

Realizzazione e gestione di una nuova infrastruttura
informatica al servizio della Pubblica Amministrazione
denominata Polo Strategico Nazionale (“PSN”), di cui al comma 1
dell’articolo 33-septies del d.l. n. 179 del 2012

CUP: J51B21005710007

CIG: 9066973ECE

PSN
Manuale Operativo
DRaaS

Data: 27/07/2023
PSN_UserGuide_DRaaS
Ed. 1 - ver. 2.1

**QUESTA PAGINA È LASCIATA INTENZIONALMENTE
BIANCA**

STATO DEL DOCUMENTO

TITOLO DEL DOCUMENTO			
PSN Manuale Operativo DRaaS			
EDIZ.	REV.	DATA	AGGIORNAMENTO
1	1.0	03/03/2023	Prima versione del documento finalizzata al rilascio di un manuale utente del servizio DRaaS
2	2.0	23/03/2023	Revisione Formale
2	2.1	27/07/2023	Revisione immagini

NUMERO TOTALE PAGINE:	32
-----------------------	----

AUTORE:	
Team di lavoro PSN	Unità operative Solution Development, Technology Hub e Sicurezza

REVISIONE:	
Referente del Servizio	Paolo Trevisan

APPROVAZIONE:	
Direttore del Servizio	Giovanni Santocchia

LISTA DI DISTRIBUZIONE

INTERNA A:

- Funzione Solution Development
- Funzione Technology Hub
- Funzione Sicurezza
- Referente Servizio
- Direttore Servizio

ESTERNA A:

- Direttore dell'Esecuzione Contrattuale (DEC) PSN ing. Fabrizio Marchese

INDICE

1	Definizioni e Acronimi	8
1.1	DEFINIZIONI	8
1.2	ACRONIMI	8
2	Panoramica Generale	10
2.1	SCOPO DEL DOCUMENTO	10
3	Descrizione Del Servizio	11
4	Introduzione al Servizio	14
4.1	ESISTONO DEI PREREQUISITI?	14
4.2	COME SI ACCEDE AL SERVIZIO?	14
4.3	QUALI ATTIVITÀ SONO INCLUSE NEL SERVIZIO?	15
4.4	QUALI COMPONENTI NON SONO INCLUSE NEL SERVIZIO?	15
4.5	COME SI UTILIZZA IL SERVIZIO?	16
4.6	QUALI TIPOLOGIE DI REPLICHE ESISTONO?	16
4.7	COME PROTEGGO I MIEI WORKLOAD?	16
4.8	L'OPERAZIONE DI REPLICA È BIDIREZIONALE?	21
4.9	COME VERIFICO LO STATO DELLE REPLICHE?	21
4.10	COME CONFIGURO LA RETE DELLE VM/VAPP REPLICATE?	23
4.11	COSA VISUALIZZO NELLA DASHBOARD DEL SERVIZIO?	24
4.12	CHE COSA È UN PIANO DI RIPRISTINO?	25
4.13	COME CREO UN PIANO DI RIPRISTINO?	25
4.14	POSSO INSERIRE NUOVE VM AD UN PIANO DI RIPRISTINO?	27
4.15	COME ESEGUO DEI TEST SUL PIANO DI RIPRISTINO?	27
4.16	I WORKLOAD USATI PER I TEST DI DR, POSSONO ESSERE RIUTILIZZATI?	27
4.17	COSA ACCADE ALLA PROTEZIONE NEL MOMENTO DEL TEST?	28
4.18	COME ESEGUO UN CLEANUP?	28
4.19	POSSO PROCEDERE IN AUTONOMIA AD ESEGUIRE I TEST?	28

4.20	COME ATTIVO UN PIANO DI RIPRISTINO?	28
4.21	IN CASO DI DISASTRO REALE, COSA POSSO FARE?	30
4.22	POSSO ESEGUIRE UN LE ATTIVITÀ DI TEST, CLEAN-UP E FAILOVER PER UNA SINGOLA VM?.....	30

LISTA DELLE FIGURE

Figura 1: Schema ad alto livello delle caratteristiche basilari del DRaaS	11
Figura 2: Dashboard della Console Tecnica IaaS	17
Figura 3: Configurazione Outgoing Replications	17
Figura 4: Sezione Cloud vApps and Vs del wizard New Outcoming Replication	18
Figura 5: Sezione Destination VDC and Storage Policy del wizard New Outgoing Replication	18
Figura 6: Sezione Settings del wizard New Outgoing Replication	19
Figura 7: Sezione Ready To Complete del wizard New Outgoing Replication	19
Figura 8: Task Manager, monitoraggio creazione Replica	20
Figura 9: Dashboard DRaaS	21
Figura 10: Incoming & Outcoming Dashboard	22
Figura 11: Configurazione Network per VM Replicate	23
Figura 12: Network Settings	24
Figura 13: Esempio di Piano di Ripristino	26
Figura 14: Attivazione Piano di Ripristino	29

LISTA DELLE TABELLE

Tabella 1: Glossario Definizioni	8
Tabella 2: Nomenclatura	8
Tabella 3: Glossario Acronimi	9

1 Definizioni e Acronimi

1.1 Definizioni

Definizione	Descrizione
NewCo	È la nuova società (New Company) che è stata costituita nell'ambito del progetto del Cloud Nazionale
TBC	Il tema è stato discusso ma è in attesa di conferma dalle parti coinvolte
TBD	Il tema non è ancora stato discusso

Tabella 1: Glossario Definizioni

Definizione	Descrizione
PSN Cloud Platform	Identifica tutte le componenti della piattaforma Cloud offerta dal PSN
Console Tecnica IaaS	Identifica il Portale Tecnico di amministrazione del Servizio IaaS
Cloud Industry Standard IaaS	Identifica il Servizio IaaS offerto dal PSN

Tabella 2: Nomenclatura

1.2 Acronimi

Acronimo	Descrizione
DR	Disaster Recovery
DRaaS	Disaster Recovery as a Service
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
IP	Internet Protocol
IPS	Intrusion Prevention System
LAN	Local Area Network
NAT	Network Address Translation
MAC	Media Access Control
MPLS	MultiProtocol Label Switching
PaaS	Platform as a Service
PA	Pubblica Amministrazione
PSN	Polo Strategico Nazionale
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SaaS	Software as a Service
SNAT	Source Network Address Translation
vApp	Virtual Appliance

Acronimo	Descrizione
VM	Virtual Machine

Tabella 3: Glossario Acronimi

2 Panoramica Generale

Il “*Disaster Recovery as a Service*” è un modello di servizio cloud computing che consente di ripristinare l’accesso e la funzionalità di un Infrastruttura in un ambiente di “*cloud computing*” di terze parti, dopo un evento disastroso. Il presente documento fornisce le linee di utilizzo e una panoramica di dettaglio e della soluzione di “**Disaster Recovery as a Service**” (di seguito identificato anche come DRaaS) prevista tra le architetture tecnologiche necessarie all'erogazione dei servizi di cui all’art. 5, comma 1 della Convenzione, redatto e presentato dal concessionario PSN S.p.A. (di seguito identificato anche come “PSN”) secondo quanto stabilito dal Capitolo Tecnico per la componente Industry Standard.

La soluzione DRaaS, mediante la Console Tecnica IaaS, offre un servizio di protezione (DR) alla PA permettendo di proteggere server virtuali, ospitati in una Cloud Region verso un'altra Cloud Region (Sito Secondario/DR). Il servizio è accessibile mediante interfaccia web.

Il **PSN Cloud Provider** rende disponibili delle risorse di calcolo, storage e rete dalle proprie infrastrutture cloud e le raggrupperà in un Organization Virtual Data Center (Organization VDC) dedicato al Tenant della Pubblica Amministrazione in una Cloud Region remota, nella quale predisporre le repliche dei “*virtual workload*”. Le risorse computazionali messe a disposizione nella Cloud Region secondaria saranno uguali a quelle della Cloud Region primaria.

2.1 Scopo del documento

Questo documento rappresenta un manuale con le linee guida di utilizzo della soluzione oltre a contenere una raccolta delle domande più comuni sul servizio e le relative risposte. Il manuale e le FAQ saranno integrati nel tempo in base ad eventuali altri argomenti che si riveleranno di interesse comune

3 Descrizione Del Servizio

La soluzione “Disaster Recovery as a Service” è servizio add-on previsto nella Console Tecnica IaaS che permette alla PA di aggiungere alla propria infrastruttura virtuale IaaS Private o IaaS Shared la funzionalità di protezione delle Macchine Virtuali e delle vAPP (definite congiuntamente di seguito “workload”) in caso di eventi disastrosi che possano inficiare sull’erogazione del servizio infrastrutturale in un sito (Datacenter) del PSN; tale funzionalità di protezione e ripristino dei workload è nota con la locuzione “Disaster Recovery” e permette appunto la ripartenza dei propri workload in un altro sito del PSN quando si verifica una interruzione nel sito primario (tale da dichiarare evento di disastro).

La figura seguente rappresenta uno schema ad alto livello contenente le caratteristiche basilari del servizio DRaaS.

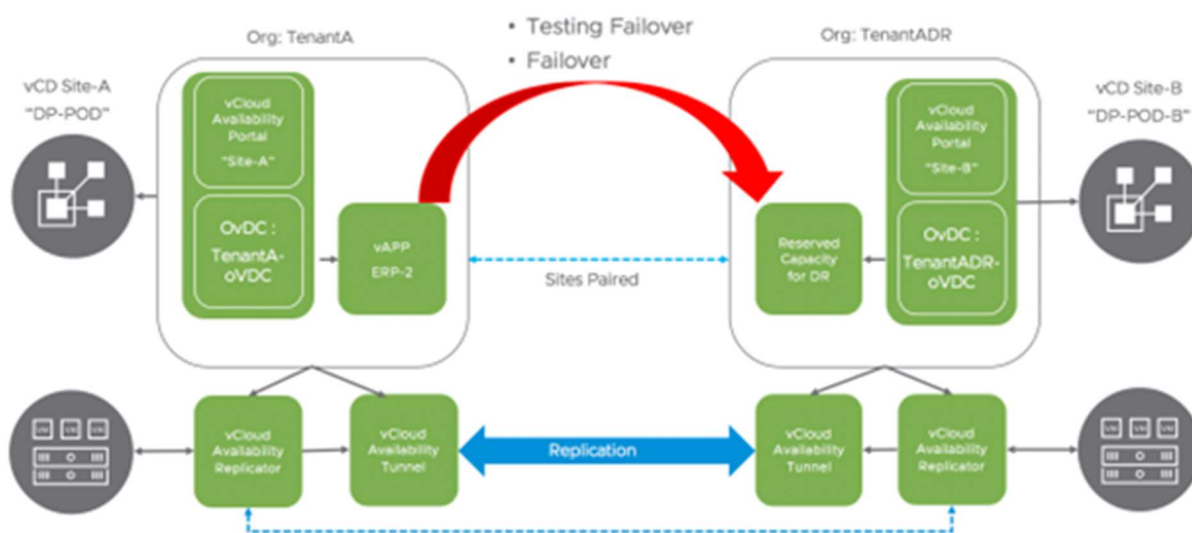


Figura 1: Schema ad alto livello delle caratteristiche basilari del DRaaS

Il Servizio Disaster Recovery è disponibile per le seguenti tipologie di servizi IaaS:

- IaaS Private
- IaaS Shared

Le PA potranno gestire le funzionalità di protezione dei workload direttamente nella console Tecnica IaaS di gestione del proprio Tenant che ricordiamo essere disponibile nel portale d'accesso Console Unica accessibile via web. La protezione di un workload è basata sull'utilizzo di repliche in modalità asincrona effettuate a partire dal workload in esecuzione sul Sito Primario verso il Sito di DR.

Le PA, con il servizio DRaaS, potranno autonomamente gestire direttamente dalla Console Tecnica IaaS:

- La Configurazione delle Repliche dei workload.
- I Piani di Ripristino ¹dei workload

Ogni PA può selettivamente individuare e selezionare uno o più workload (che ricordiamo, possono essere singole Macchine Virtuali o più Macchine Virtuali parte di una vApp) che saranno soggetti a replica e quindi alla protezione con tecnologia VCDA, rispettando i necessari prerequisiti per permettere il loro completo ripristino. Infine, per attivare il Servizio DRaaS, è necessario che la PA abbia sottoscritto almeno un servizio IaaS in entrambe le Region, Nord e Sud, in modo da poter eleggere una delle due Region come Sito Primario e l'altra come Sito di DR.

Solo qualora dovesse verificarsi un evento disastroso tale da obbligare il PSN a dichiarare “disastro”, le PA potranno attivare i loro Piani di Ripristino e riattivare i workload (virtuali e/o fisici) nel Sito di DR.

Nel caso specifico in cui la PA avesse esclusivamente un servizio di tipo IaaS Private/Shared in configurazione DR, può essere autonoma nella gestione del Piano di Ripristino. Nel Caso di soluzioni tecnologiche Ibride (IaaS Private e/o Shared e Infrastrutture Fisiche) la PA dovrà coinvolgere i supporti del PSN mediante richiesta specifica al Service Manager di riferimento.

Le repliche dei workload sono soggette ad un Punto di Ripristino (RPO, *Recovery Point Objective*) di 10 minuti, ciò significa che in caso di disastro sarà possibile ripristinare un workload sul Sito di DR tollerando una perdita di dati non superiore a 10 minuti.

¹ La definizione del “Piano di Ripristino” è una responsabilità della stessa PA

L'Obiettivo Temporale di ripristino (RTO, *Recovery Time Objective*) è invece dettato da due componenti:

- il tempo necessario al PSN per garantire il ripristino **dell'infrastruttura base²** sul Sito di DR, tempistica fissata in 25 minuti
- il tempo necessario alla PA – a partire dal ripristino dell'infrastruttura di base – **per avviare e portare a conclusione il Piano di Ripristino³** da avviarsi quando il PSN dichiara lo stato di disastro di una Cloud Region

² Per **infrastruttura base** si intendono quelle componenti come Network WAN, Hosting Bare Metal server, NAS share e quanto altro esula dal puro contesto IaaS Private/Shared ma pur sempre parte integrante del perimetro tecnologico del cliente finale.

³ **L'Obiettivo Temporale di Ripristino** di questa fase non è noto al PSN in quanto è specifico di ciascuna PA e dipenderà dal numero di workload da attivare, dalle dipendenze tra gli stessi, dalle tempistiche di avvio degli applicativi, etc.

4 Introduzione al Servizio

In questa sezione sono riportate alcune definizioni dei costrutti logici utilizzati all'interno del servizio DRaaS. Tali principi consentiranno una migliore comprensione dei successivi capitoli del manuale che si focalizzeranno su alcune aree 'verticali' di gestione del servizio.

4.1 Esistono dei prerequisiti?

Si.

Di seguito l'elenco dei prerequisiti:

- Per attivare il Servizio DRaaS è necessario che la PA abbia sottoscritto almeno un servizio IaaS in entrambe le Cloud Region, Nord e Sud, in modo da poter eleggere una delle due Cloud Region come Sito Primario e l'altra come Sito di DR
- Nel caso in cui una PA abbia più Tenant sul Sito Primario dovrà averne altrettanti sul Sito Secondario, sarà quindi necessario attivare, con espressa richiesta nel Piano dei Fabbisogni, sottoscrizioni dei servizi IaaS affinché il rapporto tra i Tenant dei due siti sia sempre 1 ad 1
- Dimensionare opportunamente il Sito di DR in base ai workload che si vogliono proteggere; qualora le risorse computazionali richieste dai workload per la ripartenza sul Sito di DR dovessero essere maggiore di quelle disponibili parte di essi non potranno essere riaccesi. ***Nel caso cui è necessario eseguire test periodici (simulazioni) di Disaster Recovery è necessario richiedere il doppio dello spazio storage, al fine di ospitare i dati necessari, previsto nel Piano dei Fabbisogni.***

4.2 Come si accede al Servizio?

Il servizio è usufruibile mediante l'accesso alla "Console Tecnica IaaS", dalla quale le PA, che hanno sottoscritto la soluzione DRaaS, potranno gestire le funzionalità di protezione dei workload. Ricordiamo che la console tecnica IaaS è disponibile nel portale di accesso "Console Unica", raggiungibile dalla seguente URL: <https://console.polostrategiconazionale.it>

4.3 *Quali attività sono incluse nel Servizio?*

Il Servizio DRaaS include due attività principali:

- Replica dei workload da un Sito Primario
- Ripristino su Sito di DR

4.4 *Quali componenti non sono incluse nel Servizio?*

Le componenti Network e Bare-Metal. Ogni PA deve provvedere in modo autonomo all'allineamento delle configurazioni di rete tra il Sito Primario ed il Sito di DR. Per rete si intende tutto il contesto di Virtual Networking del workload oggetto del DR. Per le componenti Bare-Metal è necessario richiedere specifiche progettazioni al supporto specialistico PSN.

Nel Sito di DR, quindi, vanno ricreati tutti gli asset di rete necessari al funzionamento dei workload che dovranno essere ripristinati in caso di disastro. Nello specifico, gli asset che andranno necessariamente ricreati sono i seguenti:

- Subnet, sia pubbliche che private/MPLS
- Bilanciatori di carico
- Regole NAT
- Regole Firewall
- Logical Segment
- Configurazioni IPSec VPN
- Servizio DHCP

È necessario preconfigurare gli asset di rete sul Sito Secondario, a prescindere dal workload attivo nel Sito Primario e oggetto di replica, al fine di rendere molto più immediata la ripartenza del workload di una PA in caso di disastro (Vedi 4.10).

4.5 Come si utilizza il Servizio?

Una volta effettuato l'accesso alla Console Tecnica IaaS, la PA può accedere ad un'apposita sezione per la configurazione della Protezione che abilita le Repliche dei workload da un Sito Primario ad un Sito Secondario.

4.6 Quali tipologie di Repliche esistono?

Esistono due tipologie di Repliche:

- **Full synchronization:** è la prima Replica e prevede una Replica integrale di tutti i dati del workload, ossia dischi virtuali e file di configurazione
- **Delta synchronization:** sono repliche incrementali ed interesseranno solo i cambi avvenuti sul workload del Sito Primario (ad es. creazione, modifica o cancellazioni dei dati) permettendo quindi di ridurre la quantità di dati da trasferire via rete e di conseguenza le tempistiche per ciascuna replica

NOTA: Solo al termine della prima replica il workload sarà “protetto”, ossia sarà possibile utilizzare la replica per la ripartenza del workload in caso di disastro.

4.7 Come proteggero i miei workload?

La protezione dei workload si basa sulla definizione delle relazioni di replica a partite dal workload in esecuzione nel Sito Primario verso il Sito di DR (*“Outcoming Replication”*).

Una PA che ha attivato un Servizio IaaS erogato sulla Region Nord, ad esempio, può proteggere i suoi workload replicandoli con la soluzione DRaaS sulla Region Sud; qualora un evento disastroso dovesse colpire la Region Nord, la PA può far ripartire i workload protetti sulla Region Sud secondo un piano prestabilito definito “Piano di Ripristino”.

Di seguito sono illustrati gli step necessari alla configurazione di una Protezione.

- Posizionarsi nella sezione *“Availability”* del Sito Primario:
 1. Posizionarsi nella scheda del Sito Primario
 2. Espandere il menu *“More/Altro”*
 3. Cliccare *“Availability Sito Primario”*

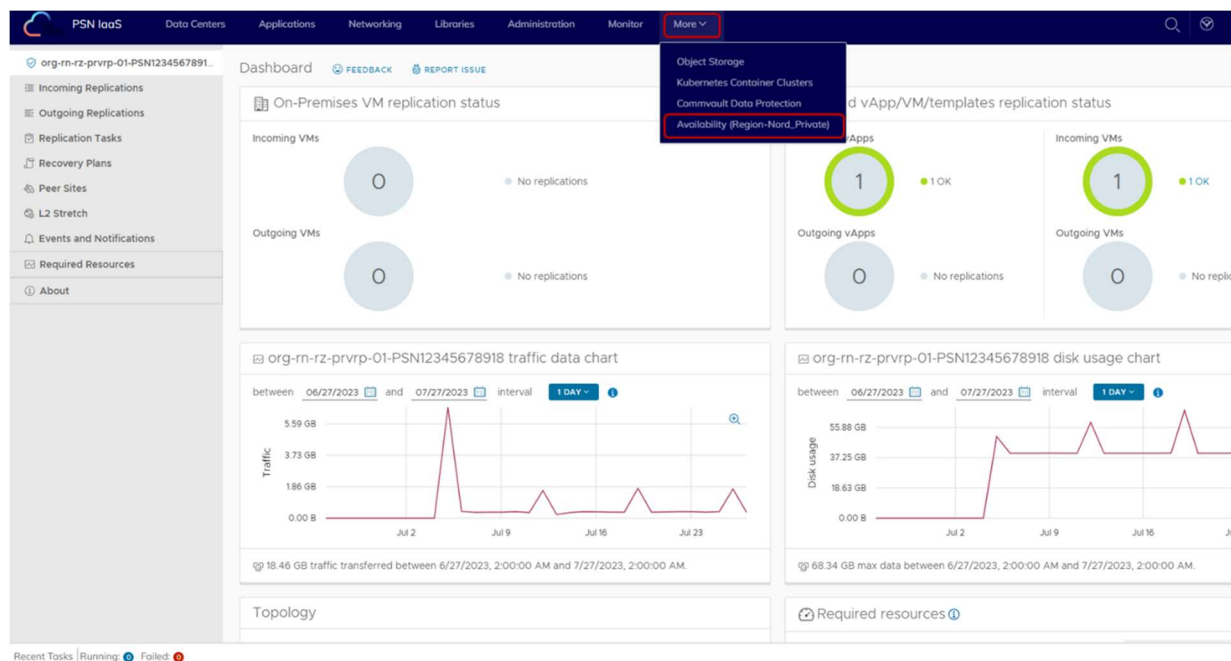


Figura 2: Dashboard della Console Tecnica IaaS

■ Configurazione nuova Protezione da Sito Primaio a Sito Secondario:

1. Posizionarsi nella sezione "Outgoing Replications"
2. Cliccare su "New Protection"

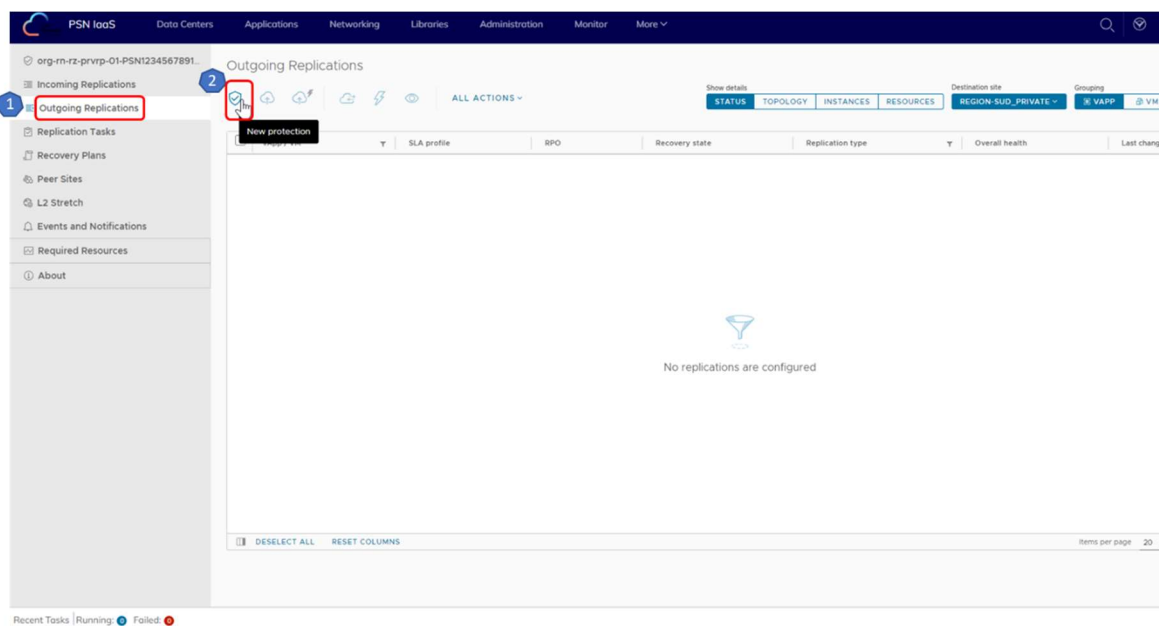


Figura 3: Configurazione Outgoing Replications

- Seguire le indicazioni del wizard, *“New Outgoing Replication”*:
 1. Nella sezione *“Source VMs and vApps”*
 2. Selezionare i workload sorgente
 3. Cliccare su *“Next”*

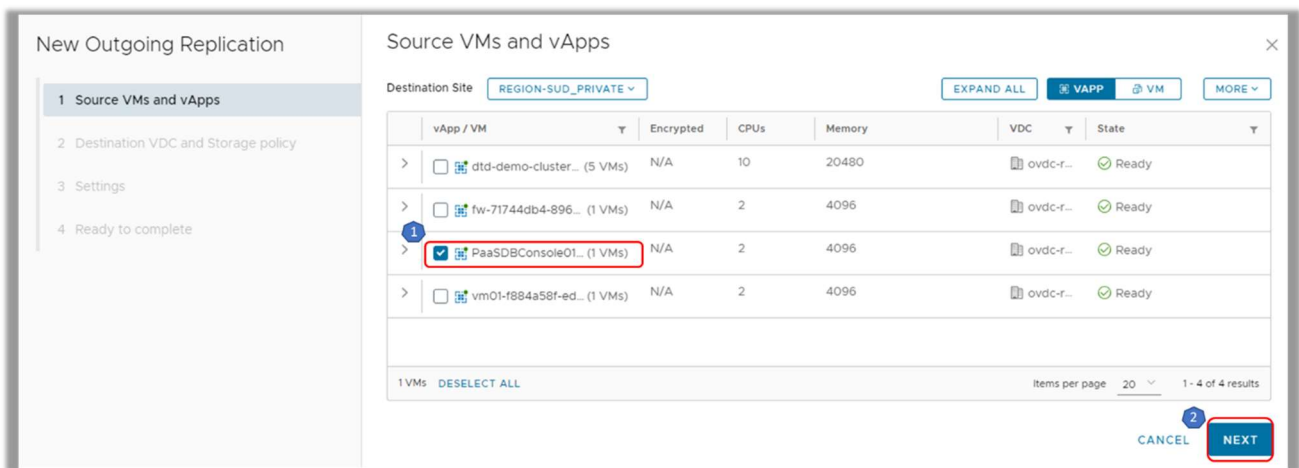


Figura 4: Sezione Cloud vApps and Vs del wizard New Outcoming Replication

4. Nella sezione *“Destination and Storage policy”* selezionare il vDC di destinazione⁴, e la storage policy per il posizionamento dei workload recuperati, cliccare su *“Next”*

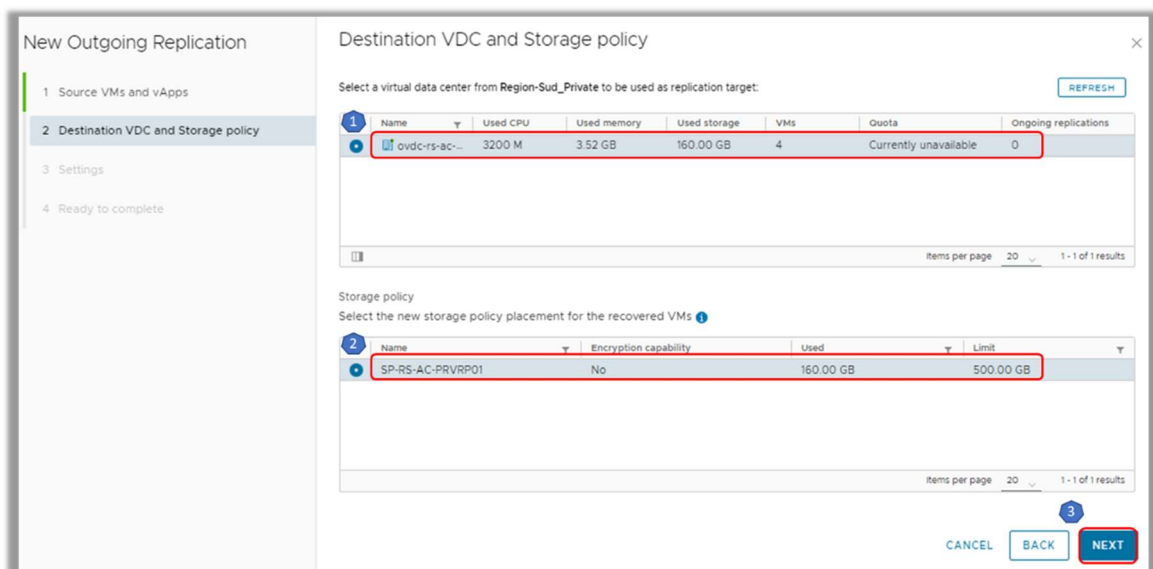


Figura 5: Sezione Destination VDC and Storage Policy del wizard New Outgoing Replication

⁴ Potrebbe essere richiesto l’inserimento delle credenziali dell’Organization ID di Destinazione

5. Nella sezione “Settings”, configurare le impostazioni di protezione

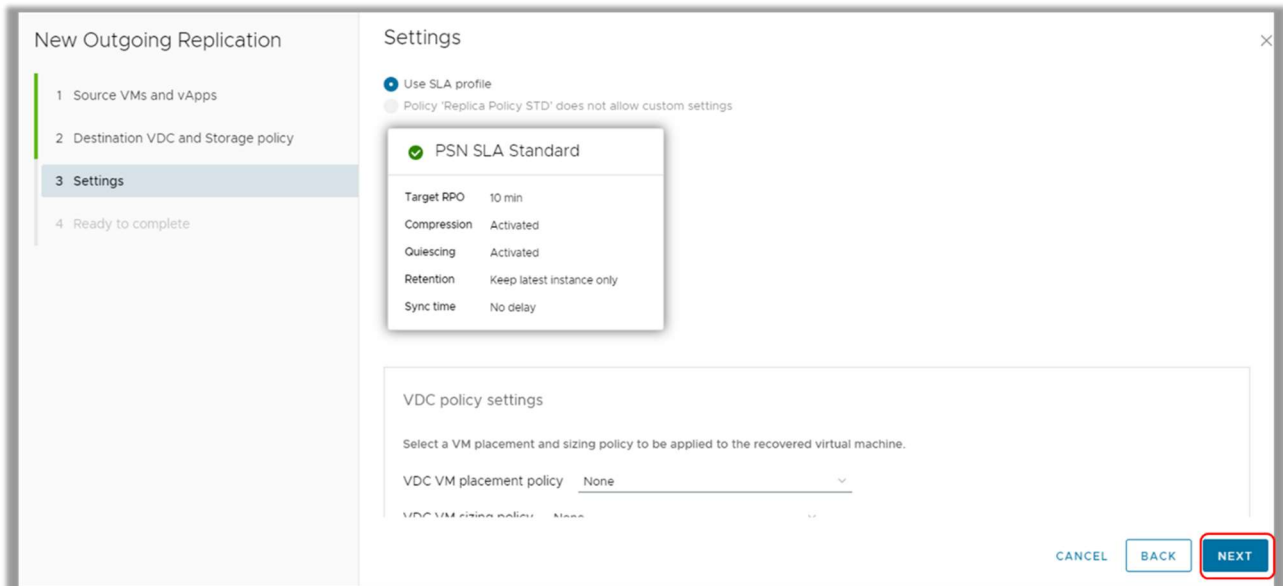


Figura 6: Sezione Settings del wizard New Outgoing Replication

6. Nella sezione “Ready to Complete”, verificare che le informazioni di protezione inserite siano corrette e cliccare su “Finish”

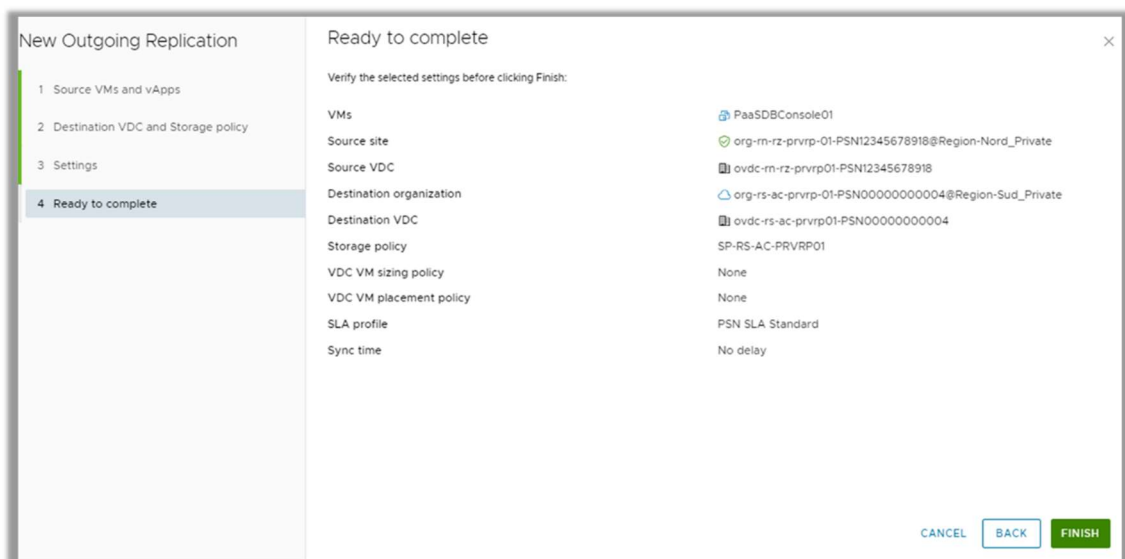
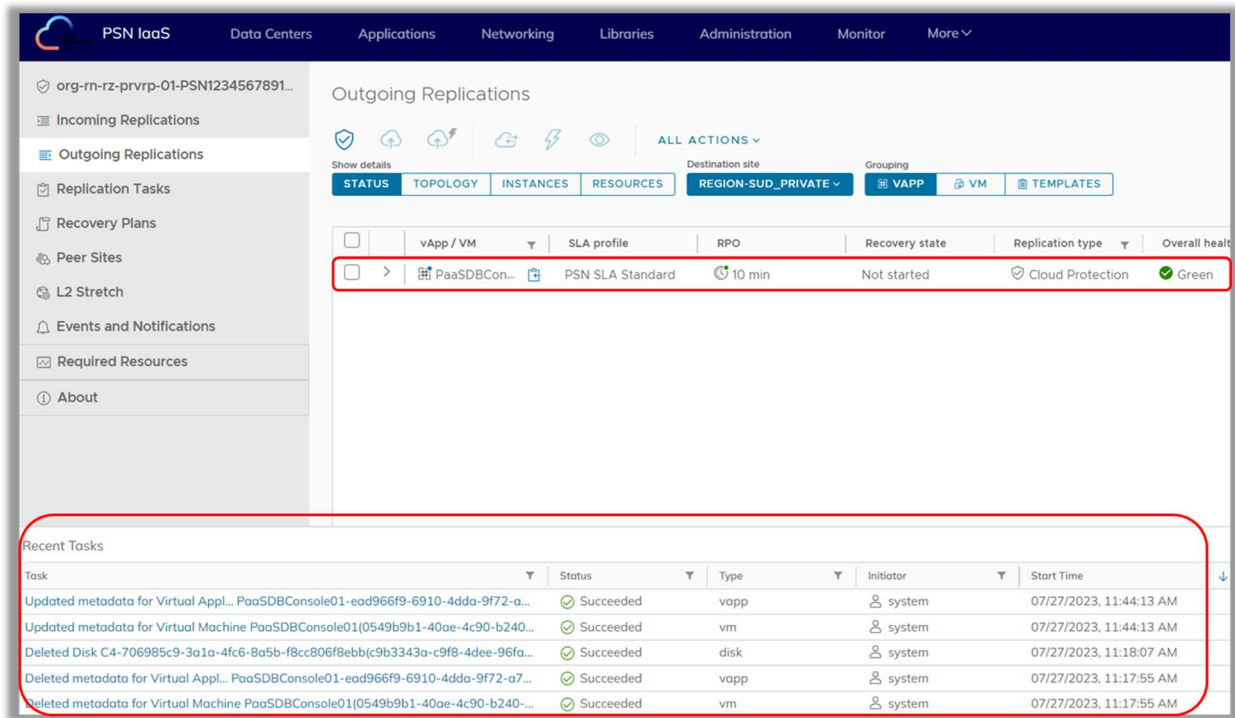


Figura 7: Sezione Ready To Complete del wizard New Outgoing Replication

È possibile esaminare lo stato di creazione della Replica tramite il task manager a fondo alla pagina, come mostrato dalla figura seguente:



The screenshot displays the PSN IaaS Task Manager interface. The top navigation bar includes links for Data Centers, Applications, Networking, Libraries, Administration, Monitor, and More. The left sidebar lists various management options: Incoming Replications, Outgoing Replications, Replication Tasks, Recovery Plans, Peer Sites, L2 Stretch, Events and Notifications, Required Resources, and About. The main content area is titled 'Outgoing Replications' and features a table with columns for vApp / VM, SLA profile, RPO, Recovery state, Replication type, and Overall health. A red box highlights the first row of the table, which shows a replication task with an 'Overall health' of 'Green'. Below the table, the 'Recent Tasks' section is also highlighted with a red box, showing a list of tasks with columns for Task, Status, Type, Initiator, and Start Time. The tasks listed include 'Updated metadata for Virtual Appl...', 'Updated metadata for Virtual Machine', 'Deleted Disk', and 'Deleted metadata for Virtual Appl...'.

Task	Status	Type	Initiator	Start Time
Updated metadata for Virtual Appl... PaaSDBConsole01-ead966f9-6910-4dda-9f72-a...	Succeeded	vapp	system	07/27/2023, 11:44:13 AM
Updated metadata for Virtual Machine PaaSDBConsole01(0549b9b1-40ae-4c90-b240-...	Succeeded	vm	system	07/27/2023, 11:44:13 AM
Deleted Disk C4-706985c9-3a1a-4fc6-8a5b-f8cc806f8ebb(c9b3343a-c9f8-4dee-96fa-...	Succeeded	disk	system	07/27/2023, 11:18:07 AM
Deleted metadata for Virtual Appl... PaaSDBConsole01-ead966f9-6910-4dda-9f72-a7...	Succeeded	vapp	system	07/27/2023, 11:17:55 AM
Deleted metadata for Virtual Machine PaaSDBConsole01(0549b9b1-40ae-4c90-b240-...	Succeeded	vm	system	07/27/2023, 11:17:55 AM

Figura 8: Task Manager, monitoraggio creazione Replica

Una volta configurata correttamente la replica l'“Overall health” è in “Green”.

4.8 L'operazione di Replica è bidirezionale?

Sì, nel limite di gestione definito con le sole regole di “Outgoing”. Nello specifico possiamo dire che i workload potranno essere sottoposti a protezione con le opportune regole dal Sito Primario verso il Sito Secondario.

Ad esempio, una PA può avere dei workload attivi sia sulla Region Nord che sulla Region Sud, di conseguenza le regole di protezione dovranno essere impostate nel seguente modo:

- Workload attivi nella Region Nord; configuro una protezione in Outgoing verso la Region Sud
- Workload attivi nella Region Sud; configuro una protezione in Outgoing verso la Region Nord

4.9 Come verifico lo stato delle Repliche?

Il servizio offre uno stato delle Repliche visibile nelle sezioni “Outgoing Replications” e/o “Incoming Replications”. Le verifiche lato “Outgoing” avvengono nel Sito Primario, mentre l’“Incoming” nel Sito di Destinazione. Nelle Dashboard di sintesi i possibili stati sono:

- Verde: dato allineato
- Giallo: dato in sincronizzazione
- Grigio: sincronizzazione da avviare
- Rosso: errore di sincronizzazione

Di seguito la schermata esemplificativa:

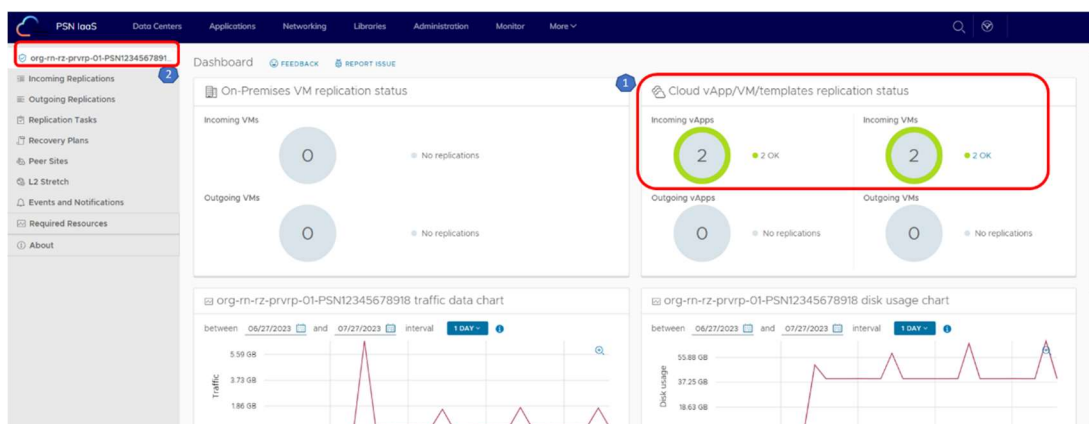


Figura 9: Dashboard DRaaS

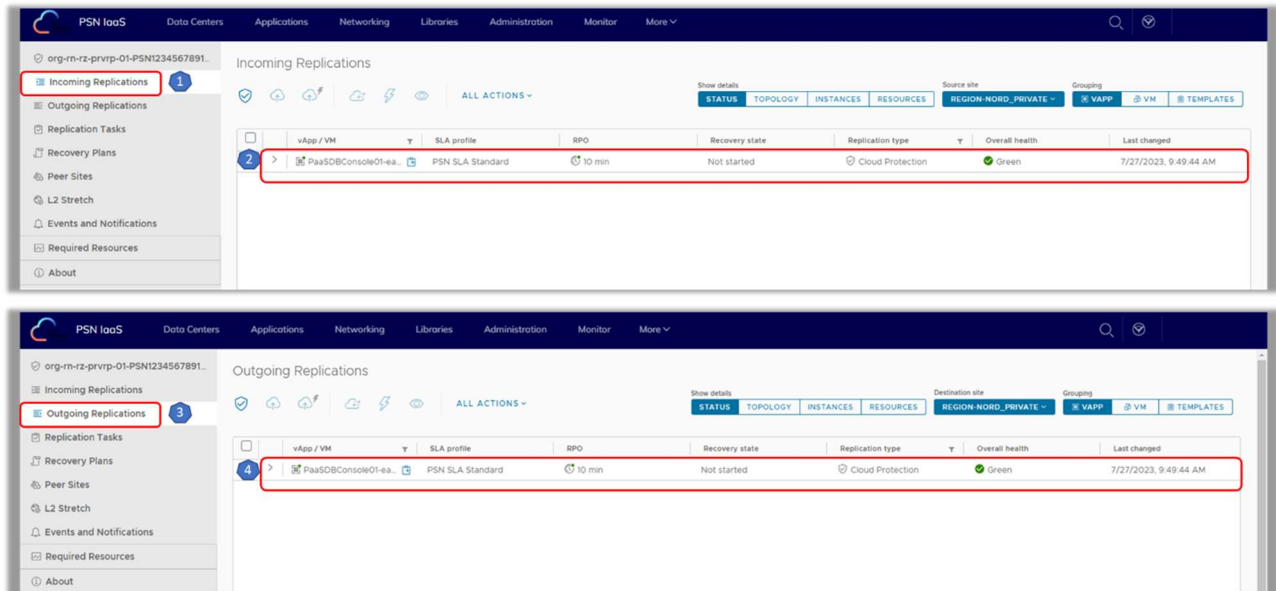


Figura 10: Incoming & Outcoming Dashboard

Per eseguire le diverse verifiche, sul Sito Primario (“Outcoming”) o sul Sito Secondario (“Incoming”), è necessario selezionare il Sito di interesse mediante la seguente procedura:

1. Cliccare sulla dashboard del Sito Primario
2. Selezionare “More/Altro”
3. Cliccare sul link “Availability” Sito Secondario

4.10 Come configuro la rete delle VM/VAPP replicate?

Come descritto in precedenza, la configurazione di Rete non è incluso nel servizio DRaaS; pertanto, la PA dovrà necessariamente accedere al Sito Secondario e configurare in modo autonomo tutti gli asset di rete per VM e vApp.

Di seguito viene illustrata la procedura operativa per associare gli oggetti di network preconfigurati ai workload sottoposti a protezione:

1. Posizionarsi in “Outgoing Replication”
2. Selezionare la casella di controllo per VM/VAPP
3. Espandere “All Action”
4. Cliccare “Recovery Settings”

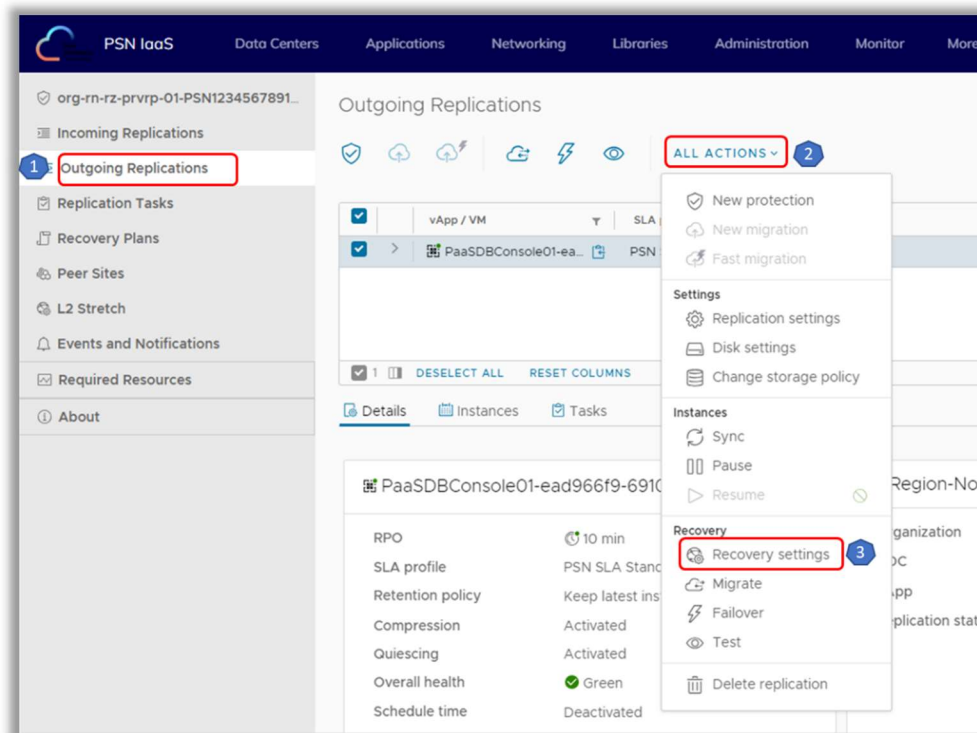


Figura 11: Configurazione Network per VM Replicate

In “Network”, eseguire le seguenti azioni:

- Selezionare la “network target” per la vApp /VM (tale rete deve essere selezionata come descritto nel paragrafo che tratta le componenti non incluse nel servizio, vedi 4.4)

In “Nics”

- Fleggare la casella “Connected at Power On”

- Selezionare l'“IP mode” desiderato
- Cliccare su “Apply”

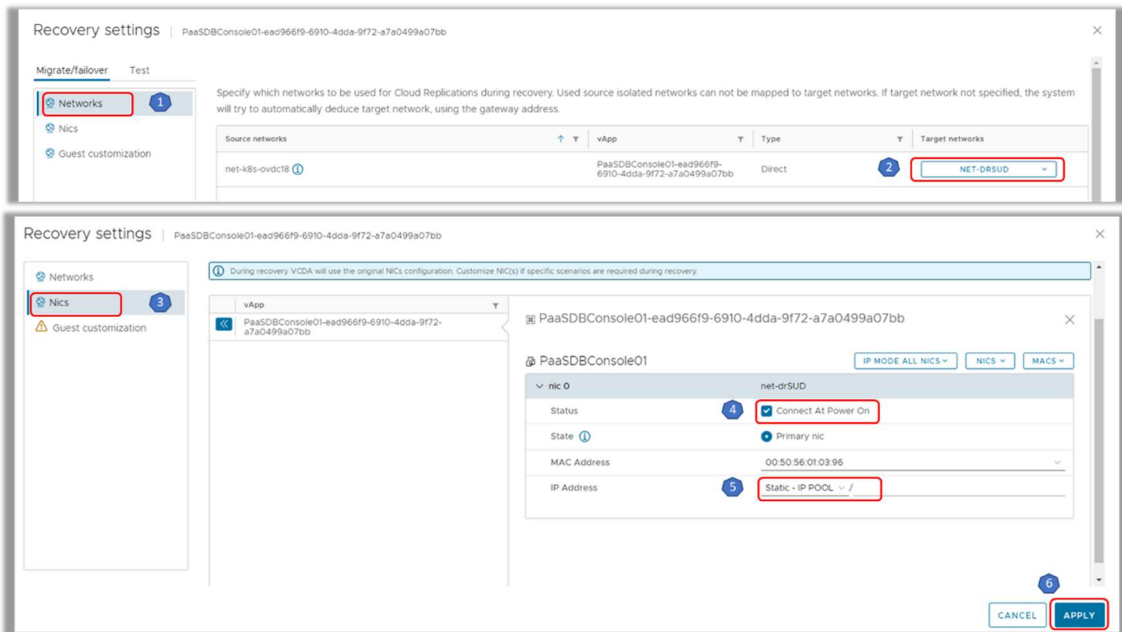


Figura 12: Network Settings

4.11 Cosa visualizzo nella Dashboard del Servizio?

La Dashboard della PA, che ha sottoscritto il Servizio DR, consente di ottenere le seguenti informazioni:

- numero di repliche in entrata e in uscita
- spazio su disco consumato
- utilizzo della larghezza di banda della rete con possibilità di analisi ad intervalli predefiniti e periodi selezionabili
- dettagli sui pairing dell'organizzazione specifica
- risorse (CPU, memoria e spazio disco) necessarie per eseguire il failover delle repliche in entrata

4.12 *Che Cosa è un Piano di Ripristino?*

Il Piano di Ripristino stabilisce come gestire in caso di un'interruzione del servizio o di un disastro la ripresa del lavoro in modo rapido ed efficace. Nel dettaglio definisce l'ordine di ripartenza dei workload che ospitano le applicazioni della PA. Dopo aver configurato le Repliche, è possibile creare uno o più Piani di Ripristino e devono essere configurati sul Servizio DRaaS, attraverso la Console Tecnica IaaS.

In conclusione, il Piano di ripristino è un attuatore di azioni (start, configurazioni Network) definite nel piano stesso dal Referente tecnico della PA.

4.13 *Come Creo un Piano di Ripristino?*

Nella fase di creazione di un Piano di Ripristino è necessario indicare degli elementi di configurazione di seguito riportati:

- **Steps:** permette di dettagliare i vari passaggi che il servizio dovrà eseguire in caso di attivazione del Disaster Recovery
- **Delay:** permette di stabilire un tempo di attesa al termine di un passaggio (Steps), necessario ad es. per attendere che un sistema operativo e la relativa applicazione parta su un gruppo di workload riattivati
- **Prompt:** strumento di interazione per gli IT del Tenant che possono attivare/sospendere uno step in attesa di approvazione manuale prima di procedere al passaggio successivo.

L'immagine seguente mostra un esempio di un Piano di Ripristino, si possono osservare i workload da riavviare sul Sito di DR ed il relativo stato delle repliche ("*Recovery state*"):

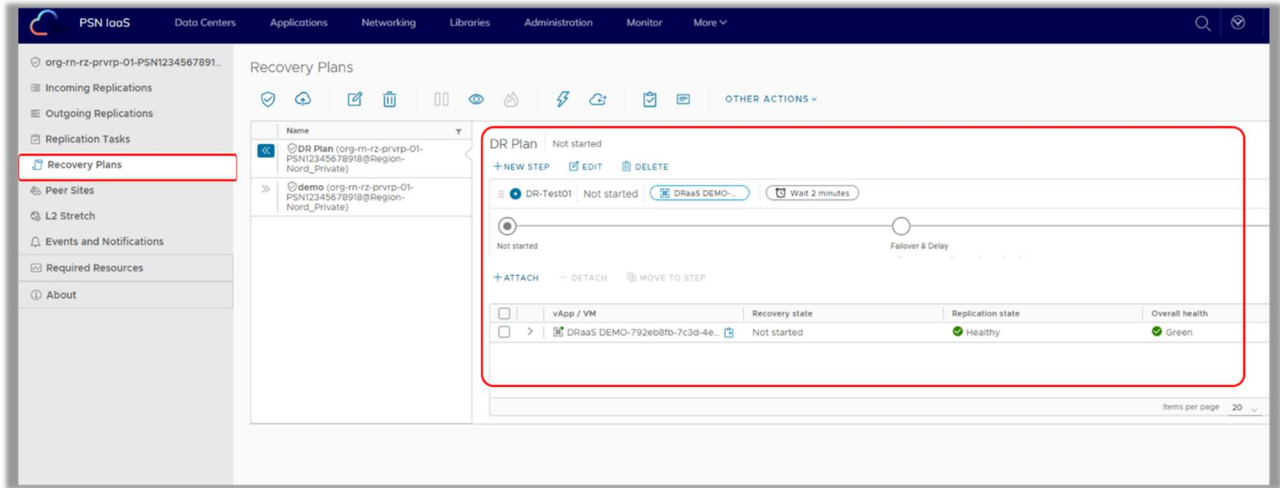


Figura 13: Esempio di Piano di Ripristino

Di seguito la procedura operativa per la creazione di un Piano di Ripristino:

- Posizionarsi sul tab *“Recovery Plans”*
- Cliccare il tasto *“New Recovery Plan”*; si apre una finestra nella quale inserire il nome del piano e una descrizione (facoltativa). È possibile abilitare l'auto sincronizzazione e associargli data ed orario
- Cliccare su *“OK”*
- Posizionarsi nella sezione *“DR Plan”*
- Cliccare *“New Step”* e seguire le indicazioni del wizard
- Nella sezione *“Step Settings”*, inserire lo Step Name, il Delay cioè il tempo necessario per verificare che le operazioni siano andate a buon fine,
- Cliccare *“Next”*
- Nella Sezione *“Recover Replications”*, selezionare le protezioni che si vogliono inserire nel piano
- Cliccare *“Next”*
- In *“Ready to Complete”*, verificare i dati inseriti
- Cliccare su *“Finish”*

NOTA: Se si vogliono aggiungere altri Step, ripetere l'operazione *“New Step”*

4.14 *Posso inserire nuove VM ad un Piano di Ripristino?*

Sì, è possibile aggiungere nuovi workload ad un piano di Ripristino, precedentemente configurato, mediante la Console Tecnica IaaS editando il Piano di Ripristino.

4.15 *Come eseguo dei Test sul Piano di Ripristino?*

Si possono effettuare dei test di Disaster Recovery per verificare la robustezza dell'intera pianificazione e la correttezza delle configurazioni adottate sul Sito di DR.

I Test possono essere effettuati dalla Console Tecnica IaaS e prevedono i seguenti step:

- attivazione dei workload sul Sito di DR all'interno di una rete isolata in modo da non compromettere il funzionamento dei workload in esecuzione nel Sito Primario
- verifica integrità del sistema operativo, degli applicativi e dei dati

Nel dettaglio la procedura operativa da utilizzare nella Console Tecnica IaaS:

- Posizionarsi nella sezione *"Recovery Plan"*
- Selezionare il DR Plan di interesse
- Cliccare il Tasto Test 
- Si apre una finestra, nella quale si chiede all'utente se è sicuro di voler procedere con il Test
- Cliccare *"OK"*
- Attendere i Risultati del Test

NOTA: Se si ha necessità di effettuare dei Test di Disaster Recovery, si deve prevedere un quantitativo doppio dello spazio storage sul Sito di DR, al fine di poter attivare i workload che serviranno per effettuare i test, garantendo l'integrità delle repliche necessarie per un eventuale Disaster Recovery.

4.16 *I workload usati per i test di DR, possono essere riutilizzati?*

No.

I workload usati per i test, essendo generati da una procedura interna di *"Hot-Cloning"*, verranno resi disponibili per l'esecuzione dei test. I relativi Workload di test saranno comunque compromessi e non più

utilizzabili per un Disaster Recovery reale; pertanto, sarà necessario procedere alla loro cancellazione al termine del test (fase di “cleanup”, vedi 4.18).

4.17 Cosa accade alla protezione nel momento del Test?

Durante l’esecuzione di un Test Fail-over, le attività di allineamento dei dati rimangono attive, in quanto i workload generati per la fase di test sono delle copie estemporanee dei dati replicati.

Questo garantisce la consistenza dei dati di protezione dei Workload.

4.18 Come eseguo un cleanup?

Di seguito la procedura di “cleanup”:

- Posizionarsi nella sezione “Recovery Plan”
- Selezionare il DR Plan di interesse
- Cliccare il tasto Test Cleanup 
- Si apre una finestra, nella quale si chiede all’utente se è sicuro di voler procedere con il Cleanup
- Cliccare “OK”. Questa azione elimina tutte le vApp e le Vm create in fase di test.
- Attendere la pulizia di tutti gli elementi creati in fase di test

4.19 Posso procedere in autonomia ad eseguire i Test?

Sì, nel momento in cui la PA utilizzi esclusivamente dei servizi di tipo virtuale.

Nel caso di utilizzo di servizi erogati da servizi *Bare-Metal* o generalmente diversi dal servizio IaaS, sarà necessario coinvolgere il Service Manager del PSN per pianificare i test di Disaster Recovery esaustivi che comprendano tutte le componenti del servizio.

4.20 Come Attivo un Piano di Ripristino?

Per poter eseguire il Piano di Ripristino si dovrà accedere al servizio DRaaS dalla Console Tecnica IaaS del Portale di accesso Console Unica e, come mostrato nella figura 14, cliccare sul tasto Failover nella sezione “Piani di Ripristino”.

Il servizio procederà in autonomia ad eseguire il piano di ripartenza dei workload in base alla sequenza definita nella configurazione del Piano.

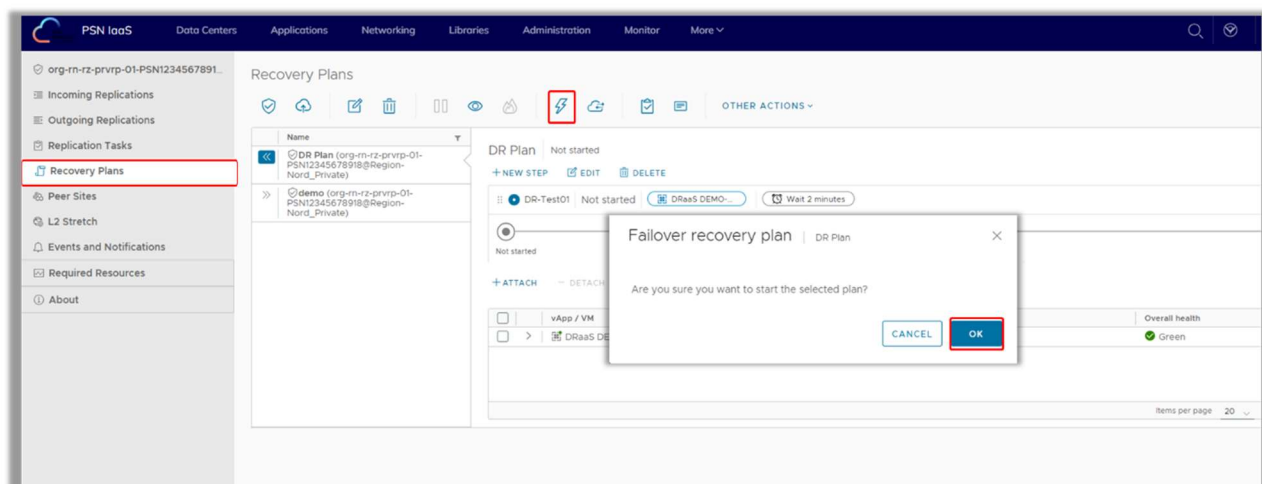


Figura 14: Attivazione Piano di Ripristino

Si Ricorda che il servizio DRaaS è distribuito tra le due Region (Sito Primario e di DR) e configurato in alta affidabilità. Tali configurazioni rendono il servizio sempre accessibile in modo da consentire alla PA di entrare nel proprio Tenant per eseguire le necessarie operazioni di ripristino.

4.21 *In caso di Disastro Reale, cosa posso fare?*

Nel momento in cui si verifica un disastro, la PA elegge il Sito di DR a Sito Primario ma i workload non saranno più soggetti a replica e quindi a protezione in caso di ulteriore disastro.

A questo punto, non appena la Cloud Region che ha subito il disastro torna operativa, si può procedere al ripristino della normale operatività in due modalità diverse:

- Spostare i workload attivi sul Sito di DR nel Sito Primario
- Trasformare il Sito di DR in Sito Primario e il precedente Sito Primario in Sito di DR

In entrambi i casi è comunque prevista la necessità di configurazione della Protezione dal Sito attivo verso il Sito ripristinato a valle del disastro e il ripristino delle configurazioni di rete.

Se si vogliono **spostare i workload attivi sul Sito di DR nel Sito Primario** si dovrà procedere ad un ulteriore operazione di Failover pianificata sul precedente Sito Primario.

Se invece si vuole **Trasformare il Sito di DR in Sito Primario** sarà sufficiente creare un Piano di Ripristino che preveda l'attivazione dei workload su quello che precedentemente era noto come Sito Primario e che invece diverrà il Sito di DR.

4.22 *Posso eseguire un le attività di Test, Clean-up e Failover per una singola VM?*

Sì, in base alle seguenti procedure:

- **Failover Test**
 - Nel riquadro, scegliere una direzione di Replica (Outgoing), cliccando *“Outgoing Replications”*
 - Selezionare una Protezione esistente per il failover
 - Cliccare *“All Action” > “Test”*
 - Seguire le indicazioni del wizard Test, contenente varie sezioni. A seconda dai siti di sorgente e destinazione configurare diverse impostazioni di failover per i workload selezionati

- La sezione *“Default Settings”* mostra il caso in cui la replica selezionata è già configurata con le impostazioni di recovery e vengono saltati i passaggi successivi selezionando *“Use preset Recovery Settings”*
- Nella sezione *“VM folder”*, selezionare la destinazione per l'archiviazione delle VM di test e cliccare *“Next”*
- In *“Compute Resource”*, selezionare una risorsa di calcolo di destinazione per le macchine virtuali di test fallite, quindi fare cliccare su *“Next”*
- In *“Network Mappings”*, selezionare una mappatura di rete per ogni adattatore collegato a ciascuna macchina virtuale, cliccare su *“Next”*
- Nella sezione *“Recovery Settings”*, selezionare la configurazione per i workload di test recuperati in base al sito di destinazione, cliccare su *“Next”*
- In *“Recovery Instance”*, se le istanze sono conservate, selezionare il punto di ripristino e cliccare su *“Next”*
- Nella sezione *“Ready To Complete”*, verificare che le impostazioni di failover siano corrette e cliccare su *“Finish”*

• **Clean-up**

- Selezionare la Replica da eliminare
- Cliccare su *“All Action”* > *“Test Cleanup”*
- Si apre una finestra, cliccare *“Cleanup”*

• **Failover**

- Nel riquadro, scegliere una direzione di Replica (*“Outcoming”*), cliccando *“Outgoing Replications”*
- Selezionare una replica esistente per il failover
- Cliccare *“All Action”* > *“Failover”*
- Seguire le indicazioni del wizard *“Failover”*, contenente varie sezioni. A seconda dai siti di sorgente e destinazione configurare diverse impostazioni di failover per i workload selezionati.
- La sezione *“Default Settings”* mostra il caso in cui la replica selezionata è già configurata con le impostazioni di recovery e vengono saltati i passaggi successivi selezionando *“Use preset Recovery Settings”*
- Nella sezione *“VM folder”*, selezionare la destinazione per l'archiviazione delle VM e cliccare *“Next”*

-
- In “Compute Resource”, selezionare una risorsa di calcolo di destinazione per le macchine virtuali fallite, quindi fare cliccare su “Next”
 - In “Network Mappings”, selezionare una mappatura di rete per ogni adattatore collegato a ciascuna macchina virtuale, cliccare su “Next”
 - Nella sezione “Recovery Settings”, selezionare la configurazione per i workload recuperati in base al sito di destinazione, cliccare su “Next”
 - In “Recovery Instance”, se le istanze sono conservate, selezionare il punto di ripristino e cliccare su “Next”
 - Nella sezione “Ready To Complete”, verificare che le impostazioni di failover siano corrette e cliccare su “Finish”