

CREAZIONE VM SU CLOUD INSIEL

MATRICE DELLE REVISIONI					
REVISION	DATA	DESCRIZION	REDAZION	VERIFICATA	APPROVATA
00	22.10.2024	1a emissione	Gruppo di lavoro	RSGI/RQ/RSPPGA/RSTRUUTT	DG/DS/DA/DSS

GRUPPO DI LAVORO PER LA REDAZIONE		
<i>Cognome e nome</i>	<i>Qualifica</i>	<i>Struttura di appartenenza</i>
Jarc Borut		ASUGI
Chiffi Francesco	System Senior Expert	BV-Tech

INDICE

1. SCOPO	5
2. AMBITO DI APPLICAZIONE	5
3. ACRONIMI E DEFINIZIONI	5
4. RESPONSABILITÀ	5
5. MODALITÀ ESECUTIVE	6
5.1. CONFIGURAZIONE DELL'INFRASTRUTTURA	6
5.1.1. VMWARE VSPPHERE	6
5.1.2. VMWARE NSX	6
5.1.3. VMWARE ARIA.....	8
5.2. IMPLEMENTAZIONE DELL'INFRASTRUTTURA.....	9
5.2.1. LOCALIZZAZIONE	9
5.2.2. CONNETTIVITÀ DI RETE	9
5.2.2.1. CONNETTIVITÀ FISICA	9
5.2.2.2. CONNETTIVITÀ LOGICA	9
5.3. CLOUD INSIEL	11
5.3.1. ACCESSO AL CLOUD INSIEL	11
5.3.1.1. LOGIN	11
5.3.1.2. RESET PASSWORD.....	13
5.3.1.3. PROBLEMI DI ACCESSO.....	15
5.3.2. CARATTERISTICHE DEL CLOUD INSIEL	16
5.3.2.1. CLOUD MANAGER.....	16
5.3.2.1.1. ACCESSO AL CLOUD MANAGER.....	16
5.3.2.1.2. OVERVIEW.....	17
5.3.2.1.3. CATALOG	18
5.3.2.1.3.1.CREAZIONE DI UNA NUOVA VM	19
5.3.2.1.4. DEPLOYMENTS.....	22
5.3.2.1.4.1.DEPLOYMENTS.....	22
5.3.2.1.4.2.RESOURCES	29
5.3.2.1.4.3.VIRTUAL MACHINES	31
5.3.2.1.4.4.VOLUMES	35
5.3.2.1.4.5.NETWORKING E SECURITY.....	37
5.4. CLOUD FIREWALL	39
5.4.1.1.1. ACCESSO AL CLOUD FIREWALL.....	39
5.4.1.1.2. HOME	40
5.4.1.1.2.1.PANORAMICA	40
5.4.1.1.2.2.AVVISI.....	41
5.4.1.1.3. RETE	42
5.4.1.1.3.1.PANORAMICA DELLE RETE	42
5.4.1.1.4. GATEWAY DI LIVELLO 1.....	43
5.4.1.1.5. SEGMENTI	44
5.4.1.1.5.1.NSX.....	44
5.4.1.1.5.2.PROFILI	45
5.4.1.1.6. NAT 47	47
5.4.1.1.7. DNS	48
5.4.1.1.7.1.SERVIZI DNS	48
5.4.1.1.7.2.ZONE DNS	49
5.4.1.1.8. SICUREZZA.....	49
5.4.1.1.8.1.FIREWALL DISTRIBUITO.....	50
5.4.1.1.9. INVENTARIO	53
5.4.1.1.9.1.SERVIZI	54
5.4.1.1.9.2.GRUPPI	56
5.4.1.1.9.3.PROFILI	58
5.4.1.1.9.4.MACCHINE VIRTUALI.....	58
5.5. PROCESSO DI CREAZIONE VM	58

5.5.1. CREAZIONE VM	58
5.5.1.1. ACCESSO A CLOUD MANAGER	58
5.5.1.2. SELEZIONE SISTEMA OPERATIVO	58
5.5.1.3. SELEZIONE T-SHIRT	58
5.5.1.4. VERIFICA CAPIENZA	59
5.5.1.5. DISCHI AGGIUNTIVI	59
5.5.1.6. ESPANSIONE DISCO DI SISTEMA	59
5.5.1.7. CAMBIO DENOMINAZIONE VM	59
5.5.1.8. PRIMO ACCESSO ALLA VM	59
5.5.2. REGOLE FIREWALL	59
5.5.2.1. ACCESSO A NSX	59
5.5.2.2. CONFIGURAZIONE REGOLE	59
5.5.2.3. PROBLEMI DI RETE	59
5.5.3. CONFIGURAZIONE VM	59
5.5.3.1. MODIFICA NOME HOST	59
5.5.3.1.1. Microsoft Windows Server	59
5.5.3.1.2. Linux	59
5.5.3.2. AGGIUNTA A DOMINIO	60
5.5.3.3. ESPANSIONE DISCO DI SISTEMA	60
5.5.3.4. AGGIORNAMENTO SISTEMA OPERATIVO	60
5.5.3.4.1. VERIFICA SU CONSOLE WSUS	60
5.5.3.4.2. AGGIORNAMENTO e patching	60
5.5.3.5. INSTALLAZIONE ANTIVIRUS	60
5.5.3.5.1. VERIFICA FUNZIONAMENTO SU CONSOLE ANTIVIRUS	60
6. APPENDICE 1 – CRITERI DI ASSEGNAZIONE DEGLI INDIRIZZI IP	61
6.1. SEGMENTI DI RETE	61
6.2. RANGE DI IP DEDICATI PER TIPOLOGIA DI SERVIZIO	61
7. APPENDICE 2 – NAMING CONVENTION	61
7.1. NOMI MACCHINE VIRTUALI	62
7.2. NOMI GRUPPI	62
8. GESTIONE DELLA DOCUMENTAZIONE	62
9. RIFERIMENTI (NORMATIVI E BIBLIOGRAFICI)	62
9.1. VMWARE VSOPHERE	62
9.2. VMWARE NSX	62
9.3. VMWARE ARIA	62
10. DOCUMENTI COLLEGATI	63
11. ALLEGATI (SE PRESENTI)	63
12. INDICE DELLE FIGURE	64

1. SCOPO

Scopo del presente documento è la definizione delle istruzioni operative relative a:

- Creazione di VM su cloud INSIEL.
- Configurazione regole di rete.
- Gestione di eventuali anomalie.

2. AMBITO DI APPLICAZIONE

L'ambito di applicazione del presente documento è inerente alla configurazione dei 'Wireless controller', degli 'Access point' e dei terminali che devono usufruire della rete wireless gestita dagli apparati precedentemente citati.

NOTA BENE:

- Tutti i parametri e le configurazioni per le quali non venga esplicitamente indicata una azione di modifica nel presente documento, devono essere lasciati inalterati ai valori di default già presenti. La modifica di tali valori potrebbe causare anomalie di funzionamento.

3. ACRONIMI E DEFINIZIONI

4. RESPONSABILITÀ'

5. MODALITÀ ESECUTIVE

5.1. CONFIGURAZIONE DELL'INFRASTRUTTURA

5.1.1. VMWARE VSPPHERE

L'infrastruttura di virtualizzazione di INSIEL è 'on premise' ovvero è gestita direttamente da INSIEL su proprio hardware, ed è basata sulla architettura VMWare VSPHERE di cui si riporta uno schema semplificato di seguito:

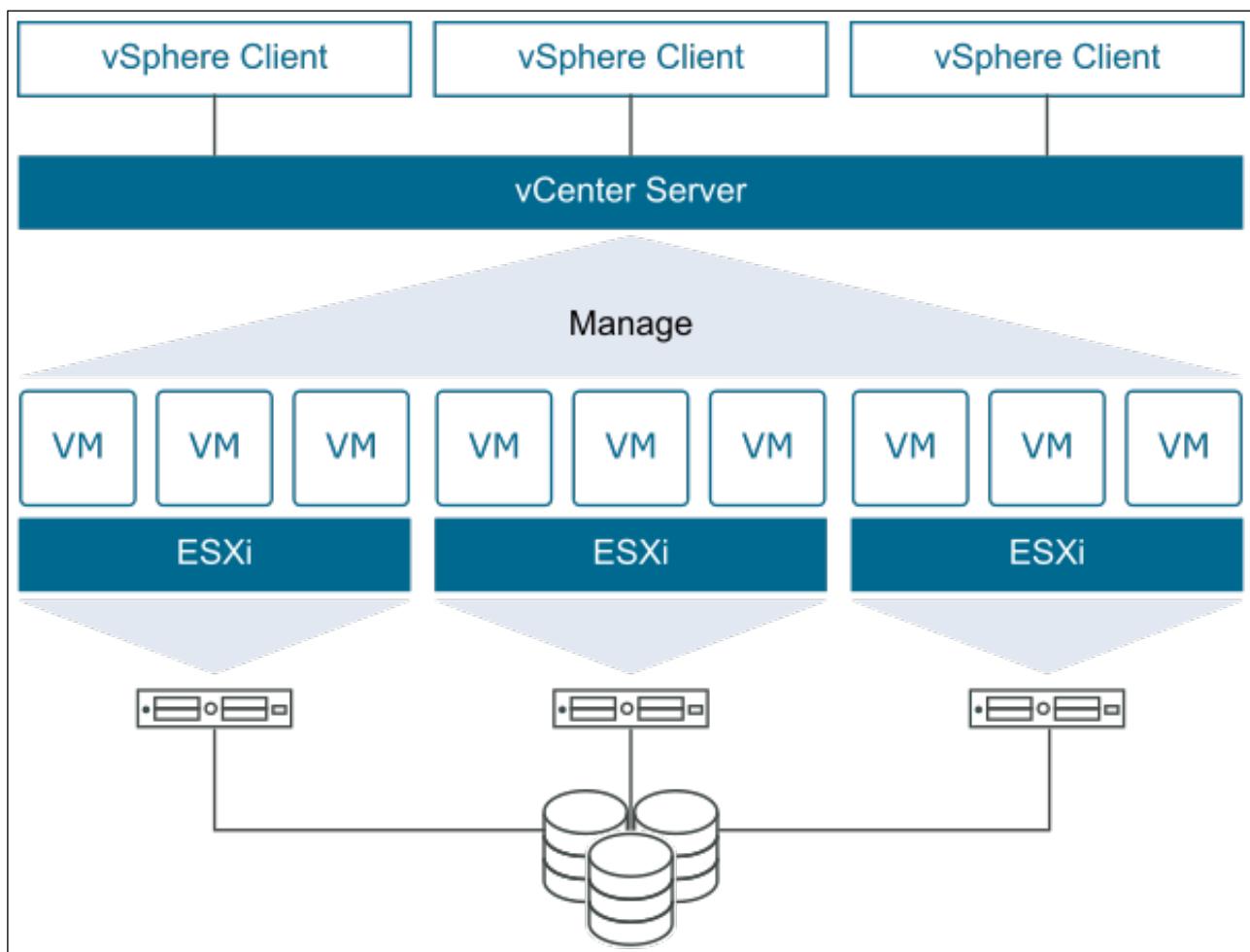


Figura 1 - VMWare Vsphere

In breve, semplificando al massimo:

- Sono disponibili un certo numero di host fisici.
- Sono disponibili un certo numero di dispositivi di storage.
- Su ogni host fisico è presente un hypervisor VMWare ESXi.
- Su ogni host fisico dotato di ESXi sono presenti le VM.
- Tutti gli host fisici dotati di hypervisor sono gestiti centralmente da un VCenter Server, che tipicamente è esso stesso una appliance virtuale.
- Gli utenti gestiscono l'infrastruttura mediante appositi client.

5.1.2. VMWARE NSX

VMWare VSpher dispone di una propria infrastruttura di rete, tuttavia dovendo gestire configurazioni più complesse e articolate, solitamente viene utilizzato VMWare NSX.
Di seguito descriviamo brevemente l'architettura di NSX:

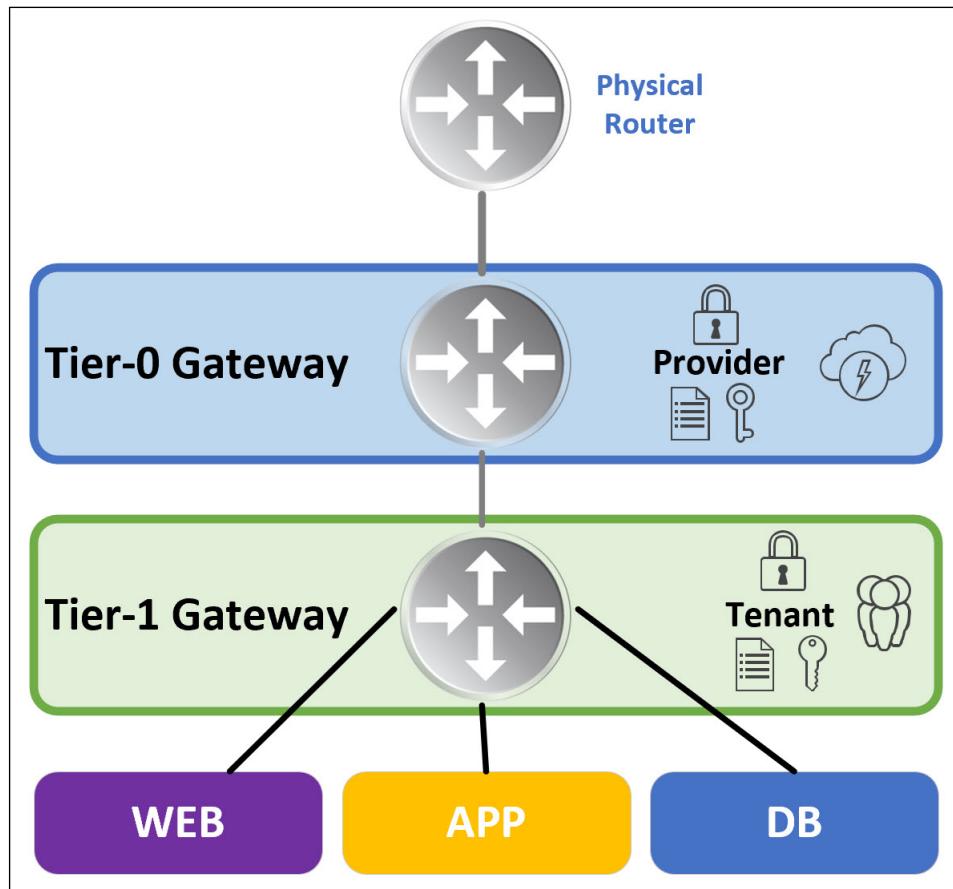


Figura 2 - VMWare NSX – Architettura

- **Il Tier-0 Gateway:** in totale gestione a carico di INSIEL, controlla il traffico da fuori a dentro e viceversa (Nord-Sud) ed include le interfacce verso la rete fisica.
- **Il Tier-1 Gateway:** in totale gestione a carico di ASUGI per ciò che concerne la parte di rete di propria pertinenza, controlla il traffico tra le VM (Est-Ovest). Il Tier-1 Gateway funziona per segmenti e non per subnet, in pratica ogni indirizzo IP è taggato. Un segmento del Tier-1 Gateway coincide con una VLAN del Tier-0 Gateway.

5.1.3. VMWARE ARIA

VMWare Aria è un orchestratore utilizzato per la gestione della infrastruttura di INSIEL. In sostanze mentre VClient necessita molta attività manuale da parte dell'utente che desideri creare una nuova VM, un orchestratore consente di avere un alto livello di automazione nell'esecuzione di attività ripetitive.

Di seguito uno schema sommario dell'architettura di VMWare ARIA:

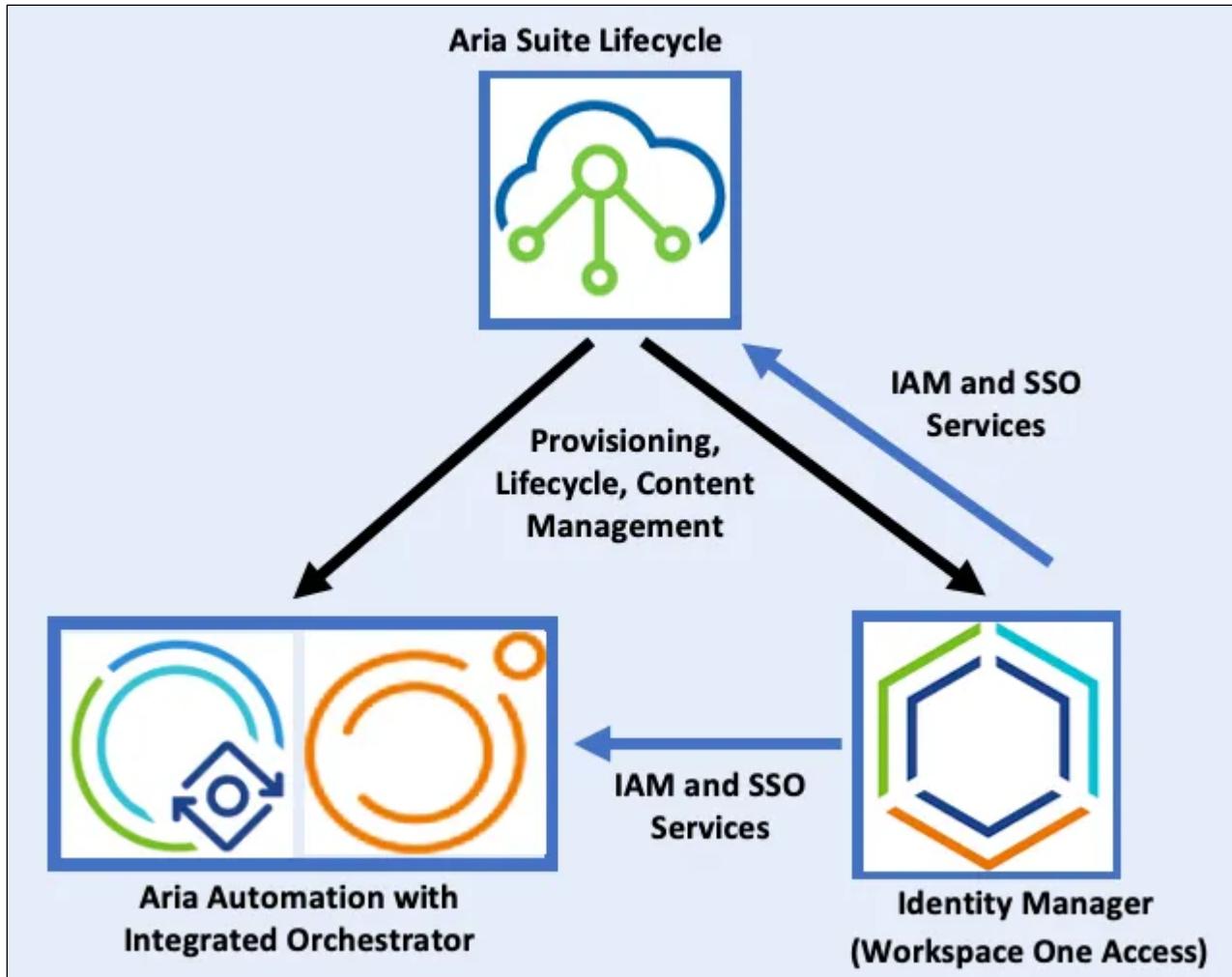


Figura 3 - VMWare ARIA

5.2. IMPLEMENTAZIONE DELL'INFRASTRUTTURA

5.2.1. LOCALIZZAZIONE

Lo IaaS INSIEL è diviso in due datacenter:

- Il nodo primario si trova a Trieste, in via San Francesco, presso la sede INSIEL;
- Il nodo secondario - di backup - si trova a Palmanova, nella sede della Protezione Civile.

Il nodo secondario viene utilizzato solo in caso di disastro. Lo switch avviene spostando il Tier 0 NSX sul datacenter di Palmanova. L'operazione dovrebbe essere trasparente, ovvero non è richiesto un cambio di indirizzamento delle macchine virtuali.

5.2.2. CONNETTIVITA' DI RETE

5.2.2.1. CONNETTIVITA' FISICA

Dal punto di vista fisico, INSIEL ha dedicato la rete 10.128.188.0/22, inserita nel contesto VRF ASUGI, alle macchine virtuali ASUGI; quindi, di fatto l'indirizzamento dell'infrastruttura IaaS è parte del contesto VRF ASUGI.

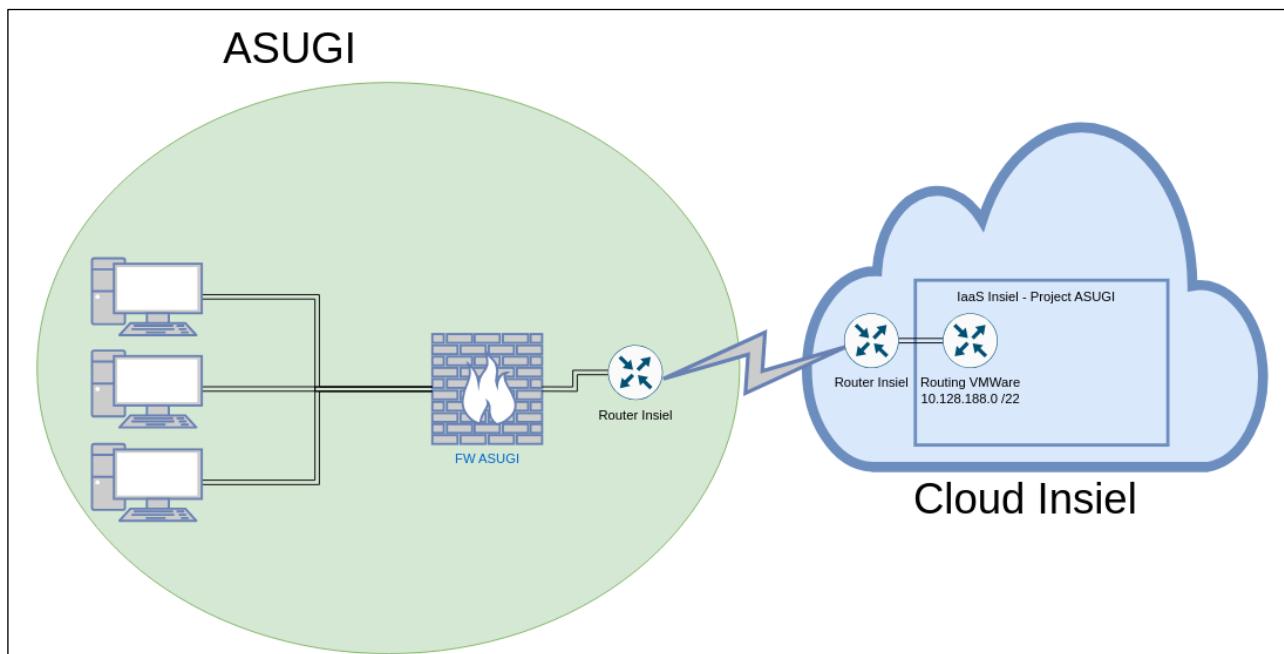


Figura 4 - Infrastruttura fisica cloud INSIEL

Dal punto di vista della sicurezza questo implica che il traffico da e per l'infrastruttura IaaS non viene filtrato in alcun modo da INSIEL.

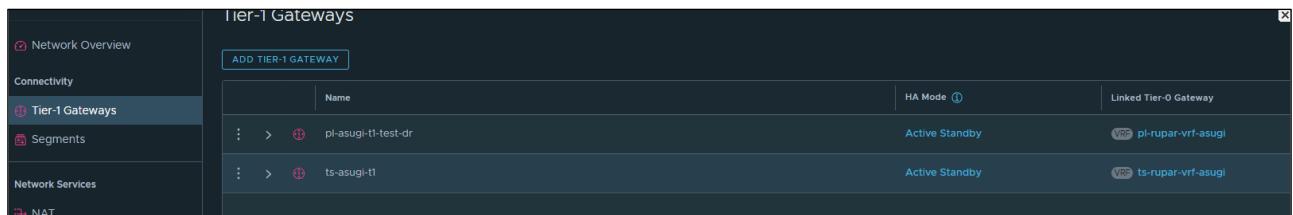
5.2.2.2. CONNETTIVITA' LOGICA

Dal punto di vista logico, il networking a livello IaaS viene gestito con NSX-T. INSIEL gestisce sia il livello 0 o Tier 0, che il livello 1 o Tier 1, delegando ad ASUGI parte delle regole di visibilità al livello Tier 1.

- Al livello Tier 0 esistono due gateway:
 - ts-rupar-vrf-asugi - Gateway primario, agganciato alla VRF ASUGI.

- pl-rupar-vrf-asugi - Gateway secondario, agganciato al sito di Disaster Recovery
- Al livello Tier 1 esistono due gateway:
 - ts-asugi-t1 - Gateway primario.
 - pl-asugi-t1-test-dr - Gateway per i test di Disaster Recovery.

La rete 10.128.188.0 /22 è stata assegnata ad un segmento, agganciato al gateway ts-asugi-t1 del Tier 1, agganciato a sua volta al gateway ts-rupar-vrf-asugi del Tier 0. In caso di disastro, il gateway gateway ts-asugi-t1 verrebbe spostato sul gateway pl-rupar-vrf-asugi del Tier 0, spostando l'operatività sul sito di DR.



The screenshot shows the 'Tier-1 Gateways' section of the NSX interface. On the left, there's a sidebar with 'Network Overview', 'Connectivity', 'Tier-1 Gateways' (which is selected), 'Segments', 'Network Services', and 'NAT'. The main area has a header 'Tier-1 Gateways' with a 'ADD TIER-1 GATEWAY' button. Below it is a table with two entries:

Name	HA Mode	Linked Tier-0 Gateway
pl-asugi-t1-test-dr	Active Standby	VRF pl-rupar-vrf-asugi
ts-asugi-t1	Active Standby	VRF ts-rupar-vrf-asugi

Figura 5 - Tier 1 gateways su NSX

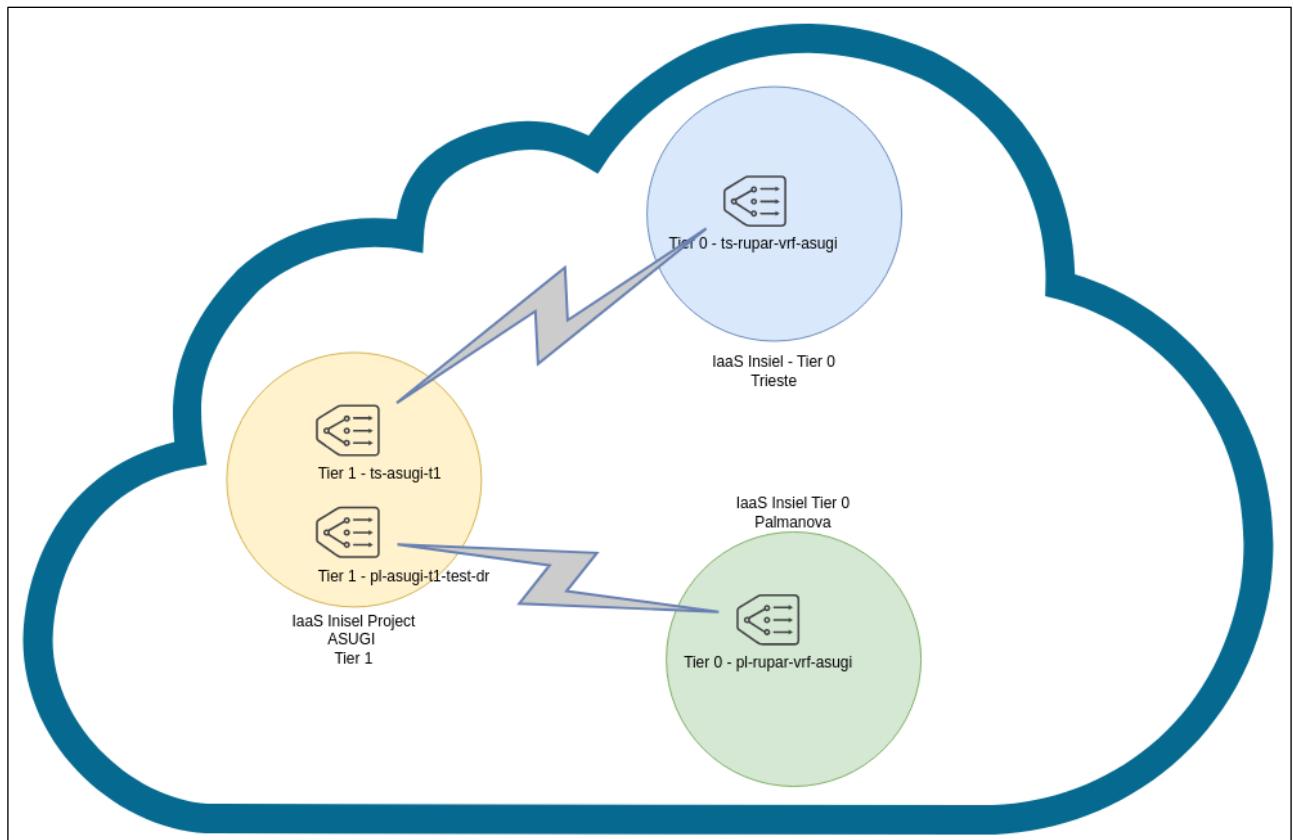


Figura 6 - Infrastruttura logica Cloud INSIEL

5.3. CLOUD INSIEL

5.3.1. ACCESSO AL CLOUD INSIEL

5.3.1.1. LOGIN

L'accesso al cloud INSIEL viene effettuato all'indirizzo:

<HTTPS://CLOUDSERVICE.INSIEL.IT/SAAS/AUTH/LOGIN>

NOTA BENE:

- Alcune funzionalità sono raggiungibili anche al di fuori della rete ASUGI o in assenza della VPN ASUGI; tuttavia, per un corretto funzionamento è sempre preferibile accedere da un terminale connesso alla rete ASUGI, o utilizzando la VPN ASUGI.

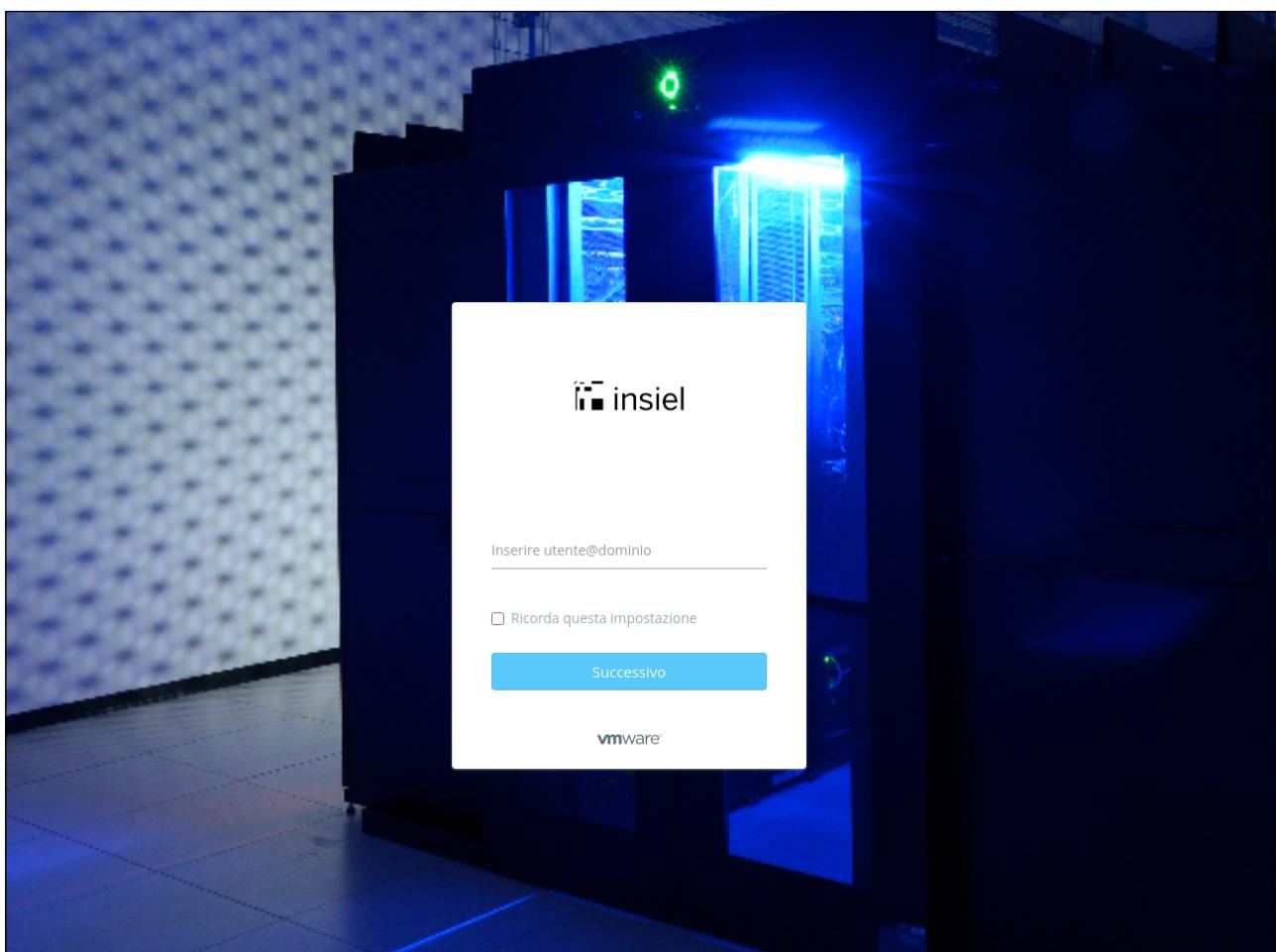


Figura 7 - Accesso al cloud INSIEL – Inserimento user name

L'autenticazione avviene inserendo in un primo momento lo user name, fornito da INSIEL, e su una schermata successiva la password:

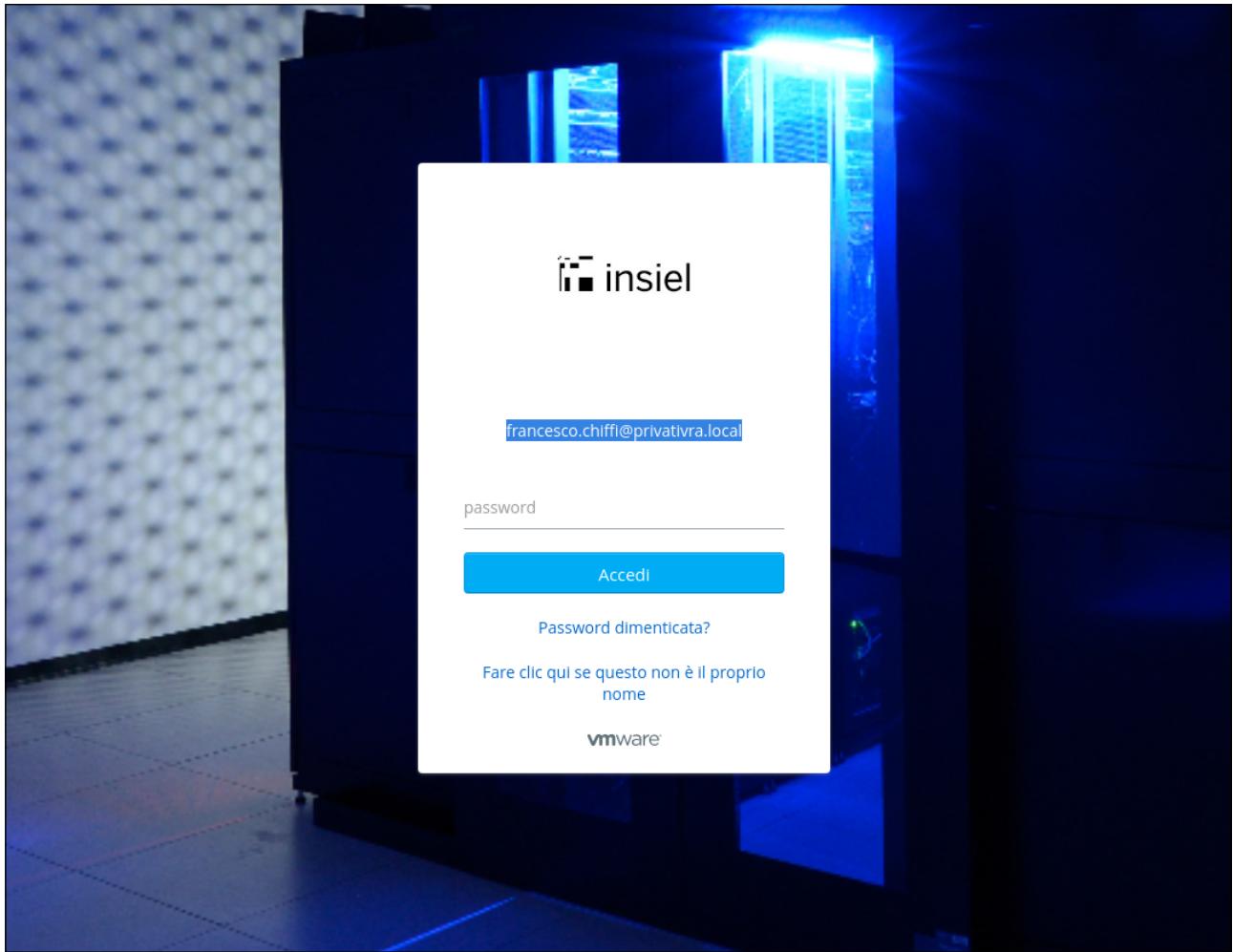


Figura 8 - Accesso al cloud INSIEL - Inserimento password

Si verrà portati così alla schermata principale:

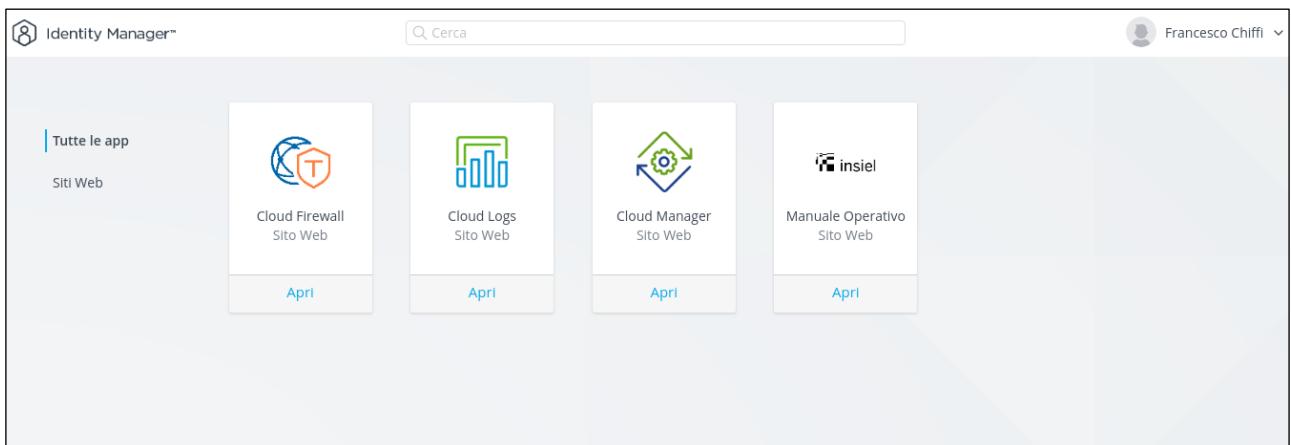


Figura 9 - Cloud INSIEL - Schermata principale

5.3.1.2. RESET PASSWORD

In caso di problemi di accesso è possibile procedere in autonomia al reset della password utilizzando il link:

<HTTPS://MGMT.INSIEL.IT/CP/VRA3KLL1W/SITEPAGES/CKVRAKKK1.ASPX?ENV=EMBEDDED>

Verrà richiesto preliminarmente l'inserimento delle credenziali INSIEL:

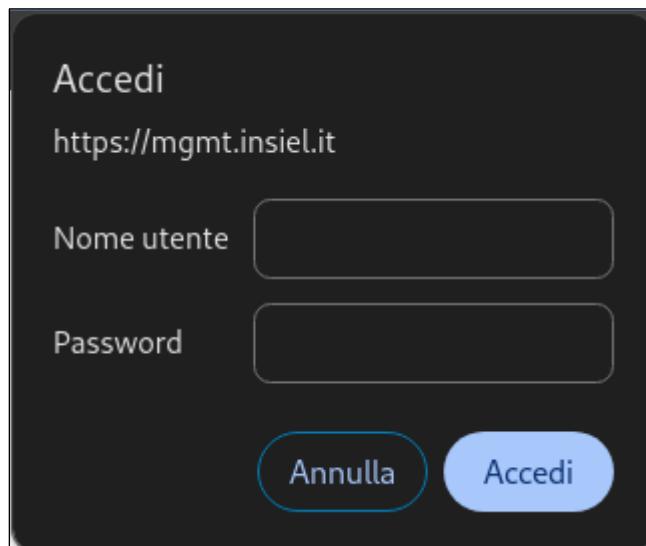
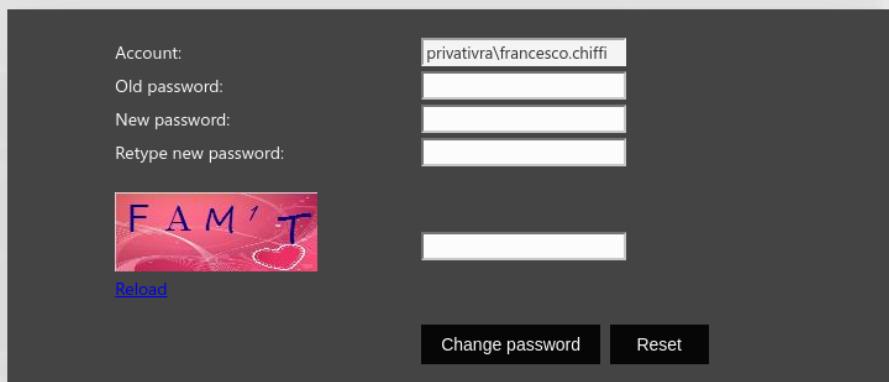


Figura 10 - Richiesta credenziali INSIEL

E successivamente si avrà accesso alla schermata che consente l'effettivo cambio password:

Insiel S.p.A. - Cambio password PRIVATIVRA



Requisiti della password

- lunghezza minima: 8 caratteri
- diversa dalle ultime 5 password utilizzate
- non deve contenere parte del nome, del cognome o dello username
- deve contenere almeno 3 delle seguenti categorie di caratteri:
 - caratteri maiuscoli
 - caratteri minuscoli
 - numeri
 - caratteri non alfanumerici
- scadenza password: 180 giorni

Figura 11 - Cambio password INSIEL

Ove sarà popolato il campo relativo all'account, e sarà necessario inserire:

- Vecchia password
- Nuova password
- Conferma nuova password
- Capthca

Rispettando i criteri elencati nella pagina.

5.3.1.3. PROBLEMI DI ACCESSO

È possibile che si verifichino problemi di accesso, in tal caso verificare di non trovarsi sulla seguente pagina di login:

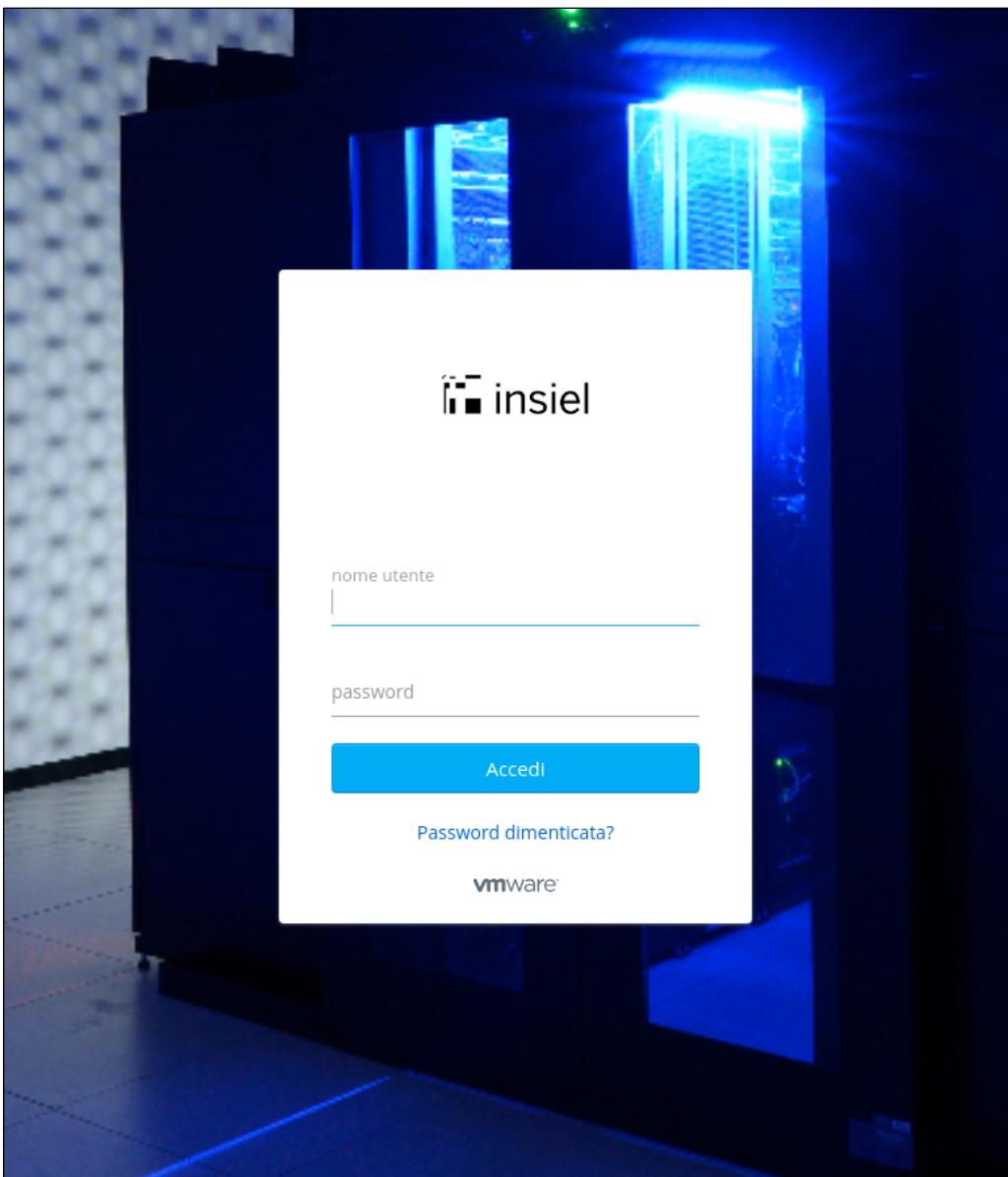


Figura 12 - Cloud INSIEL - Pagina di login errata

Si osservi che a differenza di quanto visto prima, in questa schermata l'inserimento di user name e password avviene in una singola pagina. Si avrà sempre e comunque errore di autenticazione. Verificare che l'indirizzo utilizzato non sia:

<HTTPS://CLOUDSERVICE.INSIEL.IT/SaaS/Auth/Login?Login>

ma quello mostrato nei paragrafi precedenti.

5.3.2. CARATTERISTICHE DEL CLOUD INSIEL

5.3.2.1. CLOUD MANAGER

5.3.2.1.1. ACCESSO AL CLOUD MANAGER

Selezionando ‘Cloud Manager’:

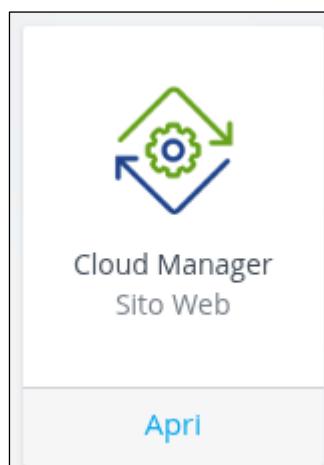
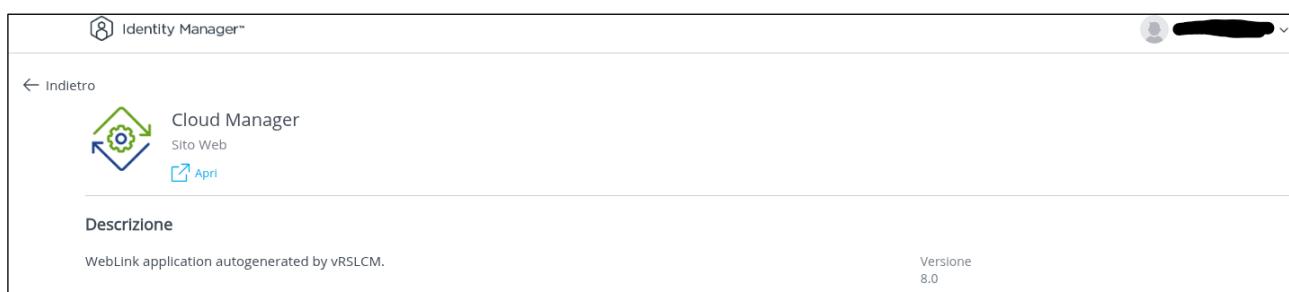


Figura 13 - Tasto 'Cloud Manager'

Si avrà accesso ad una schermata ulteriore:



The screenshot shows a web-based application titled "Identity Manager". In the left sidebar, there is a link labeled "Cloud Manager" with a sub-link "Sito Web" and an "Apri" (Open) button. Below the sidebar, there is a section titled "Descrizione" containing the text "WebLink application autogenerated by vRSCLM." and "Versione 8.0".

Figura 14 - Accesso a Cloud Firewall

Da qui cliccando sull’icona ‘Apri’:  si avrà finalmente accesso al ‘Cloud Service Broker’:

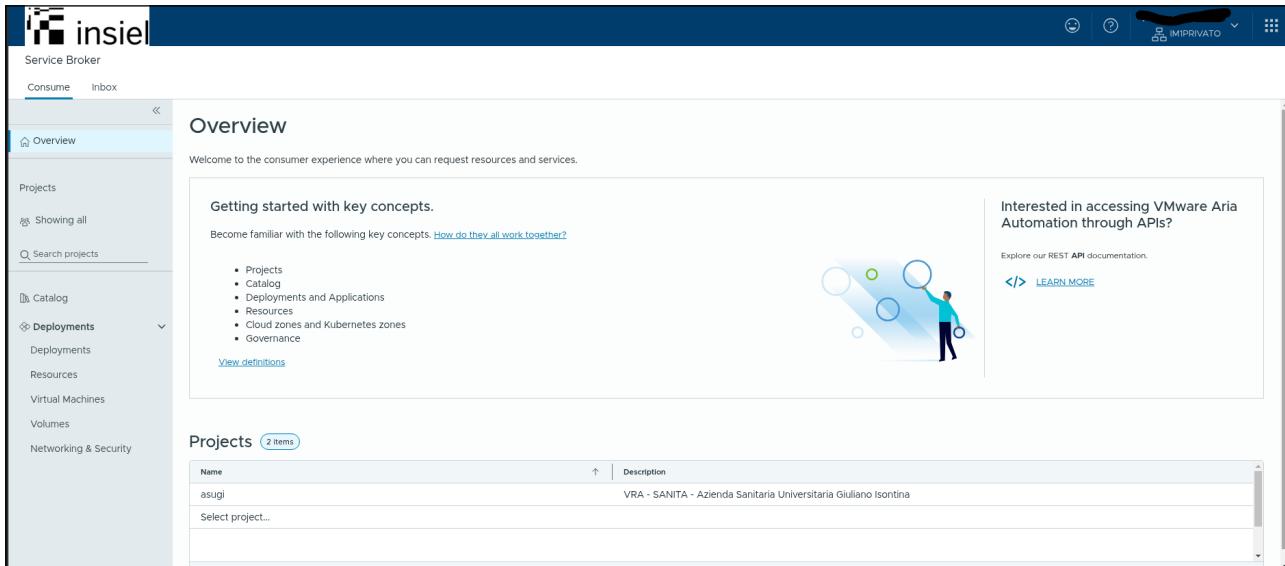


The screenshot shows a "My Services" page. There is a single item listed: "Service Broker" with an associated icon.

Figura 15 - Accesso a Service Broker

Cliccando sull’icona ‘Service broker’ si avrà accesso al dettaglio dell’interfaccia utente.

5.3.2.1.2. OVERVIEW



Name	Description
asugi	VRA - SANITA - Azienda Sanitaria Universitaria Giuliano Isontina

Figura 16 - Service Broker

La ‘Home page’ mostrerà la schermata ‘Overview’ con informazioni di carattere generale e l’elenco dei progetti disponibili per l’utente.

Il cloud INSIEL è strutturato secondo un modello multi tenant, di fatto ogni progetto viene associato ad un tenant che viene poi a coincidere con la specifica azienda sanitaria cui esso è dedicato.

Nella griglia ‘Projects’ sono visualizzati due campi:

- **Name:** nome del progetto.
- **Description:** descrizione del progetto.

Nello specifico è visualizzato un unico progetto dedicato all’ ‘Azienda Sanitaria Universitaria Giuliano Isontina’ (ASUGI).

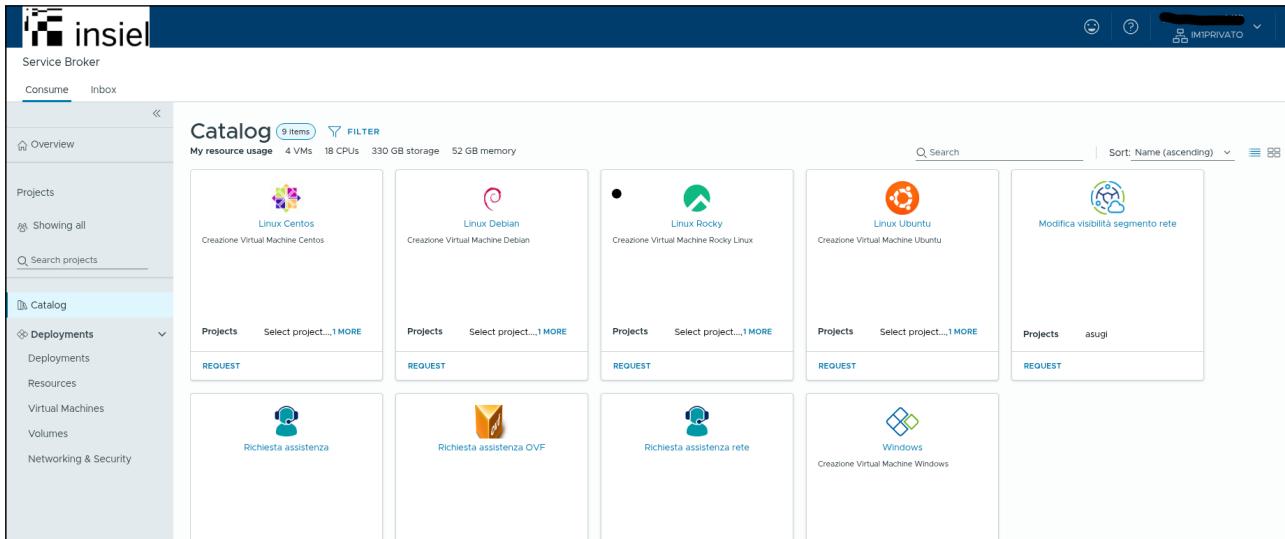
Saranno quindi come minimo presenti altri due progetti riservati a:

- ‘Azienda Sanitaria Universitaria Friuli Centrale’ (ASUFC)
- ‘Azienda Sanitaria Friuli Occidentale’ (ASFO)

Che tuttavia non sono ivi visibili.

Sulla barra sinistra sono visibili i link che danno accesso ad ulteriori funzionalità.

5.3.2.1.3. CATALOG



The screenshot shows the 'Catalog' section of the insiel Service Broker interface. On the left, a sidebar lists navigation options: Overview, Projects (Showing all), Search projects, Catalog (selected), Deployments (with a dropdown menu for Deployments, Resources, Virtual Machines, Volumes, Networking & Security), REQUEST, and asugi. The main area displays a grid of 10 items under the heading 'Catalog (9 items)'. The items are arranged in two rows of five. The first row includes: 'Linux Centos' (Icon: gear), 'Linux Debian' (Icon: person), 'Linux Rocky' (Icon: dot), 'Linux Ubuntu' (Icon: orange circle), and 'Modifica visibilità segmento rete' (Icon: globe). The second row includes: 'Richiesta assistenza' (Icon: headset), 'Richiesta assistenza OVF' (Icon: yellow cube), 'Richiesta assistenza rete' (Icon: headset), 'Windows' (Icon: blue diamond), and 'REQUEST' (Icon: question mark). At the top of the main area, there are filters for 'My resource usage' (4 VMs, 18 CPUs, 330 GB storage, 52 GB memory), a search bar, and a sort option ('Sort: Name (ascending)').

Figura 17 - Catalog

Selezionando ‘Catalog’ sulla sinistra si ha accesso al catalogo delle immagini di sistema operativo e dei servizi disponibili nel ‘Service Broker’.

Il campo ‘My resource usage’ al momento non fornisce informazioni affidabili.

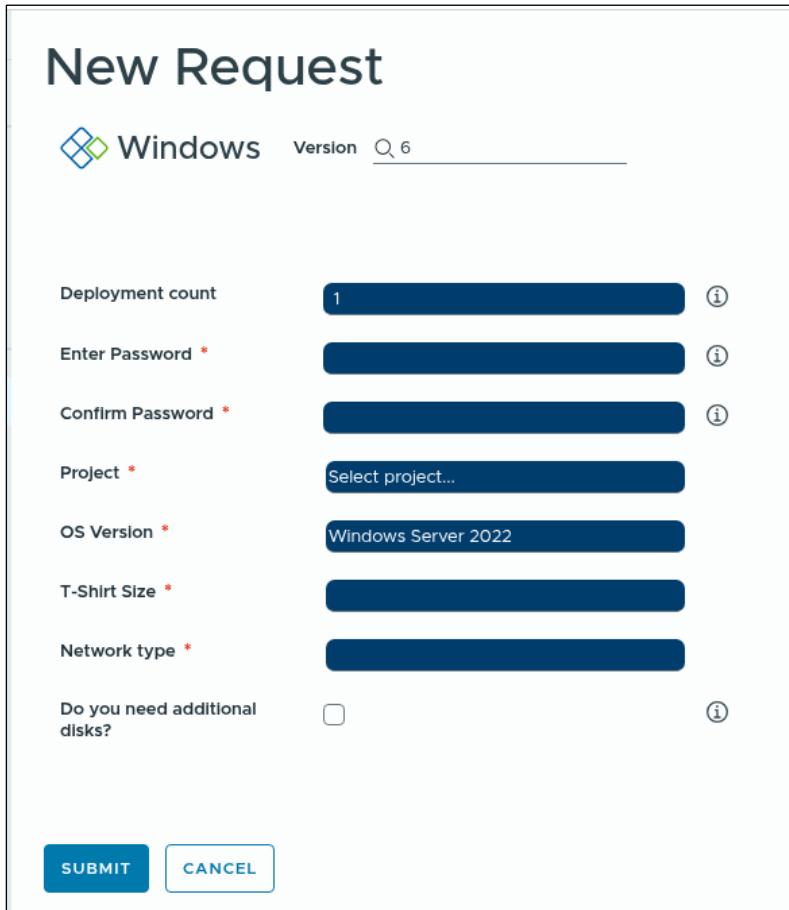
Le voci disponibili in ‘Catalog’ sono:

- **Linux Centos:** template per vm con sistema operativo Linux Centos.
- **Linux Debian:** template per vm con sistema operativo Linux Debian.
- **Linux Rocky:** template per vm con sistema operativo Linux Rocky.
- **Linux Ubuntu:** template per vm con sistema operativo Linux Ubuntu.
- **Modifica visibilità segmento rete:** funzionalità da non utilizzare di norma.
- **Richiesta assistenza:** generazione ticket per richiesta assistenza generica ad INSIEL.
- **Richiesta assistenza OVF:** generazione ticket per richiesta assistenza su OVF ad INSIEL.
- **Richiesta assistenza rete:** generazione ticket per richiesta assistenza su rete ad INSIEL.
- **Windows:** template per vm con sistema operativo Microsoft Windows.

In alcuni casi, ad esempio per Linux Ubuntu, è possibile selezionare successivamente anche la versione del sistema operativo desiderato.

5.3.2.1.3.1.CREAZIONE DI UNA NUOVA VM

Cliccando su un template relativo ad un sistema operativo, sarà possibile procedere alla creazione di una nuova macchina virtuale dalla seguente schermata:



New Request

Windows Version 6

Deployment count: 1

Enter Password *

Confirm Password *

Project * Select project...

OS Version * Windows Server 2022

T-Shirt Size *

Network type *

Do you need additional disks?

SUBMIT CANCEL

Figura 18 – New request

È stata richiesta la creazione di una VM con le seguenti caratteristiche:

- Sistema operativo: Microsoft Windows Server
- Core: 2
- RAM: 8 GB
- HD: 100 GB

Esaminiamo i singoli campi mostrati, i campi con * sono obbligatori:

- **Deployment count:** popolato automaticamente.
- **Enter Password:** la password di root da assegnare alla nuova virtual machine, tipicamente si inserisce: 'P@ssw0rd'.

- **Confirm Password:** conferma la password inserita nel campo precedente.
- **Project:** potrà assumere solo il valore ‘asugi’.
- **OS Version:** versione del sistema operativo, in tal caso: ‘Windows Server 2022’.
- **T-Shirt Size:** per ‘T-Shirt Size’ si intende la combinazione di numero di core e quantità di RAM da attribuire alla VM. La scelta disponibile è molto ampia, tuttavia nel caso in cui non ci dovesse essere il ‘taglio’ desiderato è possibile farlo inserire aprendo un ticket ad INSIEL con il link visto in precedenza.

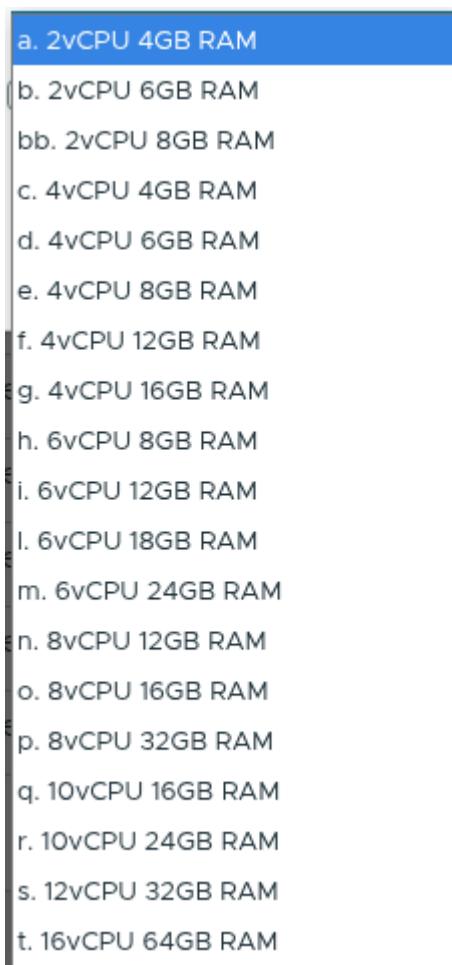
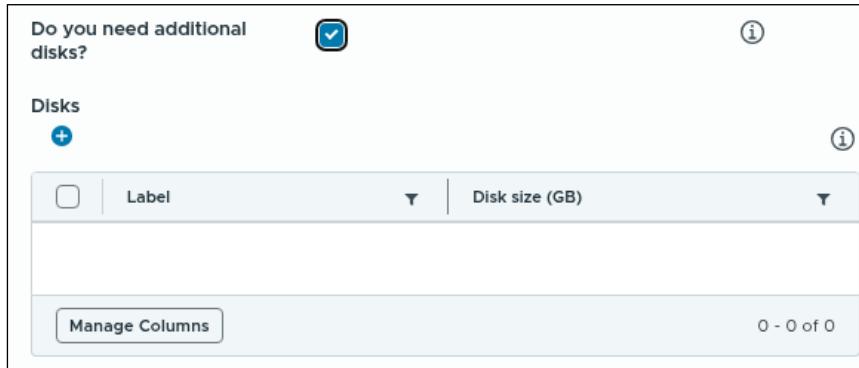


Figura 19 – T-Shirt Size

- **Network type:** verrà popolato automaticamente alla sezione del progetto.
- **Do you need additional disk:** da utilizzare nel caso in cui si vogliano aggiungere alla VM dischi suppllettivi. Selezionando si aprirà una ulteriore griglia per l'inserimento dei dischi suppllettivi.



<input type="checkbox"/>	Label	Disk size (GB)	
		0	

Figura 20 – Dischi aggiuntivi

In tal caso non aggiungeremo alcun disco.

A termine compilazione vedremo quanto segue:

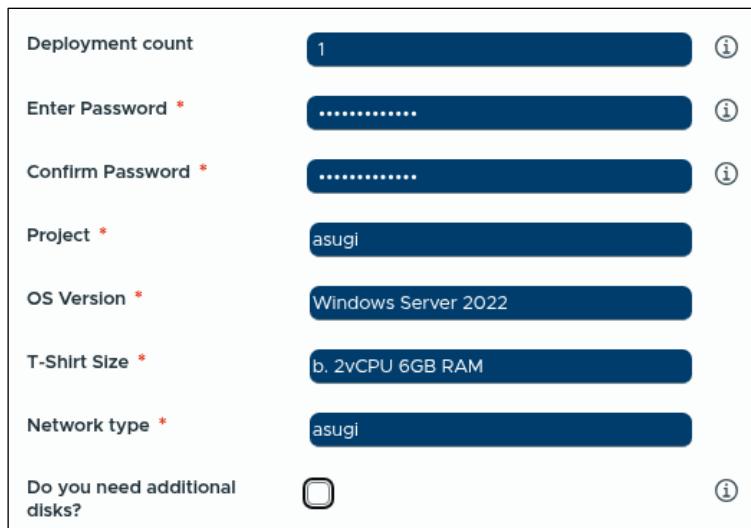


Figura 21 – New request compilata

Al di sotto di questa griglia è di estremo interesse una ulteriore griglia che riporta il totale delle risorse computazionali disponibili ed utilizzate:

RESOURCE CLOUD ZONE	
Project CPU *	82 vCpu / 100 vCpu -> Free: 18 vCpu
Project RAM *	243712 MB / 262144 MB -> Free: 18432 MB
Project DISK *	3870 GB / 20000 GB -> Free: 16130 GB

Figura 22 – Risorse computazionali

Infine, cliccando sul tasto **SUBMIT** sarà possibile procedere alla creazione di una nuova VM.

5.3.2.1.4. DEPLOYMENTS

Il nodo ‘Deployments’ da accesso ad una serie ulteriori sotto nodi che consentono di verificare la situazione attuale del cloud INSIEL e le operazioni in atto al momento:

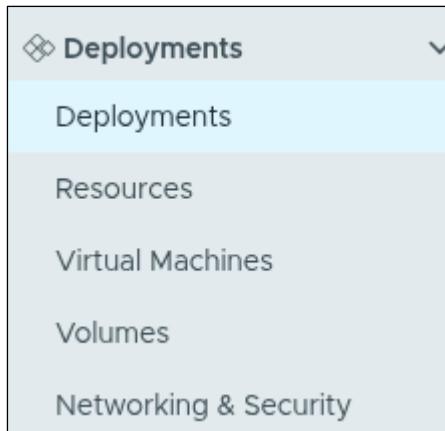


Figura 23 – Deployments menu

Dettagliamo di seguito il funzionamento delle singole voci di menu.

5.3.2.1.4.1. DEPLOYMENTS

La griglia ‘Deployments’ fornisce informazione sulle attività in atto, ad esempio la creazione di una nuova VM:

Deployments 20 items							
	Name	Owner	Project	Status	Expires on	Created on	
:>	Windows / 6 - 27fb0clb-3428-4046-8bb5-e5cf6736bfee	francesco.chiffi@privativra.local	asugi	1 CANCEL	Never	a few seconds ago	
:>	deployment_ddeef9bf5-4b6f-45de-b2b6-0a05fbfa07c	borut.jarc@privativra.local	asugi		Never	a month ago	
:>	QI0006	borut.jarc@privativra.local	asugi		Never	a month ago	
:>	QI0013	francesco.chiffi@privativra.local	asugi		Never	2 months ago	
:>	QI0015	francesco.chiffi@privativra.local	asugi		Never	2 months ago	
:>	QI0014	francesco.chiffi@privativra.local	asugi		Never	2 months ago	

Figura 24 – Deployments

I campi presenti nella griglia sono:

- **Name:** il nome del deployment.
- **Owner:** l’utente che ha creato la VM.
- **Project:** sempre pari ad ASUGI.
- **Status:** il livello di avanzamento del deployment.
- **Expires on:** la durata della VM, di default pari a Never.

- **Created on:** data creazione VM.

Cliccando sul numero presente nel campo ‘Status’ è possibile vedere il dettaglio dell’operazione in atto:

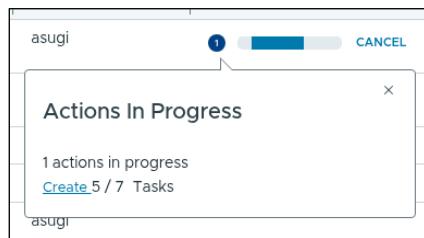


Figura 25 – Deployment – Status

Cliccando sulle due frecce a sinistra: ➤ , si aprirà una finestra con i dettagli del deployment:

Resource Name	Address	Status	Resource Type
cSasugi33	10.128.188.18	►On	Cloud.vSphere.Machine
asugi			Cloud.vSphere.Network

Figura 26 – Deployment – Dettagli

Cliccando sui tre puntini a sinistra: ⋮ si aprirà un menu contestuale che consente di effettuare alcune operazioni:

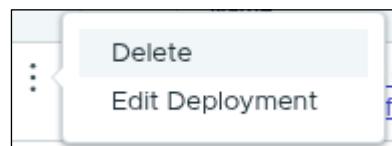


Figura 27 – Deployment – Menu contestuale

- Delete: cancellazione dell’operazione.

- Edit: modifica del nome del deployment ed aggiunta di note.

Edit Deployment

Name *

Description

Icon



Upload icon Select icon from catalog icon list

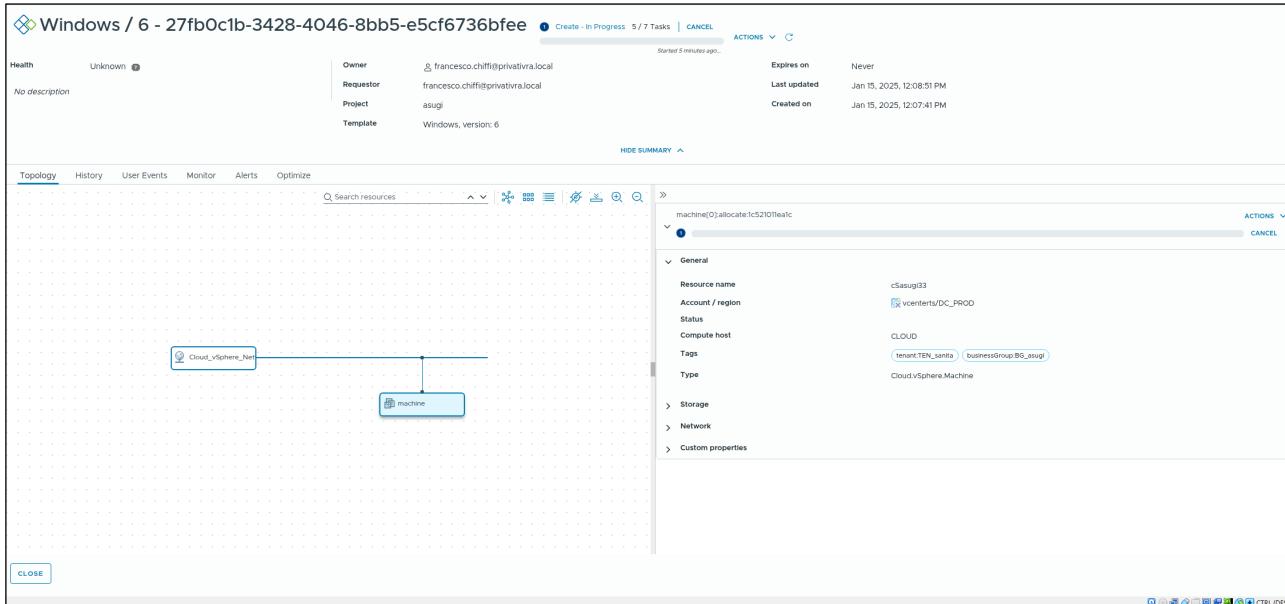
CANCEL SUBMIT

Figura 28 – Deployment – Edit

NOTA BENE:

- Le VM seguono una nomenclatura del tipo 0I00XX, pertanto sarà necessario individuare il valore più elevato già utilizzato e rinominare la VM con un valore incrementato di 1. Per maggiori dettagli consultare l'[APPENDICE 2 – NAMING CONVENTION](#)

Cliccando sul nome della VM si avrà accesso ad una schermata di dettaglio.

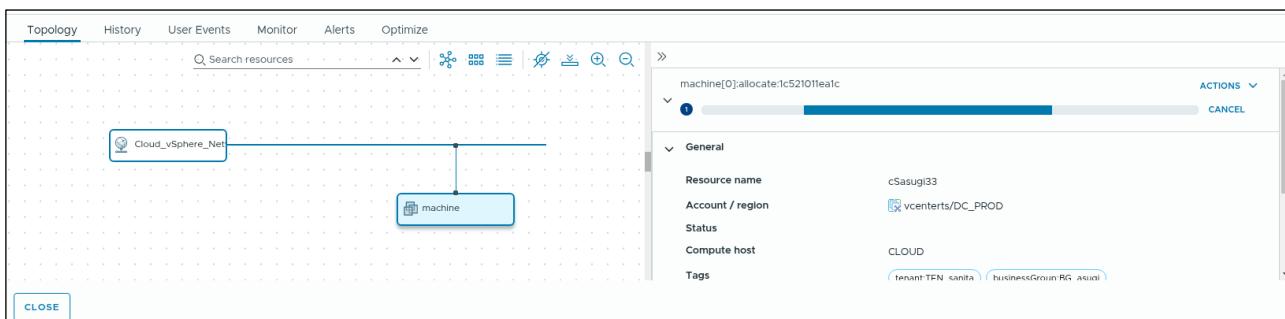


The screenshot shows the deployment details for a Windows VM named "Windows / 6 - 27fb0c1b-3428-4046-8bb5-e5cf6736bfee". The top bar indicates the task is "Create - In Progress" with 5/7 tasks completed. The right side shows the VM's status: Started 6 minutes ago, Expires on Never, Last updated Jan 15, 2025, 12:08:51 PM, Created on Jan 15, 2025, 12:07:41 PM. Below this is a "Topology" section showing a network diagram with nodes "Cloud_vSphere_Net" and "machine". The "General" tab on the right provides detailed information about the VM, including its resource name (cSasugi33), account/region (vcenterftrs/DC_PROD), status (CLOUD), compute host (Cloud), and tags (tenant:TEN_sanita, businessGroup:BG_asugi).

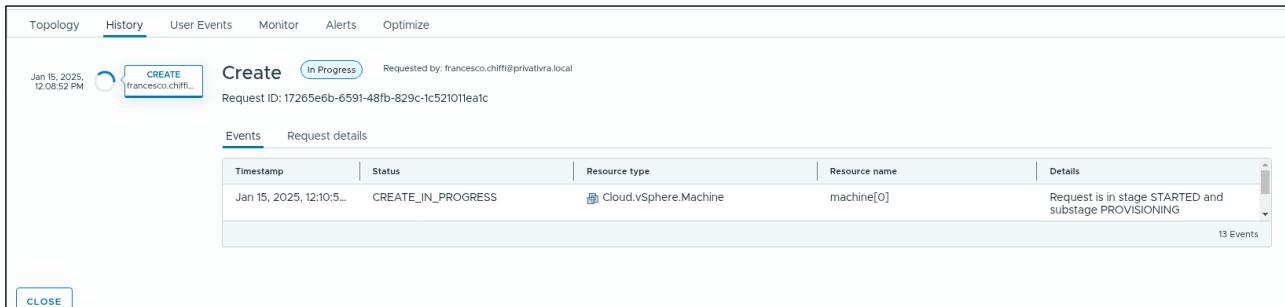
Figura 29 – Deployment – Dettaglio

Nella parte bassa della schermata sono presenti sei tab che consentono di accedere a svariate informazioni:

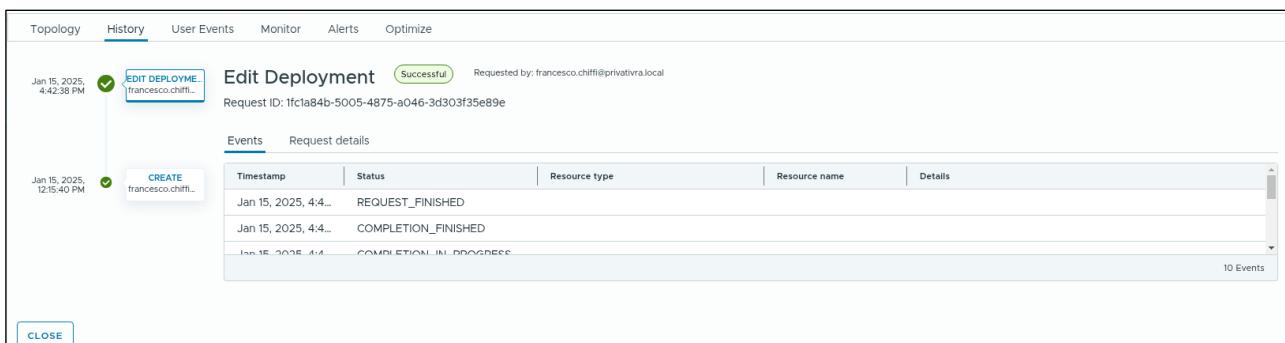
- **Topology:** topologia di rete della VM.
- **History:** elenco delle attività di deploy.
- **User Events:** elenco delle richieste dell'utente.
- **Monitor:** stato di utilizzo delle risorse della VM, popolata solo dopo il completamento del deployment della VM stessa.
- **Alerts:** eventuali allarmi.
- **Optimize:** suggerimenti di ottimizzazione, popolata solo dopo il completamento del deployment della VM stessa.



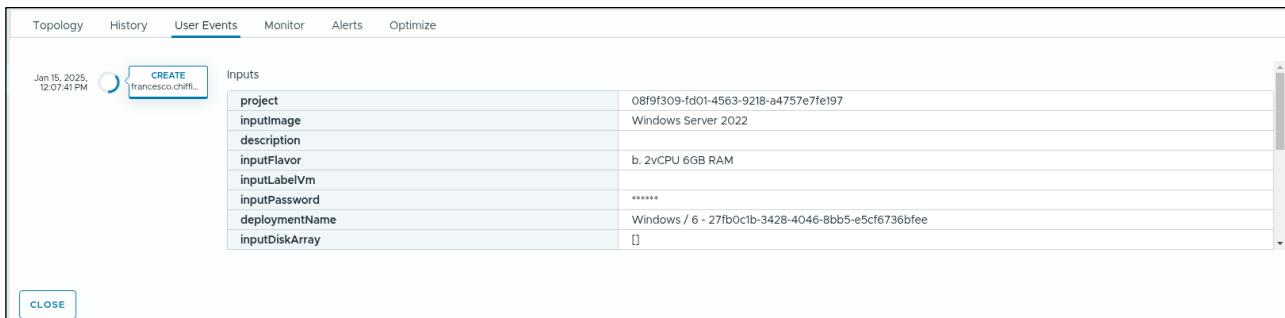
This screenshot shows the deployment details for a Windows VM named "Windows / 6 - 27fb0c1b-3428-4046-8bb5-e5cf6736bfee". The interface is identical to Figure 29, displaying the topology and general configuration of the VM.


Figura 30 – Deployment – Dettaglio - Topology


The screenshot shows the 'Topology' tab selected in the navigation bar. A deployment request for a machine named 'machine[0]' is shown in progress, requested by 'francesco.chiffi@privativra.local'. The request ID is 17265e6b-6591-48fb-829c-1c52101fea1c. The status is 'CREATE' and it is currently 'In Progress'. Below the main message, there is a table titled 'Events' showing a single entry: 'Jan 15, 2025, 12:10:5... CREATE_IN_PROGRESS'. The table has columns for 'Timestamp', 'Status', 'Resource type', 'Resource name', and 'Details'. The 'Details' column indicates that the request is in stage 'STARTED' and substage 'PROVISIONING'. A 'CLOSE' button is visible at the bottom left.

Figura 31 – Deployment – Dettaglio – History (Durante la creazione della VM)


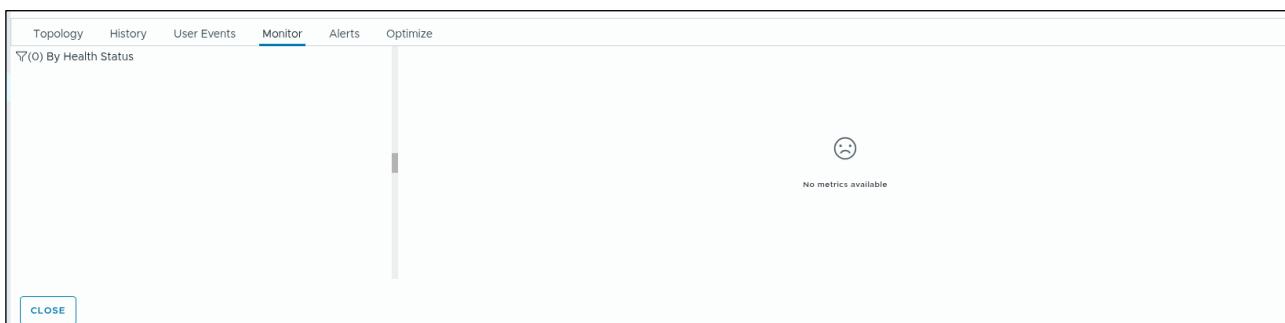
The screenshot shows the 'History' tab selected in the navigation bar. A deployment named 'francesco.chiffi...' was successfully edited, indicated by a green checkmark and the text 'EDIT DEPLOYMENT francesco.chiffi... Successful'. The request ID is 1fc1a84b-5005-4875-a046-3d303f35e89e. Below the main message, there is a table titled 'Events' showing three entries: 'REQUEST_FINISHED', 'COMPLETION_FINISHED', and 'COMPLETION_IN_PROGRESS'. The table has columns for 'Timestamp', 'Status', 'Resource type', 'Resource name', and 'Details'. A 'CLOSE' button is visible at the bottom left.

Figura 32 – Deployment – Dettaglio – History (Dopo la creazione della VM)


The screenshot shows the 'User Events' tab selected in the navigation bar. A deployment request is being processed, indicated by a blue 'CREATE' button and the text 'francesco.chiffi...'. The deployment inputs are listed in a table under the 'Inputs' section:

Input	Value
project	08f9f309-fd01-4563-9218-a4757e7fe197
inputImage	Windows Server 2022
description	
inputFlavor	b. 2vCPU 6GB RAM
inputLabelVm	
inputPassword	*****
deploymentName	Windows / 6 - 27fb0c1b-3428-4046-8bb5-e5cf6736bfee
inputDiskArray	[]

A 'CLOSE' button is visible at the bottom left.

Figura 33 – Deployment – Dettaglio – User Events


The screenshot shows the 'Monitor' tab selected in the navigation bar. A deployment status message 'VM(0) By Health Status' is displayed. The monitor interface shows a single row with a sad face icon and the text 'No metrics available'. A 'CLOSE' button is visible at the bottom left.

Figura 34 – Deployment – Monitor (Durante la creazione della VM)

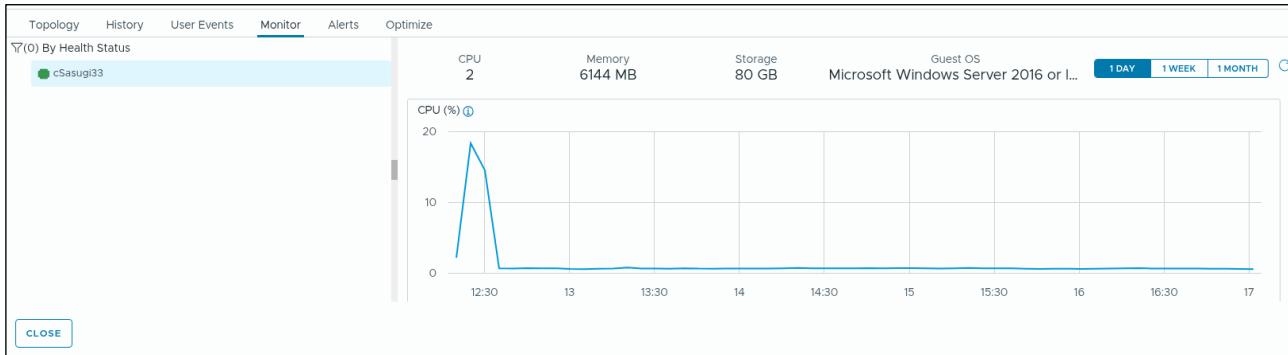


Figura 35 – Deployment – Monitor (Dopo la creazione della VM)

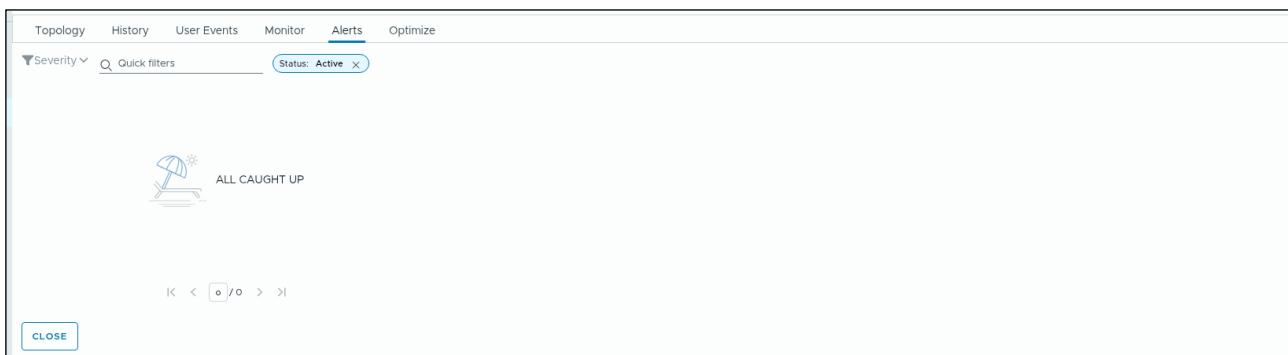


Figura 36 – Deployment – Alerts

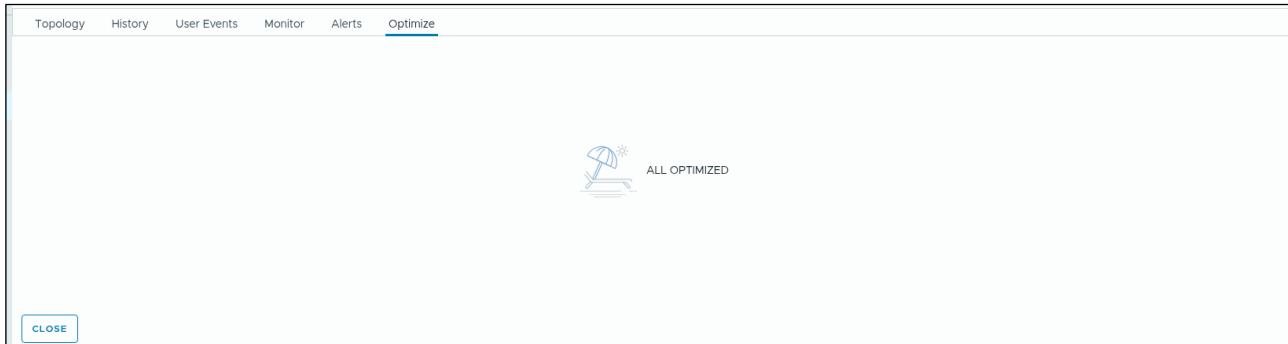


Figura 37 – Deployment – Optimize (Durante la creazione della VM)



Figura 38 – Deployment – Optimize (Dopo la creazione della VM)

NOTA BENE:

- Non è necessario tenere conto delle indicazioni di 'Optimize'.



5.3.2.1.4.2.RESOURCES

La griglia ‘Resources’ mostra le risorse computazionali attualmente impiegate, ed eventuali attività di deployment delle stesse:

Resources								
	Name	Resource Type	Deployment	Account / Region	Project	Origin	Tags	Created On
...	cSasugi33	Cloud.vSphere.Machine	Windows / 6 - 27fb0cb-3428-4046-8bb5-e5cf6736bf6e CANCEL	vcenter / DC_PROD	asugi		tenant:TEN_sanita businessGroup:BG_asugi	a minute ago
...	asugi	Cloud.vSphere.Network	Windows / 6 - 27fb0cb-3428-4046-8bb5-e5cf6736bf6e CANCEL	vcenter / DC_PROD	asugi			2 minutes ago

Figura 39 – Resources - Deployment

Anche in questo caso cliccando sul numero nel campo ‘Name’ è possibile visualizzare il dettaglio dell’attività in corso

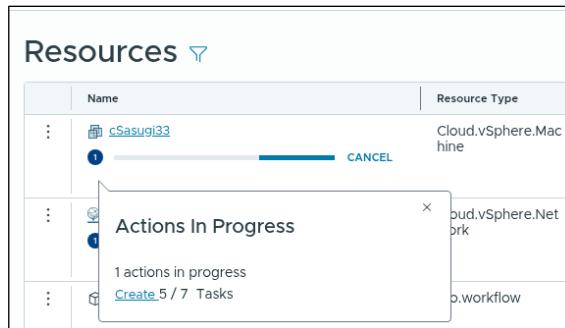


Figura 40 – Resources – Deployment - Dettagli

Resources								
	Name	Resource Type	Deployment	Account / Region	Project	Origin	Tags	Created On
...	CD/DVD drive 1	Cloud.vSphere.Disk		vcenter / Datacenter:datacenter-3	asugi			5 hours ago
...	cSasugi33	Cloud.vSphere.Machine	010016	vcenter / DC_PROD	asugi		tenant:TEN_sanita businessGroup:BG_asugi	5 hours ago
...	cSasugi33-boot-disk	Cloud.vSphere.Disk		vcenter / Datacenter:datacenter-3	asugi			5 hours ago
...	asugi	Cloud.vSphere.Network	010016	vcenter / DC_PROD	asugi			5 hours ago
...	Richiesta assistenza rete	vro.workflow	deployment_d3ee9b75-4b6f-45de-b2b6-0a05fbab07c	N/A	asugi			a month ago
...	asugi	Cloud.NSX.Network	010006	nsx / global	asugi		segment:asugi	a month ago
...	cSasugi08	Cloud.vSphere.Machine	010005	vcenter / DC_PROD	asugi		businessGroup:BG_asugi tenant:TEN_sanita	a month ago
...	CD/DVD drive 1	Cloud.vSphere.Disk		vcenter / Datacenter:datacenter-3	asugi			2 months ago

Figura 41 – Resources – Tutte le risorse

La griglia riporta i seguenti campi:

- **Name:** nome della risorsa.
- **Resource Type:** tipo di risorsa.

- **Deployment:** deployment cui è legata la risorsa.
- **Account/Region:** area del data center in cui è allocata la risorsa.
- **Project:** sempre pari ad ‘asugi’.
- **Origin:** origine delle richiesta che ha dato luogo all’istanziamento della risorsa.
- **Tag:** eventuali tag della risorsa, tipicamente popolato solo per le VM con i valori:
 - tenant: TEN_sanita
 - businessGroup: BG_asugi
- **Created on:** data creazione della risorsa.

È inoltre possibile filtrare le risorse per tipologia:

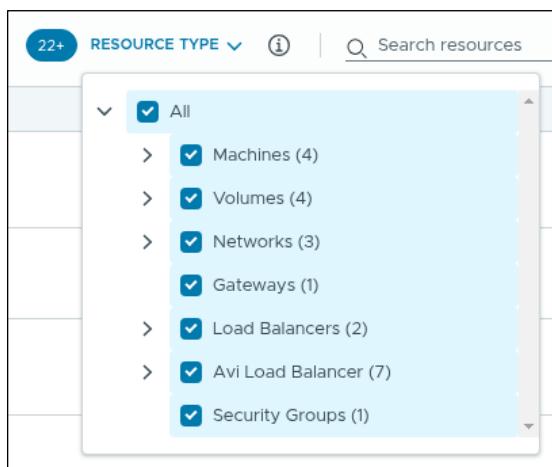


Figura 42 – Resources – Filtro risorse

Cliccando sui tre puntini a sinistra : si avrà accesso ad un menu contestuale:



Figura 43 – Resources – Menu contestuale

5.3.2.1.4.3. VIRTUAL MACHINES

La griglia ‘Virtual machines’ è una delle più rilevanti per la gestione delle VM del cloud INSIEL. In fase di creazione della VM sarà possibile verificare lo stato di avanzamento dell’operazione:

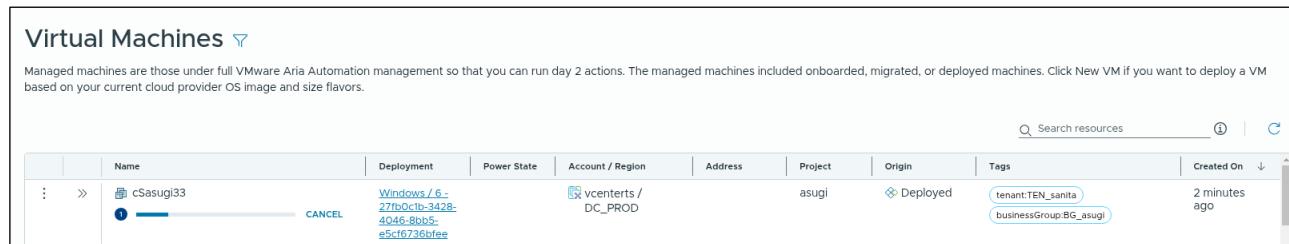


Figura 44 – Virtual Machines – Creazione nuova VM

Cliccando sul numero nel campo name sarà anche possibile verificare il dettaglio dell’attività:

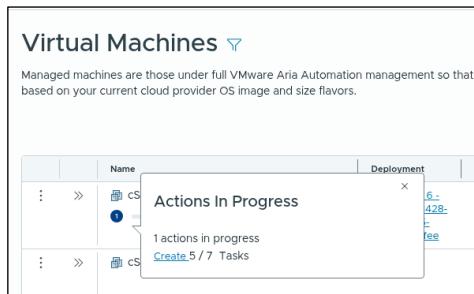


Figura 45 – Virtual Machines – Creazione nuova VM – Dettagli

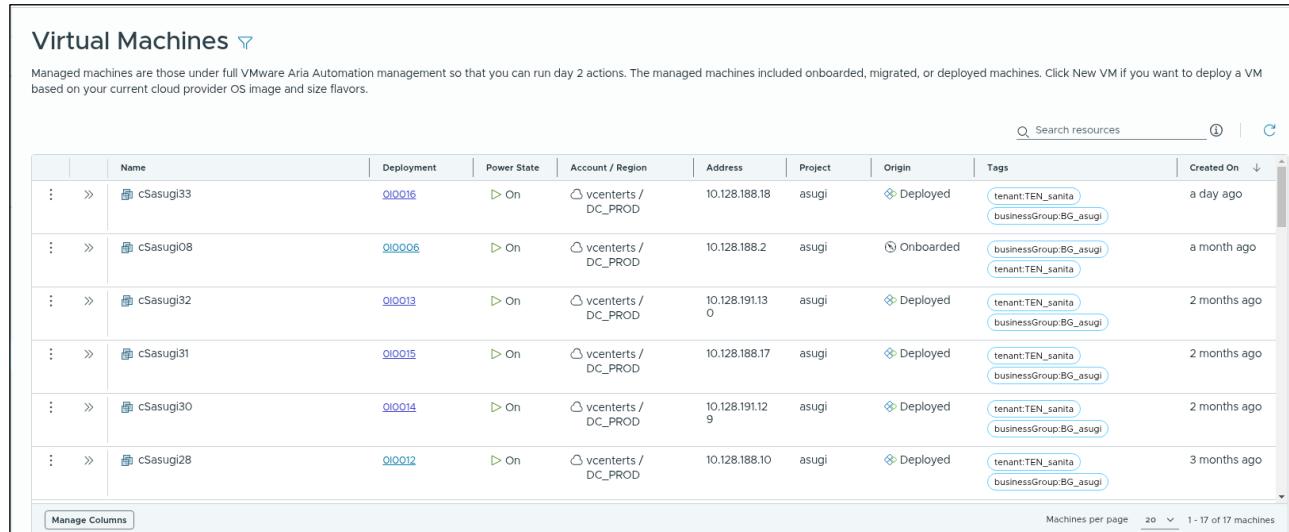


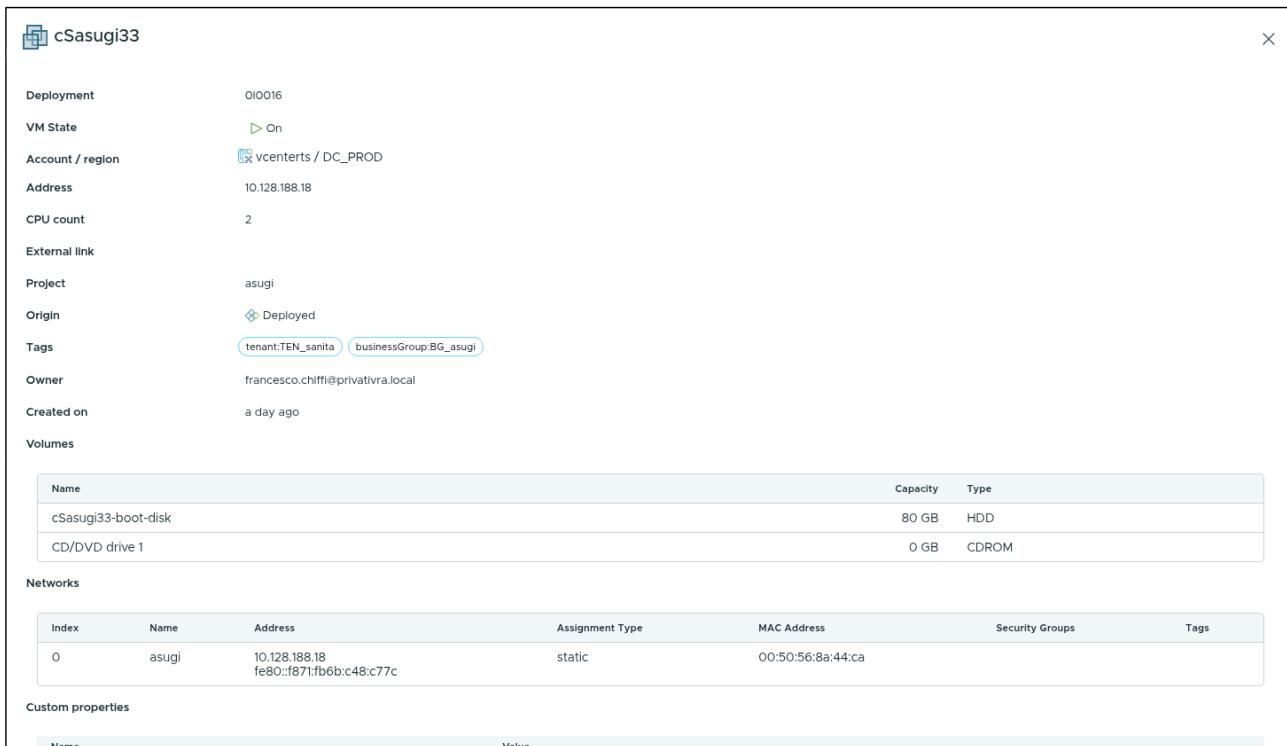
Figura 46 – Virtual Machines – Elenco VM

I campi riportati sulla griglia sono:

- **Name:** il nome della VM assegnato direttamente dall’infrastruttura.
- **Deployment:** il nome del deployment, come modificato nel [PAR 5.2.2.1.4.1](#) che dovrà coincidere con il nome host della VM.

- **Power state:** VM accesa o spenta.
- **Account/Region:** area del data center in cui è allocata la risorsa.
- **Address:** indirizzo IP della VM. Per maggiori dettagli sull'indirizzamento consultare l'[APPENDICE 1 – CRITERI DI ASSEGNAZIONE DEGLI INDIRIZZI IP](#).
- **Project:** sempre pari ad ‘asugi’.
- **Origin:** modalità di creazione della VM.
- **Tags:** i tag assegnati di default alla VM:
 - tenant: TEN_sanita
 - businessGroup: BG_asugi
- **Created on:** data creazione della risorsa.

Cliccando sul tasto  sulla sinistra, si avrà accesso ad una finestra di dettaglio della VM:



The screenshot shows the detailed configuration of a VM named 'cSasugi33'. Key details include:

- Deployment:** 010016
- VM State:** On
- Account / region:** vcenter1 / DC_PROD
- Address:** 10.128.188.18
- CPU count:** 2
- External link:** asugi
- Project:** asugi
- Origin:** Deployed
- Tags:** tenant:TEN_sanita, businessGroup:BG_asugi
- Owner:** francesco.chiffi@privativra.local
- Created on:** a day ago
- Volumes:**

Name	Capacity	Type
cSasugi33-boot-disk	80 GB	HDD
CD/DVD drive 1	0 GB	CDROM
- Networks:**

Index	Name	Address	Assignment Type	MAC Address	Security Groups	Tags
0	asugi	10.128.188.18 fe80::f871:fb6b:c48:c77c	static	00:50:56:8a:44:ca		
- Custom properties:**

Name	Value

Figura 47 – Virtual Machines – Dettaglio VM

Vengono ivi riportate varie informazioni di dettaglio sulla VM, tra cui:

- Numero di core.
- Indirizzo IP

- Dimensione disco rigido.
- Ecc.

Cliccando invece sui tre puntini sulla sinistra:  si accede al menu contestuale relativo alla VM che permette di eseguire una serie di operazioni:

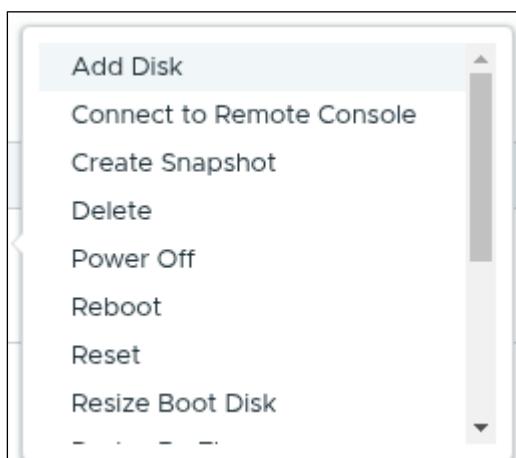


Figura 48 – Virtual Machines – Menu contestuale #1

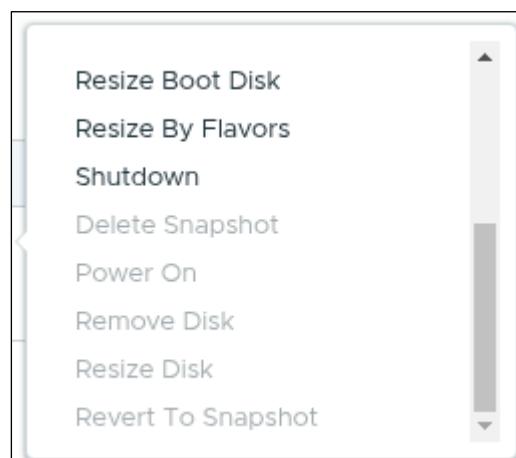


Figura 49 – Virtual Machines – Menu contestuale #2

NOTA BENE:

- Le attività disabilitate sul menu, in generale sono utilizzabili solamente con la VM spenta.
- È preferibile, tuttavia, spegnere la VM anche per attività consentite con la VM accesa che riguardino la modifica delle risorse computazionali, l'aggiunta e/o il ridimensionamento dei dischi; ciò per evitare eventuali problematiche al sistema operativo.

Utilizzando tali funzionalità procederemo a modificare la VM come richiesto.

Prima di procedere con ogni operazione è necessario spegnere la VM con l'apposito comando 'Shutdown'.

La VM prima creata ha un unico disco, creato per default con dimensioni 80 GB, è stato richiesto che venga portato a 100 GB. Pertanto, si procede con il comando 'Resize Boot Disk' per portarlo da 80 a 100 GB.

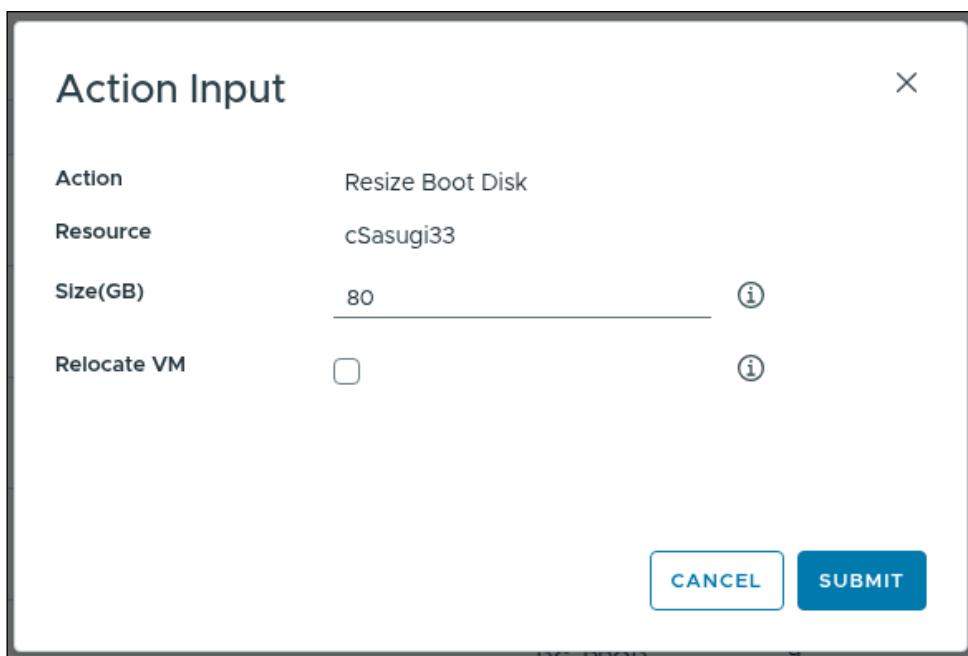


Figura 50 – Virtual Machines – Resize Boot Disk

L'operazione richiederà un po' di tempo.

NOTA BENE:

- L'espansione del disco non comporta automaticamente l'espansione del file system ivi contenuto, operazione che andrà pertanto effettuata da sistema operativo.

A termine operazione è possibile riavviare la VM.

Sempre attraverso il medesimo menu è possibile accedere alla VM con il comando 'Connect to Remote Console' per verificarne il corretto funzionamento.



5.3.2.1.4.4.VOLUMES

La griglia ‘Volumes’ mostra i dischi attualmente impiegati, ed eventuali attività di deployment in corso:

Volumes										
	Name	Deployment	Account / Region	Status	Capacity (GB)	Project	Origin	Tags	Created On	Actions
⋮	CD/DVD drive 1		vcnerts / Datacenter:datacenter-3	ATTACHED	0	asugi	Deployed		5 days ago	⋮
⋮	cSasugi33-boot-disk		vcnerts / Datacenter:datacenter-3	ATTACHED	100	asugi	Deployed		5 days ago	⋮
⋮	CD/DVD drive 1		vcnerts / Datacenter:datacenter-3	ATTACHED	0	asugi	Deployed		2 months ago	⋮
⋮	cSasugi32-boot-disk		vcnerts / Datacenter:datacenter-3	ATTACHED	30	asugi	Deployed		2 months ago	⋮
⋮	CD/DVD drive 1		vcnerts / Datacenter:datacenter-3	ATTACHED	0	asugi	Deployed		2 months ago	⋮
⋮	cSasugi31-boot-disk		vcnerts / Datacenter:datacenter-3	ATTACHED	100	asugi	Deployed		2 months ago	⋮
⋮	CD/DVD drive 1		vcnerts / Datacenter:datacenter-3	ATTACHED	0	asugi	Deployed		2 months ago	⋮
⋮	cSasugi30-boot-disk		vcnerts / Datacenter:datacenter-3	ATTACHED	100	asugi	Deployed		2 months ago	⋮
⋮	CD/DVD drive 1		vcnerts / Datacenter:datacenter-3	ATTACHED	0	asugi	Deployed		3 months ago	⋮
⋮	cSasugi28-boot-disk		vcnerts / Datacenter:datacenter-3	ATTACHED	80	asugi	Deployed		3 months ago	⋮
⋮	CD/DVD drive 1		vcnerts / Datacenter:datacenter-3	ATTACHED	0	asugi	Deployed		3 months ago	⋮
⋮	cSasugi27-boot-disk		vcnerts / Datacenter:datacenter-3	ATTACHED	100	asugi	Deployed		3 months ago	⋮
⋮	CD/DVD drive 1		vcnerts / Datacenter:datacenter-3	ATTACHED	0	asugi	Deployed		3 months ago	⋮
⋮	cSasugi26-boot-disk		vcnerts / Datacenter:datacenter-3	ATTACHED	80	asugi	Deployed		3 months ago	⋮
⋮	disk[1]-mcm7598-276873529984	010010	vcnerts / Datacenter:datacenter-3	ATTACHED	20	asugi	Deployed		3 months ago	⋮

Figura 51 – Volumes

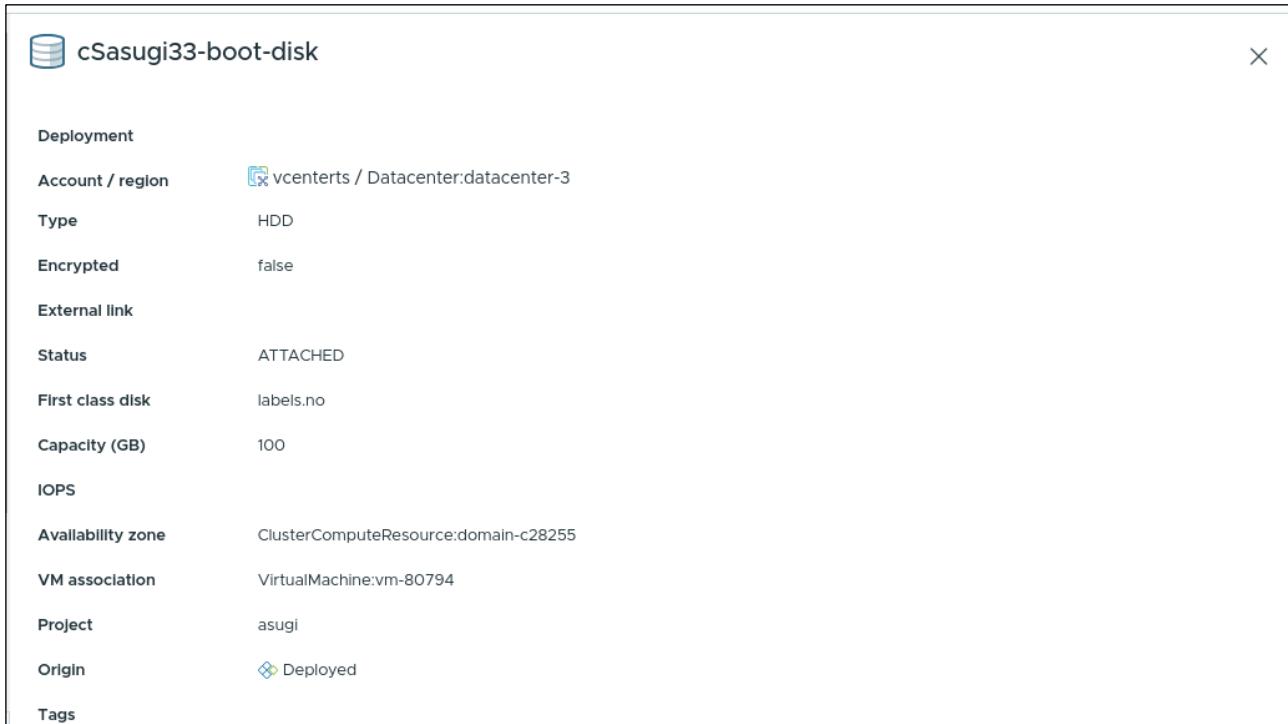
Sono presenti tre tipologie di volumi:

- Dischi di boot.
- Dischi aggiuntivi.
- CD/DVD che consentono il montaggio di una immagine ISO.

La griglia contiene i seguenti campi:

- **Name:** il nome del volume, contenente talvolta il nome del deployment con il quale è stato creato.
- **Deployment:** non sempre presente, il nome del deployment con il quale è stato creato il volume.
- **Status:** l'utilizzo del volume, se ATTACHED vuol dire che è effettivamente collegato ad una VM.
- **Capacity(GB):** le dimensioni del volume in GB.
- **Project:** sempre pari ad ‘asugi’.
- **Origin:** metodo di creazione del volume, tipicamente assume il valore ‘Deployed’.
- **Tags:** eventuali tag per il volume
- **Created on:** data di creazione del volume

Cliccando su ➤ alla sinistra di ogni riga, si avrà accesso ad una finestra di dettaglio per quel volume:



Deployment	
Account / region	vcenterts / Datacenter:datacenter-3
Type	HDD
Encrypted	false
External link	
Status	ATTACHED
First class disk	labels.no
Capacity (GB)	100
IOPS	
Availability zone	ClusterComputeResource:domain-c28255
VM association	VirtualMachine:vm-80794
Project	asugi
Origin	Deployed
Tags	

Figura 52 – Volumes - Dettaglio volume

Cliccando su ⋮ si avrà accesso ad un menu contestuale:

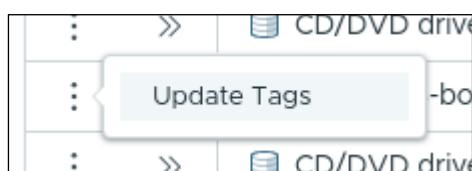


Figura 53 - Volumes - Menu contestuale

L'unica funzionalità disponibile è 'Update Tags' che permette di inserire tag nei volumi.

5.3.2.1.4.5.NETWORKING E SECURITY

La griglia ‘Networking & Security’ mostra le configurazioni di rete delle VM create, ed eventuali attività di deployment in corso:

Networking & Security											
		Name	Deployment	Account / Region	NSX Project / VPC	Network Domain	CIDR	Project	Origin	Tags	Created On
:	»	asugi	010016	 vcenter / DC_PROD			10.128.188.0/22	asugi	 Deployed		7 days ago
:	»	asugi	010006	 nsx / global	ASUGI / -		10.128.188.0/22	asugi	 Onboarded	segment:asugi	2 months ago
:	»	asugi	010013	 vcenter / DC_PROD			10.128.188.0/22	asugi	 Deployed		3 months ago
:	»	asugi	010015	 vcenter / DC_PROD			10.128.188.0/22	asugi	 Deployed		3 months ago
:	»	asugi	010014	 vcenter / DC_PROD			10.128.188.0/22	asugi	 Deployed		3 months ago
:	»	asugi	010012	 vcenter / DC_PROD			10.128.188.0/22	asugi	 Deployed		3 months ago
:	»	asugi	010004	 vcenter / DC_PROD			10.128.188.0/22	asugi	 Deployed		3 months ago
:	»	asugi	010010	 vcenter / DC_PROD			10.128.188.0/22	asugi	 Deployed		3 months ago

Figura 54 - Networking & Security

La griglia contiene i seguenti campi:

- **Name:** il nome della rete cui è collegata la VM.
- **Deployment:** il nome del deployment con il quale è stato assegnato l'indirizzo di rete contestualmente alla creazione della VM.
- **Account/Region:** la localizzazione della rete.
- **NSX Project / VPC:** in genere non popolato.
- **Network Domain:** in genere non popolato.
- **CIDR:** indirizzo di rete assegnato per quello specifico deployment.
- **Project:** sempre pari ad ‘asugi’.
- **Origin:** metodo di creazione del volume, tipicamente assume il valore ‘Deployed’.
- **Tags:** eventuali tag per il volume
- **Created on:** data di creazione del volume

Cliccando su » alla sinistra di ogni riga, si avrà accesso ad una finestra di dettaglio per quella riga:

asugi	
Deployment	OI0013
Global	No
Account / region	vcentersts / DC_PROD
NSX project / VPC	
Zone	
Default for zone	No
Network domain	
Domain	
IPv4 CIDR	10.128.188.0/22
IPv4 default gateway	10.128.188.1
IPv6 CIDR	
IPv6 default gateway	
DNS servers	172.17.254.13
DNS search domains	172.17.253.13
Support public IP	No
Project	asugi
Origin	Deployed
Tags	
Owner	francesco.chiffi@privativra.local
Created on	3 months ago

Figura 55 - Networking & Security – Dettagli

Cliccando su  si avrà accesso ad un menu contestuale:

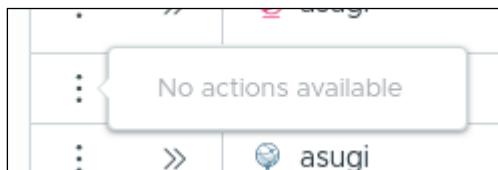


Figura 56 - Networking & Security - Menu contestuale

Che tuttavia non dà accesso ad alcuna funzionalità.

5.4. CLOUD FIREWALL

5.4.1.1.1. ACCESSO AL CLOUD FIREWALL

Selezionando ‘Cloud Firewall’:

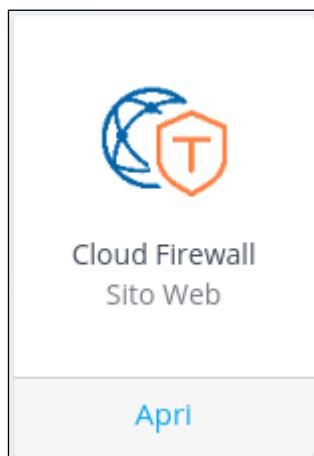


Figura 57 - Tasto 'Cloud Firewall'

Si avrà accesso ad una schermata ulteriore:

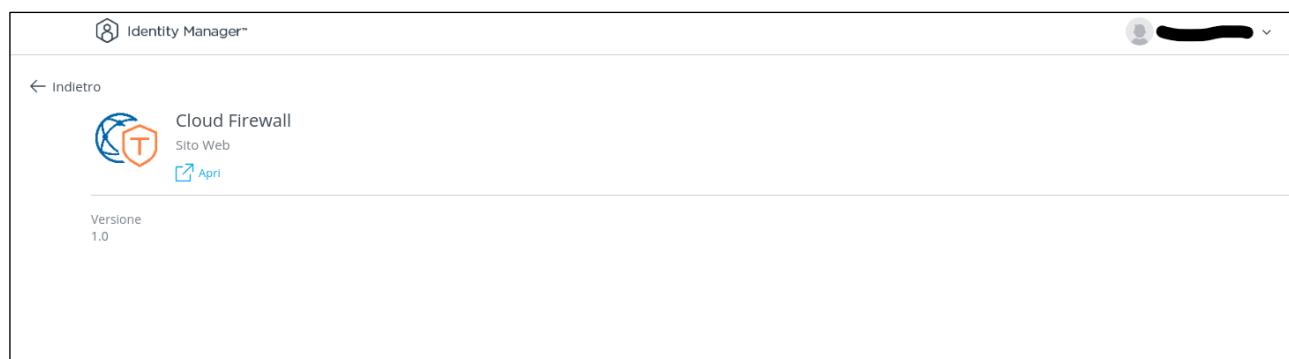


Figura 58 - Accesso a Cloud Firewall

Da qui cliccando sull’icona ‘Apri’:  si avrà finalmente accesso all’interfaccia utente di VMWare NSX.

Si tratta di una interfaccia estremamente strutturata che dà accesso a numerose funzionalità. Tuttavia scopo del presente documento non è necessaria una esaustiva e completa spiegazione delle funzionalità di VMWare NSX, ci si concentrerà pertanto sulle sole funzionalità necessarie alla creazione di una VM.

NOTA BENE:

- La sessione con NSX scade anche durante un periodo di attività, tale comportamento è del tutto regolare ed è necessario ri effettuare il log.

5.4.1.1.2. HOME

Il tab ‘Home’ non dà accesso a funzionalità particolari, ma consente solamente di prendere visione delle configurazioni generali di NSX.

5.4.1.1.2.1.PANORAMICA

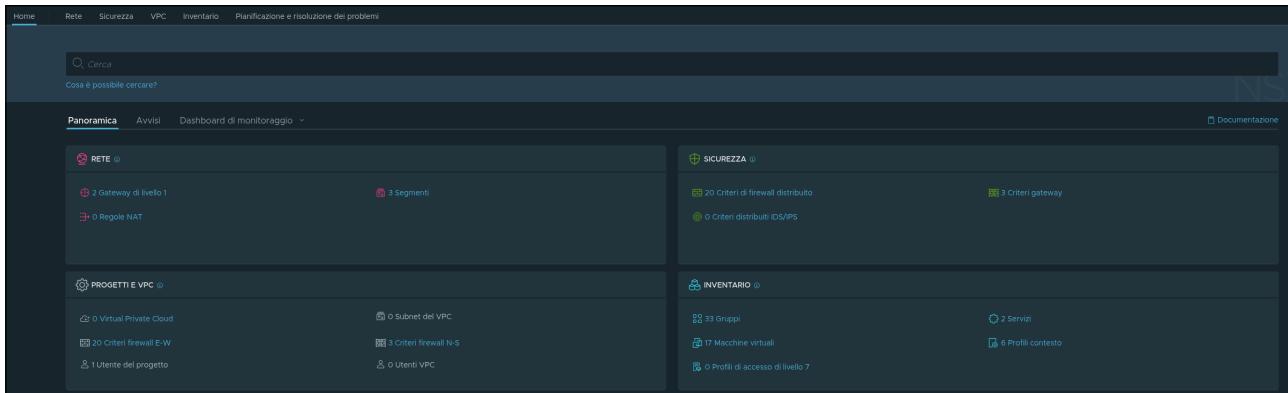


Figura 59 - VMWare NSX – Home - Panoramica

La griglia ‘Home’ è il punto di accesso di NSX, vengono mostrati nei quattro riquadri, informazioni di carattere generale:

- Rete:
 - 2 Gateway di livello 1 (vedi [PAR. 5.2.2.2](#)).
 - 0 Regole NAT.
 - 3 Segmenti (di rete).
- Sicurezza:
 - 20 criteri di firewall distribuito: coincide con il numero di criteri presenti nel firewall distribuito (vedi [PAR. 5.4.1.1.3.1](#)).
 - 0 criteri distribuiti IDS/IPS: questa funzionalità è infatti disabilitata.
 - 3 criteri gateway: coincide con i tre criteri presenti nel firewall gateway di cui due di default, ed uno custom.
- Progetti E VPC:
 - 0 Virtual Private Cloud, coincide con quanto visualizzato nel tab VPC.
 - 20 criteri firewall E-W: coincide con il numero di criteri presenti nel firewall distribuito¹.
 - 3 criteri firewall N-S: coincide con il numero di criteri gateway visto in precedenza².
 - 1 utente del progetto.
 - 0 subnet del VPC, infatti non sono configurati VPC.
 - 0 utenti VPC, per lo stesso motivo della voce precedente.
- Inventario:
 - 33 gruppi (vedi [PAR. 5.4.1.1.4.2](#)).
 - 17 macchine virtuali (vedi [PAR. 5.4.1.1.4.4](#)).

¹ Regole est-ovest: per la connettività orizzontale nell’infrastruttura, ovvero tra le VM appartenti all’infrastruttura.

² Regole nord-sud: per la connettività verticale nell’infrastruttura, ovvero da e per l’esterno.

- 0 profili di accesso a Livello 7 (vedi [PAR. 5.4.1.1.4.3](#)).
- 2 sevizi (vedi [PAR 5.4.1.1.4.1](#))
- 6 profili contesto (vedi [PAR. 5.4.1.1.4.3](#)).

5.4.1.1.2.2.AVVISI

Nel tab ‘Avvisi’ sono presenti due sotto tab:

- Avvisi
- Definizione avvisi

Figura 60 - VMWare NSX – Home – Avvisi

Funzionalità	Tipo di evento	Gravità	Abilità rilevamento	Creare allarmi	Creare trap SNMP
> Capacità	Capacità massima	■ Critica	Sì	No	No
> Capacità	Soglia capacità massima	■ Alta	Sì	No	No
> Capacità	Soglia capacità minima	■ Media	Sì	No	Sì
> DHCP	Allocazione lease pool non riuscita	■ Alta	Sì	Sì	Sì
> DHCP	Pool sovraccarico	■ Media	No	Sì	Sì
> Firewall distribuito	Utilizzo CPU DFW molto elevato	■ Critica	Sì	Sì	Sì
> Firewall distribuito	Utilizzo CPU DFW molto elevato in DPU	■ Critica	Sì	Sì	Sì
> Firewall distribuito	Limite flood DFW critico	■ Critica	Sì	Sì	Sì
> Firewall distribuito	Limite flood DFW avviso	■ Media	Sì	Sì	Sì
> Firewall distribuito	Utilizzo memoria DFW molto elevato	■ Critica	Sì	Sì	Sì
> Firewall distribuito	Utilizzo memoria DFW molto elevato in DPU	■ Critica	Sì	Sì	Sì
> Firewall distribuito	Il limite delle regole DFW per host sta per essere superato	■ Media	Sì	Sì	Sì
> Firewall distribuito	Limite delle regole DFW per host superato	■ Critica	Sì	Sì	Sì
> Firewall distribuito	Il limite delle regole DFW per vNIC sta per essere superato	■ Media	Sì	Sì	Sì
> Firewall distribuito	Limite delle regole DFW per vNIC superato	■ Critica	Sì	Sì	Sì
> Firewall distribuito	Numero sessioni DFW elevato	■ Critica	Sì	Sì	Sì

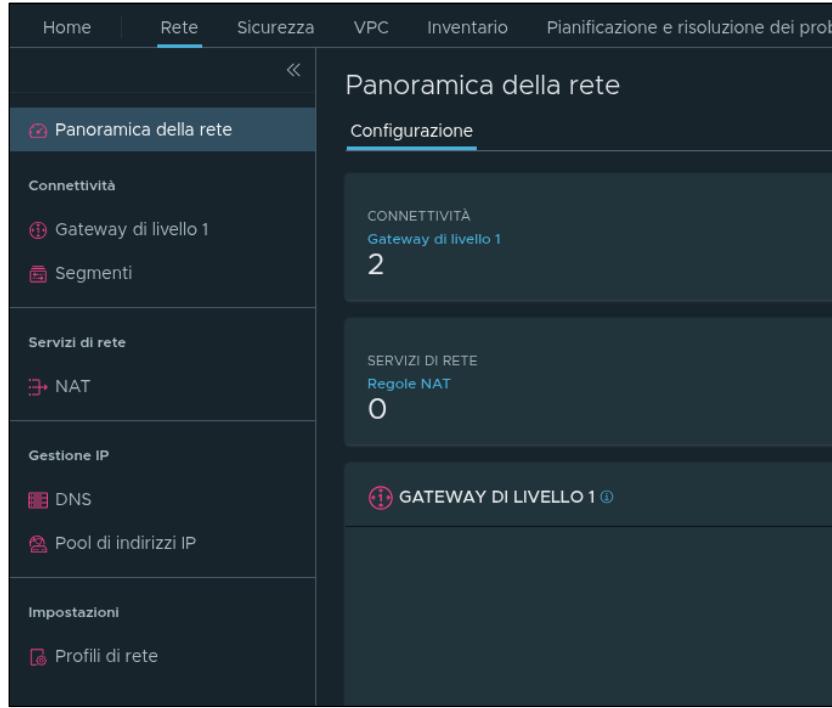
Figura 61 - VMWare NSX – Home – Definizione avvisi

Queste funzionalità non sono utilizzate, non vi sono avvisi configurati.



5.4.1.1.3. RETE

Il tab ‘Rete’ permette di prendere visione delle vari configurazioni di rete di NSX, è utile per consultazione, ma su di esso non deve mai essere effettuato alcun intervento.



The screenshot shows the VMware NSX interface with the 'Rete' (Network) tab selected. On the left, there's a sidebar with categories: Connattività, Servizi di rete, Gestione IP, and Impostazioni. Under Connattività, it shows 2 Gateway di livello 1 and 3 Segmenti. Under Servizi di rete, it shows 0 Regole NAT. Under Gestione IP, it shows 0 DNS and 0 Pool di indirizzi IP. The main panel is titled 'Panoramica della rete' and 'Configurazione'. It displays three cards: 'CONNETTIVITÀ' with 2 Gateway di livello 1, 'SERVIZI DI RETE' with 0 Regole NAT, and 'GATEWAY DI LIVELLO 1' which is expanded to show details for 'Gateway di livello 1'.

Figura 62 - VMWare NSX – Rete

5.4.1.1.3.1. PANORAMICA DELLE RETE

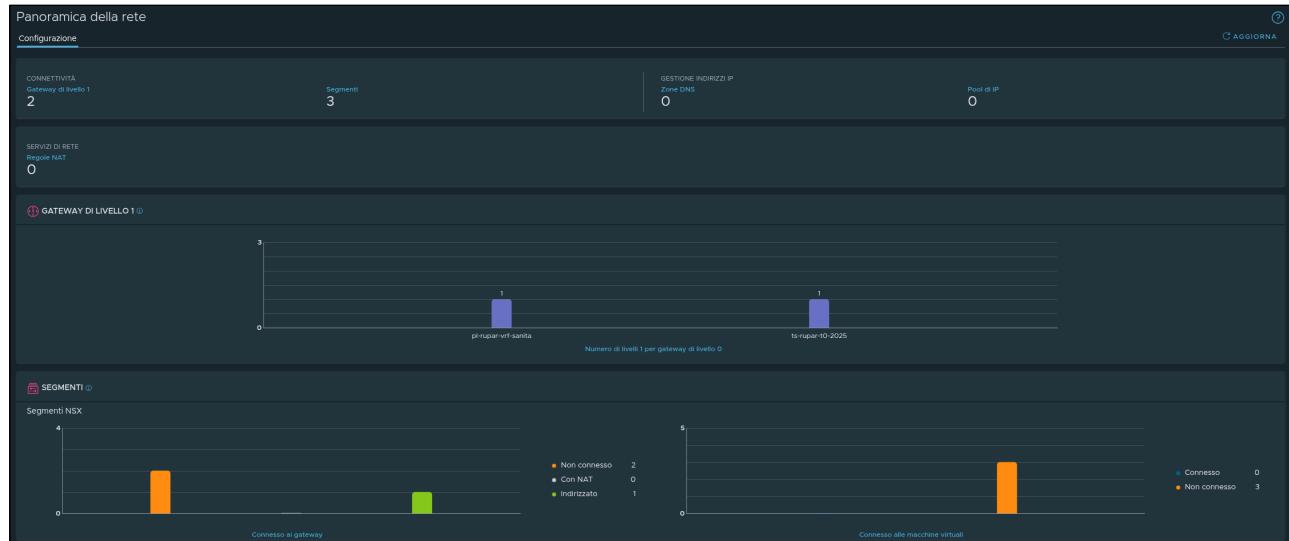


Figura 63 - VMWare NSX – Rete – Panoramica della rete

Vengono mostrate indicazioni generali sulla configurazione della rete:

- Connattività:
 - Gateway di livello 1: 2 (vedi [PAR. 5.2.2.2](#)).
 - Segmenti: 3.

- Gestione indirizzi IP:
- Zone DNS: 0.
- Pool di IP: 0.
- Gateway di livello 1:
 - Numeri di livelli 1 per gateway di livello 0: 2 (si osservi che i nomi coincidono con quanto riportato nel [PAR. 5.2.2.2](#)).
- Segmenti:
- Segmenti NSX:
 - Connesso al gateway:
 - Non connesso: 2
 - Con NAT: 0
 - Indirizzato: 1
 - Connesso alle macchine virtuali:
 - Connesso: 0
 - Non connesso: 3

5.4.1.1.4. GATEWAY DI LIVELLO 1

Gateway di livello 1					
		Nome	Modalità HA	Gateway di livello 0 collegato	Segmenti collegati
:	>	pl-asugi-t1-test-dr	Attivo/Standby	 pl-rupar-vrf-sanita	0
:	>	ts-asugi-t1	Attivo/Standby	ts-rupar-t0-2025	1

Figura 64 - VMWare NSX – Rete – Gateway di Livello 1

La griglia riporta i seguenti campi:

- Nome.
- Modalità HA.
- Gateway di livello 0 collegato.
- Segmenti collegati.

- Stato.
- Avvisi

E' evidente la corrispondenza tra quanto mostrato nella griglia e quanto descritto nel [PAR. 5.2.2.2](#), ovvero il gateway di livello 1: pl-asugi-t1-test-dir è connesso al gateway di livello 0: pl-rupar-vrf-sanita, questo è il backup in caso di disaster recovery; il gateway di livello 1: ts-asugi-t1 è connesso al gateway di livello 0: ts-rupar-t0-2025, questa è la linea primaria per la connettività.

5.4.1.1.5. SEGMENTI

Tale pagina fornisce indicazioni sui segmenti di rete utilizzati, è suddivisa su due tab:

- NSX
- Profili

5.4.1.1.5.1.NSX

Segmenti							
		Nome	Gateway connesso	Zona di trasporto	Subnet	Porte / Interfacce	Stato ⓘ
NSX		asugi	ts-asugi-t1	Zona di trasporto predefinita progetto ⓘ	10.128.188.1/22	17	Operazione eseg... C 0 —
Profili		test-asugi	Nessuno	Zona di trasporto predefinita progetto ⓘ	Non impostato	0	Operazione eseg... C 0 —
		test-asugi-test-dr	Nessuno	Zona di trasporto predefinita progetto ⓘ	Non impostato	0	Operazione eseg... C 0 —

[AGGIORNA](#) | Mostra: Oggetti condivisi ⓘ Oggetti VPC realizzati ⓘ

1 - 3 di 3

Figura 65 - VMWare NSX – Rete – Segmenti – NSX

Nella griglia sono presenti i seguenti campi:

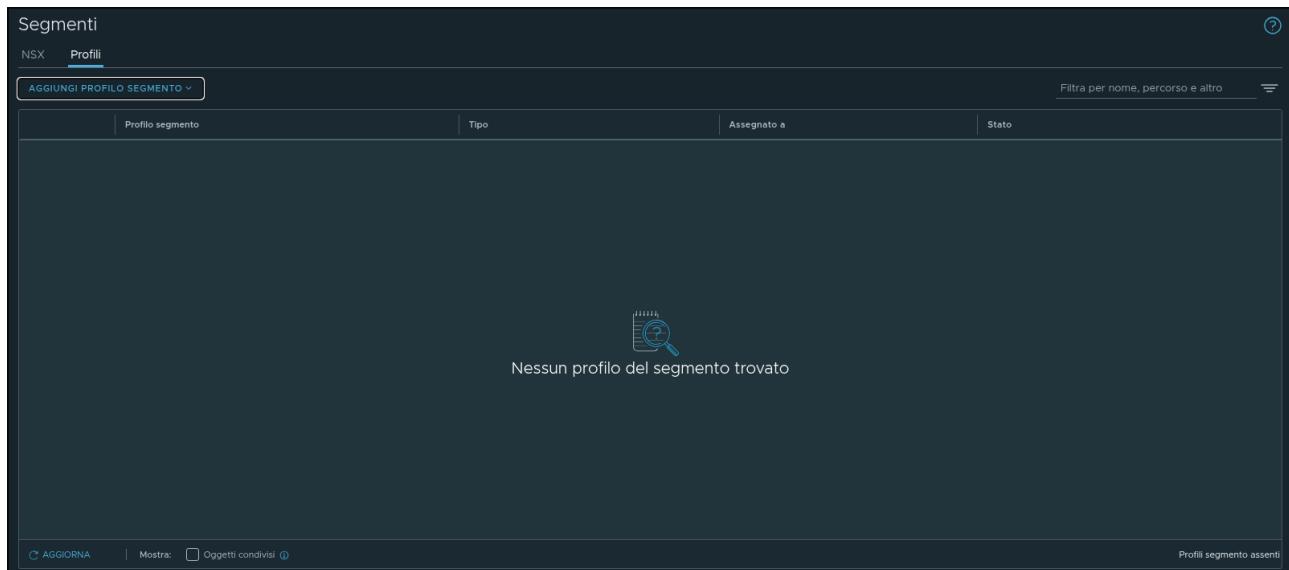
- Nome
- Gateway connesso
- Zona di trasporto
- Subnet
- Porte / interfacce
- Stato

- Avvisi

Consideriamo la prima riga:

- Il nome della rete è ‘asugi’ e coincide con la rete assegnata di default in fase di creazione di una VM (vedi [PAR 6.1](#)) ed è la rete di produzione normalmente utilizzata.
- La rete è collegata al gateway (di livello 1) principale: ts-asugi-t1.
- La subnet è effettivamente quella da cui vengono attinti gli indirizzi IP da assegnare alle VM create.
- Il numero di porte / Interfacce coincide con il numero di VM esistenti nell’infrastruttura (vedi [PAR. 5.3.2.1.4.3](#)).

5.4.1.1.5.2.PROFILI



The screenshot shows the VMware NSX interface for managing network segments. The top navigation bar has tabs for 'NSX' and 'Profili', with 'Profili' being the active tab. Below the tabs is a button labeled 'AGGIUNGI PROFILO SEGMENTO'. A search bar is present with the placeholder 'Filtro per nome, percorso e altro'. The main area is a table with columns: 'Profilo segmento', 'Tipo', 'Assegnato a', and 'Stato'. A message at the bottom of the table says 'Nessun profilo del segmento trovato' (No segment profile found). At the bottom of the interface are buttons for 'AGGIORNA', 'Mostra:', 'Oggetti condivisi', and 'Profilo segmento assenti'.

Figura 66 - VMWare NSX – Rete – Segmenti – Profili

Nella griglia sono presenti i seguenti campi:

- Profilo segmento
- Tipo
- Assegnato a
- Stato

I ‘profili’ sono ulteriori configurazioni che è possibile aggiungere ai segmenti NSX:



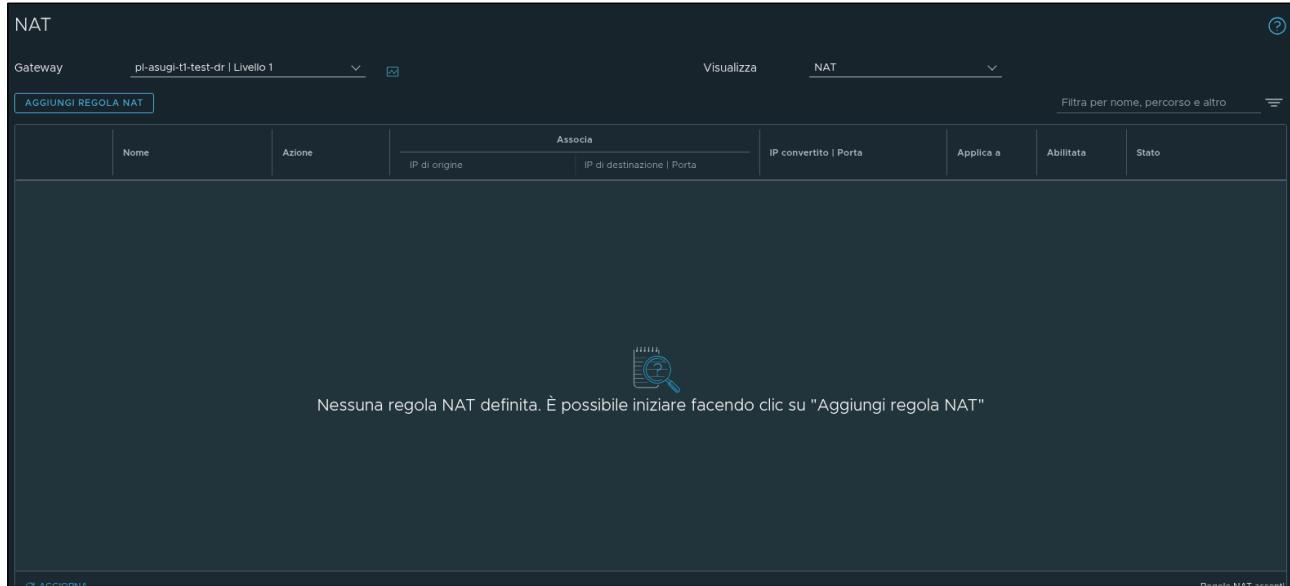
Figura 67 - VMWare NSX – Rete – Segmenti – Profili – Tipo profili

In dettaglio:

- SpoofGuard
- Rilevamento IP
- Rilevamento MAC
- Sicurezza segmento
- QoS

Al momento non vi è nessun profilo configurato.

5.4.1.1.6. NAT



The screenshot shows the VMware NSX interface for managing Network Address Translation (NAT) rules. The top navigation bar includes tabs for 'Gateway' (selected), 'pi-asugi-t1-test-dr | Livello 1', 'Visualizza' (set to 'NAT'), and 'Filtro per nome, percorso e altro'. Below the navigation is a search bar with a magnifying glass icon. The main area is a table titled 'NAT' with columns: Nome, Azione, Associa, IP di origine, IP di destinazione | Porta, IP convertito | Porta, Applica a, Abilitata, and Stato. A button labeled 'AGGIUNGI REGOLA NAT' is located at the top left of the table. A message at the bottom center states: 'Nessuna regola NAT definita. È possibile iniziare facendo clic su "Aggiungi regola NAT"' (No NAT rule defined. You can start by clicking on "Add NAT rule").

Figura 68 - VMWare NSX – Rete – NAT

Sono presenti nella griglia i seguenti campi:

- Nome.
- Azione.
- Associa.
- IP di origine.
- IP di destinazione/Porta.
- IP convertito/Porta.
- Applica a.
- Abilitata.
- Stato.

Figura 69 - VMWare NSX – Rete – NAT – Configurazione NAT

Questa funzionalità è utile per configurare NAT nel contesto di un gateway di Livello 1 predefinito. Al momento non sono presenti NAT configurati.

5.4.1.1.7. DNS

Tale pagina fornisce indicazioni sui segmenti di rete utilizzati, è suddivisa su due tab:

- Servizi DNS
- Zone DNS

5.4.1.1.7.1. SERVIZI DNS

Figura 69 - VMWare NSX – DNS – Servizi DNS

Sono presenti nella griglia i seguenti campi:

- Nome

- Gateway
- IP servizio DNS
- Zona DNS predefinita
- Zona FQDN
- Stato

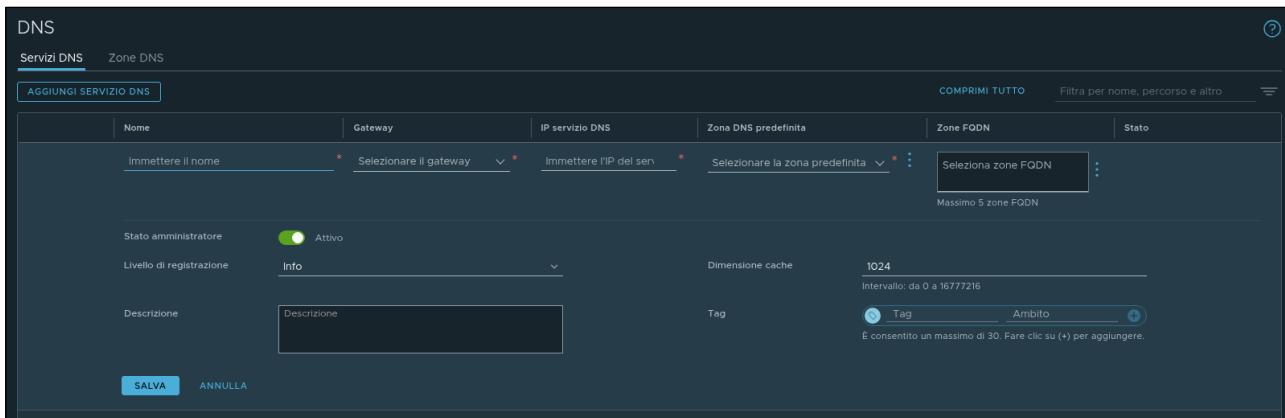


Figura 69 - VMWare NSX – DNS – Servizi DNS – Configurazione DNS

Non vi sono servizi DNS configurati a livello di NSX.

NOTA BENE:

- I servizi DNS vengono forniti nel contesto dell'Active Directory.
- Tipicamente i servizi DNS vengono configurati manualmente sia per le VM collegate al dominio che per le VM non collegate al dominio.

5.4.1.1.7.2.ZONE DNS

5.4.1.1.8. SICUREZZA

Nello specifico sono di nostro interesse le funzionalità accessibili cliccando sul tab ‘Sicurezza’:

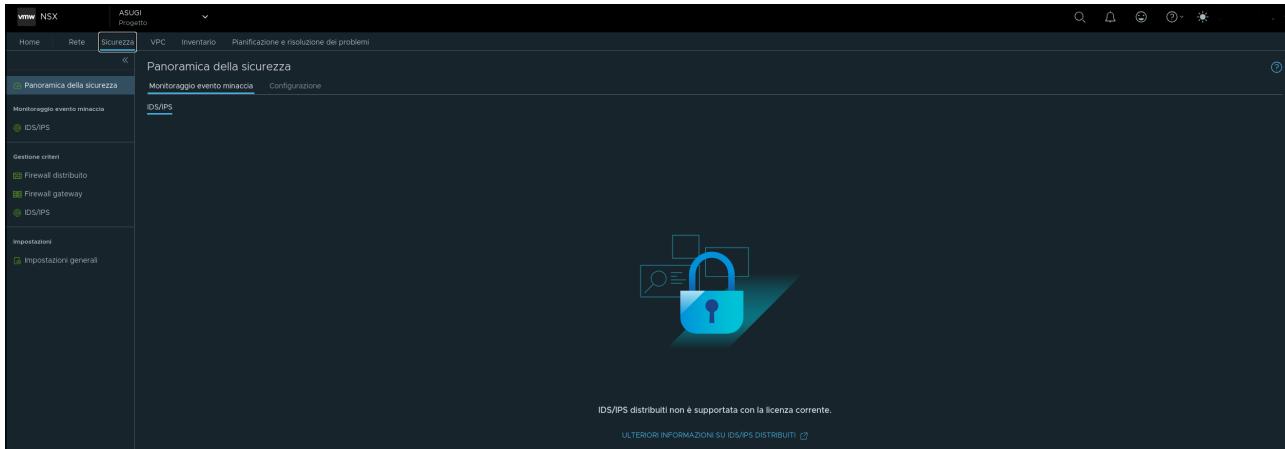


Figura 70 - VMWare NSX - Sicurezza

L'alert che appare è del tutto regolare e specifica come le funzionalità IDS/IPS non siano attive in VMWare NSX.

Sulla sinistra sono disponibili varie funzionalità, l'unica rilevante per le finalità di questo documento è 'Firewall gateway'.

Selezionando 'Firewall gateway' vengono mostrate le regole generiche a livello di gateway NSX. In generale in questa schermata non deve essere apportata alcuna modifica.

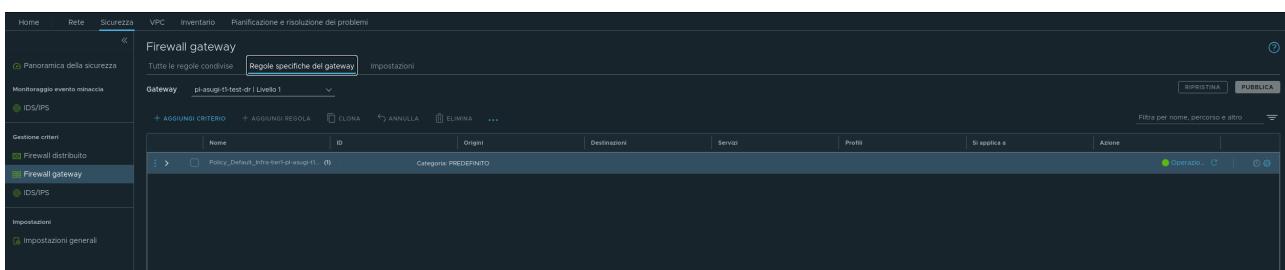


Figura 71 - VMWare NSX - Sicurezza -Firewall Gateway

I gateway normalmente sono su base geografica e gestiscono regole firewall generiche.

5.4.1.1.8.1.FIREWALL DISTRIBUITO

Per le finalità di questo documento è necessario concentrarsi invece su 'Firewall distribuito':

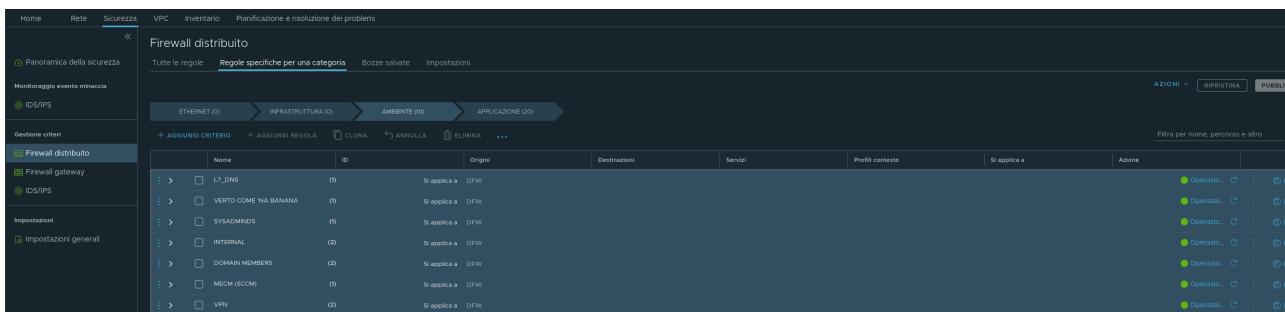


Figura 72 - VMWare NSX - Firewall distribuito

Per ‘distribuito’ si intende che il firewall è, semplificando, distribuito su tutti gli host ESXi che costituiscono l’infrastruttura VMWare, e, in tal modo anche le regole in esso impostate saranno automaticamente distribuite su tutti gli host ESXi.

Per le finalità del presente documento considereremo i blocchi di ‘criteri’:

- **Ambiente:** si tratta di criteri di utilizzo generico, ad esempio, accesso a VPN, accesso ad AD, ecc.
- **Applicazione:** si tratta di criteri creati per l’utilizzo specifico con determinate infrastrutture applicative.

Ogni ‘criterio’ raggruppa una o più regole firewall.

NOTA BENE:

- Si osservi che la regola di default, quindi quella in fondo all’elenco, anche se non visibile è ‘DENY ALL’, ossia viene inibita ogni comunicazione.
- In conseguenza di ciò tutte le VM create cui non sia associata una qualsivoglia regola firewall sono completamente isolate.

Cliccando sulla freccia a sinistra si avrà accesso al dettaglio di un criterio:

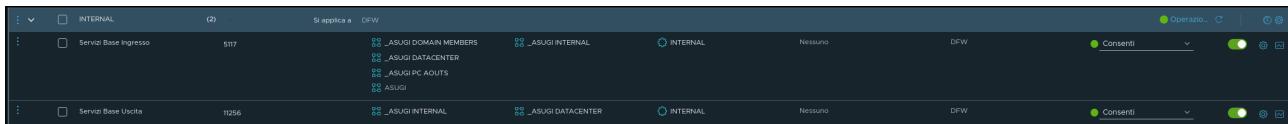


Figura 73 - VMWare NSX - Dettaglio regola firewall

Cliccando sui tre puntini del criterio, si accede ad una serie di operazioni di dettaglio:

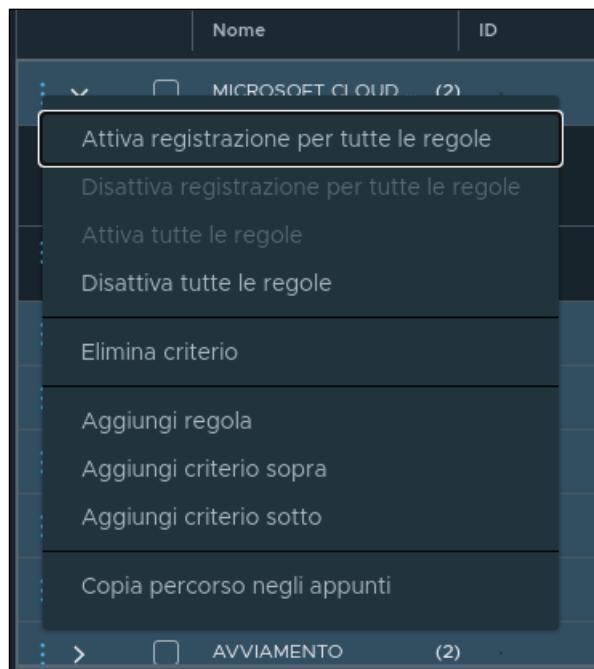


Figura 74 - VMWare NSX - Operazioni sui criteri

È bene valutare con attenzione, prima di effettuare operazioni su tale menu.

Cliccando sui tre puntini della regola si avrà accesso ad alcune operazioni di dettaglio:

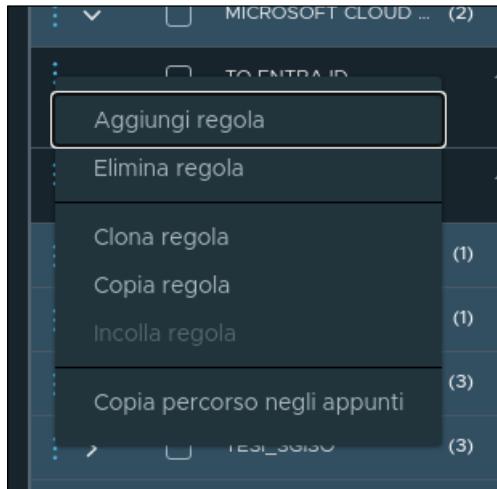


Figura 75 - VMWare NSX - Operazioni sulle regole

Si osservi che è possibile modificare la priorità delle regole firewall all'interno di un criterio, anche semplicemente trascinandole.

È possibile aggiungere un nuovo criterio cliccando sul tasto specifico: **+ AGGIUNGI CRITERIO**.

Nome	ID	Origini	Destinazioni	Servizi	Profilo contesto	Si applica a	Azione
<input checked="" type="checkbox"/> Nuovo criterio (0)		Si applica a DFW					

Figura 76 - VMWare NSX – Nuovo criterio

Un criterio privo di regole è in pratica una ‘scatola vuota’.

Successivamente si potrà premere sul tasto: **PUBBLICA 1** per confermare, o **RIPRISTINA** per annullare.

Dopo aver creato un criterio ed averlo selezionato, è possibile aggiungere una regola cliccando sul tasto specifico: **+ AGGIUNGI REGOLA**.

Nome	ID	Origini	Destinazioni	Servizi	Profilo contesto	Si applica a	Azione
<input checked="" type="checkbox"/> Nuovo criterio (1)		Si applica a DFW					
<input checked="" type="checkbox"/> Nuova regola		Qualsiasi	Qualsiasi	Nessuno	DFW	Consenti	<input checked="" type="checkbox"/>

Figura 77 - VMWare NSX – Nuova regola firewall

Anche in questo caso si potrà premere sul tasto: **PUBBLICA 1** per confermare, o **RIPRISTINA** per annullare.

L'operazione andrà ripetuta per ogni regola firewall da aggiungere.

Si osservi come talune di queste operazioni siano ugualmente eseguibili con i menu contestuali visti in precedenza.

Il criterio ‘INTERNAL’ mostrato sopra, nello specifico contiene due regole firewall:

- Servizi Base Ingresso
- Servizi Base Uscita

I dettagli forniti per ogni regola sono:

- Nome regola
- ID regola
- Gruppo origine
- Gruppo destinazione
- Servizi
- Profili contesto
- Si applica a
- Azione
- Abilitata

Nel caso specifico, a titolo di esempio la regola ‘Servizi base uscita’ riporta i seguenti valori:

- Nome regola: Servizi base uscita
- ID regola: 11256
- Gruppo origine: _ASUGI INTERNAL
- Gruppo destinazione: _ASUGI DATACENTER
- Servizi: INTERNAL
- Profili contesto: Nessuno
- Si applica a: DFW (Distributed Firewall)
- Azione: Consenti
- Abilitata: Si

Si osservi quanto segue:

- Origini e destinazioni: non possono essere indicate singole VM ma ‘Gruppi’, i ‘Gruppi’ verranno dettagliati più a fondo successivamente. Nel caso la regola interessi una singola VM sarà necessario realizzare un gruppo contenente una solo VM.
- Servizi: si possono in maniera semplificata associare i servizi alle porte cui debba essere applicata la regola. Vi sono alcuni servizi standard disponibili, quali: http (porta 80), https (porta 443), ecc. è possibile definire anche servizi con porte fuori standard. Anche tale funzionalità verrà descritta nei paragrafi seguenti.
- Profili contesto: laddove venga applicato, un ‘Profilo contesto’ viene definito come un URL, o un FQDN, o comunque una destinazione per la regola firewall. Anche tale definizione verrà approfondita in seguito.

5.4.1.1.9. INVENTARIO

Selezionando il tab ‘Inventario’ si avrà accesso ad ulteriore funzionalità complementari, ma indispensabili per l’implementazione di regole firewall in NSX:

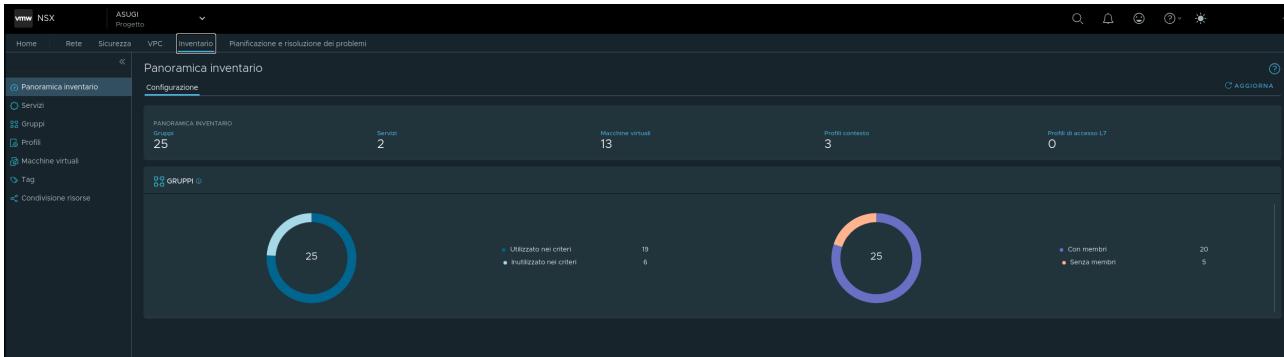


Figura 78 - VMWare NSX – Inventario

Il vantaggio principale di tali funzionalità è la possibilità di non legare le regole firewall a specifici host, sulla base del nome host, o dell'IP, o a specifici servizi, sulla base ad esempio della porta.
Le regole saranno infatti applicate a ‘tag’, pertanto ad esempio, aggiungendo una vm ad un gruppo con un certo tag, ad essa verranno automaticamente applicate le regole firewall che a quel tag fanno riferimento, identica logica per le porte o i servizi utilizzati dalla specifica regola firewall.

All'accesso al tab verrà mostrata una schermata riassuntiva delle configurazioni.

Sulla sinistra sono rilevanti le voci:

- Servizi
- Gruppi
- Profili
- Macchine virtuali
- Tag

5.4.1.1.9.1.SERVIZI

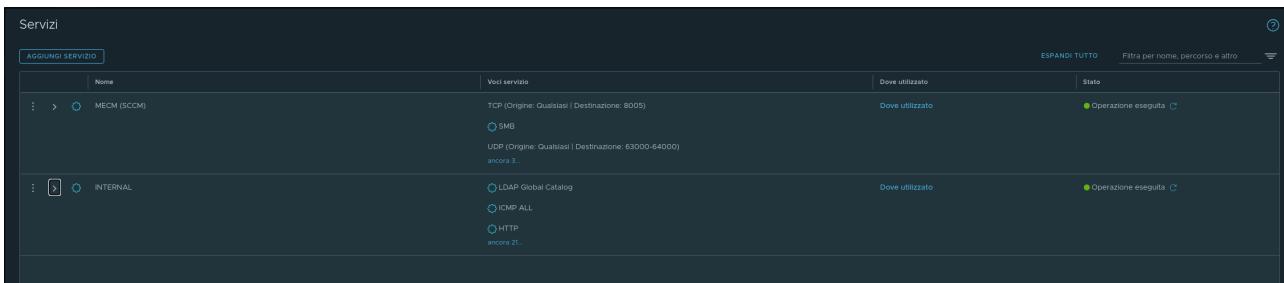


Figura 79 - VMWare NSX- Servizi

La funzionalità ‘Servizi’ serve a creare regole che associno una denominazione ad un elenco di protocolli: http, ftp, smb, ecc. Tali ‘Servizi’ potranno poi essere applicate alle regole firewall. Nello specifico la griglia mostra:

- Nome servizio
- Voci servizio
- Dove utilizzato
- Stato

Cliccando sulla freccia a sinistra del nome del servizio sarà visualizzato il dettaglio dello stesso:



Figura 80 - VMWare NSX - Servizi - Dettaglio servizio

Cliccando sui tre puntini si avrà accesso al menu contestuale:



Figura 81 - VMWare NSX - Servizi – Operazioni sui servizi

In sostanza è possibile utilizzare un servizio preconfigurato, come ad esempio: http, https, smb, ecc. oppure creare nuovi servizi composti come composizione di servizi preesistenti.

È possibile creare un nuovo servizio creando sul tasto: **[AGGIUNGI SERVIZIO]**.

Figura 82 - VMWare NSX - Servizi - Creazione di un nuovo servizio.

Si osservi come cliccando su ‘Imposta’, sarà possibile creare un nuovo singolo servizio:

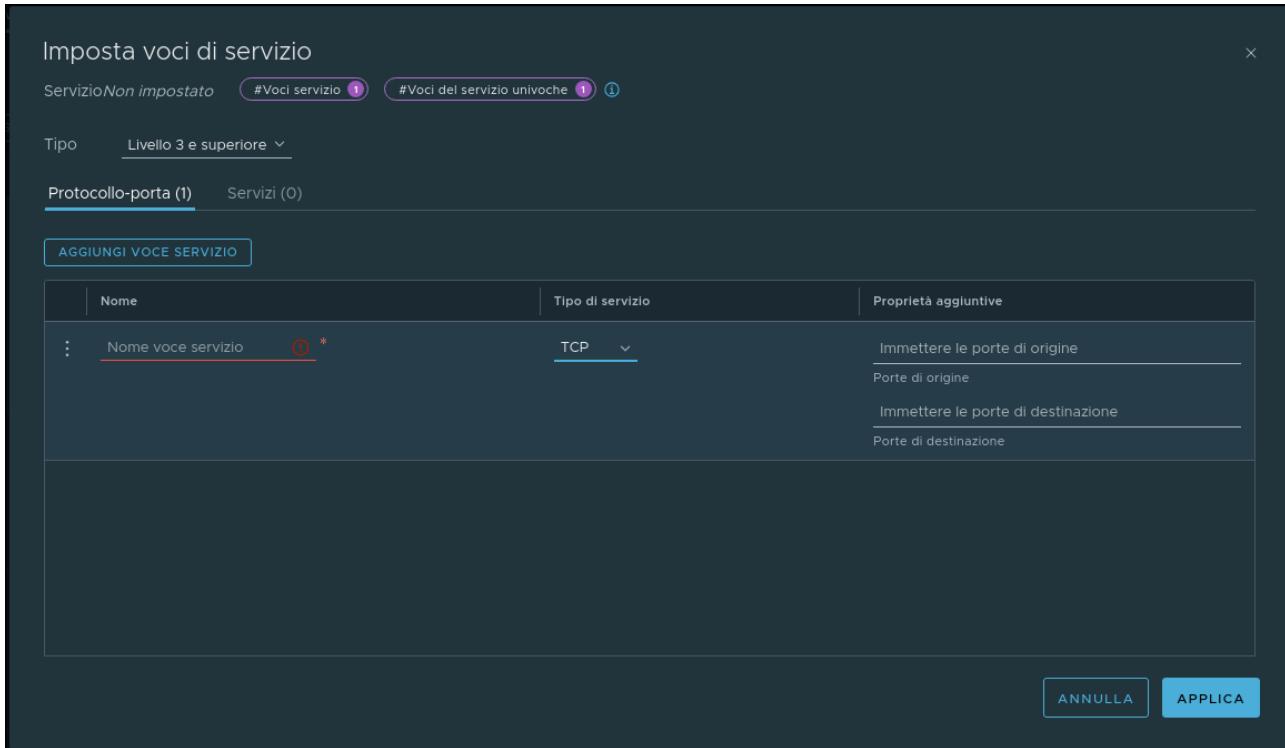


Figura 83 - VMWare NSX - Servizi - Creazione di un nuovo singolo servizio.

Cliccando su ‘tag’ sarà possibile utilizzare servizi preesistenti.

Nell’ambito della configurazione di una regola firewall non vi è alcuna differenza tra un servizio semplice ed un servizio composito.

5.4.1.1.9.2.GRUPPI

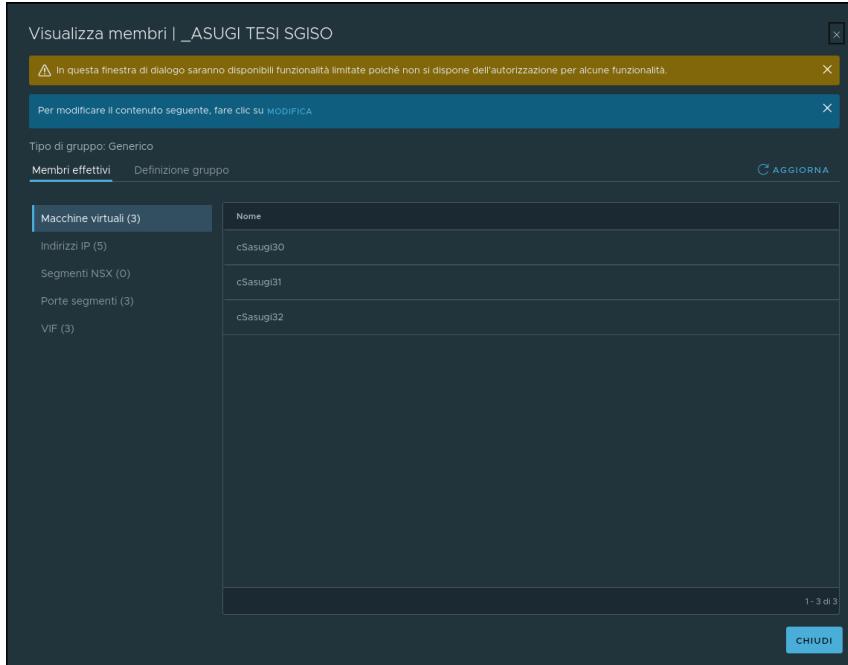
Selezionando la voce ‘Gruppi’ si avrà accesso ad una griglia che mostra un elenco di gruppi di VM:

Gruppi					
AGGIUNGI GRUPPO ESPANDI TUTTO Filtro per nome, percorso e altro					
	Nome	Tipo	Membri elaborazione	Dove utilizzato	Stato
>	0C0024	Generico	Visualizza membri	Dove utilizzato	● Operazione eseguita
>	_ASUGI APPLICAZIONE_SQL	Generico	Visualizza membri	Dove utilizzato	● Operazione eseguita
>	_ASUGI DATACENTER	Solo indirizzi IP	Visualizza membri	Dove utilizzato	● Operazione eseguita
>	_ASUGI DIARET	Generico	Visualizza membri	Dove utilizzato	● Operazione eseguita
>	_ASUGI DOMAIN MEMBERS	Generico	Visualizza membri	Dove utilizzato	● Operazione eseguita
>	_ASUGI INTERNAL	Generico	Visualizza membri	Dove utilizzato	● Operazione eseguita
>	_ASUGI MACCHINA PONTE	Generico	Visualizza membri	Dove utilizzato	● Operazione eseguita
>	_ASUGI MATRIX42	Generico	Visualizza membri	Dove utilizzato	● Operazione eseguita

Figura 84 - VMWare NSX – Gruppi

La funzionalità ‘Gruppi’ serve a creare gruppi di VM, l’associazione tra un gruppo ed una o più VM, avviene attraverso l’associazione del gruppo ad uno specifico tag cui sarà a sua volta stata associata la VM.

Selezionando il gruppo ‘_ASUGI TESI SGISO’, successivamente cliccando su ‘Visualizza membri’ sarà possibile visualizzare l’elenco delle VM associate al gruppo:



The screenshot shows a list of VMs associated with the group '_ASUGI TESI SGISO'. The list includes:

- Macchine virtuali (3)
- Indirizzi IP (5)
- Segmenti NSX (0)
- Porte segmenti (3)
- VIF (3)

On the right, there is a table with the following data:

Nome
c\$asugi30
c\$asugi31
c\$asugi32

At the bottom right of the table, it says '1-3 di 3'.

Figura 85 - VMWare NSX – VM associate al gruppo

Selezionando il gruppo '_ASUGI TESI SGISO', cliccando su modifica e poi, cliccando su 'Criteri', sarà possibile visualizzare i criteri di associazione:

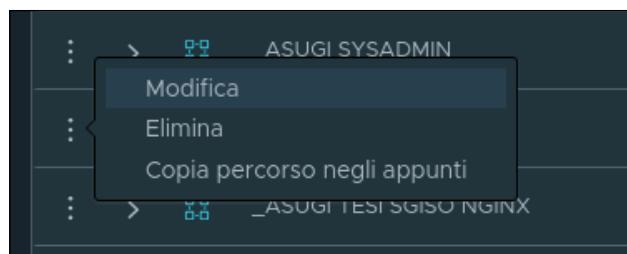


Figura 86 - VMWare NSX – Modifica gruppo



The dialog box shows the following fields:

- Nome:** _ASUGI TESI SGISO
- Descrizione:** Generico
- 1 criteri**
- Tag:** Tag (button) + Ambito (button)
- E consente un massimo di 30. Fare clic su (+) per aggiungere.
- SALVA** **ANNULLA**

Figura 87 - VMWare NSX - Dettaglio modifica gruppo

Nello specifico il criterio di appartenenza al gruppo è l'associazione ad uno specifico tag:



Figura 88 - VMWare NSX - Criterio gruppo

Nel caso specifico, il criterio di associazione è che le VM abbiano il tag 'TESI_SGISO'.

5.4.1.1.9.3. PROFILI

5.4.1.1.9.4. MACCHINE VIRTUALI

Alcuni tag rilevanti sono:

- VPN-DESTINATION: per le VM che hanno necessità di essere raggiunte da VPN
- Domain Members: per le VM che hanno necessità di essere collegate al dominio
- INTERNAL: per le VM che hanno necessità di accedere a servizi quali l'antivirus
- BS_asugi: assegnata di default
- TEN_sanita: assegnata di default

5.5. PROCESSO DI CREAZIONE VM

Di seguito verranno descritti i passaggi propedeutici per la creazione di una nuova VM.

5.5.1. CREAZIONE VM

5.5.1.1. ACCESSO A CLOUD MANAGER

Per l'accesso al cloud manager, procedere con:

- Accesso al cloud INSIEL ([PAR. 5.2.1](#)).
- Accesso al cloud manager ([PAR 5.2.2.1.1](#)).

5.5.1.2. SELEZIONE SISTEMA OPERATIVO

La selezione del sistema operativo per la nuova VM è descritta al [PAR. 5.2.2.1.3](#).

5.5.1.3. SELEZIONE T-SHIRT

La selezione delle risorse computazionali (CPU e RAM) per la nuova VM è descritta al [PAR. 5.2.2.1.3.1](#).

5.5.1.4. VERIFICA CAPIENZA

È possibile che non siano disponibili le risorse computazionali richieste per la nuova VM, tale informazione è reperibile come descritto al [PAR. 5.2.2.1.3.1](#).

5.5.1.5. DISCHI AGGIUNTIVI

È possibile che oltre al disco di sistema, per la VM vengano richiesti dischi aggiuntivi, è possibile aggiungerne in fase di creazione della VM come descritto al [PAR. 5.2.2.1.3.1](#), o dal menu contestuale relativo alla VM in una fase successiva, previo spegnimento della VM, descritto al [PAR. 5.2.2.1.4.3](#).

5.5.1.6. ESPANSIONE DISCO DI SISTEMA

In fase di creazione della VM il disco di sistema viene creato con una dimensione prestabilita e non modificabile, è comunque possibile espanderlo (ma non diminuirlo) successivamente, previo spegnimento della VM utilizzando le funzionalità del menu contestuale descritto al [PAR. 5.2.2.1.4.3](#). Si tenga presente che è poi necessario espandere manualmente il file system della VM in modo tale che occupi tutto lo spazio disponibile su disco.

5.5.1.7. CAMBIO DENOMINAZIONE VM

Dopo la creazione della VM è necessario procedere alla modifica della denominazione della stessa secondo i criteri stabiliti da ASUGI, come descritto nel [PAR 5.2.2.1.4.1](#).

5.5.1.8. PRIMO ACCESSO ALLA VM

Infine, è possibile verificare la corretta creazione della VM accedendovi da console, utilizzando il menu contestuale, come descritto nel [PAR. 5.2.2.1.4.3](#).

5.5.2. REGOLE FIREWALL

Dopo la creazione della VM è necessario procedere alla configurazione delle regole firewall secondo le necessità degli utenti della VM stessa.

5.5.2.1. ACCESSO A NSX

Per l'accesso al cloud firewall, procedere con:

- Accesso al cloud INSIEL ([PAR. 5.2.1](#)).
- Accesso al cloud firewall ([PAR 5.2.2.2.1](#)).

5.5.2.2. CONFIGURAZIONE REGOLE

5.5.2.3. PROBLEMI DI RETE

5.5.3. CONFIGURAZIONE VM

5.5.3.1. MODIFICA NOME HOST

Il nome host della VM deve essere coerente e identico al nome attribuito alla VM nel [PAR 5.3.1.7](#). Le modalità variano a seconda del sistema operativo installato.

5.5.3.1.1. MICROSOFT WINDOWS SERVER

5.5.3.1.2. LINUX

5.5.3.2. AGGIUNTA A DOMINIO

5.5.3.3. ESPANSIONE DISCO DI SISTEMA

5.5.3.4. AGGIORNAMENTO SISTEMA OPERATIVO

5.5.3.4.1. VERIFICA SU CONSOLE WSUS

5.5.3.4.2. AGGIORNAMENTO E PATCHING

5.5.3.5. INSTALLAZIONE ANTIVIRUS

5.5.3.5.1. VERIFICA FUNZIONAMENTO SU CONSOLE ANTIVIRUS

5.5.4.

6. APPENDICE 1 – CRITERI DI ASSEGNAZIONE DEGLI INDIRIZZI IP

6.1. SEGMENTI DI RETE

Nello IaaS INSIEL sono presenti: due segmenti di rete:

- **asugi** - 10.128.188.0 /22: Segmento di rete di produzione.
- **test-asugi** - 10.128.186.0 /24: Segmento di rete per attività di test.

Nello IaaS INSIEL, vengono create macchine virtuali che possiamo suddividere in tre macrocategorie:

- Server in dominio per servizi dedicati ai PC e/o dispositivi medici.
- Server per servizi dedicati alla gestione della rete (in dominio e non).
- Server non in dominio.

Queste tre tipologie di macchine devono essere raggiunte da sorgenti diverse e devono raggiungere destinazioni diverse, motivo per cui si è deciso di dividere virtualmente il segmento in produzione in modo da agevolare la creazione di regole di firewalling sulle macchine Fortigate. Per creare le regole lato Fortigate si è scelto di usare oggetti Address di tipo “IP RANGE” ovvero intervalli di indirizzi contigui di una rete, soluzione più coerente con le logiche di NSX, rispetto ad un più tradizionale subnetting.

6.2. RANGE DI IP DEDICATI PER TIPOLOGIA DI SERVIZIO

- **Server in dominio per servizi dedicati ai PC e/o dispositivi medici:**
 - IP Range: 10.128.188.2 - 10.128.189.255
- **Server per servizi dedicati alla gestione della rete (in dominio e non):**
 - IP Range: 10.128.190.0 - 10.128.190.127
- **Server non in dominio:**
 - IP Range: 10.128.190.128 - 10.128.190.254

IP iniziale	IP finale	Utilizzo
10.128.188.0	10.128.189.255	Server in dominio AOUTS
10.128.190.0	10.128.190.255	Libero
10.128.191.0	10.128.191.127	Server Management rete
10.128.191.128	10.128.191.254	Server non in dominio

7. APPENDICE 2 – NAMING CONVENTION

7.1. NOMI MACCHINE VIRTUALI

Analogamente a quanto previsto per le sedi di Maggiore e Cattinara, useremo la seguente sintassi: **0Innnnn**.

Es.: **0I0000**

7.2. NOMI GRUPPI

Per i nomi dei gruppi valgono le seguenti regole:

- Se il criterio di appartenenza al gruppo è una subnet, allora si userà la sintassi:
 - **_ASUGI [NOME SEDE]_[NOME RETE_INDIRIZZO DI RETE]_M[CIDR]**
 - Es.: **_ASUGI MAGGIORE_VLAN600_10.19.48.0_M20**
- Per tutti gli altri gruppi si userà la sintassi:
 - **_ASUGI [NOME SERVIZIO]**
 - Es.: **_ASUGI INTERNAL**
 -

L'underscore all'inizio serve solo per ordinare gli oggetti, mettendo in cima gli oggetti creati da noi.

8. GESTIONE DELLA DOCUMENTAZIONE

Nel presente documento andranno aggiornati al variare degli stessi i seguenti dati:

- Le versioni degli apparati utilizzati.
- La documentazione esterna relativa agli apparati utilizzati.
- I riferimenti alle persone da contattare in caso di problemi ed anomalie.
- Ogni altro elemento dovesse essere modificato nel tempo.

9. RIFERIMENTI (NORMATIVI E BIBLIOGRAFICI)

9.1. VMWARE VSphere

- [HTTPS://WWW.VMWARE.COM/PRODUCTS/CLOUD-INFRASTRUCTURE/VSHERE](https://www.vmware.com/products/cloud-infrastructure/vsphere)
- [HTTPS://DOCS.VMWARE.COM/IT/VMWARE-VSPHERE/INDEX.HTML](https://docs.vmware.com/it/vmware-vsphere/index.html)

9.2. VMWARE NSX

- [HTTPS://WWW.VMWARE.COM/PRODUCTS/CLOUD-INFRASTRUCTURE/NSX](https://www.vmware.com/products/cloud-infrastructure/nsx)
- [HTTPS://DOCS.VMWARE.COM/IT/VMWARE-NSX/INDEX.HTML](https://docs.vmware.com/it/vmware-nsx/index.html)

9.3. VMWARE ARIA

- [HTTPS://DOCS.VMWARE.COM/IT/VMWARE-ARIA-AUTOMATION/SAAS/GETTING-STARTED-VMWARE-ARIA-AUTOMATION/GUID-9171B94B-EC18-44A3-A29E-CB4AF05BE284.HTML](https://docs.vmware.com/it/vmware-aria-automation/saas/getting-started-vmware-aria-automation/guid-9171b94b-ec18-44a3-a29e-cb4af05be284.html)

- [HTTPS://DOCS.VMWARE.COM/IT/VMWARE-ARIA-AUTOMATION/INDEX.HTML](https://docs.vmware.com/it/vmware-aria-automation/index.html)

10. DOCUMENTI COLLEGATI

- [HTTPS://WIKI.AOUTS.IT/DOKU.PHP?ID=DOCUMENTAZIONE:IAAS_INSIEL](https://wiki.aouts.it/doku.php?id=documentazione:iaas_insiel)

11. ALLEGATI (SE PRESENTI)

- Nessuno



12. INDICE DELLE FIGURE

<u>FIGURA 1 - VMWARE VSphere</u>	6
<u>FIGURA 2 - VMWARE NSX – ARCHITETTURA</u>	7
<u>FIGURA 3 - VMWARE ARIA</u>	8
<u>FIGURA 4 - INFRASTRUTTURA FISICA CLOUD INSIEL</u>	9
<u>FIGURA 5 - TIER 1 GATEWAYS SU NSX</u>	10
<u>FIGURA 6 - INFRASTRUTTURA LOGICA CLOUD INSIEL</u>	10
<u>FIGURA 7 - ACCESSO AL CLOUD INSIEL – INSERIMENTO USER NAME</u>	11
<u>FIGURA 8 - ACCESSO AL CLOUD INSIEL - INSERIMENTO PASSWORD</u>	12
<u>FIGURA 9 - CLOUD INSIEL - SCHERMATA PRINCIPALE</u>	12
<u>FIGURA 10 - RICHIESTA CREDENZIALI INSIEL</u>	13
<u>FIGURA 11 - CAMBIO PASSWORD INSIEL</u>	14
<u>FIGURA 12 - CLOUD INSIEL - PAGINA DI LOGIN ERRATA</u>	15
<u>FIGURA 13 - TASTO 'CLOUD MANAGER'</u>	16
<u>FIGURA 14 - ACCESSO A CLOUD FIREWALL</u>	16
<u>FIGURA 15 - ACCESSO A SERVICE BROKER</u>	16
<u>FIGURA 16 - SERVICE BROKER</u>	17
<u>FIGURA 17 - CATALOG</u>	18
<u>FIGURA 18 - NEW REQUEST</u>	19
<u>FIGURA 19 – T-SHIRT SIZE</u>	20
<u>FIGURA 20 – DISCHI AGGIUNTIVI</u>	21
<u>FIGURA 21 – NEW REQUEST COMPIUTA</u>	21
<u>FIGURA 22 – RISORSE COMPUTAZIONALI</u>	22
<u>FIGURA 23 – DEPLOYMENTS MENU</u>	22
<u>FIGURA 24 – DEPLOYMENTS</u>	22
<u>FIGURA 25 – DEPLOYMENT – STATUS</u>	23
<u>FIGURA 26 – DEPLOYMENT – DETTAGLI</u>	23
<u>FIGURA 27 – DEPLOYMENT – MENU CONTESTUALE</u>	24
<u>FIGURA 28 – DEPLOYMENT – EDIT</u>	24
<u>FIGURA 29 – DEPLOYMENT – DETTAGLIO</u>	25
<u>FIGURA 30 – DEPLOYMENT – DETTAGLIO - TOPOLOGY</u>	26
<u>FIGURA 31 – DEPLOYMENT – DETTAGLIO – HISTORY (DURANTE LA CREAZIONE DELLA VM)</u>	26
<u>FIGURA 32 – DEPLOYMENT – DETTAGLIO – HISTORY (DOPO LA CREAZIONE DELLA VM)</u>	26
<u>FIGURA 33 – DEPLOYMENT – DETTAGLIO – USER EVENTS</u>	26
<u>FIGURA 34 – DEPLOYMENT – MONITOR (DURANTE LA CREAZIONE DELLA VM)</u>	27
<u>FIGURA 35 – DEPLOYMENT – MONITOR (DOPO LA CREAZIONE DELLA VM)</u>	27
<u>FIGURA 36 – DEPLOYMENT – ALERTS</u>	27
<u>FIGURA 37 – DEPLOYMENT – OPTIMIZE (DURANTE LA CREAZIONE DELLA VM)</u>	27
<u>FIGURA 38 – DEPLOYMENT – OPTIMIZE (DOPO LA CREAZIONE DELLA VM)</u>	28
<u>FIGURA 39 – RESOURCES - DEPLOYMENT</u>	29
<u>FIGURA 40 – RESOURCES – DEPLOYMENT - DETTAGLI</u>	29
<u>FIGURA 41 – RESOURCES – TUTTE LE RISORSE</u>	29
<u>FIGURA 42 – RESOURCES – FILTRO RISORSE</u>	30
<u>FIGURA 43 – RESOURCES – MENU CONTESTUALE</u>	30
<u>FIGURA 44 – VIRTUAL MACHINES – CREAZIONE NUOVA VM</u>	31
<u>FIGURA 45 – VIRTUAL MACHINES – CREAZIONE NUOVA VM – DETTAGLI</u>	31
<u>FIGURA 46 – VIRTUAL MACHINES – ELENCO VM</u>	31

<u>FIGURA 47 – VIRTUAL MACHINES – DETTAGLIO VM</u>	32
<u>FIGURA 48 – VIRTUAL MACHINES – MENU CONTESTUALE #1</u>	33
<u>FIGURA 49 – VIRTUAL MACHINES – MENU CONTESTUALE #2</u>	33
<u>FIGURA 50 – VIRTUAL MACHINES – RESIZE BOOT DISK</u>	34
<u>FIGURA 51 – VOLUMES</u>	35
<u>FIGURA 52 – VOLUMES - DETTAGLIO VOLUME</u>	36
<u>FIGURA 53 - VOLUMES - MENU CONTESTUALE</u>	36
<u>FIGURA 54 - NETWORKING & SECURITY</u>	37
<u>FIGURA 55 - NETWORKING & SECURITY – DETTAGLI</u>	38
<u>FIGURA 56 - NETWORKING & SECURITY - MENU CONTESTUALE</u>	38
<u>FIGURA 57 - TASTO 'CLOUD FIREWALL'</u>	39
<u>FIGURA 58 - ACCESSO A CLOUD FIREWALL</u>	39
<u>FIGURA 59 - VMWARE NSX – HOME - PANORAMICA</u>	40
<u>FIGURA 60 - VMWARE NSX – HOME – AVVISI</u>	41
<u>FIGURA 61 - VMWARE NSX – HOME – DEFINIZIONE AVVISI</u>	41
<u>FIGURA 62 - VMWARE NSX – RETE</u>	42
<u>FIGURA 63 - VMWARE NSX – RETE – PANORAMICA DELLA RETE</u>	42
<u>FIGURA 64 - VMWARE NSX – RETE – GATEWAY DI LIVELLO 1</u>	43
<u>FIGURA 65 - VMWARE NSX – RETE – SEGMENTI – NSX</u>	44
<u>FIGURA 66 - VMWARE NSX – RETE – SEGMENTI – PROFILI</u>	45
<u>FIGURA 67 - VMWARE NSX – RETE – SEGMENTI – PROFILI – TIPO PROFILI</u>	46
<u>FIGURA 68 - VMWARE NSX – RETE – NAT</u>	47
<u>FIGURA 69 - VMWARE NSX – RETE – NAT – CONFIGURAZIONE</u>	48
<u>FIGURA 70 - VMWARE NSX - SICUREZZA</u>	48
<u>FIGURA 71 - VMWARE NSX - SICUREZZA -FIREWALL GATEWAY</u>	49
<u>FIGURA 72 - VMWARE NSX - FIREWALL DISTRIBUITO</u>	49
<u>FIGURA 73 - VMWARE NSX - DETTAGLIO REGOLA FIREWALL</u>	50
<u>FIGURA 74 - VMWARE NSX - OPERAZIONI SUI CRITERI</u>	50
<u>FIGURA 75 - VMWARE NSX - OPERAZIONI SULLE REGOLE</u>	50
<u>FIGURA 76 - VMWARE NSX - NUOVO CRITERIO</u>	51
<u>FIGURA 77 - VMWARE NSX – NUOVA REGOLA FIREWALL</u>	51
<u>FIGURA 78 - VMWARE NSX – INVENTARIO</u>	52
<u>FIGURA 79 - VMWARE NSX- SERVIZI</u>	53
<u>FIGURA 80 - VMWARE NSX - SERVIZI - DETTAGLIO SERVIZIO</u>	53
<u>FIGURA 81 - VMWARE NSX - SERVIZI – OPERAZIONI SUI SERVIZI</u>	53
<u>FIGURA 82 - VMWARE NSX - SERVIZI - CREAZIONE DI UN NUOVO SERVIZIO.</u>	54
<u>FIGURA 83 - VMWARE NSX - SERVIZI - CREAZIONE DI UN NUOVO SINGOLO SERVIZIO.</u>	54
<u>FIGURA 84 - VMWARE NSX – GRUPPI</u>	55
<u>FIGURA 85 - VMWARE NSX – VM ASSOCIATE AL GRUPPO</u>	55
<u>FIGURA 86 - VMWARE NSX - MODIFICA GRUPPO</u>	55
<u>FIGURA 87 - VMWARE NSX - DETTAGLIO MODIFICA GRUPPO</u>	56
<u>FIGURA 88 - VMWARE NSX - CRITERIO GRUPPO</u>	56

