Servizi Cloud – InnovaPuglia S.p.A.

Guida alle funzionalità del portale Cloud

“VMware vRealize Automation 7”

Versione	**2.00**
Data	**Gennaio 2023**
Cod.Rif:	**PRQSIguida-port-cloud**

Sommario

Indice delle tabelle e delle figure

1) Diritti di Autore e Clausole di Riservatezza

La proprietà del presente documento è di InnovaPuglia S.p.A. e della Regione Puglia. Tutti i diritti sono riservati.

A norma della legge sul diritto d'autore e del Codice civile è vietata la riproduzione di questo scritto o di parte di esso con qualsiasi mezzo elettronico, meccanico, per mezzo di fotocopie, microfilm, registratori ed altro, salvo per quanto espressamente autorizzato.

2) Storia del Documento

Versione	Modifiche	Data
1.00	Prima redazione	27/04/2022
2.00	Revisione	07/11/2022
2.01	Revisione	25/11/2022

3) Acronimi e Definizioni

SDDC: Software-Defined Data Center è una struttura di archiviazione dei dati in cui tutti gli elementi dell'infrastruttura sono virtualizzati e forniti come servizio.

vRA: VMware vRealize Automation è la piattaforma di automazione dei processi di distribuzione dei servizi IT (infrastruttura, container, applicazioni e qualsiasi altro servizio IT).

Business Group: l'unità minima di Servizio Cloud, consistente in risorse computazionali, spazio disco di archiviazione e risorse di rete/connettività e sicurezza.

Blueprint: è il workflow utilizzato per eseguire il provisioning di una Virtual Machine o Virtual Datacenter, contenente le specifiche dei server, quali CPU, RAM, storage, connettività.

Deploy: attività di rilascio di una o più Virtual Machine con sistema operativo preinstallato.

BaaS: Backup as a Service è la funzionalità che permette di effettuare backup basati su immagini remotizzate delle proprie macchine virtuali e lavora a stretto contatto con l'Hypervisor di virtualizzazione (VMware), evitando di dover installare Agent di connessione a bordo delle VM da proteggere.

Security Group: è il Gruppo di sicurezza a cui appartiene una VM. I Security Group che classificano tutte le VM sono: WS (Web Server), AS (Application Server), DB (Database).

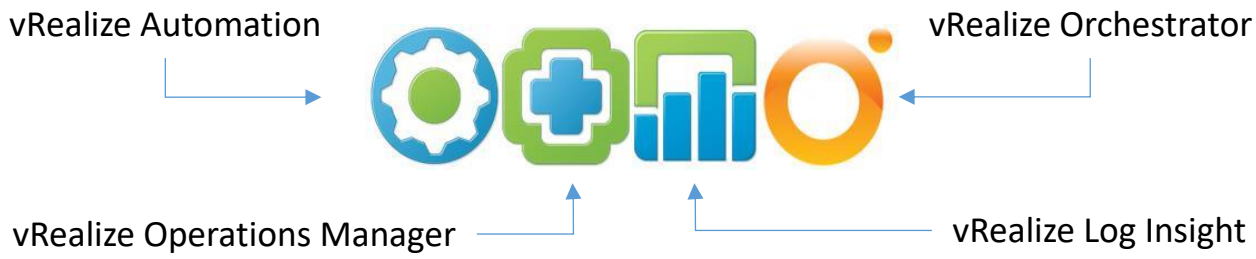
4) Premessa

InnovaPuglia eroga Servizi Cloud agli Enti pubblici regionali su incarico della Regione Puglia, definiti in questo documento come *Enti Richiedenti*, attraverso la piattaforma di cloud computing InnovaCLOUD.

La piattaforma permette la creazione e la gestione autonoma da parte dell'utente di Virtual Machine (VM) o di un Virtual Datacenter agendo sulle risorse disponibili all'interno di un pool che comprendono: Virtual CPU, vRAM, spazio Storage, nei limiti dei massimali delle risorse contrattualizzate. Le VM saranno create da un template di base e scelte da un catalogo.

L'utente potrà inoltre gestire autonomamente le politiche di Firewalling e di Network Load Balancing delle VM. Sono disponibili i servizi correlati di BaaS per la protezione delle VM e di Virtual Storage per la fruizione di Storage di tipo NFS/CIFS delle Virtual Machine.

Il presente documento ha lo scopo di agevolare l'utilizzo della piattaforma InnovaCLOUD basata sulla soluzione SDDC - VMware vRealize Suite.



5) I ruoli degli utenti

L'accesso al portale InnovaCLOUD sarà reso possibile attraverso una piattaforma web. Di seguito sono riportati i ruoli assegnati alle categorie di utenti che possono accedere al portale, riconducibili alle figure amministrative che ricoprono:

- **Amministratore Interno**: è la persona fisica incaricata/delegata dall'Ente di richiedere ad InnovaPuglia i Servizi Cloud e di nominare gli Amministratori Operativi/Tecnici dei singoli Business Group. Può inviare, per conto dell'Ente richiedente, il Modulo tecnico 05 di richiesta dei servizi cloud (Business Group) e più specificatamente può:
  - Richiedere nuove risorse cloud
  - Inoltrare modifiche di configurazione delle risorse cloud assegnate.
- **Amministratore Operativo**: è l'account assegnato ad una persona fisica che gestisce tecnicamente i Business Group e più specificatamente può:
  - Richiedere con il Modulo 04 la creazione/modifica/cancellazione degli account assegnati agli Amministratori Tecnici.
- **Amministratore Tecnico:** è l'account assegnato ad una persona fisica che ha accesso e gestisce le risorse del Business Group e più specificatamente può:
  - Accedere al *Catalogo* del portale vRA 7 per il deploy e la creazione delle VM
  - Accedere alle *Distribuzioni* per la visualizzazione e gestione delle VM facenti parte dei Business Group
  - Gestire in autonomia le regole di sicurezza tra i Security Group di un Business Group
  - Attivare/Disattivare il Servizio di "Backup as a Service" determinandone le policy temporali.

6) Il portale vRA 7 - CLOUD

Per accedere alla piattaforma InnovaCLOUD è sufficiente collegarsi all'URL https://vra7-cloud.innova.puglia.it, selezionare il dominio di autenticazione "*incloud.innova.puglia.it*" e quindi inserire le credenziali ricevute successivamente alla fase di accreditamento (così come previsto dal regolamento di erogazione dei servizi cloud).

Il form di login permette anche di effettuare in autonomia il reset della password cliccando sull'apposito link: *Password dimenticata?*.

NOTA: prima di effettuare la richiesta di reset password attraverso la funzionalità "Password dimenticata?" è importante selezionare prima il corretto dominio di autenticazione "incloud.innova.puglia.it".

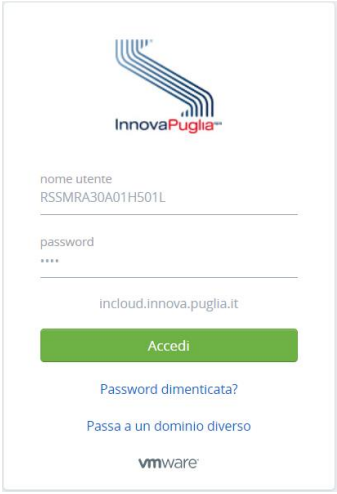


Figura 1: Form di login e reset password

Gli utenti autorizzati alla creazione e alla gestione delle risorse dei Business Group, di seguito denominati Amministratori Tecnici, hanno a disposizione, dopo la login, due sezioni principali:

- *Catalogo*
- *Distribuzioni*.

6.1 CATALOGO

All'interno della sezione *Catalogo* del portale vRA 7 sono visualizzabili tutti i Blueprint per il deploy e la creazione delle VM, secondo le specifiche fornite nell'excel "05 - Modulo tecnico di richiesta servizi cloud".

Il nome del Blueprint, uno o più di uno per ciascun Business Group, è comunicato da InnovaPuglia all'Amministratore Operativo in fase di consegna delle risorse.

Figura 2: Esempio di Blueprint e progettazione

Ogni Amministratore tecnico, in base ai propri privilegi, potrà visualizzare uno o più Blueprint con cui richiedere le VM, nei limiti delle risorse richieste.

Di seguito un esempio di Catalogo:

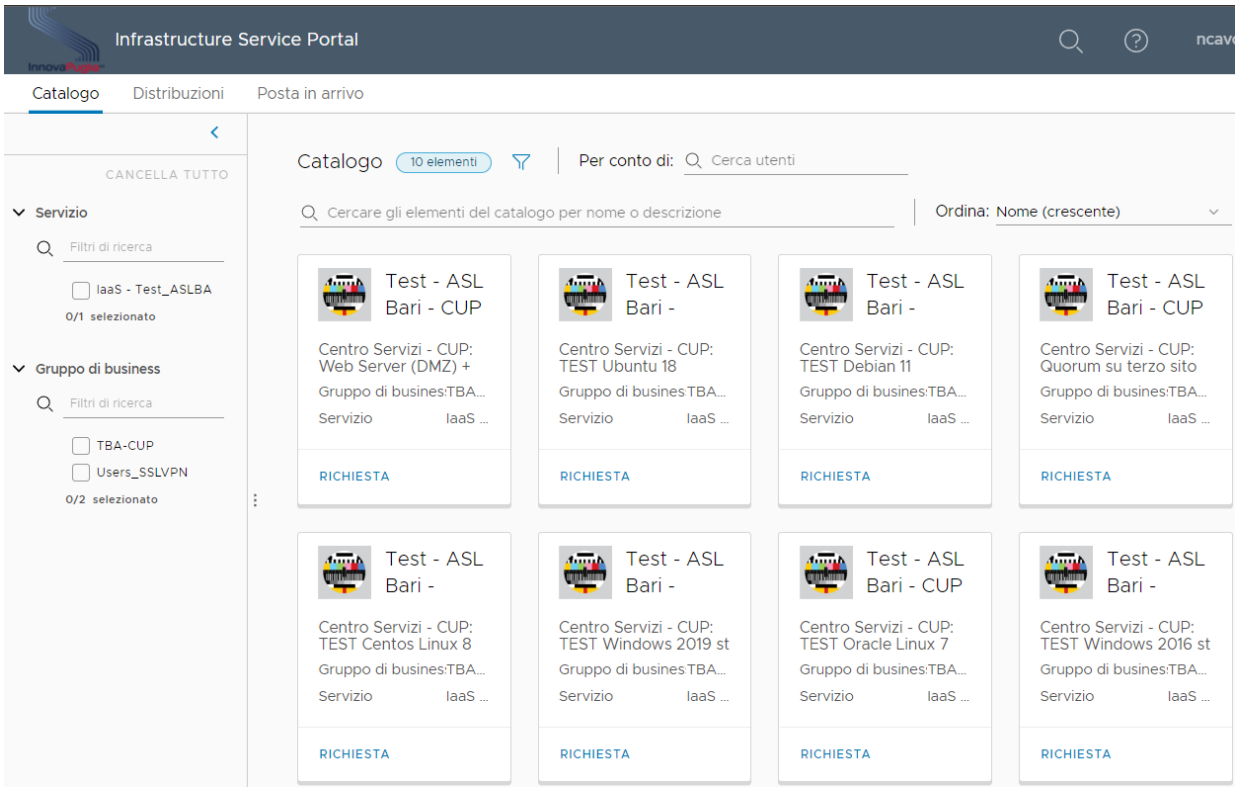


Figura 3: Esempio di Blueprint a Catalogo

Per creare le VM è sufficiente cliccare su "RICHIESTA". La videata successiva mostra l'elenco dei template da cui poter creare le VM:

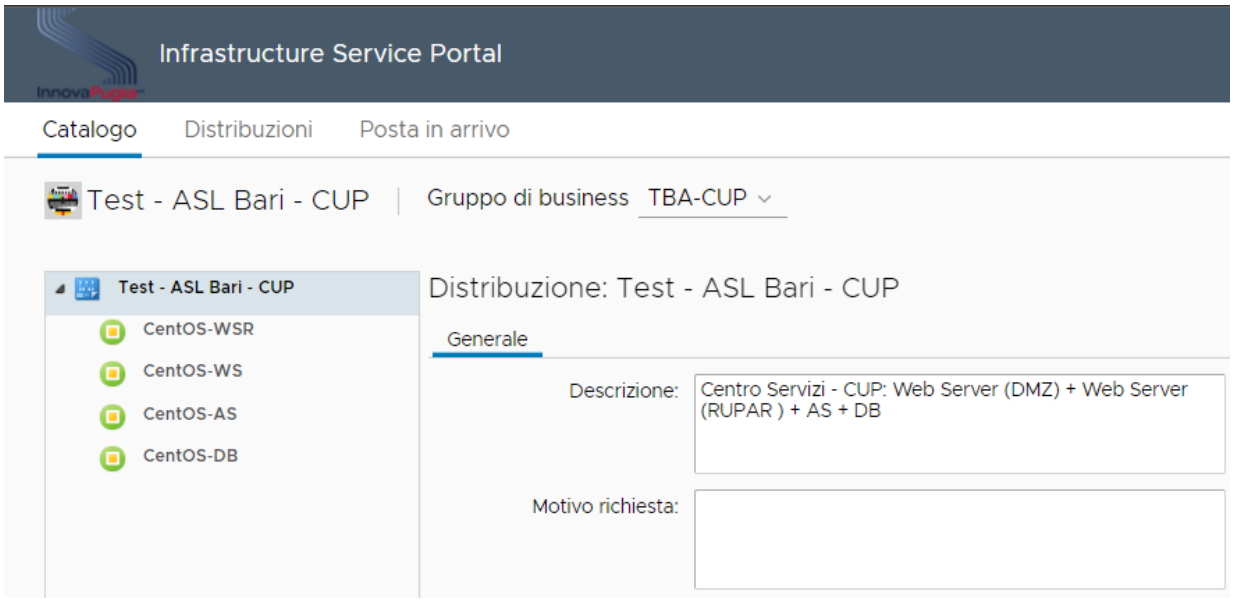


Figura 4: Form di richiesta Blueprint

Per ciascun template occorre impostare solo il numero di istanze (*quantità di VM da deployare*), **senza configurare CPU/ Memoria/ Storage**.

NOTA: al completamento del deploy sarà possibile riconfigurare ciascuna VM con le risorse richieste dal menu Distribuzioni.

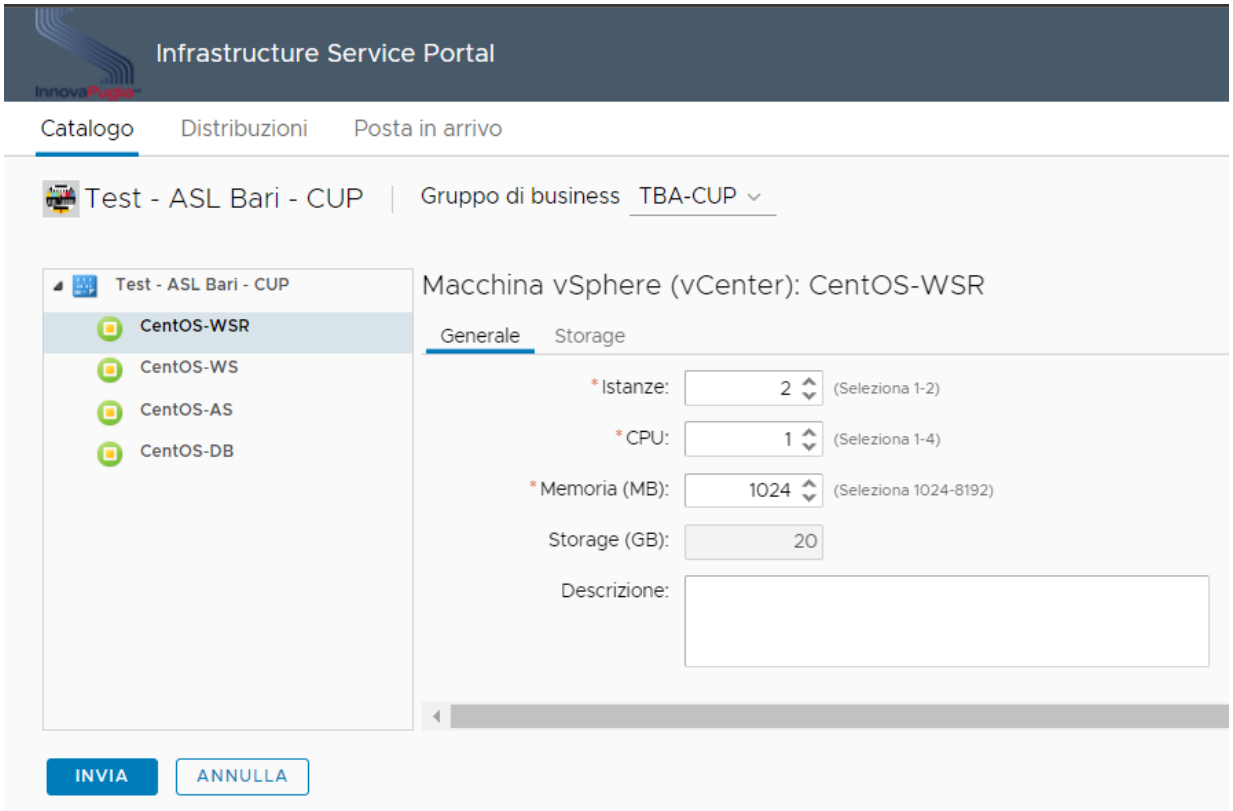


Figura 5: Form di personalizzazione Istanze

Dopo aver settato le istanze, è sufficiente cliccare su INVIA per dar seguito all'operazione di deploy. L'operazione di creazione delle VM è monitorabile all'interno del menù Distribuzioni, la cui durata varia in base alla tipologia delle VM (windows/linux) ed alla quantità delle stesse.

NOTA: qualora il numero delle istanze non fosse stato impostato correttamente, sarà possibile in seguito aggiungere la VM mancante utilizzando la funzionalità di Scalabilità Orizzontale, come riportato al paragrafo §6.2.1, senza dover richiedere l'intera distribuzione.

6.2 DISTRIBUZIONI

Nel menu Distribuzioni sono visualizzabili tutti i Deploy generati da Blueprint, e all'interno di ciascun Deploy sono visualizzabili e gestibili le VM facenti parte del Business Group.

Le VM richieste da Catalogo saranno automaticamente preconfigurate con:

1) Hostname;
2) FQDN (all'interno del dominio interno al Cloud vRA: in.cloud.innova.puglia.it);
3) IP/Subnet/Gateway;
4) DNS ed NTP.

Ogni VM sarà quindi subito raggiungibile dalla propria SSLVPN ed immediatamente operativa.

Le credenziali di default per l'accesso (con cambio obbligatorio al primo accesso) sono:

- SO Windows: administrator/password123!
- SO Linux: root/password123! (amministratore/password123!)

Di seguito un esempio di Distribuzioni:

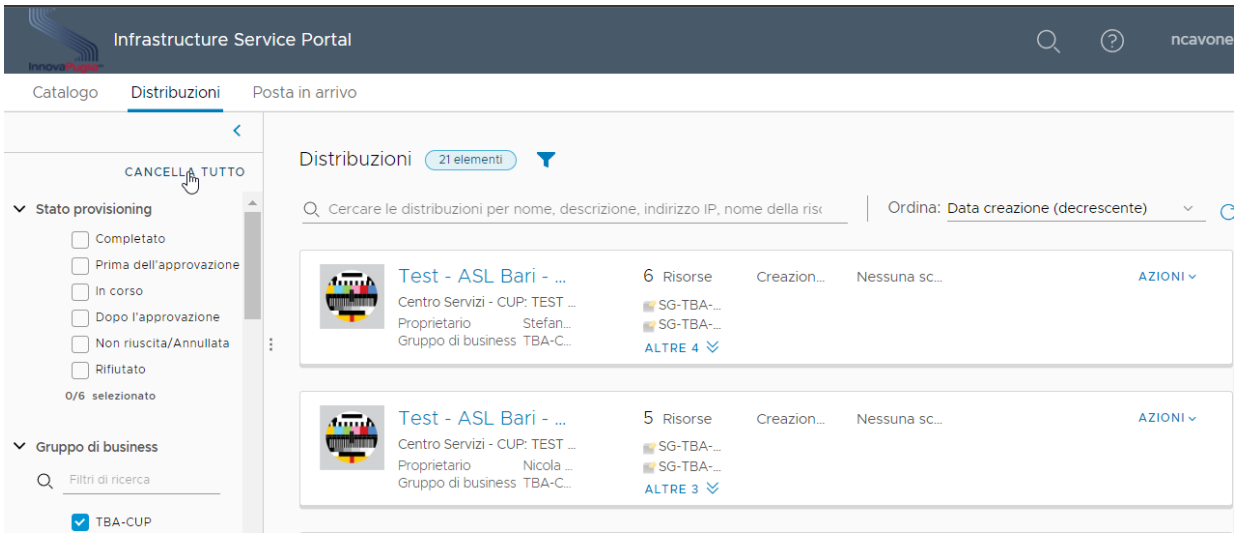


Figura 6: Esempio di menu Distribuzioni

ATTENZIONE: selezionando la voce di menu Distribuzioni, ogni utente visualizzerà soltanto le Distribuzioni da lui richieste/create; per poter visualizzare anche quelle su cui si è autorizzati ma che sono state create da altri utenti, è necessario impostare o cancellare il filtro sul proprio utente (così come rappresentato nella precedente - **Figura 6**).

6.2.1 DEPLOY

All'interno di ciascun Deploy, presente nel menu Distribuzioni, sono visualizzabili tre sezioni:

1. Info generali:
   - Nome e descrizione
   - Proprietario: chi ha effettuato la richiesta da Catalogo
   - Data provisioning: data in cui è stata effettuata la richiesta da Catalogo
   - Gruppo di business: nome del Business Group di appartenenza
   - Elemento del catalogo: nome dell'elemento a Catalogo da cui è stato generato il Deploy
   - Durata lease/scade/data eliminazione: eventuale data di eliminazione automatica del Deploy
2. Componenti / Cronologia / Monitoraggio
3. Menu azioni.

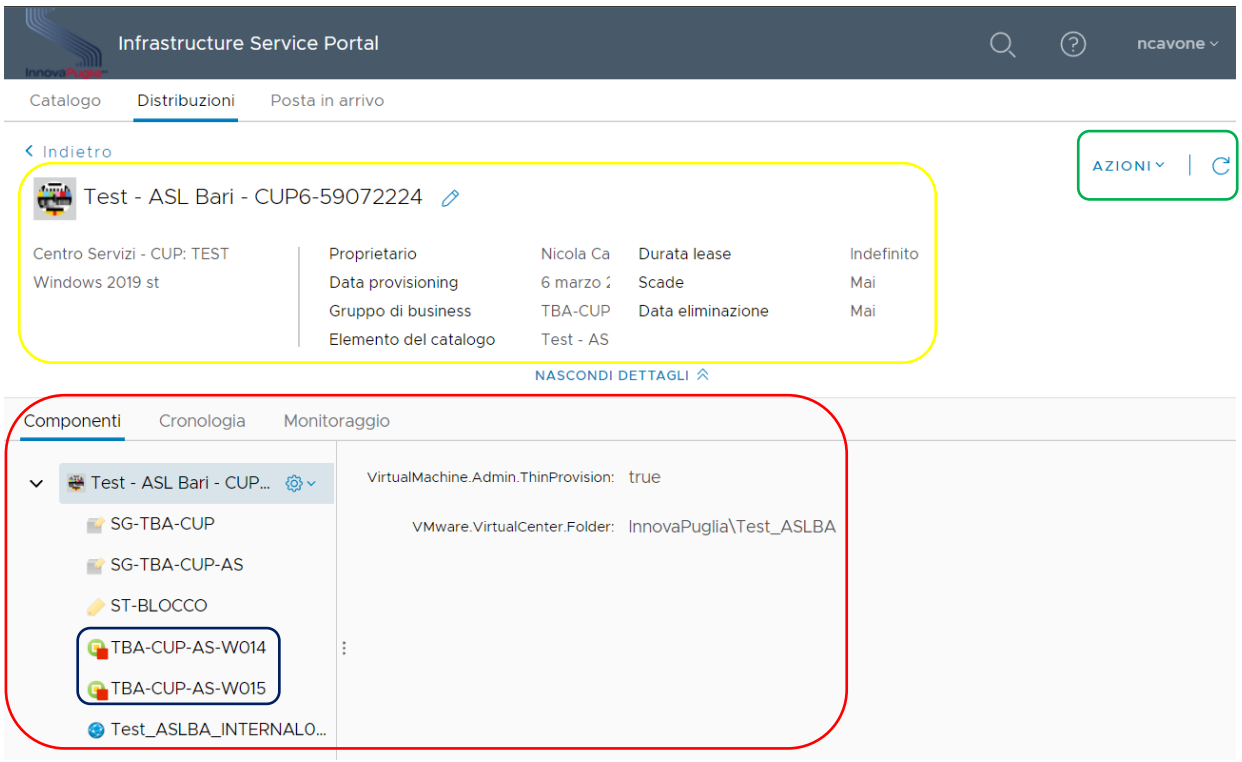


Figura 7: Esempio di Deploy

Per ogni VM all'interno di un Deploy sarà possibile eseguire una delle seguenti azioni:

- Attivare o disattivare un JOB di backup
- Eseguire un backup on-demand
- Eseguire un report che mostra i restore point di backup
- Restorare un'intera VM ad uno dei restore point disponibili
  Per le attività di backup fare riferimento al paragrafo 7
- Collegarsi alla console della VM
- Installare i VMware Tools
- Riconfigurare CPU/RAM/Disco nei limiti delle risorse disponibili per ogni Business Group
- Riavviare e fare lo Showdown della VM *(eseguibili solo se i VMTools sono correttamente installati e funzionanti)*
- Effettuare il Reset e lo Spegnimento della VM *(operazioni eseguibili anche senza VMTools)*
- Abilitare, bloccare o verificare l'apertura delle porte 80 e 443 (disponibile solo per le VM di tipo WS).

NOTA: Di default le VM di tipo Web Service hanno le porte 80 e 443 bloccate all'accesso da Internet/RUPAR. Le azioni Abilita/Blocca/Verifica 80-443 consentono la gestione degli accessi su tali porte.

Nel TAB Cronologia è possibile visualizzare il logging delle operazioni effettuate da ciascun utente autorizzato.

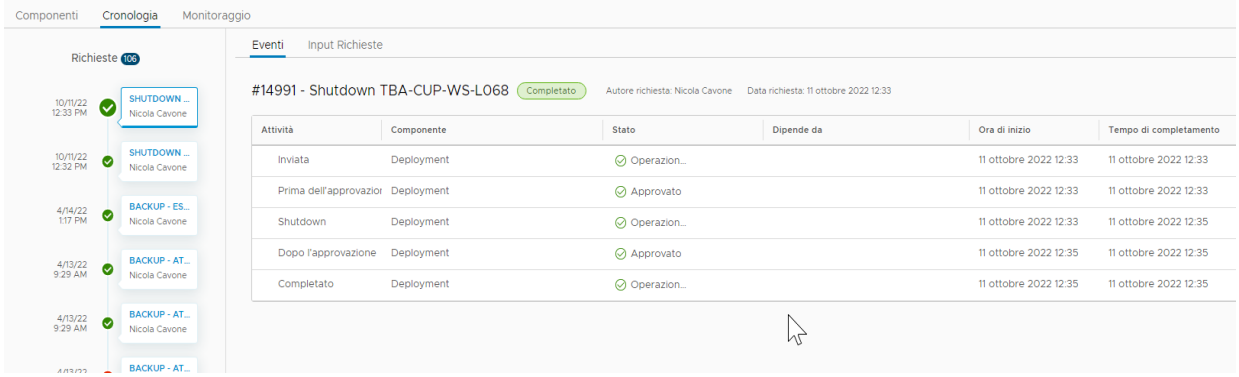


Figura 8: Esempio di monitoring delle operazioni effettuate

Nel TAB Monitoraggio è possibile visualizzare le metriche e i grafici relativi all'uso delle risorse nell'ultimo giorno, settimana o mese.

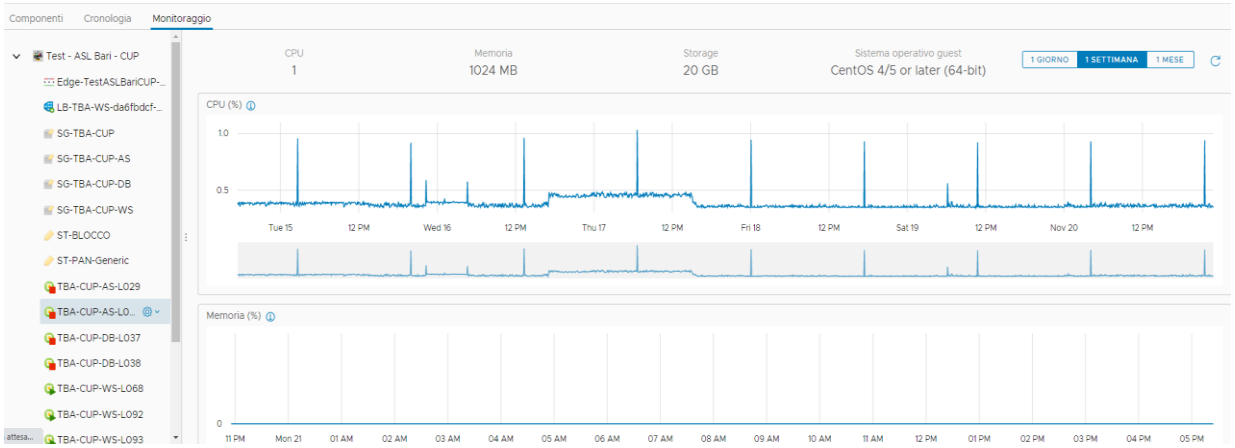


Figura 9: Esempio di monitoring del consumo di risorse

Per ogni Deploy sarà possibile dal Menu "Azioni":

- Utilizzare la funzionalità di Scalabilità orizzontale, cioè, aumentare la quantità di Istanze/VM nei limiti/quantità delle risorse assegnate al Business Group.

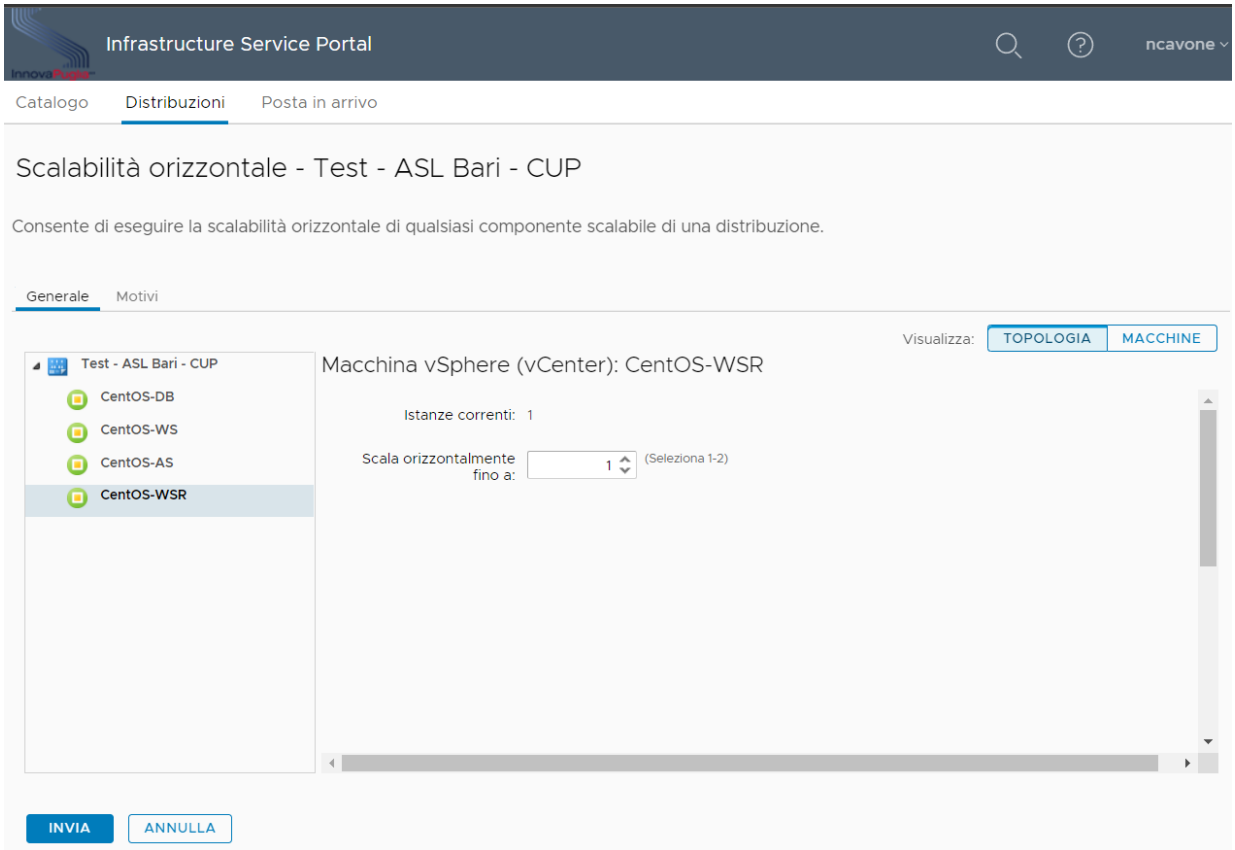


Figura 10: Funzionalità di Scalabilità orizzontale

7) vRA7 Cloud – Distributed Firewall NSX

Ogni VM di un Business Group appartiene ad almeno due «Security Group». Il Security Group è l'elemento minimo da specificare per richiedere le abilitazioni di rete all'interno del Cloud.

I Security Group NSX sono sempre 4 per ogni Business Group:

1. SG-TBA-CUP
   (tutte le VM del Business Group)
2. SG-TBA-CUP-WS
   (tutte le VM di tipo Web Server)
3. SG-TBA-CUP-AS
   (tutte le VM di tipo Application Server)
4. SG-TBA-CUP-DB
   (tutte le VM di tipo Database)

Esempio utilizzo dei Security Group nelle abilitazioni di sicurezza:

Descrizione	Sorgente	Destinazione	Servizio/Porta
Dettaglio regole firewall attive di Default:			
ANY to WS	any	SG-TBA-SIE-WS	tcp/80, tcp/443
Internet OUT	SG-TBA-SIE	any	tcp/80, tcp/443
DNS /NTP	SG-TBA-SIE	DNS-NTP_CLOUD	udp/53, tcp123
SSLVPN Management	TBA-SIE_SSLVPN	SG-TBA-SIE	any
WS to WS *	SG-TBA-SIE-WS	SG-TBA-SIE-WS	any
AS to AS *	SG-TBA-SIE-AS	SG-TBA-SIE-AS	any
DB to DB *	SG-TBA-SIE-DB	SG-TBA-SIE-DB	any
Dettaglio regole firewall da compilare in base alle proprie esigenze:			
AS to NFS	SG-TBA-SIE-AS	TBA_NFS-FAS9000	NFS-ServiceGroup
DB to NFS	SG-TBA-SIE-DB	TBA_NFS-FAS2720	NFS-ServiceGroup
WS to SMTP	SG-TBA-SIE-WS	142.250.147.109	tcp/465
AS to LDAP	SG-TBA-SIE-AS	210.2.1.30	tcp/636, tcp/389

Figura 11: Cloud Distributed Firewall Security Group

Tutte le policy di sicurezza interne al Business Group che coinvolgono i Security Group sono gestibili in autonomia dal portale Cloud utilizzando dal menu Catalogo il servizio: *Cloud – Firewall*, che permette di:

- Creare o modificare una regola di sicurezza tra i Security Group di un Business Group.
- Consultare le regole di sicurezza attive per un Business Group.

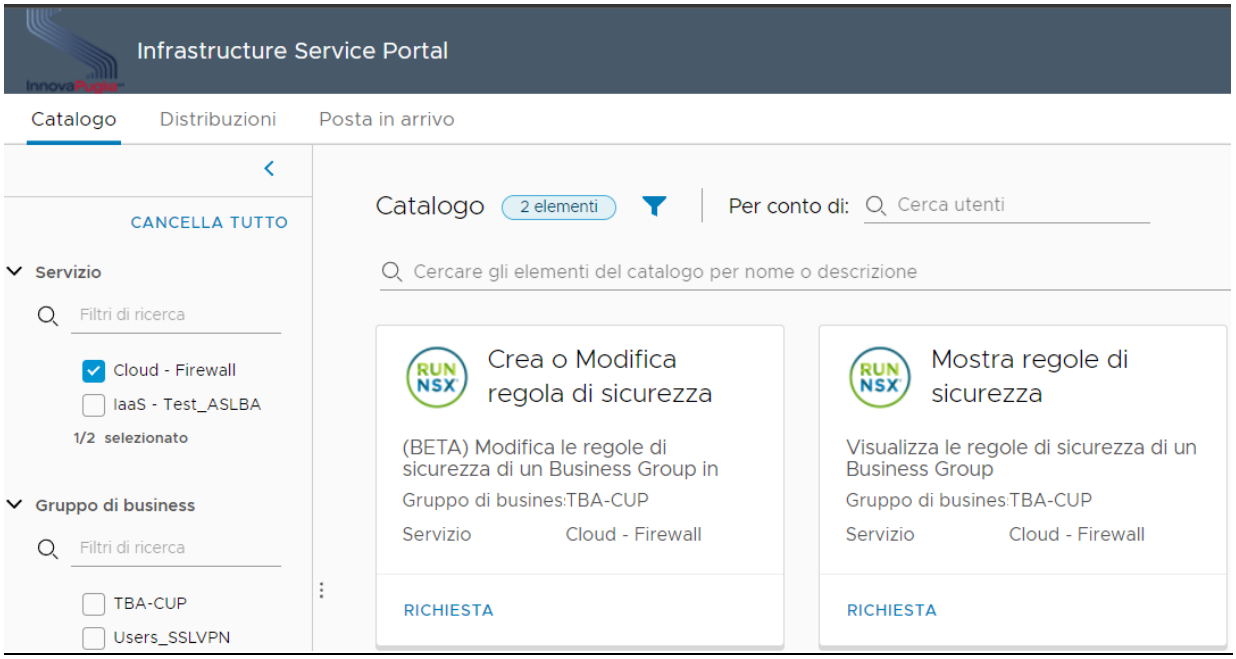


Figura 12: Cloud Distributed Firewall

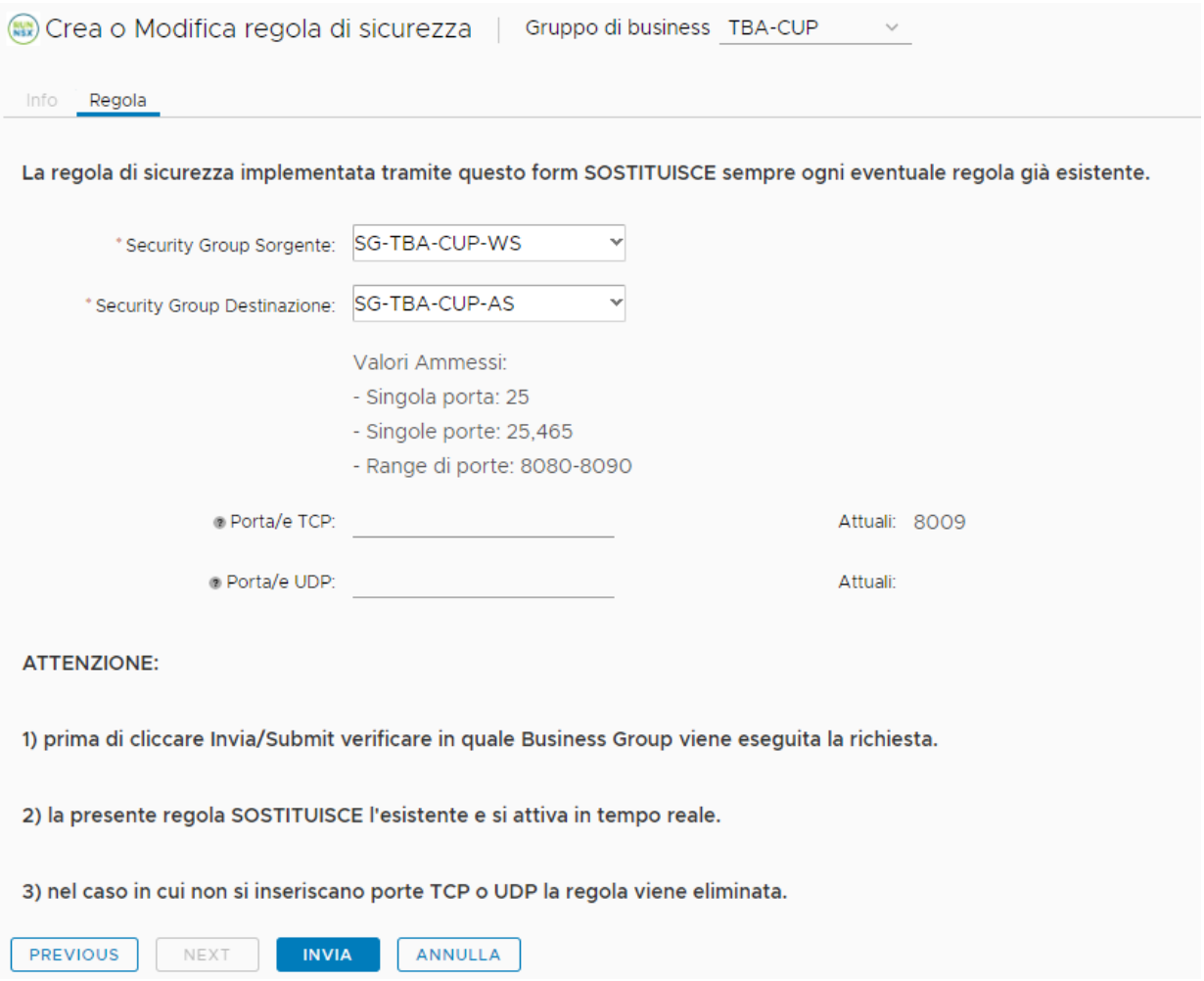


Figura 13: Creazione o modifica Regola di Sicurezza

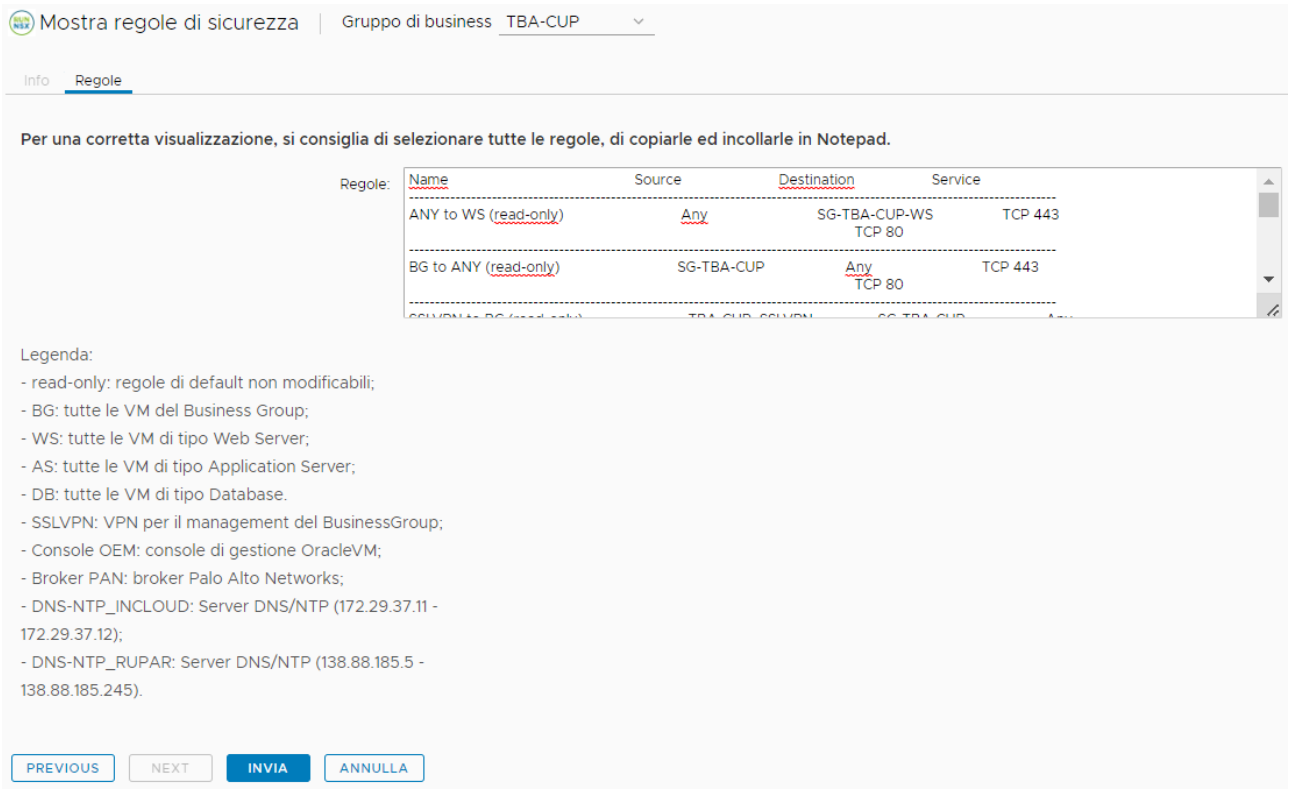


Figura 14: Mostra Regola di Sicurezza

8) Backup as a Service

Il servizio di Backup as a Service è un'opzione attivabile dall'Amministratore Tecnico per il backup delle macchine virtuali attivate sul portale vRA 7. L'Amministratore Tecnico può scegliere se attivare il backup sulle risorse selezionate e selezionare la policy più appropriata per il proprio servizio.

Tutti i backup attivati sono di tipo crash-consistent ed includono tutti i VMDK delle Virtual Machine ma non le Share NFS.

Nel caso di database o applicazioni che lo necessitano è consigliato un export consistente dei dati su storage esterno alla VM (Share NFS non in HA richiedibili utilizzando il modello 05).

Per attivare un job di backup scegliere l'azione "Backup – Attiva Job" tra le impostazioni di ciascuna macchina virtuale e selezionare la policy desiderata.

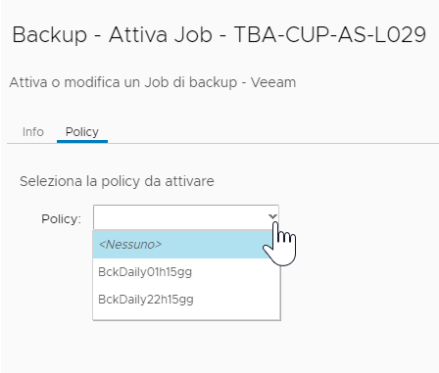


Figura 15: Schedulazione Job di Backup

Tutti i job schedulati per una virtual machine possono essere disattivati tramite l'azione "Backup – Disattiva Job".

L'attivazione del backup rende disponibili l'elenco dei restore point disponibili per ciascuna virtual machine nel caso di voglia ripristinare l'immagine di una VM ad una data specifica. Tale lista è visualizzabile utilizzando l'azione "Backup – Report Job".

L'azione "Backup – Restore VM Job" ripristina l'intera VM alla data del restore point scelto. La VM viene spenta, cancellata e quindi sostituita con il restore selezionato.

Figura 16: Restore Virtual Machine

Infine, è possibile eseguire un backup on-demand di una VM utilizzando l'azione "Backup – Esegui ora Job", ma solo dopo aver attivato i job di backup e solo dopo che il primo backup sia stato regolarmente eseguito.

9) SSLVPN

I server creati su vRA 7 possono essere amministrati tramite SSLVPN, l'abilitazione di un utente all'accesso di una SSLVPN segue l'apposito processo di accreditamento previsto dal regolamento di erogazione servizi cloud.

Gli utenti devono installare il client VPN SSL plus, scaricandolo dalla URL che l'Amministratore Operativo riceve a seguito della richiesta di risorse.

Le URL VPN seguono la seguente naming convention: https://CODICE_sslvpn.innova.puglia.it

(esempio: https://tba-cup_sslvpn.innova.puglia.it)

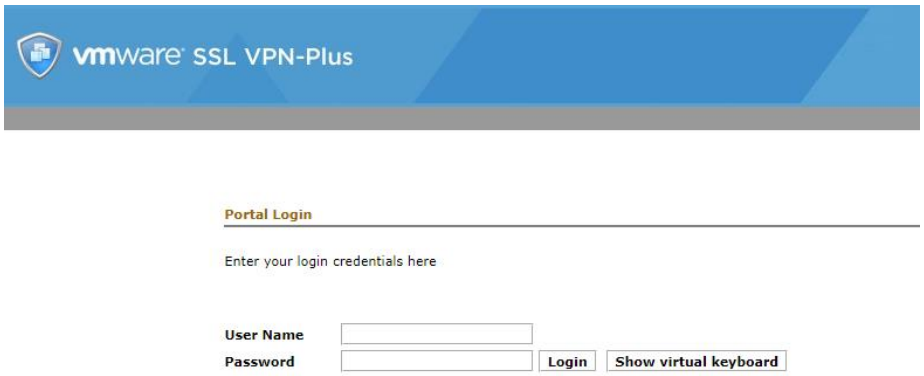


Figura 17: Pagina di login SSLVPN

Dopo essersi loggati, sarà possibile procedere con il download e installazione del client che conterrà l'endopoint già preconfigurato per l'accesso alla SSLVPN.

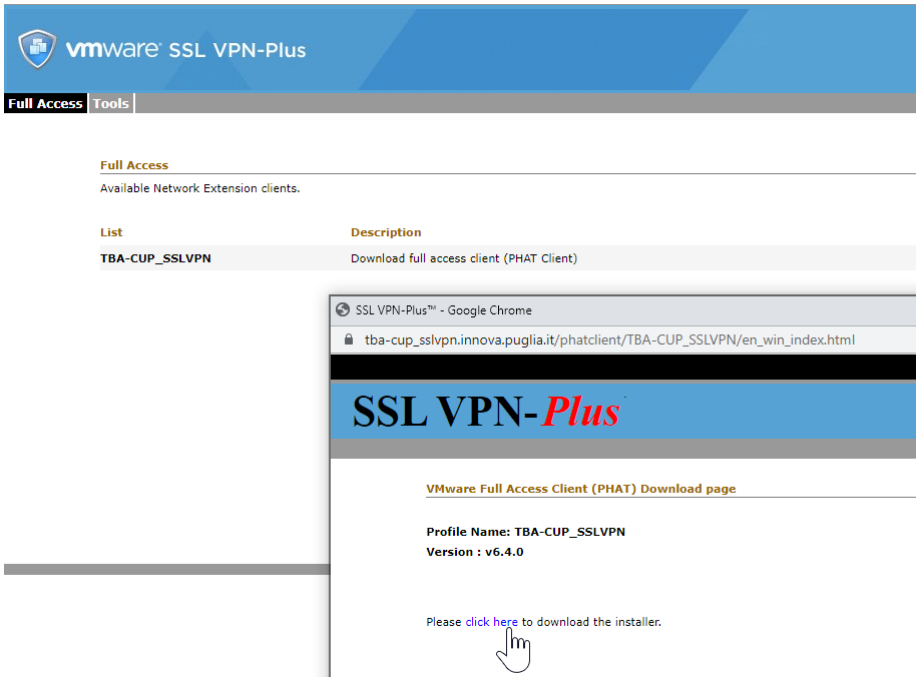


Figura 18: Download client VPN SSL plus

NOTA: le VPN di management messe a disposizione da InnovaPuglia sono basate su un meccanismo di autenticazione basate su UTENTE/PASSWORD al fine di raggiungere il Cloud (IaaS). Permane la facoltà da parte dell'utilizzatore del Cloud di installare e configurare autonome soluzioni di sicurezza, verifica e analisi degli accessi.

10) API di tipo REST/SOAP

Le API (Application Programming Interface) del servizio CLOUD sono uno strumento destinato ad amministratori e programmatori che desiderano configurare e gestire in maniera autonoma tutte le funzionalità offerte, potendo automatizzarle e integrarle senza passare dal rispettivo portale Web.

Per utilizzare gli strumenti e le API è possibile far riferimento alla documentazione seguente:

- La *Guida alla programmazione* fornisce casi d'uso comuni, incluse richieste e risposte di esempio (https://code.vmware.com/docs/8432).
- La *Guida di riferimento dell'API di vRealize Automation* include file OpenAPI per tutte le chiamate al servizio REST API (https://vra7-cloud.innova.puglia.it/component-registry/services/docs#!/apis).

Tutta la documentazione fa riferimento a vRealize Automation 7.6.

Tutte le API sono protette con account e password e richiedono un'autorizzazione per ogni operazione. Per poter invocare le API occorre quindi preventivamente generare il token di autenticazione per l'utente Amministratore Tecnico.

(esempio di invocazione per la generazione del token di autenticazione: `https://vra7-cloud.innova.puglia.it/SAAS/t/innovapuglia/auth/oauthtoken?grant_type=password)`

In alternativa è possibile loggarsi con una basic authentication utilizzando le credenziali di Amministratore Tecnico ricevute all'URL https://vra7-cloud.innova.puglia.it/component-registry/services/docs#!/apis ed inserendo come tenant la stringa "innovapuglia".

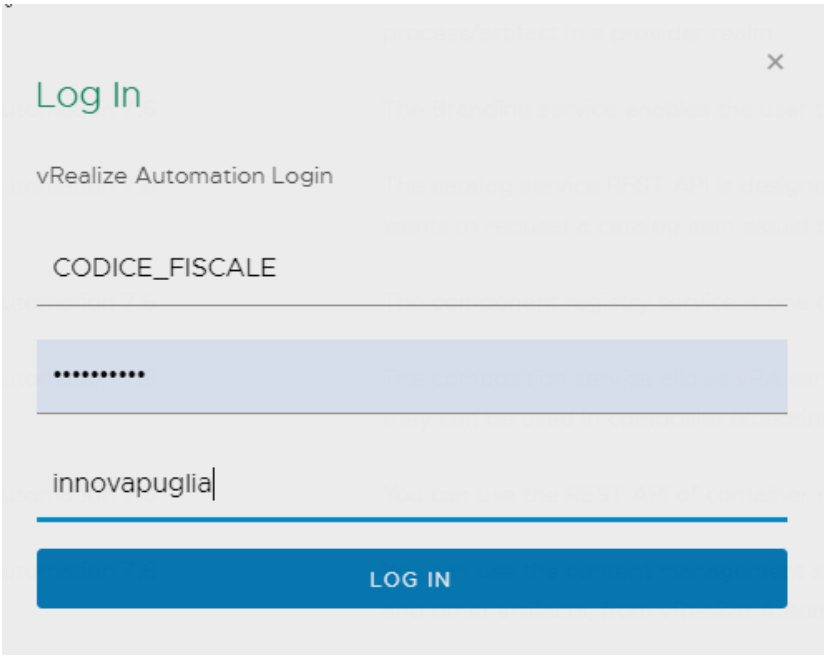


Figura 19 Login a vRealize Automation APIs

11) Sicurezza e responsabilità

InnovaPuglia eroga servizi Cloud agli enti pubblici regionali secondo il modello IaaS (Infrastructure as a Service) offrendo risorse di infrastruttura on demand, come risorse computazionali, spazio di archiviazione, risorse di rete/connettività e sicurezza fruibili in modalità cloud.

InnovaPuglia è pertanto responsabile della gestione ed aggiornamento dell'infrastruttura, tra cui calcolo, archiviazione, applicazione di patch e rete fisica, mentre l'utente è responsabile della gestione e manutenzione del sistema operativo, del middleware, della sicurezza dei dati e delle applicazioni, dei controlli di rete virtuali e dell'accesso degli utenti.

Il software utilizzato dal Cliente nell'ambito del Servizio Cloud dovrà essere originale, munito di apposita licenza d'uso e comunque compatibile con le specifiche e prescrizioni eventualmente comunicate da InnovaPuglia.

La Piattaforma Cloud attraverso la quale è erogato il servizio è composta dai seguenti prodotti:

- vRealize Automation Versione: 7.6.0 (Build: 16526925);
- NSX-v 6.4.5.13282012NSX versione XXX;
- vSphere 6.7.0.44000;
- Site Recovery Version 8.2.0, Build 14761905.

InnovaPuglia garantisce che i suoi sistemi sono sicuri e accessibili solo agli utenti autorizzati. Per eventuali vulnerabilità note, si prega di consultare la documentazione VMware dei vari stack software utilizzati:

- https://www.vmware.com/security/advisories.html