fronte di un account è possibile avere più capabilities. |
| CLI | Command Line Interface - nel progetto Nivola trattasi di command interface dedicata alla gestione di tutte le risorse della CMP. L'utilizzo è possibile anche per gli utenti accreditati e i propri fornitori attraverso opportuna profilazione. |
| CMP | Cloud Management Platform - piattaforma di integrazione ed automazione che espone tutti i servizi di business attraverso API (Application programming Interface) richiamabili dall'utente o attraverso l'uso del Service Portal. Include i servizi di accounting, profilazione, security. |
| Compute Services | Insieme di funzioni utili a creare e gestire e le Virtual Machine Categoria di servizi che permette di fruire di risorse elaborative (espresse in CPU, RAM e spazio disco) in differenti flavour e template, corredate da servizi di networking e security.<br>Sulla base del perimetro delle risorse presenti, gli utilizzatori saranno in grado di realizzare i propri tenant, istanziare le macchine virtuali selezionandole da un ampio catalogo di template e di gestirle in modo autonomo e integrato con gli altri servizi disponibili. |
| Consumer | User utilizzare della piattaforma Nivola |

1.4 D

| Acronimo/Termine | Significato |
|---|---|
| Divisione | E' il secondo livello organizzativo. Una organizzazione può avere più divisioni. Ogni Divisione ha ha associato un portafoglio chiamato Wallet che ne definisce il limite di spesa. Per un Cliente esterno può coincidere con il valore della determina o con una pòarte di essa. Non può esserci una Divisione senza un Organizzazione da cui dipendere. Nel caso l'organizzazione della divisione sia CSI il suo nome dovrà coincidere sempre l'ID della Soluzione applicativa. Nel caso l'ID non sia stato attrubuito usare "Staging" in attesa che venga attribuito |
| DBaaS | "Data Base as a Service" sono servizi gestiti costituiti da ambienti virtuali dedicati in differenti configurazioni e tecnologie, con differenti livelli di affidabilità e ridondanza in funzione delle esigenze del Cliente. Sono inclusi i servizi di backup, restore, monitoraggio, aggiornamento e patching. |

### 7.1.4 1.5 E

| Acronimo/Termine | Significato |
|---|---|

### 7.1.5 1.6 F

| Acronimo/Termine | Significato |
|---|---|
| FLAVOUR Alias TYPE | Identificano le differenti tipologie di VM le cui caratteristiche differiscono per la quantità di risorse CPU, RAM e DISCO. L'utente può scegliere tra diversi flavour in base delle proprie esigenze. |

### 7.1.6 1.7 G

| Acronimo/Termine | Significato |
|---|---|

### 7.1.7 1.8 H

| Acronimo/Termine | Significato |
|---|---|

### 7.1.8 1.9 I

| Acronimo/Termine | Significato |
|---|---|
| Immagine | Parametro che determina l'OS della VM da istanziare eventualmente arricchito del software per l'automazione come p.e. ansible o heat |

### 7.1.9 1.10 J

| Acronimo/Termine | Significato |
|---|---|

### 7.1.10 1.11 K

| Acronimo/Termine | Significato |
|---|---|
| KEY | Chiave ssh usata al momento della creazione della VM abilitando la connessione da remoto. |

### 7.1.11 1.12 L

| Acronimo/Termine | Significato |
|---|---|

### 7.1.12 1.13 M

| Acronimo/Termine | Significato |
|---|---|

### 7.1.13 1.14 N

| Acronimo/Termine | Significato |
|---|---|
| Nivola | Ci si riferisce al complesso di tutte le componenti della piattaforma: Service Portal, CMP, back-end . |
| NMSF | Nuovo Modello Server Farm |
| NSC | Nivola Support Center - Single Point of Contact per tutti i servizi cloud (Nivola, NMSF, POSC) |

### 7.1.14 1.15 O

| Acronimo/Termine | Significato |
|---|---|
| Organizzazione | E' gerarchicamente il massimo livello organizzativo. Dall'Organizzazione possono dipendere 1 o più Divisioni. Ad un organizzazione può coincidere un Ente. Il nome sarà sempre CSI per tutto ciò che dovrà ospitare prodotti del CSI. |

### 7.1.15 1.16 P

| Acronimo/Termine | Significato |
|---|---|
| Provider | CSI Piemonte, nella sua veste di Cloud provider |
| POD | Point Of Delivery - aggregato di infrastrutture elaborative, storage, rete e sicurezza autoconsistenti |

### 7.1.16 1.17 Q

| Acronimo/Termine | Significato |
|---|---|

### 7.1.17 1.18 R

| Acronimo/Termine | Significato |
|---|---|
| Region | Aggregato di una o più Availability Zone |
| Rupar | Rupar Piemonte è la Rete Unitaria della Pubblica Amministrazione a cui possono aderire tutti gli Enti locali piemontesi |

### 7.1.18 1.19 S

| Acronimo/Termine | Significato |
|---|---|
| SG Security Group | E' il firewall della istanze di Nivola. Configurabile dall'utente per controllare il traffico in entrata e in uscita da e verso le istanze. Il SG protegge ogni singola istanza al suo interno. Per far colloquiare istanze del medesimo SG tra loro si dovrà agire sulle regole di ingresso e di uscita. |
| Service Portal | È il portale di servizio a cui consumer e provider accedono per il governo dei servizi esposti da Nivola. L'interfaccia è in grado cooperare con le API di business esposte dalla CMP.<br>Il Service Portal espone inoltre funzioni proprie come l'accesso alla documentazione, ai video tutorial, alla chat e al Servizio di assistenza tramite il Team di Supporto Nivola per supportare l'utente in caso di problemi, malfunzionamenti o semplici how-to-use. |
| Site | Aggregato di uno o più POD |
| Storage as Service STAAS | Il servizio prevede la fornitura di spazio disco prestazionale raggiungibile via rete con protocolli NFS e CIFS esclusivamente dalle macchine virtuali Nivola. La messa a disposizione dei servizi di storage avviene su infrastrutture ridondate e configurate in alta affidabilità. |
| SUBNET | E' un range di IP utilizzabile all'interno del VpC. E' possibile usare delle risorse di Nivola all'interno di una specifica subnet. E' possibile usare una subnet per risorse che devono connettersi ad Internet ed una privata, per risorse che invece non hanno necessità di connettersi ad Internet. Per proteggere le risorse di Nivola in ciascuna sottorete, è possibile utilizzare più security groups. |

### 7.1.19 1.20 T

| Acronimo/Termine | Significato |
|---|---|
| Tagli | Definiscono le dimensioni massime complessive delle risorse della Virtual Machine. |
| Tags | Attraverso i TAGS la piattaforma mette a disposizione la possibilità di etichettare le proprie risorse in modo da facilitare di individuarle e ricercarle con chiavi personalizzabili. |
| Template | Sono le tipologie e le versioni del OS utilizzati per la creazione della Virtual Machine. |

### 7.1.20 1.21 U

| Acronimo/Termine | Significato |
|---|---|
| Utente/User | Persona fisica accreditata all'accesso ai servizi Nivola |

### 7.1.21 1.22 V

| Acronimo/Termine | Significato |
|---|---|
| VM: Virtual Machine | Server in grado di ospitare servizi. |
| VPC: Virtual Private Cloud | E' una rete virtuale dedicata all'account Nivola, logicamente isolata dalle altre reti di Nivola. L'istanza è utilizzabie all'interno del proprio Vpc. Il Vpc è configurabile modificando il range degli indirizzi IP. Possibile creare sottoreti, indicando route tables, network gateways e security settings. |

### 7.1.22 1.23 W

| Acronimo/Termine | Significato |
|---|---|

### 7.1.23 1.24 X

| Acronimo/Termine | Significato |
|---|---|

### 7.1.24 1.25 Y

| Acronimo/Termine | Significato |
|---|---|

### 7.1.25 1.26 Z

| Acronimo/Termine | Significato |
|---|---|

CHAPTER

EIGHT

# RELEASE NOTES

## 8.1 Service Portal 1.8.0 (2020-04-08)

**New**

- Rilasciato nuovo ruolo utente "Viewer di Account": da oggi potranno essere accreditati utenti con il ruolo di Viewer di Account. Per i dettagli operativi del ruolo si rimanda alla sezione *Utenti, Ruoli ed Account*
- l'utente Master di Divisione ha a disposizione una nuova funzionalità in modo da poter accreditare e registare utenti all'interno della propria struttura organizzativa.
- l'utente di BackOffice ha ha disposizione una nuova funzionalità di visualizzazione dei Servizi disponibili su ogni Account.

**Changed**

- La form di richiesta utenze su DBAAS è stata aggiornata con la possibilità di richiedere utenze Amministrative
- Aggiornata la procedura guidata per la creazione di VM con s.o. Windows in modo da accettare password sicure
- La grafica e il contenuto del pannello Costi e Consumi di un Account sono stati rivisti e migliorati.
- Nel pannello di gestione di una Vm è ora possibile visualizzare eventuali dischi aggiuntivi.

**Fixed**

- Risolto bug #803 sulla creazione di Vm con immagine Oracle Linux.
- Adeguati i tagli delle dimensioni degli Share e dei dischi aggiuntivi di VM e DBAAS.
- Bux fixing su alcune informazioni contenute nella home page dell'uente Master di Account (#779)

## 8.2 Service Portal 1.7.0 (2020-03-02)

New:

- rilasciata funzionalità che permette all'utente Master di Account di visualizzare il dettaglio di tutti i costi legati al proprio account

Changed

- La procedura di creazione chiavi dbaas è stata aggiornata on la richiesta del parametro Disco Aggiuntivo

Fixed:

- Bug Risolti (issue:4420,4023)

# BIBLIOGRAPHY


[Create]

[Access]

[Verify]

[Update]

[Start]

[Stop]

[Delete]

[instance]

[volume]

[json]

[flavors]

[computezones]

[others]

[Get]

[put]

[A]

[B]

[C]

[D]

[E]

[F]

[G]

[H]

[I]

[J]

[K]

[L]

[M]

[N]

[O]

[P]

[Q]

[R]

[S]

[T]

[U]

[V]

[W]

[X]

[Y]

[Z]