TR-4955: Disaster Recovery con Azure NetApp Files (ANF) e Azure VMware Solution (AVS)

NetApp public and hybrid cloud solutions

NetApp
August 18, 2025

Sommario

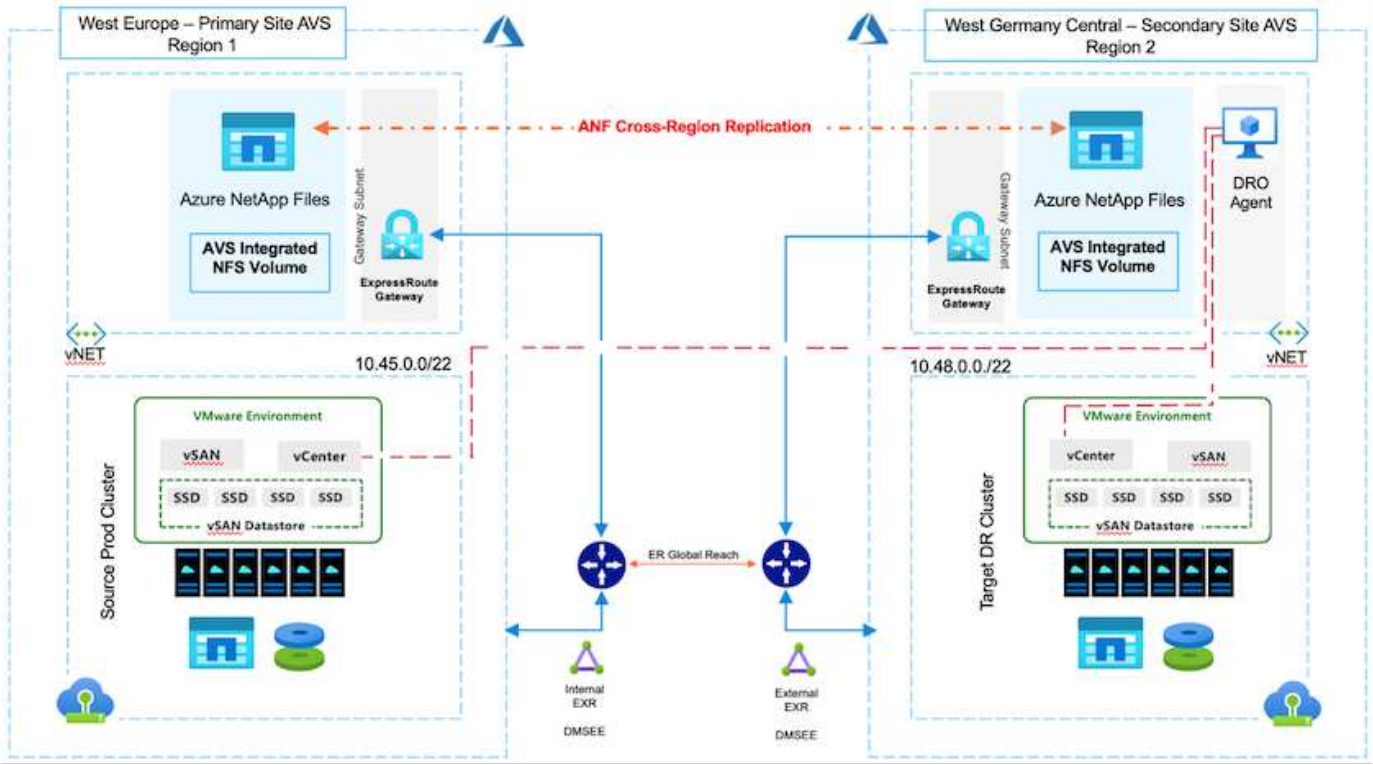
TR-4955: Disaster Recovery con Azure NetApp Files (ANF) e Azure VMware Solution (AVS)

Il disaster recovery mediante replica a livello di blocco tra regioni all'interno del cloud è un modo resiliente ed economico per proteggere i carichi di lavoro da interruzioni del sito ed eventi di danneggiamento dei dati (ad esempio, ransomware).

Panoramica

Grazie alla replica dei volumi tra regioni di Azure NetApp Files (ANF), i carichi di lavoro VMware in esecuzione su un sito SDDC di Azure VMware Solution (AVS) che utilizza volumi di Azure NetApp Files come datastore NFS sul sito AVS primario possono essere replicati su un sito AVS secondario designato nella regione di ripristino di destinazione.

Disaster Recovery Orchestrator (DRO) (una soluzione con script e interfaccia utente) può essere utilizzato per ripristinare senza problemi i carichi di lavoro replicati da un AVS SDDC a un altro. DRO automatizza il ripristino interrompendo il peering di replicazione e quindi montando il volume di destinazione come datastore, tramite la registrazione della VM su AVS, sui mapping di rete direttamente su NSX-T (incluso in tutti i cloud privati AVS).



Prerequisiti e raccomandazioni generali

- Verificare di aver abilitato la replica tra regioni creando un peering di replica. Vedere "Crea la replica del volume per Azure NetApp Files" .
- È necessario configurare ExpressRoute Global Reach tra i cloud privati di origine e di destinazione della soluzione Azure VMware.
- È necessario disporre di un'entità di servizio in grado di accedere alle risorse.

- È supportata la seguente topologia: dal sito AVS primario al sito AVS secondario.
- Configurare il "replicazione" pianificare per ogni volume in modo appropriato in base alle esigenze aziendali e alla velocità di modifica dei dati.

Le topologie a cascata e fan-in e fan-out non sono supportate.

Iniziare

Distribuisci la soluzione Azure VMware

IL "Soluzione Azure VMware" (AVS) è un servizio cloud ibrido che fornisce VMware SDDC completamente funzionali all'interno di un cloud pubblico Microsoft Azure. AVS è una soluzione proprietaria completamente gestita e supportata da Microsoft e verificata da VMware che utilizza l'infrastruttura Azure. Pertanto, i clienti ottengono VMware ESXi per la virtualizzazione del calcolo, vSAN per l'archiviazione iperconvergente e NSX per la rete e la sicurezza, il tutto sfruttando la presenza globale di Microsoft Azure, le strutture dei data center leader del settore e la vicinanza al ricco ecosistema di servizi e soluzioni Azure nativi. La combinazione di Azure VMware Solution SDDC e Azure NetApp Files garantisce le migliori prestazioni con una latenza di rete minima.

Per configurare un cloud privato AVS su Azure, seguire i passaggi descritti in questo"collegamento" per la documentazione NetApp e in questo "collegamento" per la documentazione Microsoft. Per scopi DR è possibile utilizzare un ambiente con luce pilota allestito con una configurazione minima. Questa configurazione contiene solo componenti essenziali per supportare le applicazioni critiche e può essere scalata e generare più host per gestire la maggior parte del carico in caso di failover.

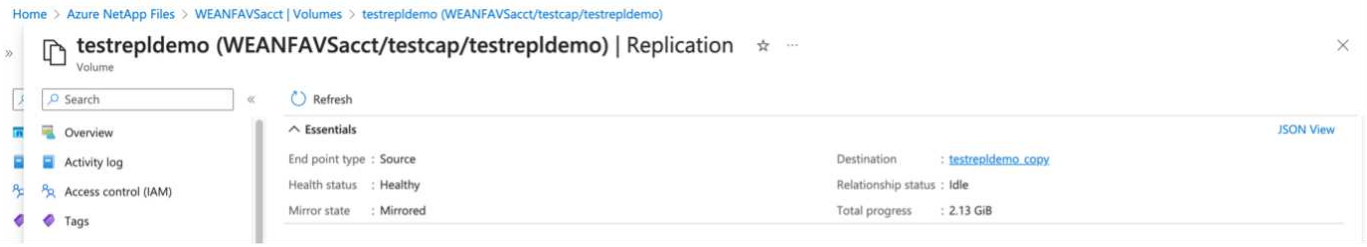
Nella versione iniziale, DRO supporta un cluster AVS SDDC esistente. La creazione di SDDC su richiesta sarà disponibile in una prossima versione.

Provisioning e configurazione Azure NetApp Files

"Azure NetApp Files"è un servizio di archiviazione file misurato, di classe enterprise e ad alte prestazioni. Segui i passaggi in questo "collegamento" per effettuare il provisioning e configurare Azure NetApp Files come datastore NFS per ottimizzare le distribuzioni cloud private AVS.

Crea la replica del volume per i volumi di datastore basati su Azure NetApp Files

Il primo passo è impostare la replica tra regioni per i volumi di datastore desiderati dal sito primario AVS al sito secondario AVS con le frequenze e le ritenzioni appropriate.



Segui i passaggi in questo "collegamento" per impostare la replicazione tra regioni creando un peering di replicazione. Il livello di servizio per il pool di capacità di destinazione può corrispondere a quello del pool di capacità di origine. Tuttavia, per questo caso d'uso specifico, è possibile selezionare il livello di servizio standard e quindi "modificare il livello di servizio" in caso di un vero disastro o di simulazioni DR.

Una relazione di replicazione tra regioni è un prerequisito e deve essere creata in anticipo.

Installazione DRO

Per iniziare a usare DRO, utilizzare il sistema operativo Ubuntu sulla macchina virtuale Azure designata e assicurarsi di soddisfare i prerequisiti. Quindi installare il pacchetto.

Prerequisiti:

- Entità del servizio che può accedere alle risorse.
- Assicurarsi che esista una connettività appropriata per le istanze SDDC di origine e di destinazione e Azure NetApp Files .
- Se si utilizzano nomi DNS, è necessario che sia attiva la risoluzione DNS. In caso contrario, utilizzare gli indirizzi IP per vCenter.

Requisiti del sistema operativo:

- Ubuntu Focal 20.04 (LTS)I seguenti pacchetti devono essere installati sulla macchina virtuale dell'agente designata:
- Docker
- Docker-componi
- JqChange `docker.sock` a questa nuova autorizzazione: `sudo chmod 666 /var/run/docker.sock`.

IL `deploy.sh` lo script esegue tutti i prerequisiti richiesti.

I passaggi sono i seguenti:

1. Scaricare il pacchetto di installazione sulla macchina virtuale designata:

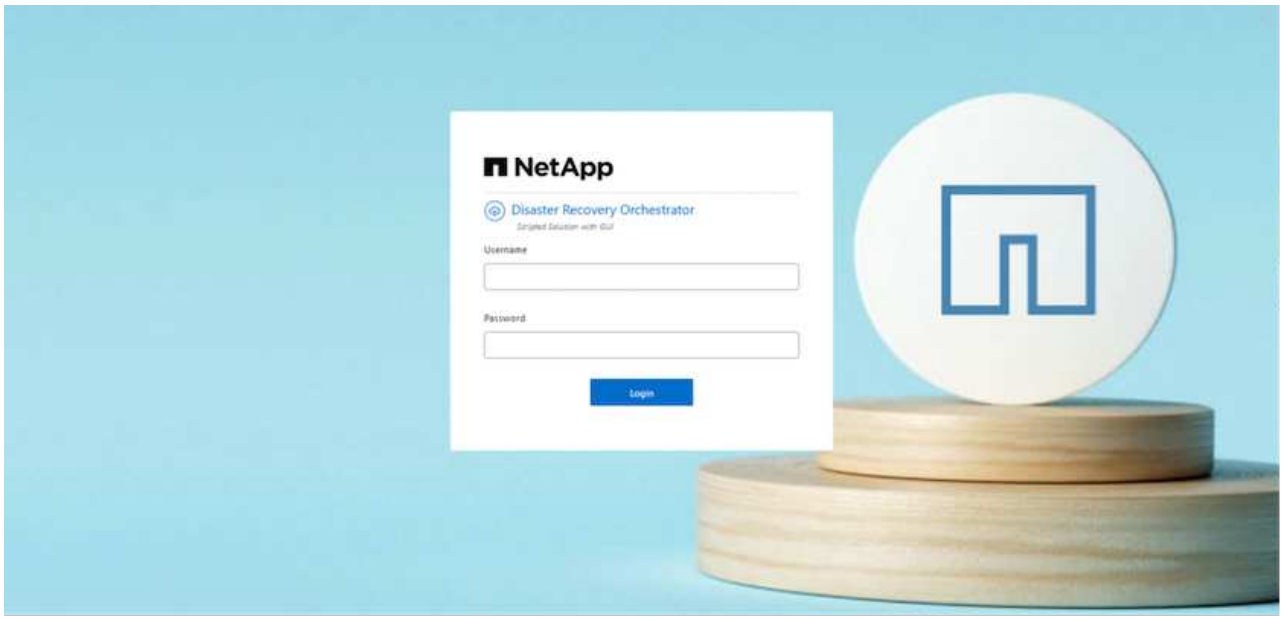
```
git clone https://github.com/NetApp/DRO-Azure.git
```

L'agente deve essere installato nella regione del sito AVS secondario o nella regione del sito AVS primario in una AZ separata rispetto all'SDDC.

2. Decomprimi il pacchetto, esegui lo script di distribuzione e inserisci l'IP host (ad esempio, `10.10.10.10`).

```
tar xvf draas_package.tar
Navigate to the directory and run the deploy script as below:
sudo sh deploy.sh
```

3. Accedi all'interfaccia utente utilizzando le seguenti credenziali:
   - Nome utente: `admin`
   - Password: `admin`



Configurazione DRO

Dopo aver configurato correttamente Azure NetApp Files e AVS, è possibile iniziare a configurare DRO per automatizzare il ripristino dei carichi di lavoro dal sito AVS primario al sito AVS secondario. NetApp consiglia di distribuire l'agente DRO nel sito AVS secondario e di configurare la connessione gateway ExpressRoute in modo che l'agente DRO possa comunicare tramite la rete con i componenti AVS e Azure NetApp Files appropriati.

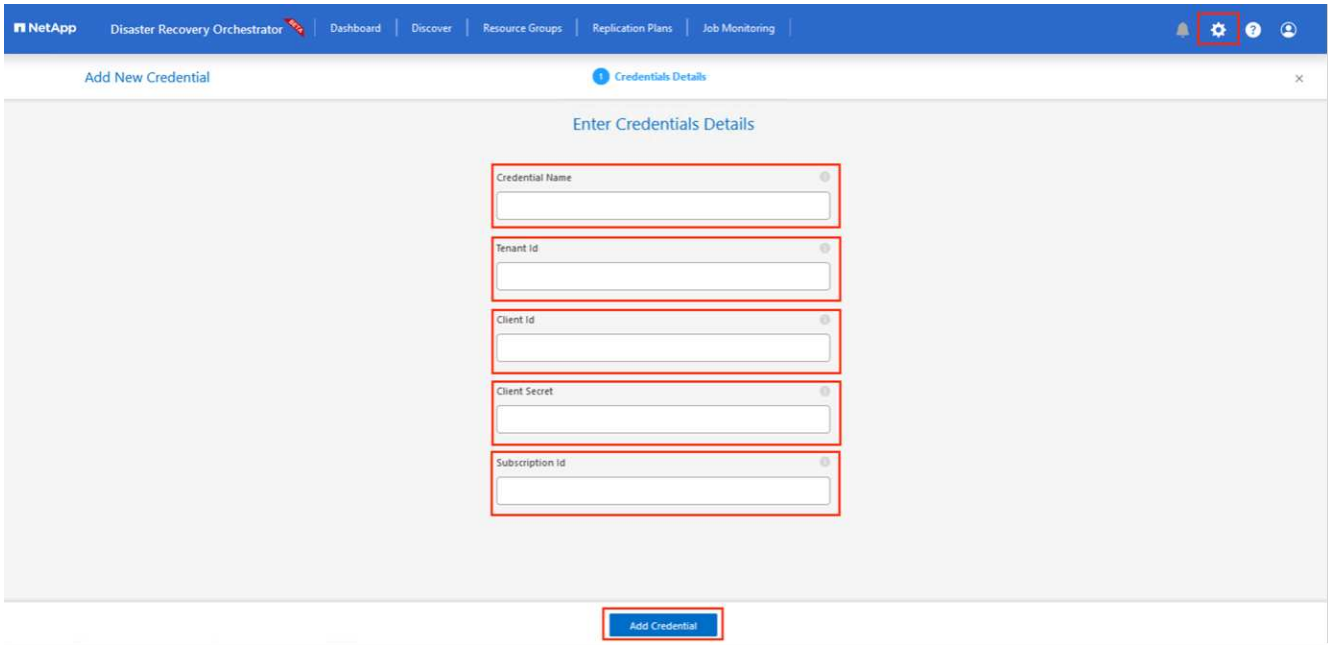
Il primo passo è aggiungere le credenziali. DRO richiede l'autorizzazione per individuare Azure NetApp Files e la soluzione Azure VMware. È possibile concedere le autorizzazioni necessarie a un account Azure creando e configurando un'applicazione Azure Active Directory (AD) e ottenendo le credenziali Azure necessarie a DRO. È necessario associare l'entità servizio alla sottoscrizione di Azure e assegnarle un ruolo personalizzato che disponga delle autorizzazioni richieste. Quando si aggiungono ambienti di origine e di destinazione, viene richiesto di selezionare le credenziali associate al servizio principale. È necessario aggiungere queste credenziali a DRO prima di poter fare clic su Aggiungi nuovo sito.

Per eseguire questa operazione, completare i seguenti passaggi:

1. Apri DRO in un browser supportato e usa il nome utente e la password predefiniti/`admin`/`admin`). La password può essere reimpostata dopo il primo accesso utilizzando l'opzione Cambia password.
2. Nell'angolo in alto a destra della console DRO, fare clic sull'icona **Impostazioni** e selezionare **Credenziali**.
3. Fare clic su Aggiungi nuove credenziali e seguire i passaggi della procedura guidata.
4. Per definire le credenziali, immettere le informazioni sull'entità servizio di Azure Active Directory che concede le autorizzazioni richieste:
   - Nome della credenziale
   - ID inquilino
   - ID cliente
   - Segreto del cliente
   - ID abbonamento

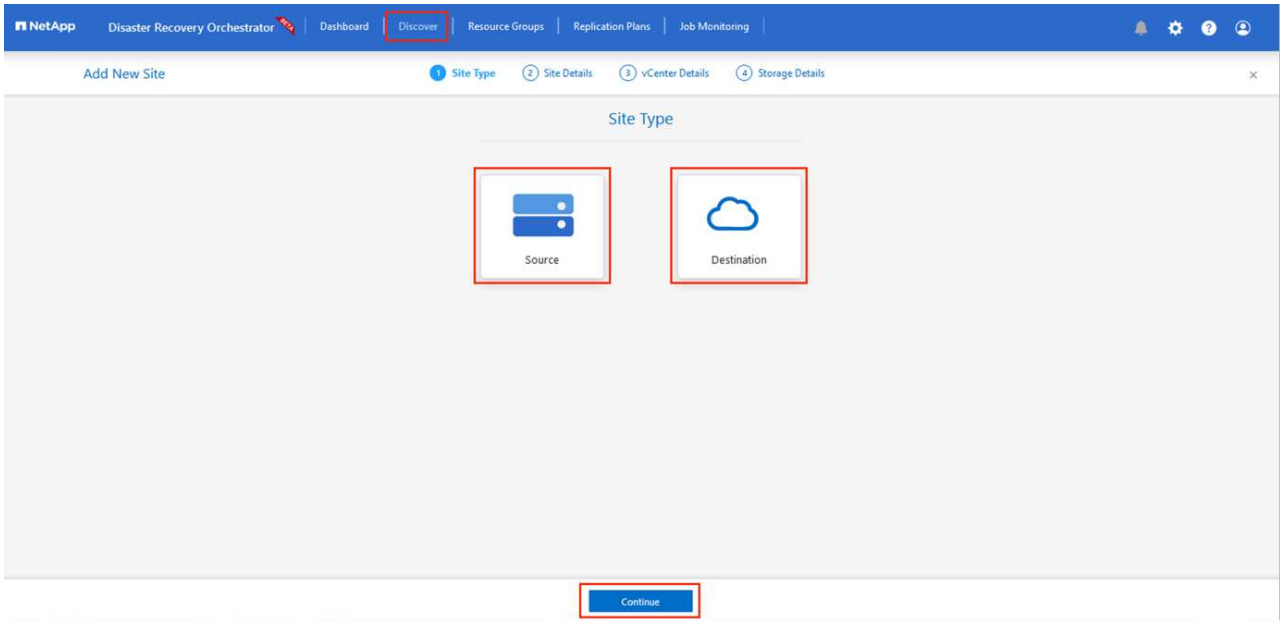
   Avresti dovuto acquisire queste informazioni quando hai creato l'applicazione AD.

5. Conferma i dettagli sulle nuove credenziali e fai clic su Aggiungi credenziale.



Dopo aver aggiunto le credenziali, è il momento di individuare e aggiungere i siti AVS primari e secondari (sia vCenter che l'account di archiviazione dei file di Azure NetApp) a DRO. Per aggiungere il sito di origine e quello di destinazione, completare i seguenti passaggi:

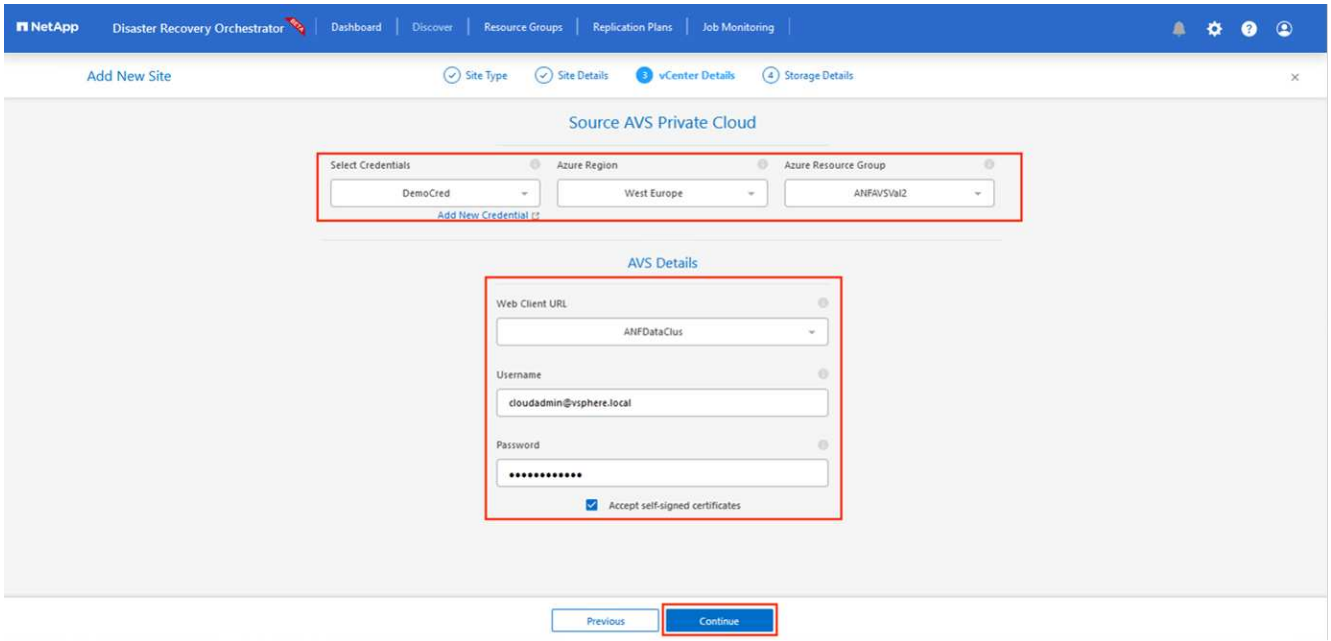
6. Vai alla scheda **Scopri**.
7. Fare clic su **Aggiungi nuovo sito**.
8. Aggiungere il seguente sito AVS primario (designato come **Origine** nella console).
   - SDDC vCenter
   - Account di archiviazione Azure NetApp Files
9. Aggiungere il seguente sito AVS secondario (designato come **Destinazione** nella console).
   - SDDC vCenter
   - Account di archiviazione Azure NetApp Files



10. Aggiungi i dettagli del sito cliccando su **Origine**, immettendo un nome descrittivo per il sito e selezionando il connettore. Quindi fare clic su **Continua**.

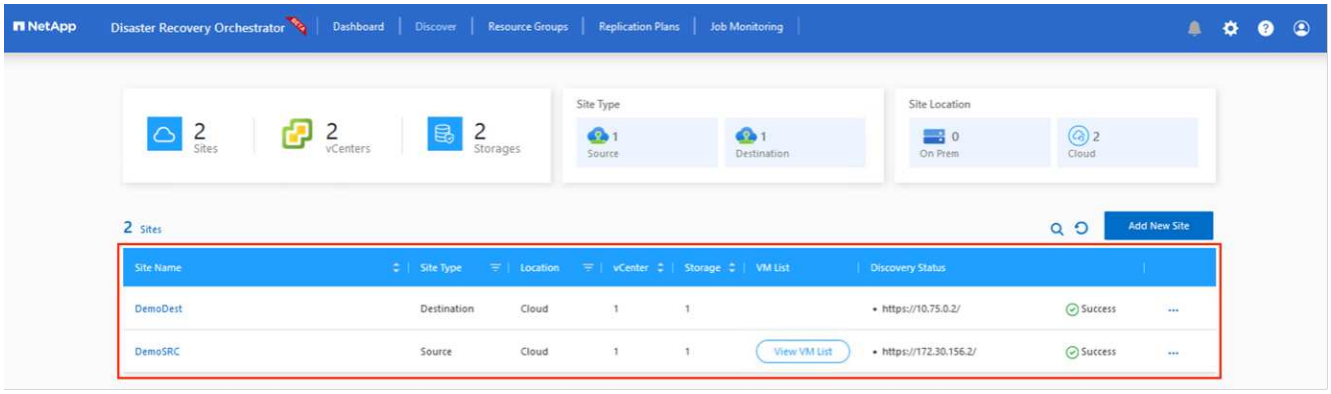
> A scopo dimostrativo, in questo documento viene trattata l'aggiunta di un sito sorgente.

11. Aggiornare i dettagli di vCenter. Per fare ciò, seleziona le credenziali, la regione di Azure e il gruppo di risorse dal menu a discesa per l'SDDC AVS primario.
12. DRO elenca tutti gli SDDC disponibili nella regione. Selezionare l'URL del cloud privato designato dal menu a discesa.
13. Entra nel `cloudadmin@vsphere.local` credenziali utente. È possibile accedervi dal portale di Azure. Seguire i passaggi indicati in questo "collegamento" . Una volta fatto, clicca su **Continua**.

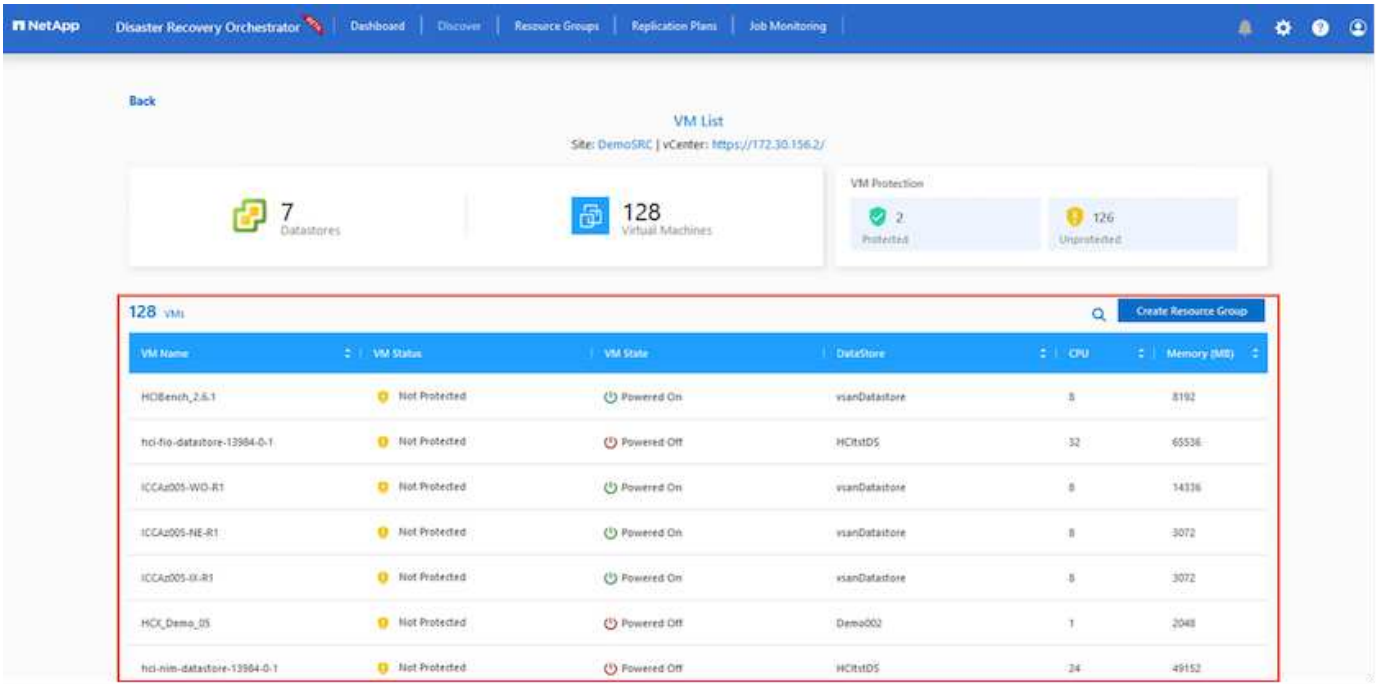


14. Selezionare i dettagli dell'archivio di origine (ANF) selezionando il gruppo di risorse di Azure e l'account NetApp .

15. Fare clic su **Crea sito**.



Una volta aggiunto, DRO esegue la rilevazione automatica e visualizza le VM che dispongono di repliche interregionali corrispondenti dal sito di origine al sito di destinazione. DRO rileva automaticamente le reti e i segmenti utilizzati dalle VM e li popola.



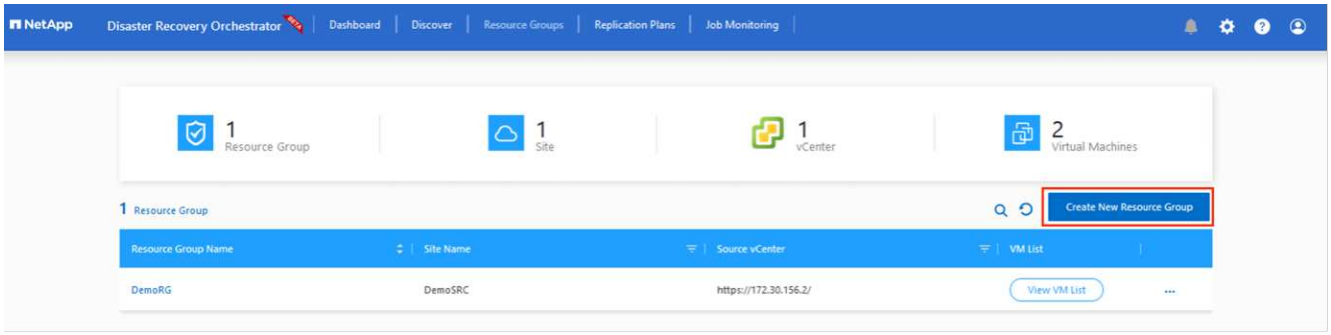
Il passaggio successivo consiste nel raggruppare le VM richieste nei rispettivi gruppi funzionali come gruppi di risorse.

Raggruppamenti di risorse

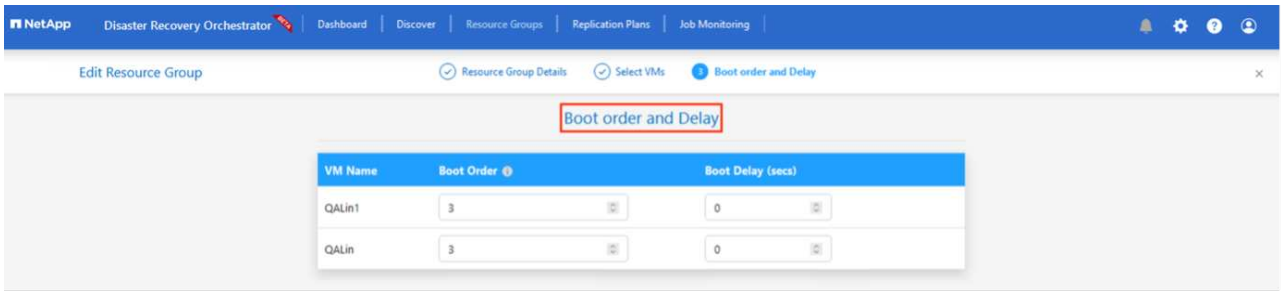
Dopo aver aggiunto le piattaforme, raggruppa le VM che desideri ripristinare in gruppi di risorse. I gruppi di risorse DRO consentono di raggruppare un set di VM dipendenti in gruppi logici che contengono i relativi ordini di avvio, ritardi di avvio e convalide facoltative delle applicazioni che possono essere eseguite al momento del ripristino.

Per iniziare a creare gruppi di risorse, fare clic sulla voce di menu **Crea nuovo gruppo di risorse**.

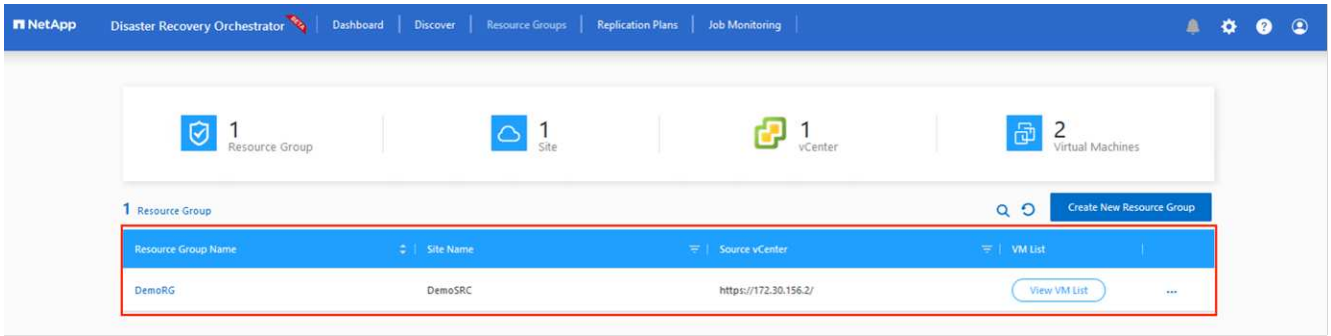
1. Accedi a **Gruppi di risorse** e fai clic su **Crea nuovo gruppo di risorse**.



2. In Nuovo gruppo di risorse, seleziona il sito di origine dal menu a discesa e fai clic su **Crea**.
3. Fornisci i dettagli del gruppo di risorse e fai clic su **Continua**.
4. Selezionare le VM appropriate utilizzando l'opzione di ricerca.
5. Selezionare **Ordine di avvio** e **Ritardo di avvio** (sec) per tutte le VM selezionate. Imposta l'ordine della sequenza di accensione selezionando ogni macchina virtuale e impostandone la priorità. Il valore predefinito per tutte le macchine virtuali è 3. Le opzioni sono le seguenti:
   - La prima macchina virtuale ad accendersi
   - Predefinito
   - L'ultima macchina virtuale ad accendersi



6. Fare clic su **Crea gruppo di risorse**.

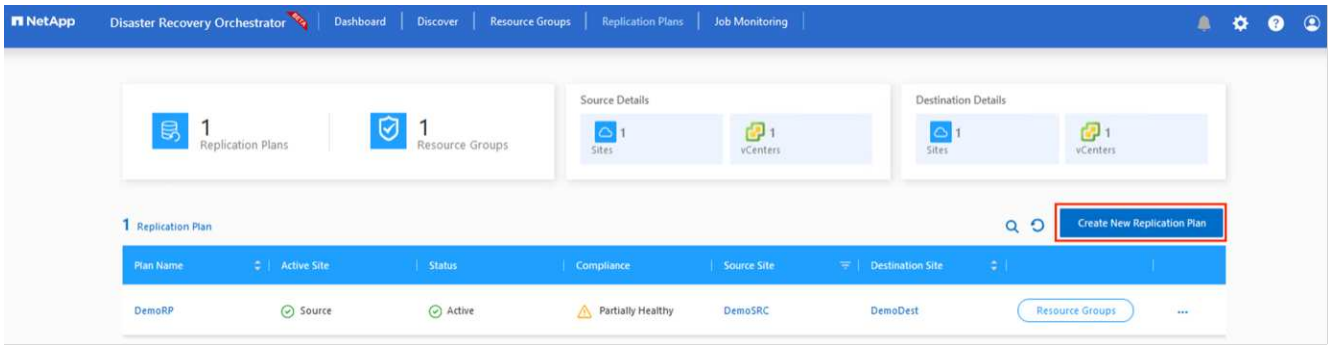


Piani di replicazione

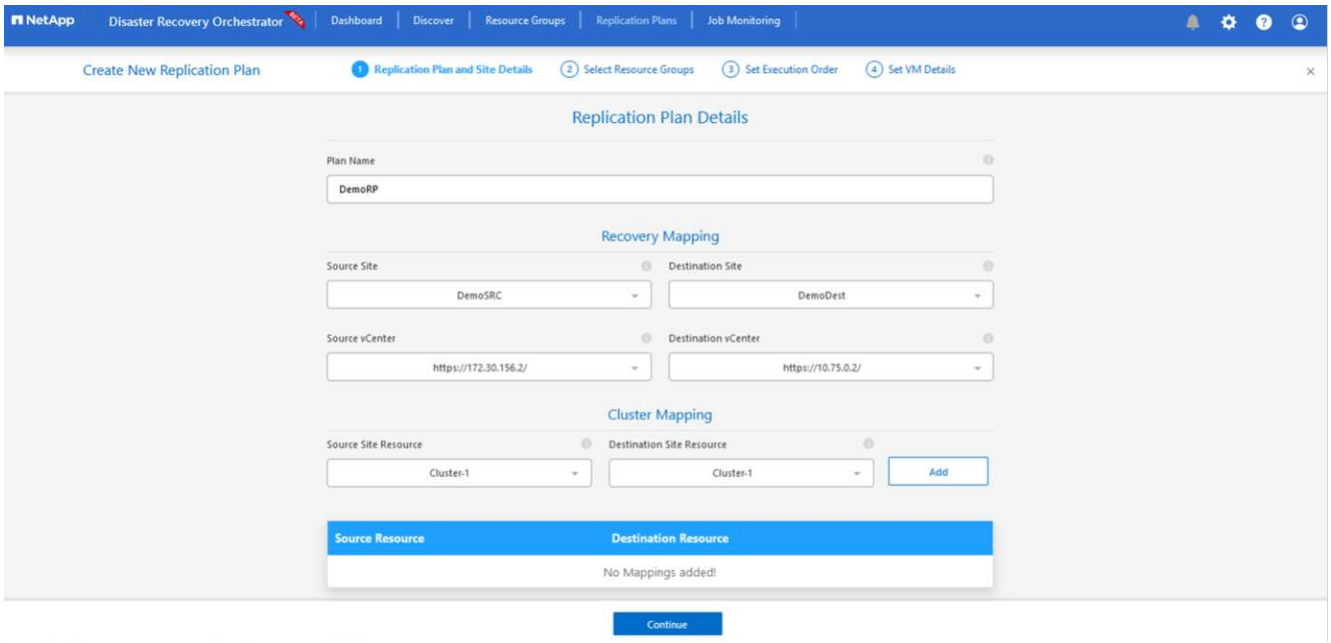
È necessario disporre di un piano per ripristinare le applicazioni in caso di disastro. Selezionare le piattaforme vCenter di origine e di destinazione dal menu a discesa, scegliere i gruppi di risorse da includere in questo piano e includere anche il raggruppamento delle modalità di ripristino e accensione delle applicazioni (ad esempio, controller di dominio, livello 1, livello 2 e così via). I piani vengono spesso chiamati anche blueprint. Per definire il piano di ripristino, accedere alla scheda Piano di replica e fare clic su **Nuovo piano di replica**.

Per iniziare a creare un piano di replicazione, completare i seguenti passaggi:

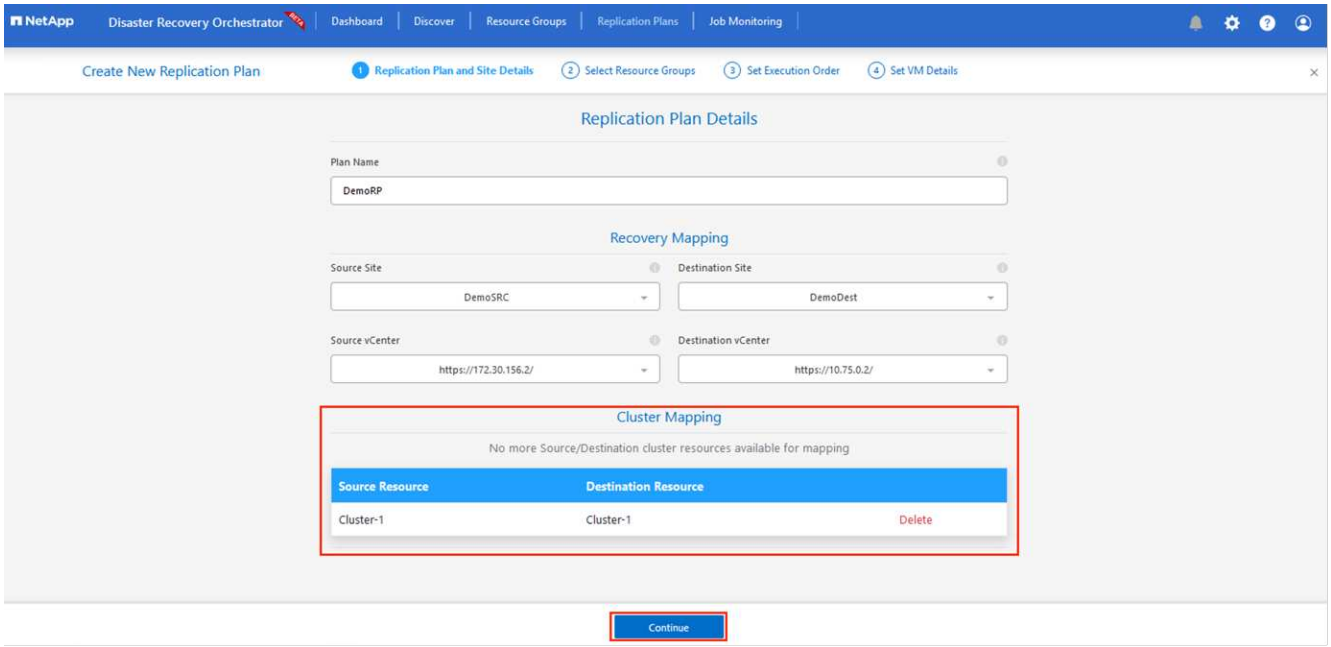
1. Passare a **Piani di replicazione** e fare clic su **Crea nuovo piano di replicazione**.



2. Nel **Nuovo piano di replica**, fornire un nome per il piano e aggiungere i mapping di ripristino selezionando il sito di origine, il vCenter associato, il sito di destinazione e il vCenter associato.

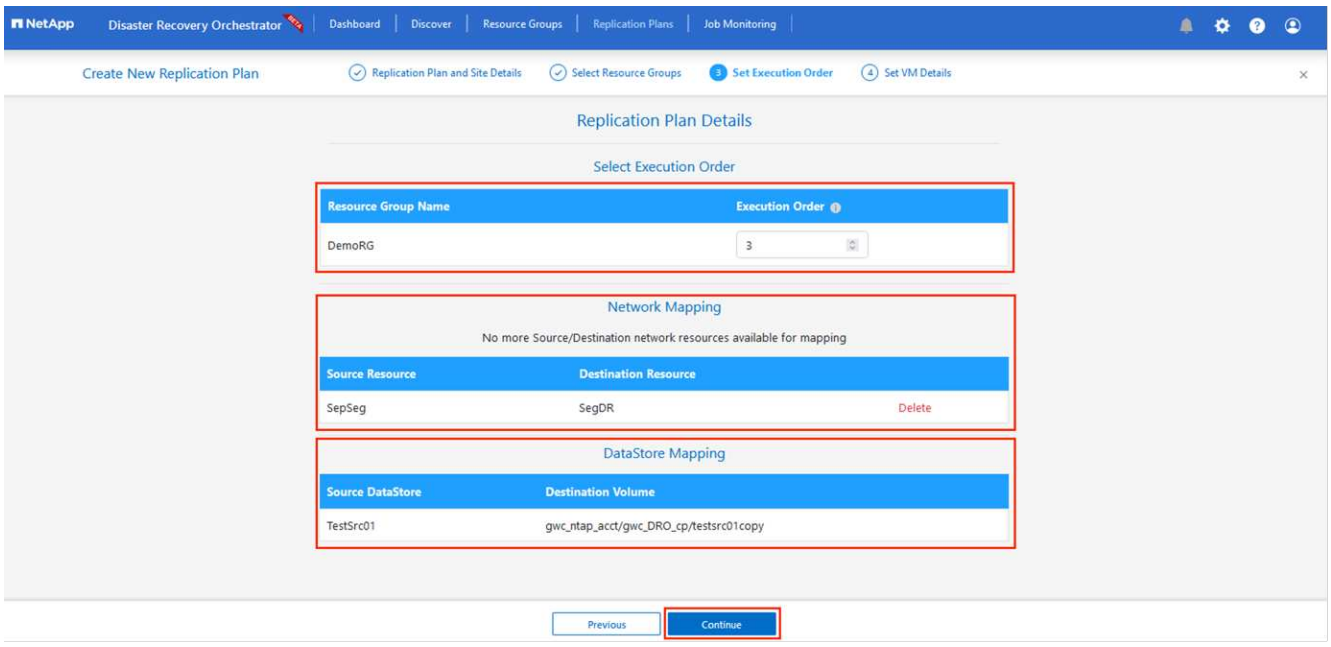


3. Una volta completata la mappatura del ripristino, selezionare **Cluster Mapping**.



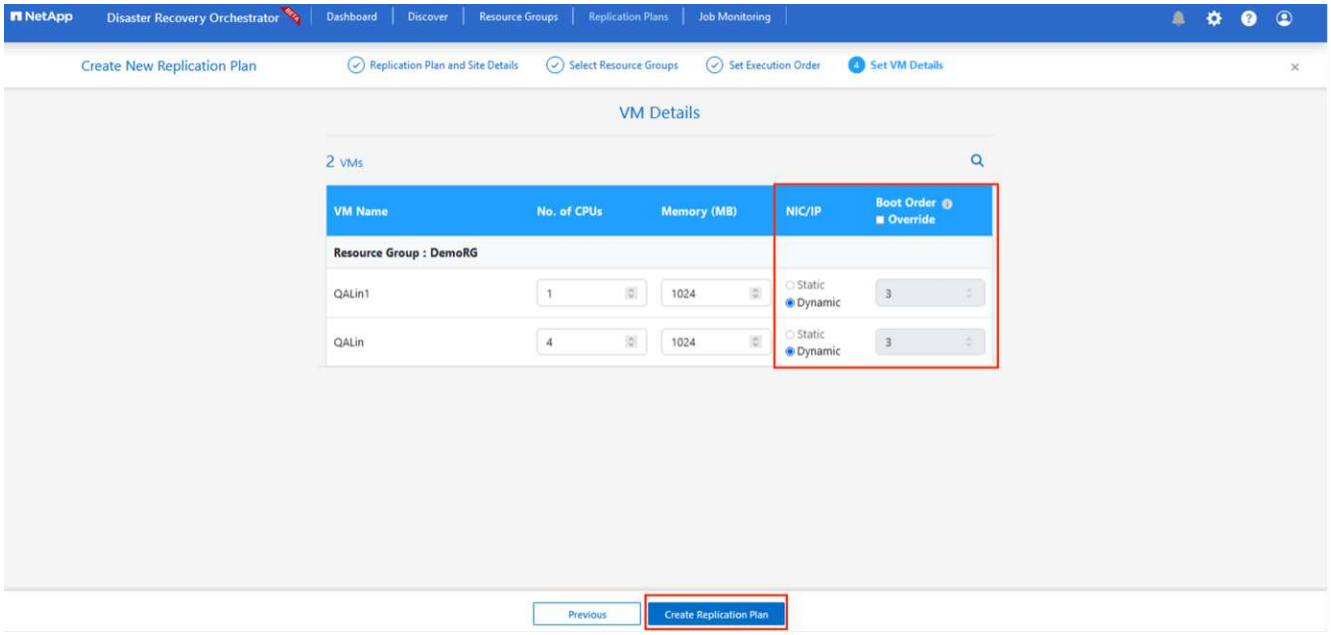
4. Selezionare **Dettagli gruppo di risorse** e fare clic su **Continua**.
5. Imposta l'ordine di esecuzione per il gruppo di risorse. Questa opzione consente di selezionare la sequenza delle operazioni quando sono presenti più gruppi di risorse.
6. Una volta fatto, imposta la mappatura di rete sul segmento appropriato. I segmenti dovrebbero essere già forniti sul cluster AVS secondario e, per mappare le VM su di essi, selezionare il segmento appropriato.
7. Le mappature dei datastore vengono selezionate automaticamente in base alla selezione delle VM.

> La replicazione interregionale (CRR) avviene a livello di volume. Pertanto, tutte le VM residenti sul rispettivo volume vengono replicate nella destinazione CRR. Assicurarsi di selezionare tutte le VM che fanno parte del datastore, perché vengono elaborate solo le macchine virtuali che fanno parte del piano di replica.

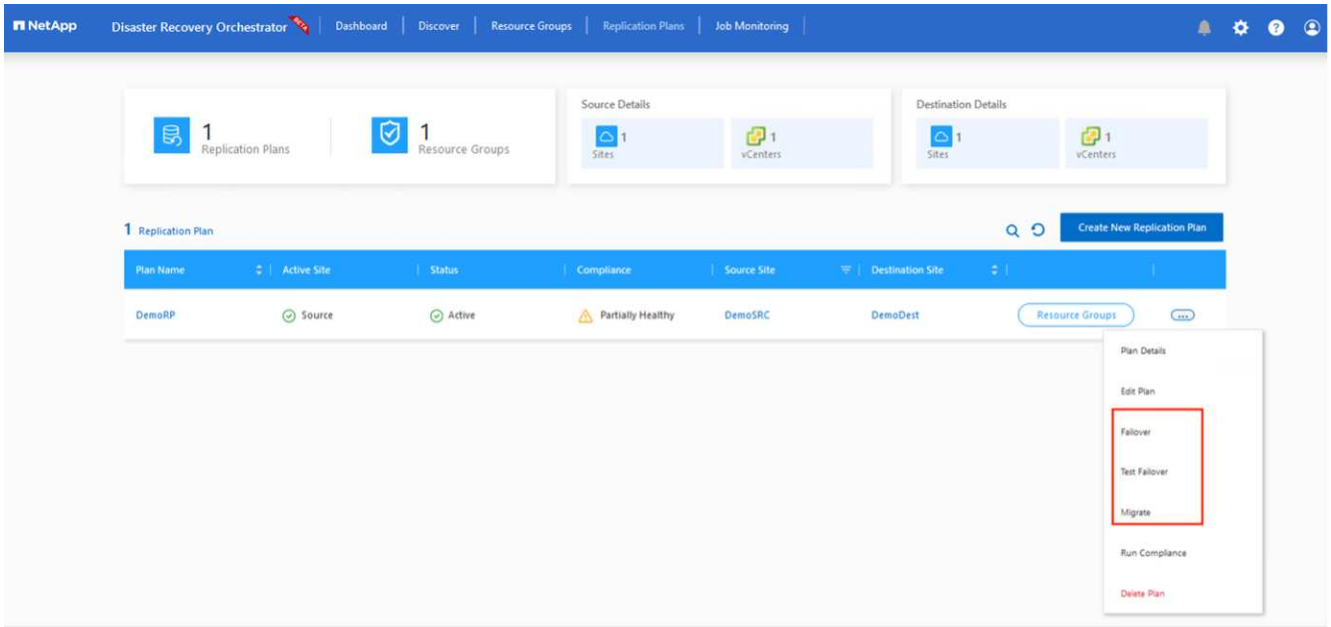


8. In Dettagli VM, è possibile ridimensionare facoltativamente i parametri CPU e RAM delle VM. Ciò può

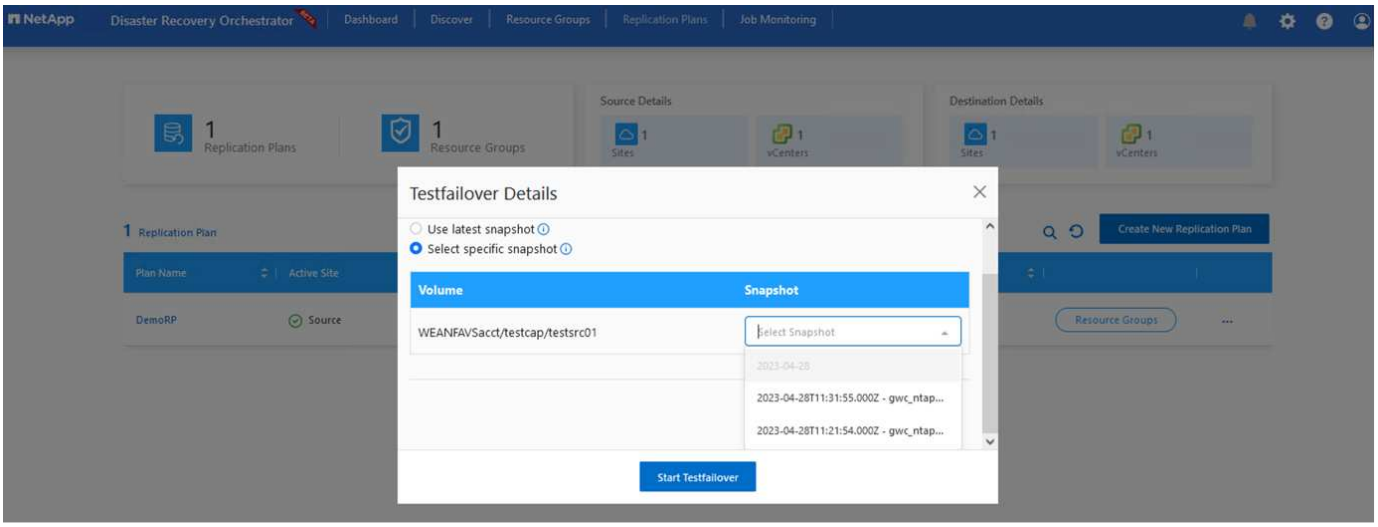
essere molto utile quando si ripristinano ambienti di grandi dimensioni in cluster di destinazione più piccoli o quando si eseguono test di ripristino di emergenza senza dover predisporre un'infrastruttura VMware fisica uno a uno. Modificare inoltre l'ordine di avvio e il ritardo di avvio (in secondi) per tutte le VM selezionate nei gruppi di risorse. Esiste un'opzione aggiuntiva per modificare l'ordine di avvio se sono necessarie modifiche rispetto a quanto selezionato durante la selezione dell'ordine di avvio del gruppo di risorse. Per impostazione predefinita, viene utilizzato l'ordine di avvio selezionato durante la selezione del gruppo di risorse, tuttavia è possibile apportare modifiche in questa fase.



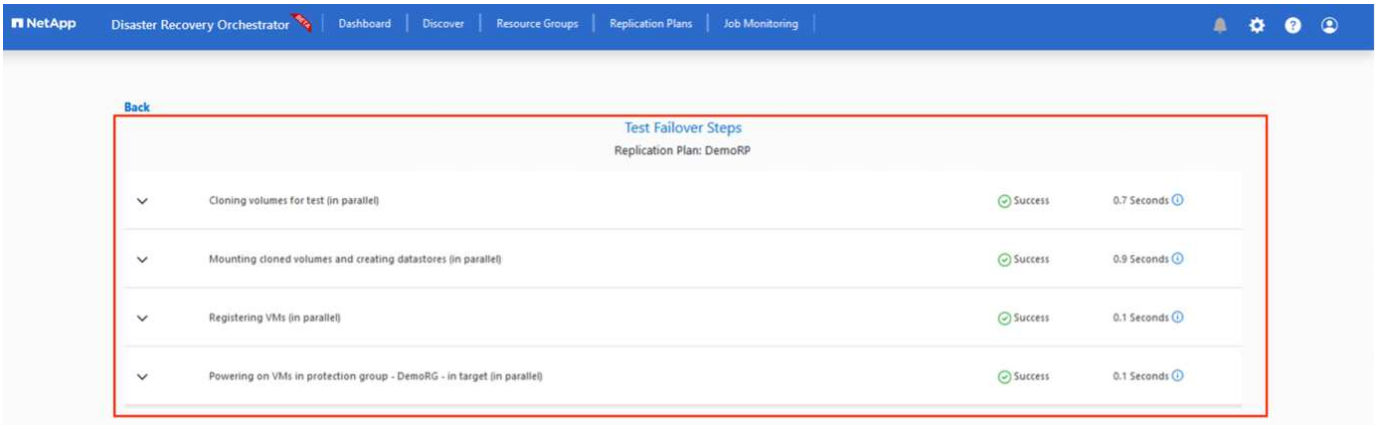
9. Fare clic su **Crea piano di replicazione**. Dopo aver creato il piano di replicazione, è possibile utilizzare le opzioni di failover, failover di prova o migrazione, a seconda delle proprie esigenze.



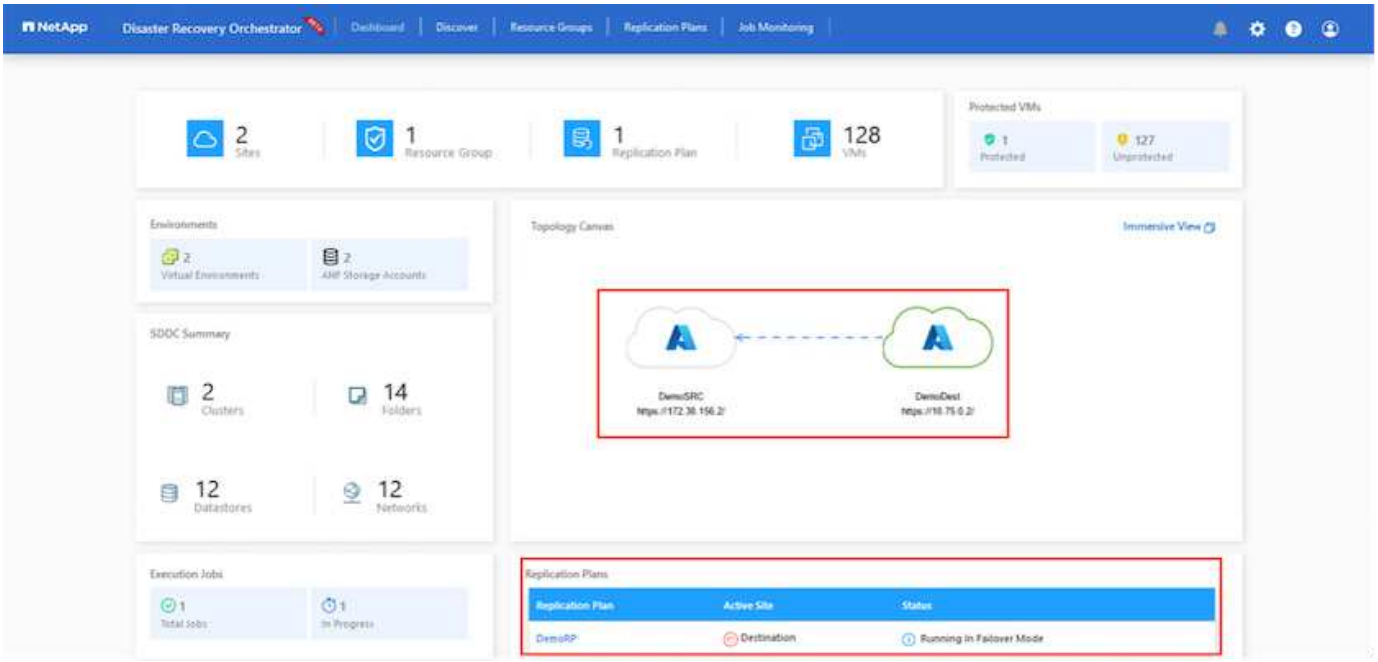
Durante le opzioni di failover e di test failover, viene utilizzato lo snapshot più recente oppure è possibile selezionare uno snapshot specifico da uno snapshot point-in-time. L'opzione point-in-time può essere molto utile se si sta affrontando un evento di corruzione come un ransomware, in cui le repliche più recenti sono già compromesse o crittografate. DRO mostra tutti i punti temporali disponibili.



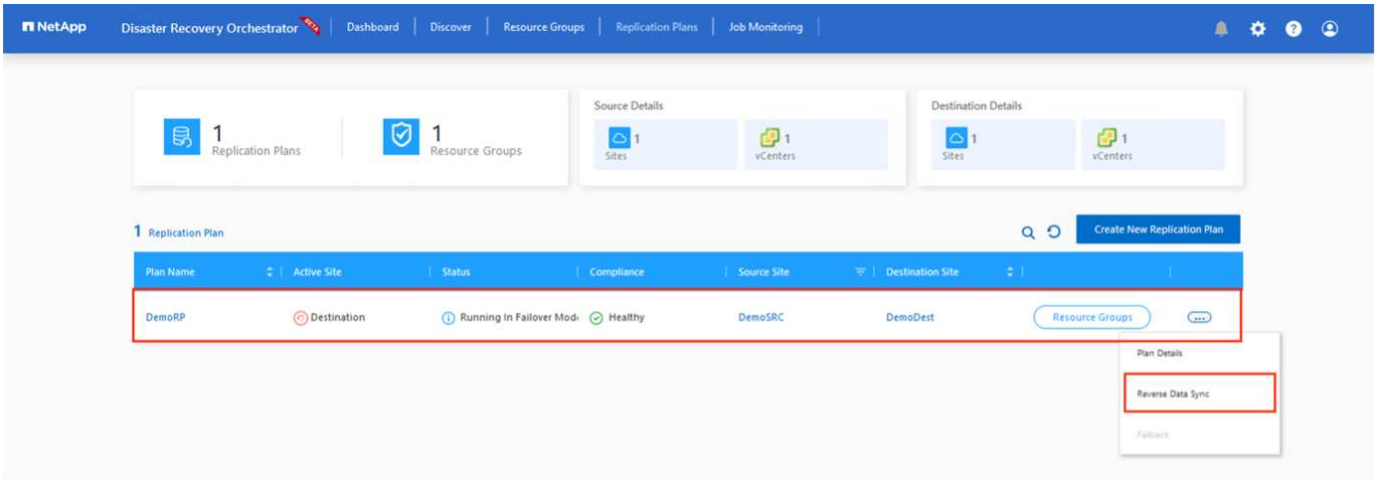
Per attivare il failover o il failover di prova con la configurazione specificata nel piano di replica, è possibile fare clic su **Failover** o **Failover di prova**. È possibile monitorare il piano di replicazione nel menu delle attività.



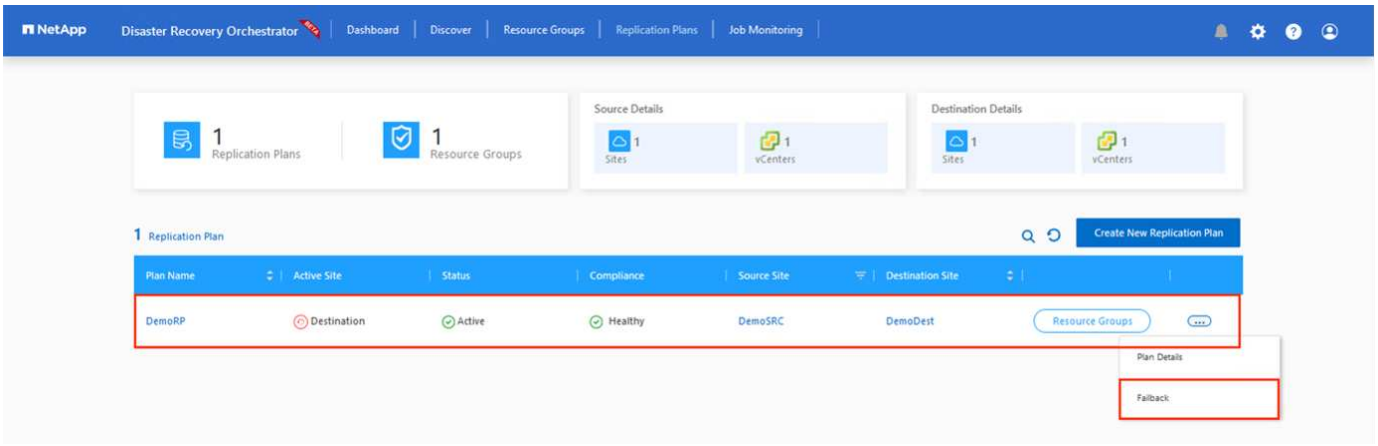
Dopo l'attivazione del failover, gli elementi recuperati possono essere visualizzati nel sito secondario AVS SDDC vCenter (VM, reti e datastore). Per impostazione predefinita, le VM vengono ripristinate nella cartella Workload.

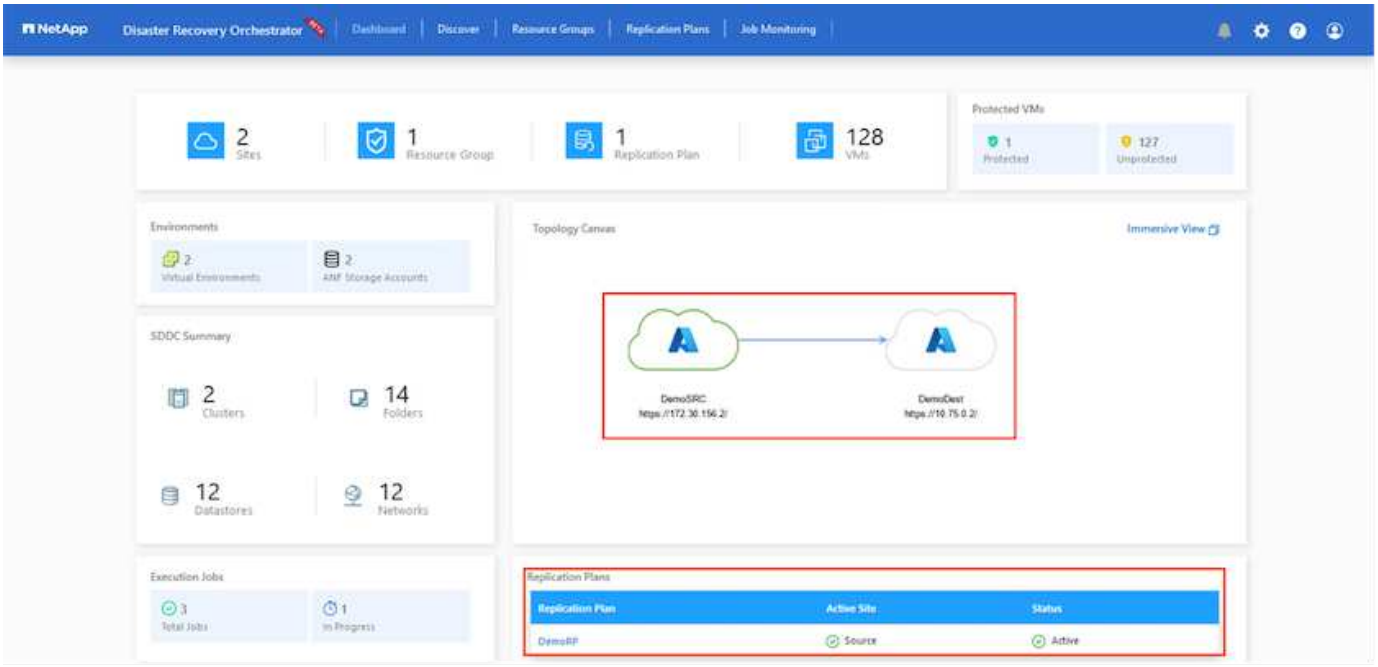


Il failback può essere attivato a livello del piano di replica. In caso di failover del test, è possibile utilizzare l'opzione tear down per annullare le modifiche e rimuovere il volume appena creato. I failback correlati al failover sono un processo in due fasi. Selezionare il piano di replicazione e selezionare **Sincronizzazione dati inversa**.



Una volta completato questo passaggio, attivare il failback per tornare al sito AVS primario.





Dal portale di Azure possiamo vedere che lo stato di integrità della replica è stato interrotto per i volumi appropriati che erano stati mappati sul sito secondario AVS SDDC come volumi di lettura/scrittura. Durante il failover di prova, DRO non mappa il volume di destinazione o di replica. Crea invece un nuovo volume dello snapshot di replica tra regioni richiesto ed espone il volume come un datastore, che consuma ulteriore capacità fisica dal pool di capacità e garantisce che il volume di origine non venga modificato. In particolare, i processi di replicazione possono continuare durante i test DR o i flussi di lavoro di triage. Inoltre, questo processo garantisce che il ripristino possa essere ripulito senza il rischio che la replica venga distrutta in caso di errori o di recupero di dati danneggiati.

Recupero da ransomware

Recuperare i dati da un ransomware può essere un compito arduo. Nello specifico, può essere difficile per le organizzazioni IT individuare con precisione qual è il punto di ritorno sicuro e, una volta determinato, come garantire che i carichi di lavoro recuperati siano protetti dagli attacchi ricorrenti (ad esempio, da malware inattivi o tramite applicazioni vulnerabili).

DRO affronta queste problematiche consentendo alle organizzazioni di recuperare da qualsiasi momento disponibile. I carichi di lavoro vengono quindi ripristinati su reti funzionali ma isolate, in modo che le applicazioni possano funzionare e comunicare tra loro senza essere esposte al traffico nord-sud. Questo processo offre ai team di sicurezza un luogo sicuro in cui condurre analisi forensi e identificare eventuali

malware nascosti o inattivi.

Conclusione

La soluzione di disaster recovery Azure NetApp Files e Azure VMware offre i seguenti vantaggi:

- Sfrutta la replica efficiente e resiliente tra più regioni Azure NetApp Files .
- Ripristina qualsiasi punto temporale disponibile con la conservazione degli snapshot.
- Automatizza completamente tutti i passaggi necessari per ripristinare centinaia o migliaia di VM dalle fasi di archiviazione, elaborazione, rete e convalida delle applicazioni.
- Il ripristino del carico di lavoro sfrutta il processo "Crea nuovi volumi dagli snapshot più recenti", che non manipola il volume replicato.
- Evita qualsiasi rischio di danneggiamento dei dati sui volumi o sugli snapshot.
- Evitare interruzioni della replica durante i flussi di lavoro dei test DR.
- Sfrutta i dati DR e le risorse di elaborazione cloud per flussi di lavoro che vanno oltre il DR, come sviluppo/test, test di sicurezza, test di patch e aggiornamenti e test di correzione.
- L'ottimizzazione di CPU e RAM può contribuire a ridurre i costi del cloud consentendo il ripristino su cluster di elaborazione più piccoli.

Dove trovare ulteriori informazioni

Per saperne di più sulle informazioni descritte nel presente documento, consultare i seguenti documenti e/o siti web:

- Crea la replica del volume per Azure NetApp Files

  "https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-create-peering"

- Replica tra regioni di volumi di Azure NetApp Files

  "https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-introduction#service-level-objectives"

- "Soluzione Azure VMware"

  "https://learn.microsoft.com/en-us/azure/azure-vmware/introduction"

- Distribuire e configurare l'ambiente di virtualizzazione su Azure

  "Configurazione di AVS su Azure"

- Distribuisci e configura la soluzione Azure VMware

  https://learn.microsoft.com/en-us/azure/azure-vmware/deploy-azure-vmware-solution?tabs=azure-portal

Informazioni sul copyright

Informazioni sul marchio commerciale