Disaster Recovery con ANF e JetStream

NetApp public and hybrid cloud solutions

NetApp
August 18, 2025

Sommario

Disaster Recovery con ANF e JetStream

Il disaster recovery nel 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). Utilizzando il framework VMware VAIO, i carichi di lavoro VMware locali possono essere replicati nell'archiviazione BLOB di Azure e ripristinati, consentendo una perdita di dati minima o quasi nulla e un RTO prossimo allo zero.

JetStream DR può essere utilizzato per ripristinare senza problemi i carichi di lavoro replicati da locale ad AVS e in particolare ad Azure NetApp Files. Consente un disaster recovery conveniente utilizzando risorse minime nel sito DR e un archivio cloud conveniente. JetStream DR automatizza il ripristino nei datastore ANF tramite Azure Blob Storage. JetStream DR recupera VM indipendenti o gruppi di VM correlate nell'infrastruttura del sito di ripristino in base alla mappatura di rete e fornisce un ripristino puntuale per la protezione dal ransomware.

Questo documento fornisce una comprensione dei principi operativi di JetStream DR e dei suoi componenti principali.

Panoramica della distribuzione della soluzione

1. Installare il software JetStream DR nel data center locale.
   a. Scarica il pacchetto software JetStream DR da Azure Marketplace (ZIP) e distribuisci JetStream DR MSA (OVA) nel cluster designato.
   b. Configurare il cluster con il pacchetto filtro I/O (installare JetStream VIB).
   c. Eseguire il provisioning di Azure Blob (account di archiviazione di Azure) nella stessa area del cluster DR AVS.
   d. Distribuisci appliance DRVA e assegna volumi di log di replicazione (VMDK da datastore esistente o storage iSCSI condiviso).
   e. Creare domini protetti (gruppi di VM correlate) e assegnare DRVA e Azure Blob Storage/ANF.
   f. Protezione iniziale.
2. Installare il software JetStream DR nel cloud privato Azure VMware Solution.
   a. Utilizzare il comando Esegui per installare e configurare JetStream DR.
   b. Aggiungere lo stesso contenitore BLOB di Azure e individuare i domini utilizzando l'opzione Scansiona domini.
   c. Distribuire gli apparecchi DRVA richiesti.
   d. Creare volumi di log di replicazione utilizzando i datastore vSAN o ANF disponibili.
   e. Importa domini protetti e configura RocVA (VA di ripristino) per utilizzare il datastore ANF per i posizionamenti delle VM.
   f. Selezionare l'opzione di failover appropriata e avviare la reidratazione continua per domini o VM con RTO prossimo allo zero.
3. Durante un evento di emergenza, attiva il failover nei datastore di Azure NetApp Files nel sito AVS DR designato.
4. Richiamare il failback al sito protetto dopo che il sito protetto è stato ripristinato. Prima di iniziare, assicurarsi che i prerequisiti siano soddisfatti come indicato in questo "collegamento" ed eseguire anche lo strumento di test della larghezza di banda (BWT) fornito da JetStream Software per valutare le potenziali prestazioni dell'archiviazione BLOB di Azure e la sua larghezza di banda di replica quando utilizzato con il software JetStream DR. Dopo aver soddisfatto i prerequisiti, inclusa la connettività, configurare e abbonarsi a JetStream DR per AVS da "Azure Marketplace" . Dopo aver scaricato il pacchetto software, procedere con il processo di installazione descritto sopra.

Quando si pianifica e si avvia la protezione per un numero elevato di VM (ad esempio, più di 100), utilizzare lo strumento di pianificazione della capacità (CPT) di JetStream DR Automation Toolkit. Fornire un elenco delle VM da proteggere insieme alle relative preferenze RTO e gruppo di ripristino, quindi eseguire CPT.

Il CPT svolge le seguenti funzioni:

- Combinazione di VM in domini di protezione in base al loro RTO.
- Definizione del numero ottimale di DRVA e delle relative risorse.
- Stima della larghezza di banda di replicazione richiesta.
- Identificazione delle caratteristiche del volume del registro di replicazione (capacità, larghezza di banda e così via).
- Stima della capacità di archiviazione degli oggetti richiesta e altro ancora.

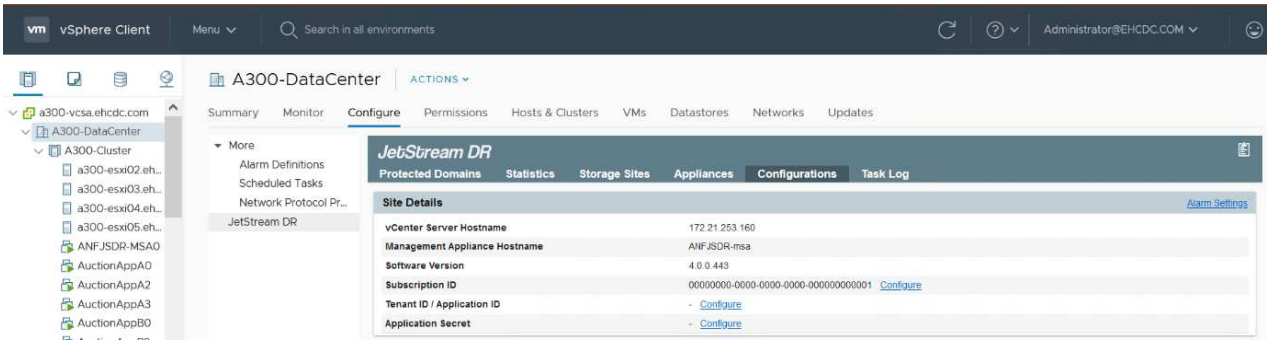
Il numero e il contenuto dei domini prescritti dipendono da varie caratteristiche della VM, come IOPS medi, capacità totale, priorità (che definisce l'ordine di failover), RTO e altro.

Installa JetStream DR nel data center locale

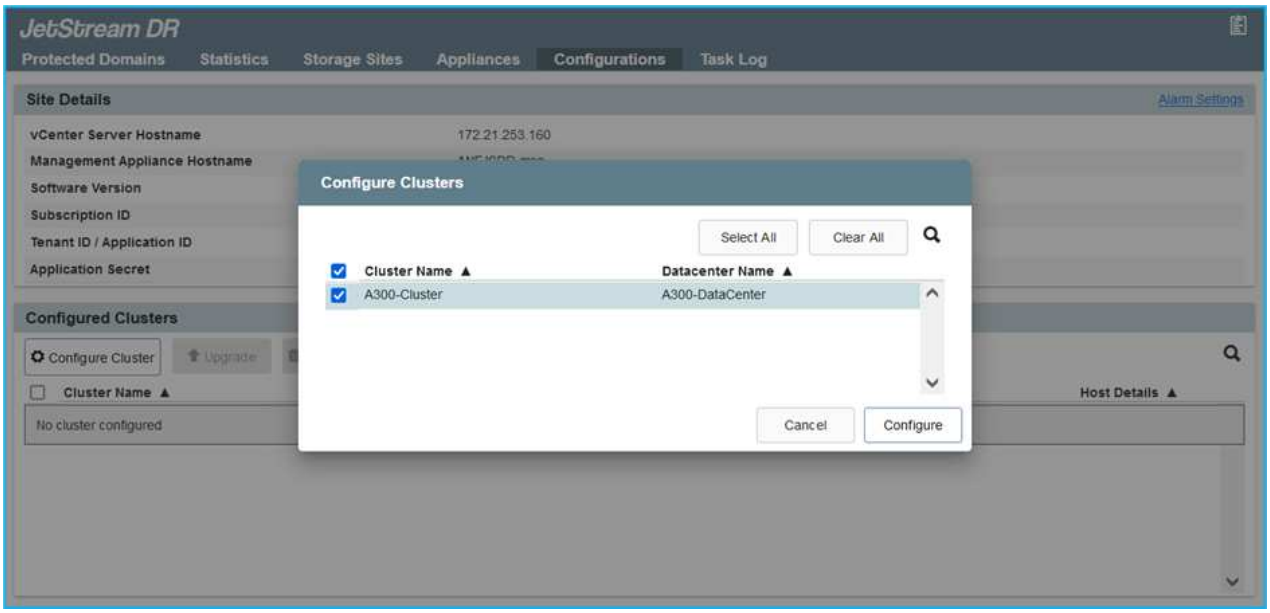
Il software JetStream DR è costituito da tre componenti principali: JetStream DR Management Server Virtual Appliance (MSA), DR Virtual Appliance (DRVA) e componenti host (pacchetti di filtri I/O). MSA viene utilizzato per installare e configurare i componenti host sul cluster di elaborazione e quindi per amministrare il software JetStream DR. L'elenco seguente fornisce una descrizione di alto livello del processo di installazione:

Come installare JetStream DR per ambienti locali

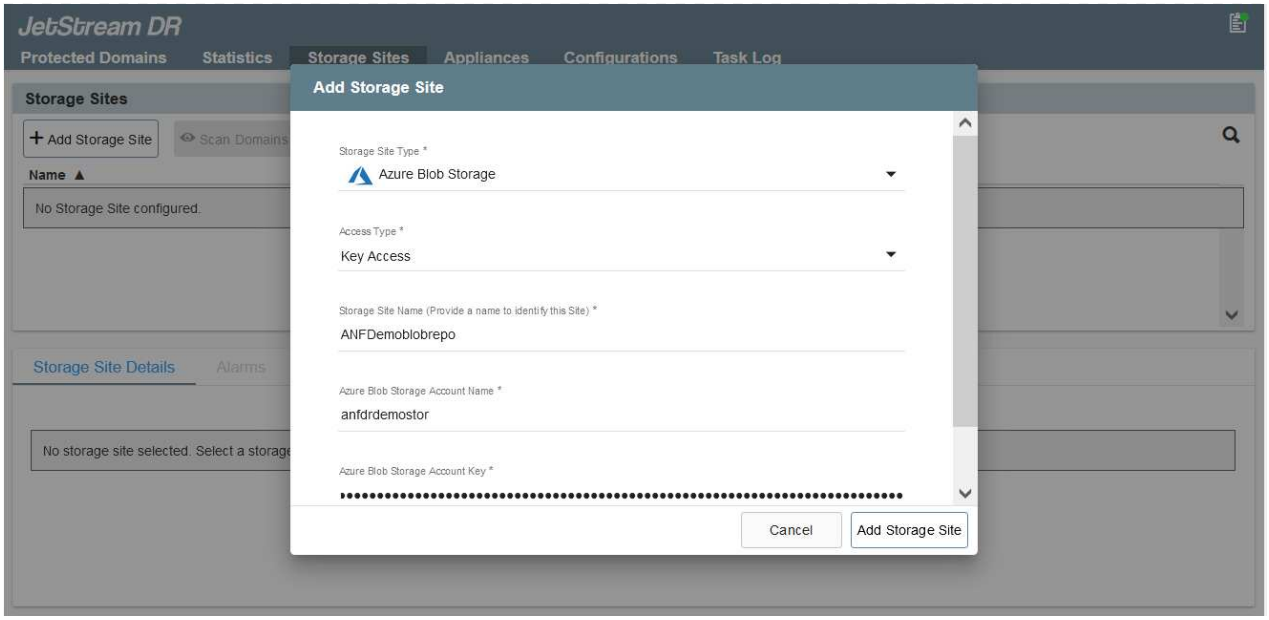
1. Verificare i prerequisiti.
2. Eseguire lo strumento di pianificazione della capacità per ottenere consigli su risorse e configurazione (facoltativo ma consigliato per le prove di proof-of-concept).
3. Distribuire JetStream DR MSA su un host vSphere nel cluster designato.
4. Avviare l'MSA utilizzando il suo nome DNS in un browser.
5. Registrare il server vCenter con MSA. Per eseguire l'installazione, completare i seguenti passaggi dettagliati:
6. Dopo aver distribuito JetStream DR MSA e registrato vCenter Server, accedere al plug-in JetStream DR tramite vSphere Web Client. Per farlo, andare su Datacenter > Configura > JetStream DR.



7. Dall'interfaccia JetStream DR, selezionare il cluster appropriato.



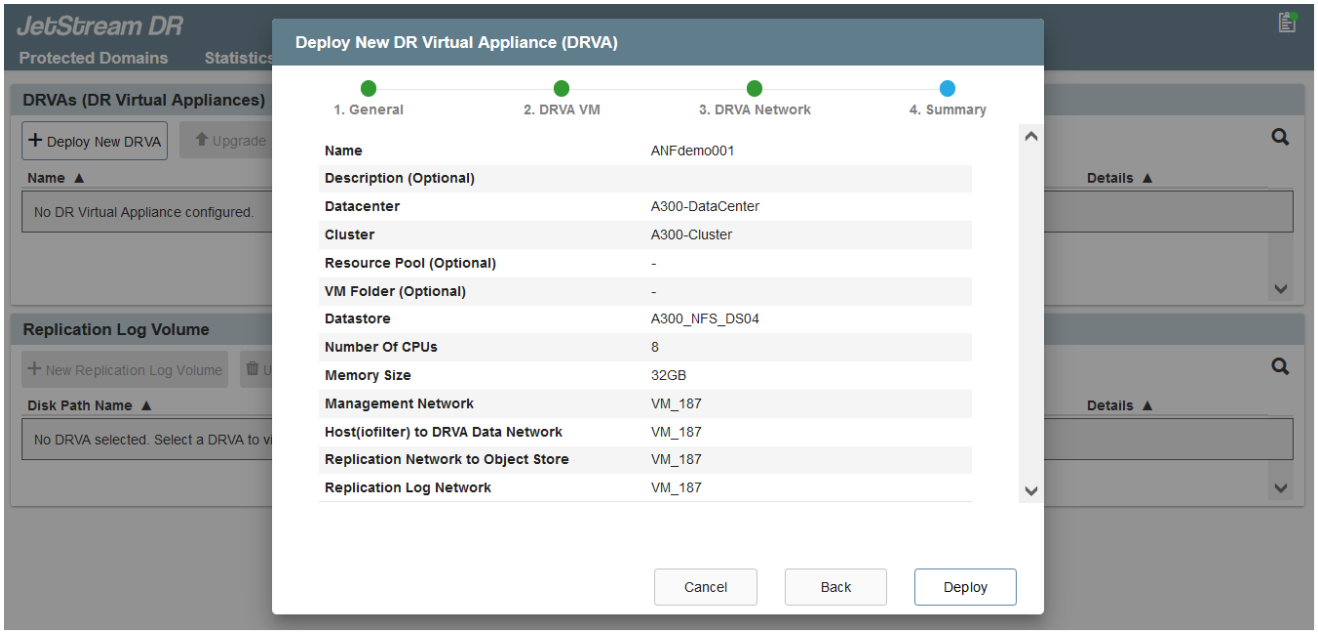
8. Configurare il cluster con il pacchetto filtro I/O.



9. Aggiungere Azure Blob Storage situato nel sito di ripristino.
10. Distribuire un DR Virtual Appliance (DRVA) dalla scheda Appliance.

> ⓘ I DRVA possono essere creati automaticamente da CPT, ma per le prove POC consigliamo di configurare ed eseguire manualmente il ciclo DR (avvio protezione > failover > failback).

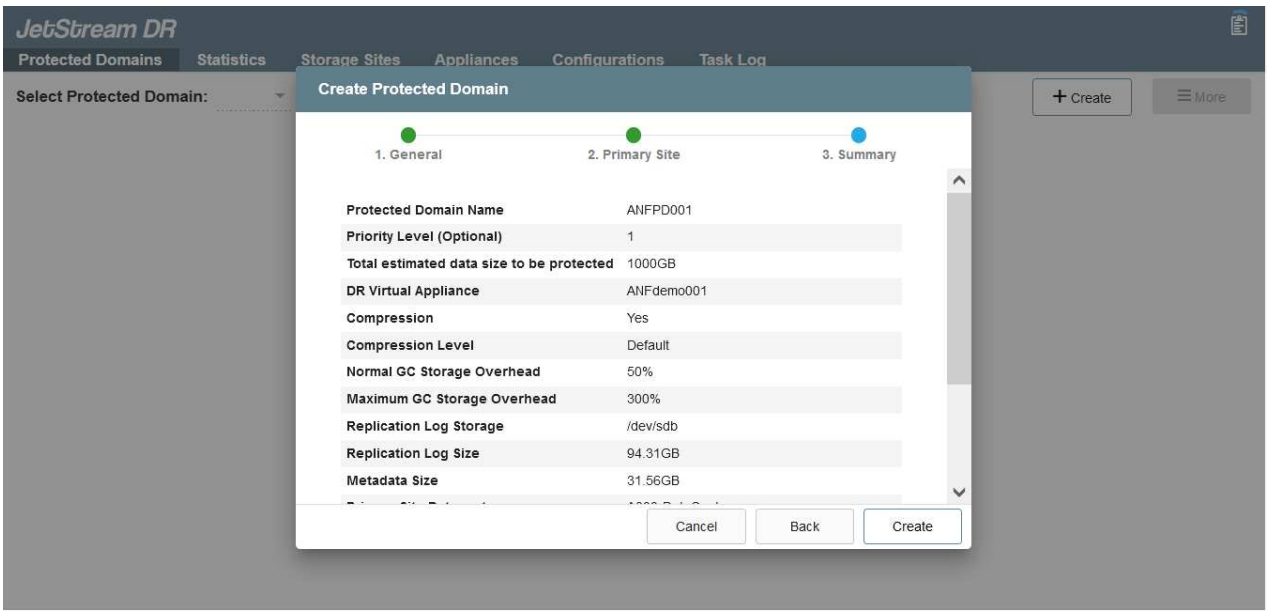
JetStream DRVA è un dispositivo virtuale che semplifica le funzioni chiave nel processo di replicazione dei dati. Un cluster protetto deve contenere almeno un DRVA e in genere ne viene configurato uno per host. Ogni DRVA può gestire più domini protetti.



In questo esempio sono stati creati quattro DRVA per 80 macchine virtuali.

1. Creare volumi di registro di replica per ogni DRVA utilizzando VMDK dai datastore disponibili o da pool di storage iSCSI condivisi indipendenti.
2. Dalla scheda Domini protetti, creare il numero richiesto di domini protetti utilizzando le informazioni

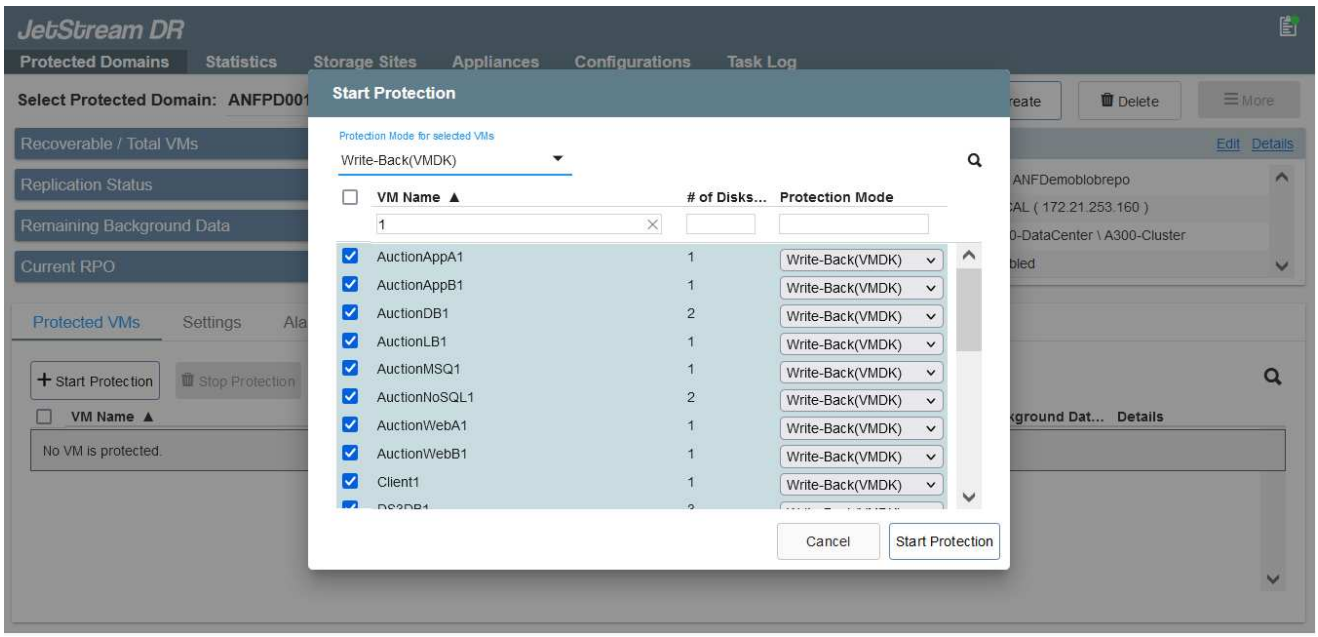
sul sito di Azure Blob Storage, l'istanza DRVA e il registro di replica. Un dominio protetto definisce una VM specifica o un set di VM all'interno del cluster, protette insieme e a cui viene assegnato un ordine di priorità per le operazioni di failover/failback.



3. Selezionare le VM che si desidera proteggere e avviare la protezione delle VM del dominio protetto. In questo modo viene avviata la replica dei dati nel Blob Store designato.

Verificare che venga utilizzata la stessa modalità di protezione per tutte le VM in un dominio protetto.

La modalità Write-Back (VMDK) può offrire prestazioni più elevate.



Verificare che i volumi del registro di replica siano posizionati su un archivio ad alte prestazioni.

I run book di failover possono essere configurati per raggruppare le VM (denominate Recovery Group), impostare la sequenza dell'ordine di avvio e modificare le impostazioni della CPU/memoria insieme alle configurazioni IP.

Installa JetStream DR per AVS in un cloud privato di Azure VMware Solution utilizzando il comando Esegui

Una buona pratica per un sito di ripristino (AVS) è quella di creare in anticipo un cluster di luci pilota a tre nodi. Ciò consente di preconfigurare l'infrastruttura del sito di ripristino, inclusi i seguenti elementi:

- Segmenti di rete di destinazione, firewall, servizi come DHCP e DNS e così via.
- Installazione di JetStream DR per AVS
- Configurazione di volumi ANF come datastore e altro ancoraJetStream DR supporta la modalità RTO prossima allo zero per domini mission-critical. Per questi domini, lo storage di destinazione dovrebbe essere preinstallato. In questo caso, l'ANF è il tipo di archiviazione consigliato.

La configurazione di rete, inclusa la creazione di segmenti, deve essere configurata sul cluster AVS in modo da soddisfare i requisiti locali.

A seconda dei requisiti SLA e RTO, è possibile utilizzare la modalità failover continuo o failover regolare (standard). Per un RTO prossimo allo zero, la reidratazione continua deve essere avviata nel sito di recupero.

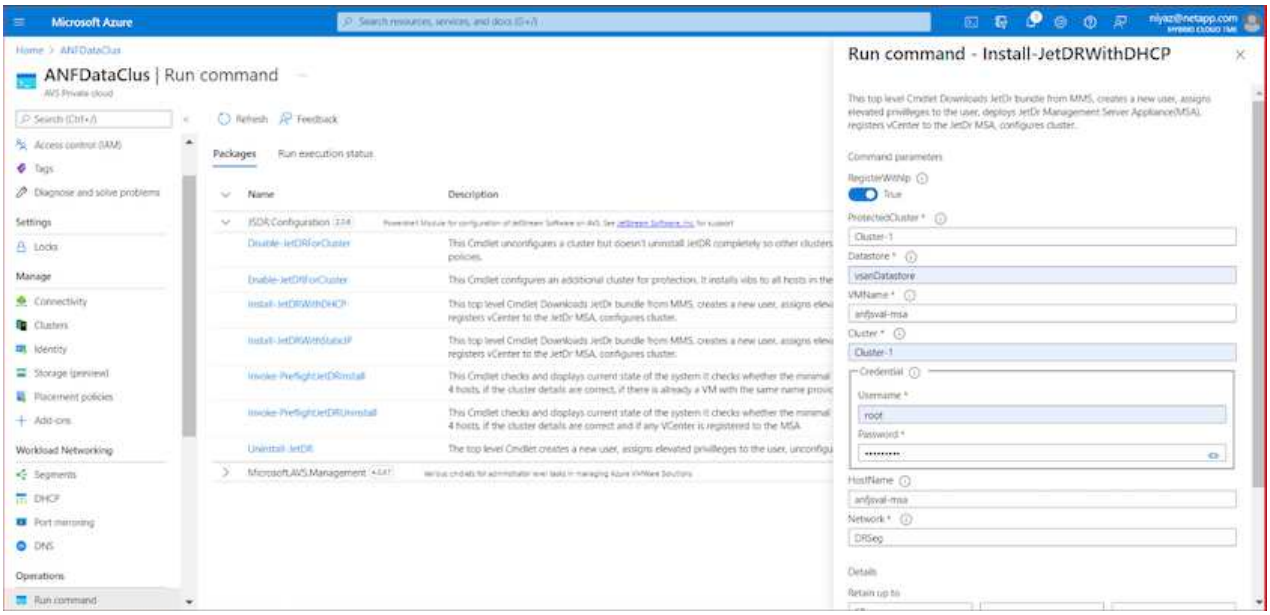
Come installare JetStream DR per AVS in un cloud privato

Per installare JetStream DR per AVS su un cloud privato di Azure VMware Solution, completare i seguenti passaggi:

1. Dal portale di Azure, vai alla soluzione Azure VMware, seleziona il cloud privato e seleziona Esegui comando > Pacchetti > JSDR.Configuration.

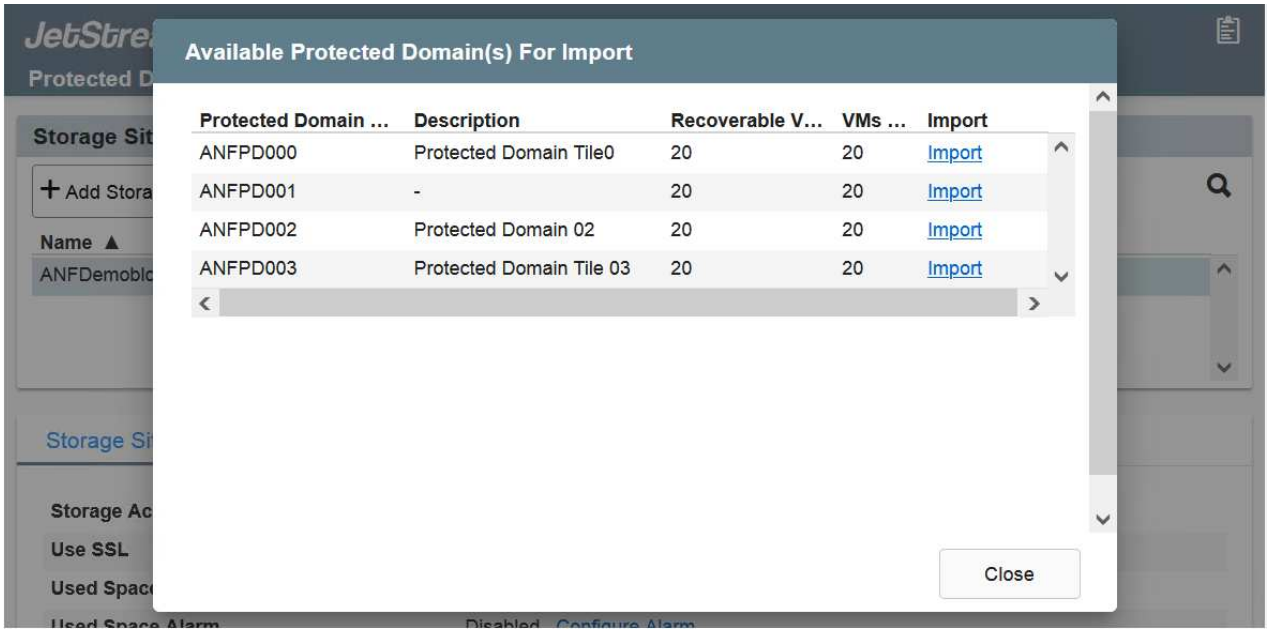
   L'utente CloudAdmin predefinito in Azure VMware Solution non dispone di privilegi sufficienti per installare JetStream DR per AVS. Azure VMware Solution consente l'installazione semplificata e automatizzata di JetStream DR richiamando il comando Esegui di Azure VMware Solution per JetStream DR.

   La seguente schermata mostra l'installazione utilizzando un indirizzo IP basato su DHCP.



2. Una volta completata l'installazione di JetStream DR per AVS, aggiornare il browser. Per accedere all'interfaccia utente di JetStream DR, andare su SDDC Datacenter > Configura > JetStream DR.

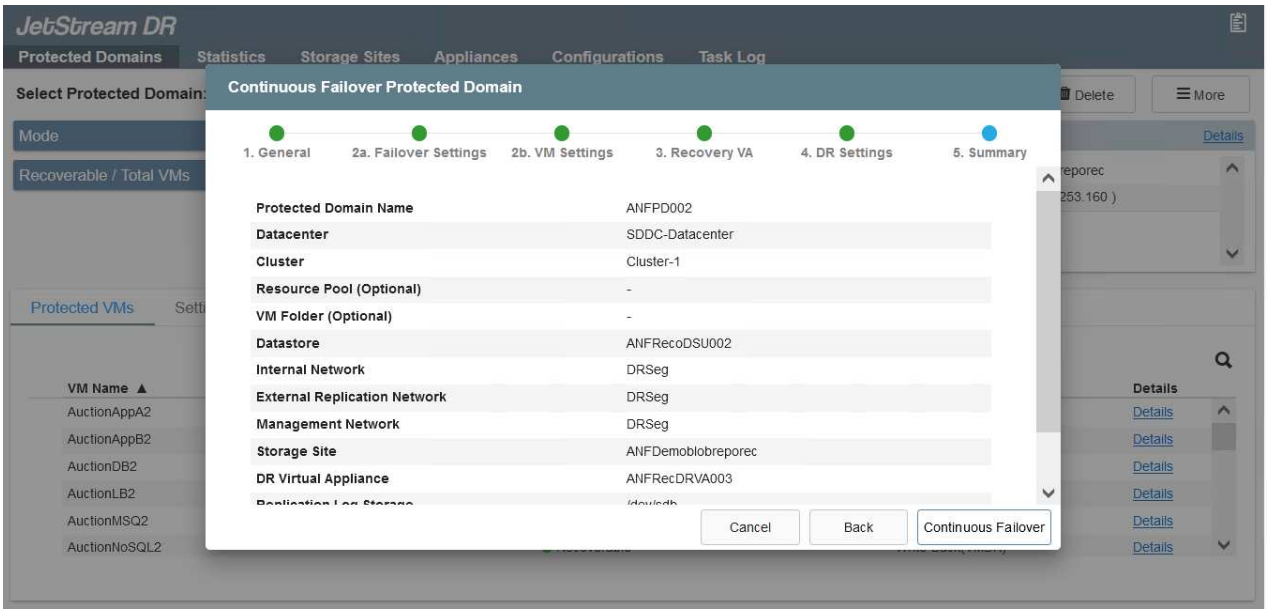
3. Dall'interfaccia JetStream DR, aggiungere l'account Azure Blob Storage utilizzato per proteggere il cluster locale come sito di archiviazione, quindi eseguire l'opzione Scansiona domini.



4. Dopo aver importato i domini protetti, distribuire gli appliance DRVA. In questo esempio, la reidratazione continua viene avviata manualmente dal sito di ripristino tramite l'interfaccia utente di JetStream DR.

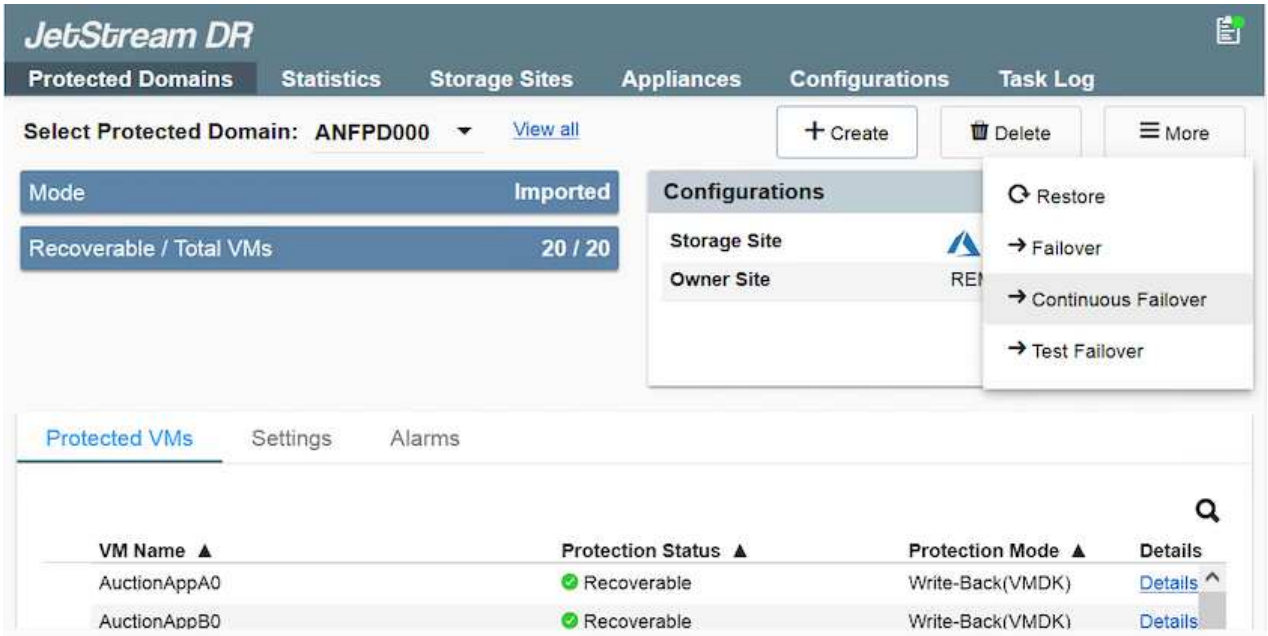
> Questi passaggi possono anche essere automatizzati utilizzando i piani creati da CPT.

5. Creare volumi di log di replicazione utilizzando i datastore vSAN o ANF disponibili.
6. Importare i domini protetti e configurare Recovery VA per utilizzare il datastore ANF per i posizionamenti delle VM.



Assicurarsi che DHCP sia abilitato sul segmento selezionato e che siano disponibili sufficienti IP. Gli IP dinamici vengono utilizzati temporaneamente mentre i domini sono in fase di ripristino. Ogni VM in fase di ripristino (inclusa la reidratazione continua) richiede un IP dinamico individuale. Una volta completato il ripristino, l'IP viene rilasciato e può essere riutilizzato.

7. Selezionare l'opzione di failover appropriata (failover continuo o failover). In questo esempio è stata selezionata la reidratazione continua (failover continuo).



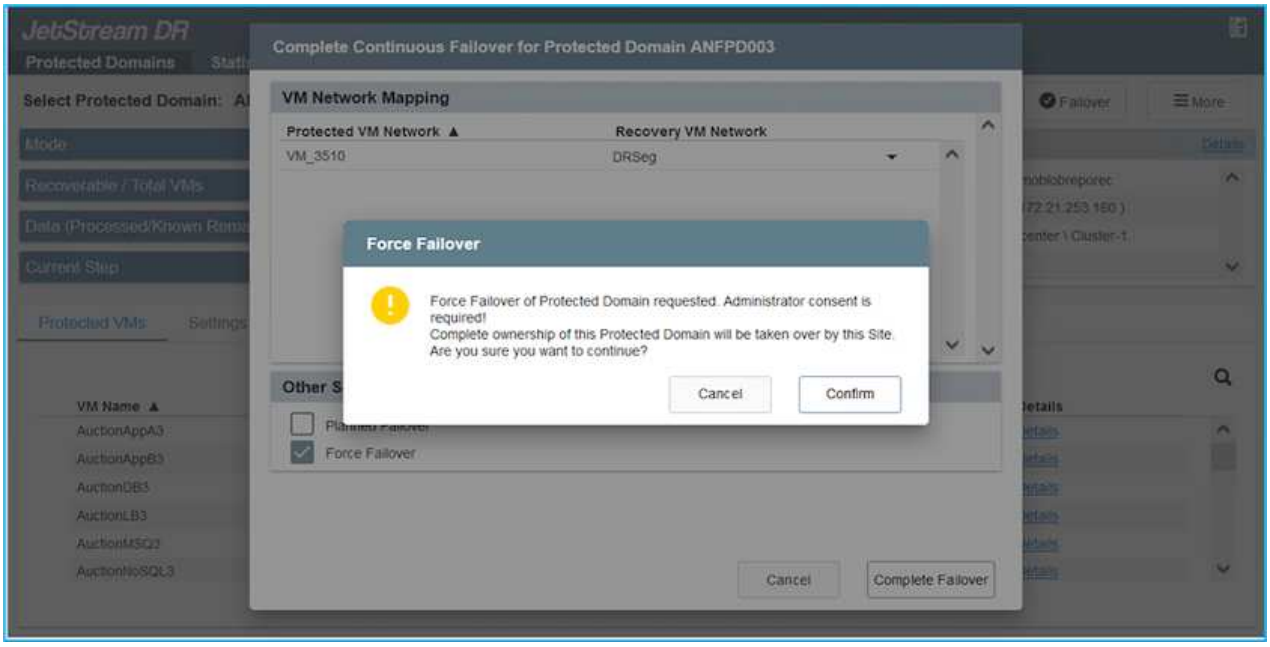
Esecuzione di failover/failback

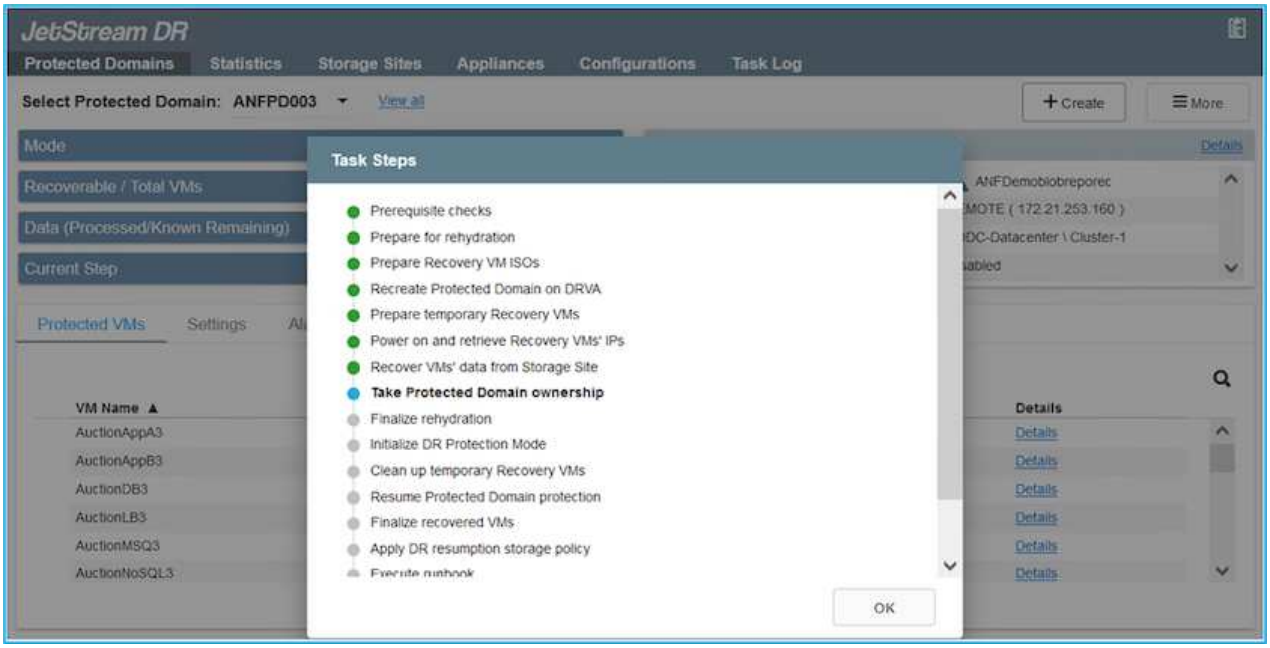
Come eseguire un Failover/Failback

1. Dopo che si è verificato un disastro nel cluster protetto dell'ambiente on-premise (guasto parziale o totale), attivare il failover.

   CPT può essere utilizzato per eseguire il piano di failover per ripristinare le VM da Azure Blob Storage nel sito di ripristino del cluster AVS.

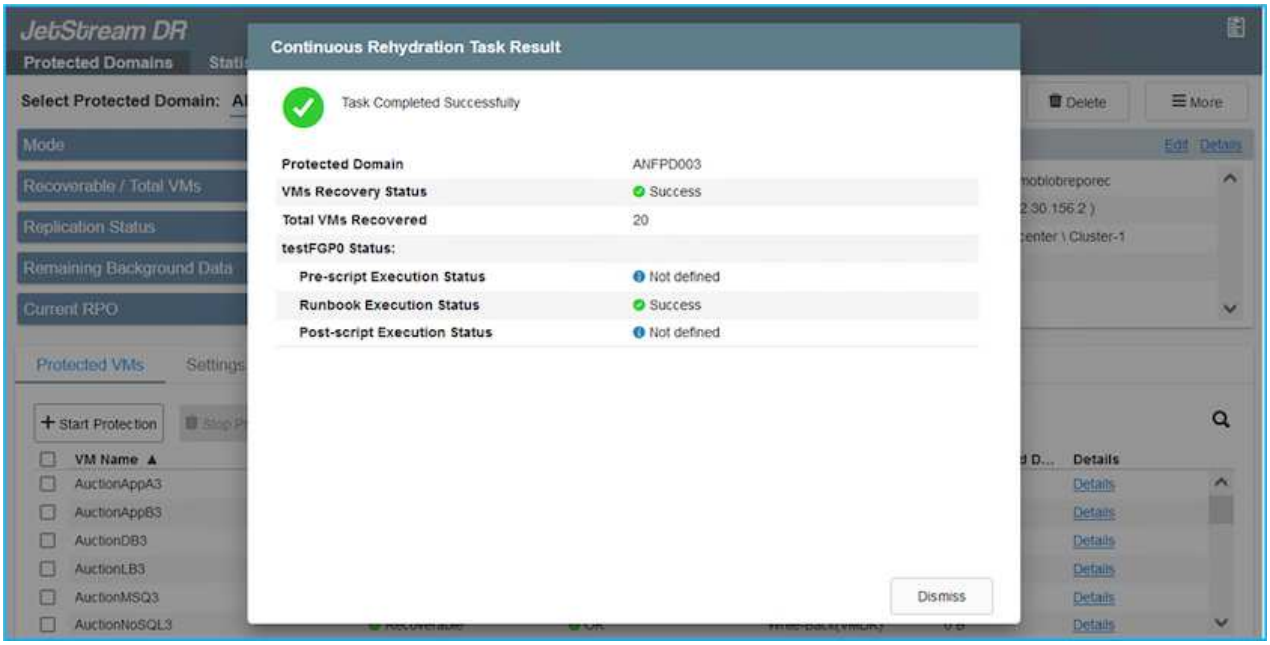
   Dopo il failover (per la reidratazione continua o standard), quando le VM protette sono state avviate in AVS, la protezione viene automaticamente ripresa e JetStream DR continua a replicare i dati nei contenitori appropriati/originali in Azure Blob Storage.





La barra delle applicazioni mostra lo stato di avanzamento delle attività di failover.

2. Una volta completata l'attività, accedi alle VM recuperate e le attività riprenderanno normalmente.

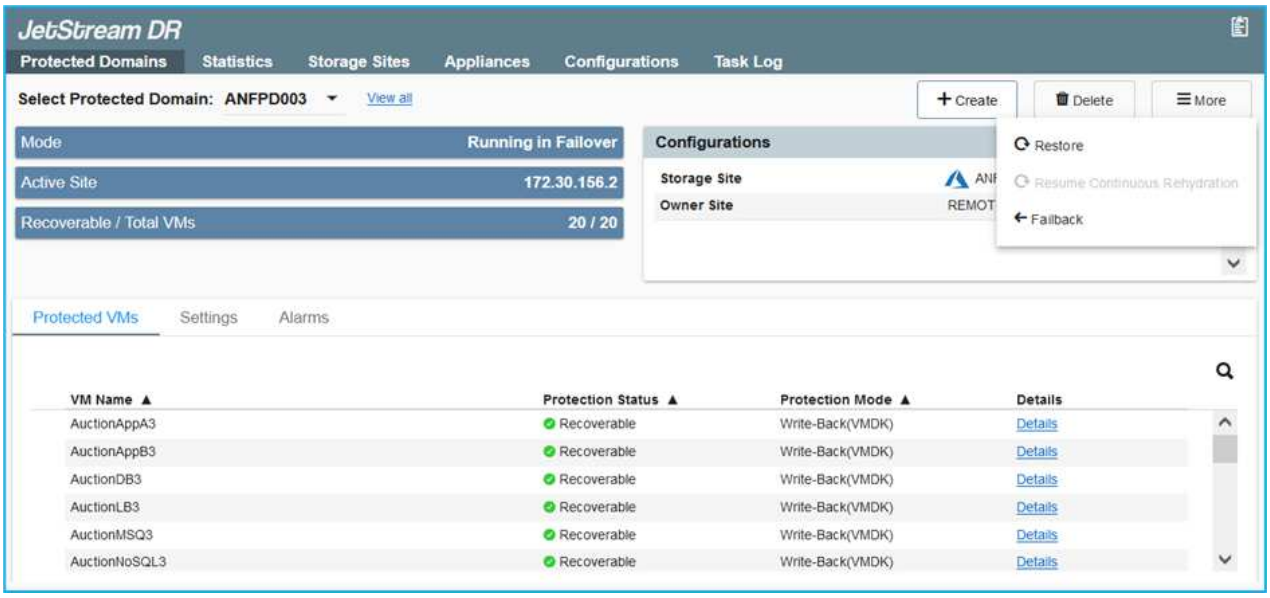


Una volta che il sito primario è di nuovo attivo e funzionante, è possibile eseguire il failback. La protezione della VM è ripristinata e occorre verificare la coerenza dei dati.

3. Ripristinare l'ambiente locale. A seconda del tipo di incidente di emergenza, potrebbe essere necessario ripristinare e/o verificare la configurazione del cluster protetto. Se necessario, potrebbe essere necessario reinstallare il software JetStream DR.

> Nota: Il `recovery_utility_prepare_failback` Lo script fornito nell'Automation Toolkit può essere utilizzato per pulire il sito protetto originale da eventuali VM obsolete, informazioni di dominio e così via.

4. Accedere all'ambiente locale ripristinato, andare all'interfaccia utente di Jetstream DR e selezionare il dominio protetto appropriato. Una volta che il sito protetto è pronto per il failback, selezionare l'opzione Failback nell'interfaccia utente.



Il piano di failback generato da CPT può essere utilizzato anche per avviare il ritorno delle VM e dei relativi dati dall'archivio oggetti all'ambiente VMware originale.

Specificare il ritardo massimo dopo la sospensione delle VM nel sito di ripristino e il riavvio nel sito protetto. Questo tempo include il completamento della replica dopo l'arresto delle VM di failover, il tempo per pulire il sito di ripristino e il tempo per ricreare le VM nel sito protetto. Il valore consigliato NetApp è 10 minuti.

Completare il processo di failback, quindi confermare la ripresa della protezione della VM e la coerenza dei dati.

Recupero da ransomware

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

JetStream DR per AVS insieme ai datastore Azure NetApp Files possono risolvere questi problemi consentendo alle organizzazioni di eseguire il ripristino da punti temporali disponibili, in modo che i carichi di lavoro vengano ripristinati su una rete funzionale e isolata, se necessario. Il ripristino consente alle applicazioni di funzionare e comunicare tra loro senza esporle al traffico nord-sud, offrendo così ai team di sicurezza un luogo sicuro in cui eseguire analisi forensi e altre azioni correttive necessarie.