

NetApp per Azure/AVS

NetApp Solutions

NetApp April 26, 2024

This PDF was generated from https://docs.netapp.com/it-it/netapp-solutions/ehc/azure-native-dr-jetstream.html on April 26, 2024. Always check docs.netapp.com for the latest.

Sommario

Multicloud ibrido NetApp con soluzioni VMware	 . 1
Protezione dei carichi di lavoro su Azure/AVS	 . 1
Migrazione dei carichi di lavoro su Azure/AVS	 63
Disponibilità regionale: Datastore NFS supplementare per ANF	 80

Multicloud ibrido NetApp con soluzioni VMware

Protezione dei carichi di lavoro su Azure/AVS

Disaster Recovery con ANF e JetStream

Il disaster recovery nel cloud è un metodo resiliente e conveniente per proteggere i carichi di lavoro da interruzioni del sito ed eventi di corruzione dei dati (ad esempio ransomware). Utilizzando il framework VMware VAIO, è possibile replicare i workload VMware on-premise sullo storage Azure Blob e ripristinarli, consentendo una perdita di dati minima o quasi nulla e un RTO quasi nullo.

Il DR Jetstream può essere utilizzato per ripristinare perfettamente i carichi di lavoro replicati da on-premise ad AVS e in particolare a Azure NetApp Files. Consente un disaster recovery conveniente utilizzando risorse minime presso il sito di DR e uno storage cloud conveniente. Jetstream DR automatizza il ripristino degli archivi dati ANF tramite Azure Blob Storage. Jetstream DR ripristina macchine virtuali indipendenti o gruppi di macchine virtuali correlate nell'infrastruttura del sito di ripristino in base alla mappatura di rete e fornisce un ripristino point-in-time per la protezione ransomware.

Il presente documento fornisce informazioni sui principi operativi di DR di JetStream e sui relativi componenti principali.

- 1. Installare il software DR JetStream nel data center on-premise.
 - a. Scarica il pacchetto software DR JetStream da Azure Marketplace (ZIP) e implementa il DR MSA (OVA) JetStream nel cluster designato.
 - b. Configurare il cluster con il pacchetto di filtri i/o (installare JetStream VIB).
 - c. Provisioning di Azure Blob (Azure Storage account) nella stessa regione del cluster DR AVS.
 - d. Implementare appliance DRVA e assegnare volumi di log di replica (VMDK da datastore esistente o storage iSCSI condiviso).
 - e. Creare domini protetti (gruppi di macchine virtuali correlate) e assegnare DRVA e Azure Blob Storage/ANF.
 - f. Protezione all'avviamento.
- 2. Installare il software DR JetStream nel cloud privato Azure VMware Solution.
 - a. Utilizzare il comando Esegui per installare e configurare il DR JetStream.
 - b. Aggiungere lo stesso container Azure Blob e individuare i domini utilizzando l'opzione Scan Domains (domini di scansione).
 - c. Implementare le appliance DRVA richieste.
 - d. Creare volumi di log di replica utilizzando datastore vSAN o ANF disponibili.
 - e. Importare domini protetti e configurare ROCvA (Recovery VA) per utilizzare il datastore ANF per il posizionamento delle macchine virtuali.
 - f. Selezionare l'opzione di failover appropriata e avviare la reidratazione continua per domini RTO o macchine virtuali quasi a zero.
- 3. Durante un evento di emergenza, attivare il failover degli archivi dati Azure NetApp Files nel sito di DR AVS designato.
- 4. Richiamare il failback sul sito protetto dopo il ripristino del sito protetto.prima di iniziare, assicurarsi che i prerequisiti siano soddisfatti, come indicato in questa sezione "collegamento" Inoltre, eseguire il Bandwidth Testing Tool (BWT) fornito dal software JetStream per valutare le performance potenziali dello storage Azure Blob e la relativa larghezza di banda di replica se utilizzato con il software DR JetStream. Una volta implementati i prerequisiti, inclusa la connettività, impostare e sottoscrivere JetStream DR per AVS da "Azure Marketplace". Una volta scaricato il pacchetto software, procedere con la procedura di installazione descritta in precedenza.

Quando si pianifica e si avvia la protezione per un gran numero di macchine virtuali (ad esempio, 100+), utilizzare il Capacity Planning Tool (CPT) di JetStream DR Automation Toolkit. Fornire un elenco di macchine virtuali da proteggere insieme alle preferenze RTO e del gruppo di ripristino, quindi eseguire CPT.

CPT esegue le seguenti funzioni:

- Combinazione di macchine virtuali in domini di protezione in base al proprio RTO.
- Definizione del numero ottimale di DRVA e delle relative risorse.
- Stima della larghezza di banda di replica richiesta.
- Identificazione delle caratteristiche del volume del registro di replica (capacità, larghezza di banda e così via).
- Stima della capacità di storage a oggetti richiesta e molto altro ancora.



Il numero e il contenuto dei domini prescritti dipendono da diverse caratteristiche delle macchine virtuali, come IOPS medi, capacità totale, priorità (che definisce l'ordine di failover), RTO e altre.

Installare JetStream DR in Datacenter on-premise

Il software Jetstream DR è costituito da tre componenti principali: Appliance virtuale Jetstream DR Management Server (MSA), appliance virtuale DR (DRVA) e componenti host (pacchetti di filtro i/o). MSA viene utilizzato per installare e configurare i componenti host sul cluster di calcolo e quindi per amministrare il software DR JetStream. Il seguente elenco fornisce una descrizione dettagliata del processo di installazione:

- 1. Verificare i prerequisiti.
- 2. Eseguire Capacity Planning Tool per ottenere consigli su risorse e configurazione (facoltativo ma consigliato per le prove proof-of-concept).
- 3. Implementare l'MSA DR JetStream su un host vSphere nel cluster designato.
- 4. Avviare MSA utilizzando il nome DNS in un browser.
- 5. Registrare il server vCenter con MSA.per eseguire l'installazione, attenersi alla seguente procedura dettagliata:
- Una volta implementato JetStream DR MSA e registrato vCenter Server, accedere al plug-in JetStream DR utilizzando vSphere Web Client. Per eseguire questa operazione, accedere a Datacenter > Configure > JetStream DR.

vm vSphere Client	Menu 🗸 🛛 🔍 Search in all	environments		C @~	Administrator@EHCDC.COM ~
□ □ □ ● ~ ⊡ a300-vcsa.ehcdc.com ^	A300-DataCent Summary Monitor Co	ACTIONS ~ Figure Permissions Hosts & Clusters VMs Datastores	Networks Updates		
 A300-Datacenter A300-Cluster a300-esxi02.eh 	 More Alarm Definitions Scheduled Tasks 	JebSbream DR Protected Domains Statistics Storage Sites Appliances	Configurations Task Log		É.
a300-esxi03.eh a300-esxi04.eh	Network Protocol Pr JetStream DR	Site Details	en.		Alarm Settings
ANFJSDR-MSA0		Management Appliance Hostname ANFJSDR-Im	sa		
AuctionAppA0		Software Version 4.0.0.443 Subscription ID 0000000-0	000-0000-0000-000000000000000000000000		
AuctionAppA3		Tenant ID / Application ID - Configure Application Secret - Configure			

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

te Details					Alarm Settin
Center Server Hostname	172.21.253.160				
lanagement Appliance Hostname	AUT 1000				
oftware Version	Configure Clusters				
ubscription ID				0	
enant ID / Application ID		Select All	Clear All		
pplication Secret	Cluster Name 🛦	Datacenter Name 🔺			
onfigured Clusters	A300-Cluster	A300-DataCenter			
Configure Cluster					c
] Cluster Name 🛦				~	Host Details 🔺
No cluster configured		Ca	ancel Co	nfigure	
	-				
	-				

8. Configurare il cluster con il pacchetto di filtri i/O.

JetStream DR		1
Protected Domains Statistics	Storage Sites Appliances Configurations Task Log	
Storage Sites	Add Storage Site	
+ Add Storage Site Scan Domains	Shrane StaTine *	(
Name 🛦	▲ Azure Blob Storage	
No Storage Site configured.		
	Access Type * Key Access	
	Sinzana Sile Nama (Brovide a name in identify this Sile) *	
	ANFDemoblobrepo	
Storage Site Details Alarms		
	anfdrdemostor	
No storage site selected. Select a storage		
	Azure Blob Storage Account Key *	
	Cancel Add Storage Site	

- 9. Aggiungere Azure Blob Storage situato nel sito di ripristino.
- 10. Implementare un'appliance virtuale DR (DRVA) dalla scheda Appliances (appliance).



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

JetStream DRVA è un'appliance virtuale che facilita le funzioni chiave nel processo di replica dei dati. Un cluster protetto deve contenere almeno un DRVA e, in genere, un DRVA viene configurato per host. Ogni DRVA può gestire più domini protetti.

Jet:Stream DR Protected Domains Statistics	Deploy New DR Virtual App	liance (DRVA)						
DRVAs (DR Virtual Appliances)	1. General	2. DRVA VM	3. DRVA Net	work	4. Summary	- 1		
+ Deploy New DRVA	Name	,	ANFdemo001			^		Q
Name 🛦	Description (Optional)						Details 🔺	
No DR Virtual Appliance configured.	Datacenter	,	A300-DataCenter					
	Cluster	,	A300-Cluster					
	Resource Pool (Optional)							
	VM Folder (Optional)							\sim
Replication Log Volume	Datastore	/	A300_NFS_DS04					
	Number Of CPUs	٤	3					0
+ New Replication Log Volume	Memory Size	;	32GB					Q
Disk Path Name 🔺	Management Network	N N	/M_187				Details 🔺	
No DRVA selected. Select a DRVA to vi	Host(iofilter) to DRVA Data	Network	/M_187					
	Replication Network to Obj	ect Store	/M_187					
	Replication Log Network	١	/M_187			\sim		\sim
			Cancel	Back	Deploy			

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

1. Creare volumi di log di replica per ogni DRVA utilizzando VMDK dagli archivi dati disponibili o da pool di storage iSCSI condivisi indipendenti.

2. Dalla scheda Protected Domains (domini protetti), creare il numero richiesto di domini protetti utilizzando le informazioni relative al sito Azure Blob Storage, all'istanza DRVA e al registro di replica. Un dominio protetto definisce una macchina virtuale specifica o un insieme di macchine virtuali all'interno del cluster che sono protetti insieme e assegnati a un ordine di priorità per le operazioni di failover/failback.

JetStream DR			Ê
Select Protected Domains Statistics Sto	rage Sites Appliances Configur	ations lask Log	+ Create = More
	1. General 2. Pri	imary Site 3. Summary	
	Protected Domain Name	ANFPD001	
	Priority Level (Optional)	1	
	Total estimated data size to be protected	1000GB	
	Compression	Yes	
	Compression Level	Default	
	Normal GC Storage Overhead	50%	
	Maximum GC Storage Overhead	300%	
	Replication Log Storage	/dev/sdb	
	Replication Log Size	94.31GB	
	Metadata Size	31.56GB	v
		Cancel Back Cr	ireate
	_		

3. Selezionare le macchine virtuali che si desidera proteggere e avviare la protezione delle macchine virtuali del dominio protetto. In questo modo viene avviata la replica dei dati nell'archivio Blob designato.

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



i.

La modalità Write-Back (VMDK) può offrire performance superiori.

Select Protected Domain: ANFPD001	Start	t Protection					reate Delete	
Recoverable / Total VMs	Protec	tion Mode for selected VMs				0		Edit Detail
Replication Status		VM Name		# of Disks	Protection Mode	4	ANFDemoblobrepo	^
Remaining Background Data	_	1	×				AL (172.21.253.160)	
Current PPO		AuctionAppA1		1	Write-Back(VMDK)	~	bled	
Gunent IV O		AuctionAppB1		1	Write-Back(VMDK)	~		
Protected VMs Settings Ala		AuctionDB1		2	Write-Back(VMDK)	~		
		AuctionLB1		1	Write-Back(VMDK)	~		
+ Start Protection		AuctionMSQ1		1	Write-Back(VMDK)	~		Q
		AuctionNoSQL1		2	Write-Back(VMDK)	~		
U VM Name 🔺		AuctionWebA1		1	Write-Back(VMDK)	~	kground Dat Details	
No VM is protected.		AuctionWebB1		1	Write-Back(VMDK)	~)		
		Client1		1	Write-Back(VMDK)	~		
	177	- חפסחפו		0		~		
					Cancel Start	Protection		
							J.	

Verificare che i volumi dei log di replica siano posizionati su uno storage dalle performance elevate.



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

Installare JetStream DR per AVS in un cloud privato Azure VMware Solution utilizzando il comando Run

Una Best practice per un sito di recovery (AVS) consiste nella creazione anticipata di un cluster 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 dei volumi ANF come datastore e inoltre JetStream DR supporta la modalità RTO quasi zero per i domini mission-critical. Per questi domini, lo storage di destinazione deve essere preinstallato. ANF è un tipo di storage consigliato in questo caso.



La configurazione di rete, inclusa la creazione di segmenti, deve essere configurata sul cluster AVS per soddisfare i requisiti on-premise.

A seconda dei requisiti SLA e RTO, è possibile utilizzare il failover continuo o la normale modalità di failover (standard). Per un RTO vicino allo zero, è necessario avviare una procedura di reidratazione continua presso il sito di ripristino.

Per installare JetStream DR per AVS su un cloud privato Azure VMware Solution, attenersi alla seguente procedura:

1. Dal portale Azure, accedere alla soluzione Azure VMware, selezionare il cloud privato e selezionare Esegui comando > pacchetti > Configurazione JSDR.



L'utente CloudAdmin predefinito in Azure VMware Solution non dispone di privilegi sufficienti per installare JetStream DR per AVS. Azure VMware Solution consente un'installazione semplificata e automatica del DR JetStream invocando il comando Azure VMware Solution Run per il DR JetStream.

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

Microsoft Azure	37. Seath movies a	ervices, and door (5+7)	🛛 🖓 🕒 🗇 🖉 🖉 🕫 🖉 🖉 👘 Mactinetapp.com
Home > ANFDataClus			Run command - Install-JetDRWithDHCP ×
ANFDataClus Run	command		This truth level Crimited Descentionaris furthe truther from NMMS, creaters a new user, ansates
P Seinth (Ch1+/)	O Refeish R Feedback		elevated provideges to the user, deploys JetDr Management Server Appliance/MSA), registers vCenter to the JetDr MSA, configures cluster.
Access control (AM)	Packages Fun execution statue		Command parameters
Diagnose and solve problems	 Name 	Description	RegisterWorkp 🕤
Settings	 ISDRConfiguration 224 Processes lines. 	in for configuration of informer furthers on Arth for uniforms furthers, inc. for summit	ProtectedCluster *
A Loda	Duate-letDRiceChater	This Crediet unconfigures a cluster but doesn't unrestall letDR completely so other clusters	Outer-1
		polos.	Datastore * (j)
Manage	Unable-Jet010 orCluster	This Cridlet configures an additional cluster for protection. It installs vibs to all hosts in the	vsecDatestore
👲 Connectivity	Install-SetDRAMINDERCH	This top level Critiket Downloads JetDr bundle from MMS, creates a new user, assigns eleve	VMName* ()
Chaters		registers vCenter to the JetDr MSA, configures cluster.	antywal-msa
Identity	Install-JetD/GW:trGtatecl/	This top level Crindlet Downloads JerDr bundle from MMS, orestes a new user, assigns elevi registers (Center to the JerDr MSA, configures cluster.	Date-1
C Stocage (preview)	Involve PrefightietDSmith8	This Crediet checks and doplays current state of the system it checks whether the minimal	- Credential ()
Recement policies		4 boots if the charter details are correct, if there is already a VM with the same name provid	Otername 50
+ Add-one	Invole-PrefightletDRUmmtall	This Critilet checks and displays current state of the system it checks whether the minimal	root
Magnetic excernes.	100000000000000000000000000000000000000	4 hours if the cluster details are correct and if any VLenter is registered to the MSA.	Password.*
Workload Networking	Univital ArtD4	The top level Ondlet creates a new user, assigns elevated prolifeges to the user, unconfigu	
🚭 Segments	> Microsoft/WS/Management (433) and	us chidats thi administration evel laaks in managing Adves KinWeet Southers	HostName ()
T DHCF			anfpoal-maa
Port memoring			Network 1 (j)
O DNS			DRSeg
2010.0			Parate -
Operation			Letters
The Run command			Network up to

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

						Alarm Cott	tir
						Aldini Seu	un
vCenter Server Hostname	172.30.15	6.2					
Management Appliance Hostname	anfjsval-n	nsa					
Software Version	4.0.2.450						
Subscription ID	- Configu	ure					
Tenant ID / Application ID	- Configu	ure					
Application Secret	- Configu	ure					
Configure Cluster	Dunconfigure	🛠 Resolv	ve Configure Is	ssue			(
Cluster Name	Datacenter	Name 🔺	Status 🔺	Software V	ersion 🔺	Host Details	2
Cluster-1	SDDC-Data	center	🕝 Ok	4.0.2.132		Details	

3. Dall'interfaccia DR di JetStream, aggiungere l'account Azure Blob Storage utilizzato per proteggere il cluster on-premise come sito di storage, quindi eseguire l'opzione Scan Domains.

	Available Protected	Domain(s) For Import						Ê
Totocica D	Protected Domain	Description	Recoverable V	VMs	Import		^	
Storage Sit	ANFPD000	Protected Domain Tile0	20	20	Import	1	•	
+ Add Stora	ANFPD001	-	20	20	Import			Q
ame 🛦	ANFPD002	Protected Domain 02	20	20	Import			
FDemoble	ANFPD003	Protected Domain Tile 03	20	20	Import			^
	<					>		
								~
orage Si								
orage Ac							~	
SSL								
d Space					Clos	se		
d Space A	larm	Disabled Configure	Alarm					

4. Una volta importati i domini protetti, implementare le appliance DRVA. In questo esempio, la reidratazione continua viene avviata manualmente dal sito di ripristino utilizzando l'interfaccia utente DR JetStream.



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

- 5. Creare volumi di log di replica utilizzando datastore vSAN o ANF disponibili.
- 6. Importare i domini protetti e configurare Recovery VA in modo che utilizzi il datastore ANF per il posizionamento delle macchine virtuali.

ect Protected Domain:	Continuous Fa	ilover Protected Dom	ain					Delete	=	More
ode	•	•	•)	•		1111		De
coverable / Total VMs	1. General	2a. Failover Settings	2b. VM Settings	3. Reco	very VA	4. DR Settings	5. Summary	reporec		
	Destanted De	main Nama						253.160)		
	Protected Do	omain Name		SDDC Datas	optor					
	Cluster			Cluster 1	chilei					
	Basourse Bo	ol (Optional)		Ciuster-1						
Protected VMs Setti	VM Folder (C	ontional)								
	Datastore	ptional)			1002					
	Internal Netw	vork		DRSed	1002					
VM Name 🔺	External Ren	lication Network		DRSeg					Details	
AuctionAppA2	External Rep	Network		DRSeg					Details	
AuctionAppB2	Management	INELWORK		ANEDomobio	bronoroa			-	Details	
AuctionDB2	Storage Site			ANFDERIODIO					Details	
AuctionLB2	DR VIRtual Ap	opliance		ANFRECDRV	4003			~	Details	
AuctionMSQ2	Panination	an Fiorino			Cancel	Back	Continuous Failow	er	Details	
AuctionNoSOL 2					Gancer	Dack	Continuous railovi	<u> </u>	Details	

Assicurarsi che DHCP sia attivato sul segmento selezionato e che sia disponibile un numero sufficiente di IP. Gli IP dinamici vengono temporaneamente utilizzati durante il ripristino dei domini. Ogni macchina virtuale 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 o failover continuo). In questo esempio, viene selezionata la reidratazione continua (failover continuo).

Protected Domains	Statistics	Storag	ge Sites	Appliances	Configuratio	ons	Task Log	_
Select Protected Dom	ain: ANFPD00	0 -	View all		+ Create		Delete	■More
Mode			Imported	Configura	itions		O Restore	
Recoverable / Total VM	s		20 / 20	Storage Si	te	1	→ Failover	
				Owner Site	•	REI	→ Continuo	us Failover
							→ Test Faild	over
Protected VMs 5	Settings Ala	ırms						
								¢
VM Name 🔺			Prote	ection Status 🔺	F	rotectic	on Mode 🔺	Details
AuctionAppA0			🕝 Re	coverable	1	Vrite-Bac	ck(VMDK)	Details
Augtine A == 00			O De	covorable	i.	Alrita Ray	W/MDK)	Detaile

Esecuzione di failover/failover

i.

1. In caso di disastro nel cluster protetto dell'ambiente on-premise (errore parziale o completo), attivare il failover.



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

Dopo il failover (per la reidratazione continua o standard) quando le macchine virtuali protette sono state avviate in AVS, la protezione viene automaticamente ripristinata e JetStream DR continua a replicare i propri dati nei container 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, accedere alle macchine virtuali ripristinate e il business continua normalmente.

JetiSbream DR Protected Domains Sta	Continuous Rehydration Task Result			Ē
Select Protected Domain:	Al Task Completed Successfully		🖬 Delete 🔤 🗉	lore
Vlode			Eat	
Contraction of Contraction	Protected Domain	ANFPD003	nobiobresourer	~
cecoverable / Total VMs	VMs Recovery Status	Success	2.90.155.2.1	
Replication Status	Total VMs Recovered	20	Loop (Store)	
	testFGP0 Status:		center (Gusser-)	
Remaining Background Data	Pre-script Execution Status	Not defined		
Surrent RPO	Runbook Execution Status	O Success		V
	Post-script Execution Status	Not defined		
Protected VMs Setting	15.			
+ Start Protection	p-			٩
VM Name A			d D Details	
AuctionAppA3			Detaits	~
AuctionApp83			Detans	
AuctionDB3			Details	
AuctionLB3			Details	
AuctionMSQ3			Dismiss Details	
AuctionNoSOL3	STREET, STREET	THE THE POST OF TH	Details	×

Una volta che il sito primario è stato nuovamente operativo, è possibile eseguire il failback. La protezione delle macchine virtuali viene ripristinata e la coerenza dei dati deve essere verificata.

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



Nota: Il recovery_utility_prepare_failback Lo script fornito nel toolkit di automazione può essere utilizzato per pulire il sito protetto originale di tutte le macchine virtuali obsolete, le informazioni di dominio e così via.

4. Accedere all'ambiente on-premise ripristinato, accedere all'interfaccia utente DR Jetstream e selezionare il dominio protetto appropriato. Una volta che il sito protetto è pronto per il failback, selezionare l'opzione failover nell'interfaccia utente.

Select Protected Domain: ANFPD003	View all		+ Create	Delete	■More
Mode	Running in Failover	Configurations		O Restore	
Active Site	172.30.156.2	Storage Site	ANF	O Resume Continu	ous Rehydratio
Recoverable / Total VMs	20 / 20	Owner Site	REMOT	Failback	
Protected VMs Settings Alarms					
VM Name	Protection Star	tus 🛦 Protection M	ode 🛦	Details	c
AuctionAppA3	Recoverable	Write-Back(VM	DK)	Defails	-
AuctionAppB3	Recoverable	Write-Back(VM	DK)	Details	
	Recoverable	Write-Back(VM	DK)	Details	
AuctionDB3	- 110001010000				
AuctionDB3 AuctionLB3	Recoverable	Write-Back(VM	DK)	Details	
AuctionDB3 AuctionLB3 AuctionIMSQ3	 Recoverable Recoverable 	Write-Back(VM Write-Back(VM	DK) DK)	Details Details	

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

Specificare il ritardo massimo dopo la pausa delle macchine virtuali nel sito di ripristino e il riavvio nel sito protetto. Questo tempo include il completamento della replica dopo l'arresto delle macchine virtuali di failover, il tempo necessario per pulire il sito di recovery e il tempo necessario per ricreare le macchine virtuali in un sito protetto. Il valore consigliato da NetApp è di 10 minuti.

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

Recovery di Ransomeware

(;)

(i)

Il ripristino dal ransomware può essere un compito scoraggiante. In particolare, 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 che si verificano nuovamente (dal malware in sospensione o attraverso applicazioni vulnerabili).

Jetstream DR per AVS e gli archivi dati Azure NetApp Files possono risolvere questi problemi consentendo alle organizzazioni di eseguire il ripristino dai punti disponibili nel tempo, in modo che i carichi di lavoro vengano ripristinati in una rete funzionale e isolata, se necessario. Il ripristino consente alle applicazioni di funzionare e comunicare tra loro senza esporre le applicazioni al traffico nord-sud, offrendo così ai team di sicurezza un luogo sicuro per eseguire analisi forensi e altre azioni correttive necessarie.

JetStream DR									E.
Protected Domains S	tatistics Sta	orane Sites Apoliar	ares Configu	rations Task I	oa			-	
Select Protected Domai	Failback Prote	ected Domain						Delete	≡More
Mode	0 1. General	2a. Failback Settings	2b. VM Settings	3. Recovery VA	4. DR 5) Settings	5. Summary		Ealt Details
Active Site							6 . M. B. M. B 19 - M. B. M. B 19 - M. B. M. B 19 - M. B. M.	^ :po	^
Recoverable / Total VMs	Protected D	omain Name		ANFPD003				56.2)	
	Failback Da	tacenter		A300-DataCenter					
	Failback Clu	uster		A300-Cluster					×
Destastad Mile Se	Failback Re	source Pool		÷					
Protected VMS de	VM Folder (Optional)		s				1.000	
	Failback Da	tastore		A300_NFS_DS02				- 200	0
VII Name A	Maximum D	elay After Stopping		60 Minutes					~
AuctionAppA3	Internal Net	twork		VM_187					^
AuctionAppB3	External Re	plication Network		VM_187					
Auction/DB3	Managemen	nt Network		VM_187				~	
AuctionLB3					Cancel	Back	Failback		
AuctionMSQ3			Recoverab	le	Write-Back(VMDK)	Deta	105	
AuctionNoSQL3			O Recoverat	le	Write-Back(VMDK)	Deta	ills	×

Disaster Recovery con CVO e AVS (storage connesso agli ospiti)

Panoramica

Autori: Ravi BCB e Niyaz Mohamed, NetApp

Il disaster recovery nel cloud è un metodo resiliente e conveniente per proteggere i workload da interruzioni del sito e eventi di corruzione dei dati come ransomware. Con NetApp SnapMirror, è possibile replicare i workload VMware on-premise che utilizzano lo storage connesso con gli ospiti su NetApp Cloud Volumes ONTAP in esecuzione in Azure. Ciò riguarda i dati delle applicazioni, ma le macchine virtuali effettive. Il disaster recovery dovrebbe coprire tutti i componenti dipendenti, tra cui macchine virtuali, VMDK, dati applicativi e altro ancora. A tale scopo, SnapMirror e Jetstream possono essere utilizzati per ripristinare perfettamente i carichi di lavoro replicati da on-premise a Cloud Volumes ONTAP utilizzando lo storage vSAN per VM VMDK.

Questo documento fornisce un approccio passo per passo per la configurazione e l'esecuzione del disaster recovery che utilizza NetApp SnapMirror, JetStream e Azure VMware Solution (AVS).



Presupposti

Questo documento si concentra sullo storage in-guest per i dati delle applicazioni (noto anche come guest Connected) e si presume che l'ambiente on-premise stia utilizzando SnapCenter per backup coerenti con le applicazioni.



Questo documento si riferisce a qualsiasi soluzione di backup o ripristino di terze parti. A seconda della soluzione utilizzata nell'ambiente, seguire le Best practice per creare policy di backup che soddisfino gli SLA dell'organizzazione.

Per la connettività tra l'ambiente on-premise e la rete virtuale Azure, utilizzare la portata globale di instradamento espresso o una WAN virtuale con un gateway VPN. I segmenti devono essere creati in base alla progettazione della VLAN on-premise.



Esistono diverse opzioni per connettere i data center on-premise ad Azure, che ci impediscono di delineare un workflow specifico in questo documento. Consultare la documentazione di Azure per il metodo di connettività on-premise-to-Azure appropriato.

Implementazione della soluzione DR

Panoramica sull'implementazione della soluzione

- 1. Assicurarsi che il backup dei dati dell'applicazione venga eseguito utilizzando SnapCenter con i requisiti RPO necessari.
- 2. Eseguire il provisioning di Cloud Volumes ONTAP con la dimensione dell'istanza corretta utilizzando Cloud Manager all'interno dell'abbonamento appropriato e della rete virtuale.
 - a. Configurare SnapMirror per i volumi applicativi rilevanti.

- b. Aggiornare i criteri di backup in SnapCenter per attivare gli aggiornamenti di SnapMirror dopo i processi pianificati.
- 3. Installare il software DR JetStream nel data center on-premise e iniziare la protezione per le macchine virtuali.
- 4. Installare il software DR JetStream nel cloud privato Azure VMware Solution.
- Durante un evento di emergenza, interrompere la relazione di SnapMirror utilizzando Cloud Manager e attivare il failover delle macchine virtuali su Azure NetApp Files o su datastore vSAN nel sito di DR AVS designato.
 - a. Ricollegare I LUN ISCSI e i montaggi NFS per le macchine virtuali dell'applicazione.
- 6. Richiamare il failback sul sito protetto risyncing inverso di SnapMirror dopo il ripristino del sito primario.

Dettagli sull'implementazione

Configurare CVO su Azure e replicare i volumi su CVO

Il primo passaggio consiste nella configurazione di Cloud Volumes ONTAP su Azure ("Collegamento") E replicare i volumi desiderati su Cloud Volumes ONTAP con le frequenze desiderate e le ritentioni di snapshot.

Health Status	Source Volume		Target Volume =		Total Transfer Time	Status	Mirror State	Last Successful Transfer	e
0	gcsdrsqldb_sc46 ntaphci-a300e9u25	×	gcsdrsqldb_sc46_copy ANFCVODRDemo	8	17 seconds	idle	snapmirrored	May 6, 2022, 11:43:18 AM 105.06 KiB	
0	gcsdrsqlhld_sc46_copy ANFCVODRDemo		gcsdrsqlhld_sc46 ntaphci-a300e9u25		7 seconds	idle	snapmirrored	May 6, 2022, 11:42:20 AN 7.22 MiB	
0	gcsdrsqilog_sc46 ntaphcisa300e9u25		gcsdrsqilog_sc46_copy ANFCVODRDemo		16 seconds	idle	snapmirrored	May 6, 2022, 11:43:52 AN 130.69 KiB	

Configurare gli host AVS e l'accesso ai dati CVO

Due fattori importanti da considerare durante l'implementazione di SDDC sono le dimensioni del cluster SDDC nella soluzione VMware di Azure e il tempo necessario per mantenere il SDDC in servizio. Queste due considerazioni chiave per una soluzione di disaster recovery contribuiscono a ridurre i costi operativi complessivi. Il controller SDDC può contenere fino a tre host, fino a un cluster multi-host in un'implementazione su larga scala.

La decisione di implementare un cluster AVS si basa principalmente sui requisiti RPO/RTO. Con la soluzione VMware Azure, il provisioning SDDC può essere eseguito in tempo, in preparazione di test o di un evento di disastro effettivo. Un SDDC implementato Just in Time consente di risparmiare sui costi degli host ESXi quando non si affronta un disastro. Tuttavia, questa forma di implementazione influisce sull'RTO di alcune ore durante il provisioning di SDDC.

L'opzione implementata più comunemente è l'esecuzione di SDDC in una modalità di funzionamento always-on, con illuminazione pilota. Questa opzione offre un ingombro ridotto di tre host sempre disponibili e accelera le operazioni di recovery fornendo una base di riferimento per le attività di simulazione e i controlli di conformità, evitando così il rischio di deriva operativa tra i siti di produzione e DR. Il cluster pilota-light può essere scalato rapidamente fino al livello desiderato quando necessario per gestire un evento DR effettivo.

Per configurare AVS SDDC (sia esso on-demand o in modalità pilota-light), vedere "Implementare e configurare l'ambiente di virtualizzazione su Azure". Come prerequisito, verificare che le macchine virtuali guest che risiedono sugli host AVS siano in grado di utilizzare i dati provenienti da Cloud Volumes ONTAP dopo aver stabilito la connettività.

Dopo aver configurato correttamente Cloud Volumes ONTAP e AVS, iniziare a configurare Jetstream per automatizzare il ripristino dei carichi di lavoro on-premise su AVS (macchine virtuali con VMDK delle applicazioni e macchine virtuali con storage in-guest) utilizzando il meccanismo VAIO e sfruttando SnapMirror per le copie dei volumi delle applicazioni su Cloud Volumes ONTAP.

Il software Jetstream DR è costituito da tre componenti principali: L'appliance virtuale JetStream DR Management Server (MSA), l'appliance virtuale DR (DRVA) e i componenti host (pacchetti di filtri i/o). MSA viene utilizzato per installare e configurare i componenti host sul cluster di calcolo e quindi per amministrare il software DR JetStream. La procedura di installazione è la seguente:

- 1. Verificare i prerequisiti.
- 2. Eseguire Capacity Planning Tool per consigli su risorse e configurazione.
- 3. Distribuire l'MSA DR JetStream su ciascun host vSphere nel cluster designato.
- 4. Avviare MSA utilizzando il nome DNS in un browser.
- 5. Registrare il server vCenter con MSA.
- Una volta implementato JetStream DR MSA e registrato vCenter Server, accedere al plug-in JetStream DR con vSphere Web Client. Per eseguire questa operazione, accedere a Datacenter > Configure > JetStream DR.



- 7. Dall'interfaccia DR JetStream, completare le seguenti attività:
 - a. Configurare il cluster con il pacchetto di filtri i/O.

JetStream DR				
Protected Domains Statistics Storage Sites A	ppliances Configurations	Task Log		
Site Details				Alarm Settings
vCenter Server Hostname	172.21.253.160			
Management Appliance Hostname	ANFJSDR-msa			
Software Version	4.0.0.443			
Subscription ID	00000000-0000-0000	0-0000-000000000001 Configure		
Tenant ID / Application ID	- <u>Configure</u>			
Application Secret	- <u>Configure</u>			
Configured Clusters	Configure Clusters			
Configure Cluster 1 Upprade D Unconfigure & Res		Select All Clear All	۹	٩
Cluster Name 🔺	Cluster Name 🔺	Datacenter Name	sion 🔺	Host Details 🔺
No cluster configured	A300-Cluster	A300-DataCenter	*	
		l≽		
		Cancel	gure	

b. Aggiungere lo storage Azure Blob situato nel sito di ripristino.

Storage Sites	Add Storage Site	
+ Add Storage Site	Storage Ste Tury *	
Name A	Azure Blob Storage	
No Storage Site configured.		
	Access Type *	
	Noy HUUGSS	
	Storage Site Name (Provide a name to identify this Site) *	
	ANFDemoblobrepo	
Storage Site Details Alarms	Acure Blob Storage Account Name *	
	anfdrdemostor	
No storage site selected. Select a storage		
	Ature Bob Storage Account Key*	

8. Implementare il numero richiesto di DRVA (DR Virtual Appliances) dalla scheda Appliances (appliance).



Utilizzare lo strumento di pianificazione della capacità per stimare il numero di DRA richiesti.

JebSbream DR Protected Domains Statistics Storage Sites Applia	nces Configurations	Task Log			Ē
DRVAs (DR Virtual Appliances)					
+ Deprov New DRVA TUpgrade					Q
Name 🔺	Status 🔺	Child Alarm 🔺	Software Version 🔺	Details 🔺	
No DR Virtual Appliance configured.					
Replication Log Volume					
+ New Replication Log Volume					Q
Disk Path Name 🔺	Status	Child Alarm 🔺	Size (available/total)	Details 🔺	
No DRVA selected. Select a DRVA to view replication log volumes.					



9. Creare volumi di log di replica per ogni DRVA utilizzando VMDK dagli archivi dati disponibili o dal pool di storage iSCSI condiviso indipendente.

JetStream DR								E
Protected Domains	Statistics	Storage Sites	Appliances	Configurations	Task Log			
DRVAs (DR Virtual Ap	pliances)							
+ Deploy New DRVA	t uppade	Duconfigure						Q
Name A				Status A	Child Alarm 🔺	Software Version 🔺	Details A	
GCSDRPD001				Running	00	4.0.0.134	Details	•
+ New Replication Log Volum	lolume 🛙 Ur	canadure.						c
Disk Path Name				Status	Child Alarm	Size (available/total)	Details A	
idev/sct				O Ok	0 0	179.88 GB / 200 GB	Detats	
Replication Log Volur	ne Details							
No redirection los uniterna	coloriant datas	t a unitiona to olace date	and the					

10. Dalla scheda Protected Domains (domini protetti), creare il numero richiesto di domini protetti utilizzando le informazioni relative al sito Azure Blob Storage, all'istanza DRVA e al registro di replica. Un dominio protetto definisce una macchina virtuale specifica o un insieme di macchine virtuali dell'applicazione all'interno del cluster che sono protetti insieme e assegnati un ordine di priorità per le operazioni di failover/failback.

I. General 2. Primary Site 3. Summary Protected Domain Name GCSDRPD_Damo01 Priority Level (Optional) - Description Protection domain ANF Total estimated data size to be protected 1000GB DR Virtual Appliance GCSDRPD01 Compression Yes Compression Level Default Normal GC Storage Overhead 300% Replication Log Storage devisdb	elect Protected Domain: - <u>Mex.all</u>	Create Protected Domain				+ Create = 1.1
Protected Domain NameGCSDRPD_Demo01Priority Level (Optional)-DescriptionProtection domain ANFTotal estimated data size to be protected1000GBDR Virtual ApplianceGCSDRPD001Compression LevelDefaultNormal GC Storage Overhead50%Maximum GC Storage300%Replication Log Storagedevisdo		1. General 2.	Primary Site	J. Summary		
Priority Level (Optional)-DescriptionProtection domain ANFTotal estimated data size to be protected1000GBDR Virtual ApplianceGCSDRPD001CompressionYesCompression LevelDefaultNormal GC Storage Overhead300%Replication Log Storageidevisdo		Protected Domain Name	GCSDRPD_Demo01			
Description Protection domain ANF Total estimated data size to be protected 1000GB DR Virtual Appliance 0CSDRPD001 Compression Yeis Compression Level Default Normal GC Storage Overhead 50% Maximum GC Storage Overhead 300% Replication Log Storage idevisido		Priority Level (Optional)				
Total estimated data size to be protected 1000GB DR Virtual Appliance GCSDRPD001 Compression Yes Compression Level Default Normal GC Storage Overhead 300% Replication Log Storage /devisdb		Description	Protection domain ANF			
DR Virtual Appliance GCSDRPD001 Compression Yes Compression Level Default Normal GC Storage Overhead 50% Maximum GC Storage 300% Replication Log Storage devisidb		Total estimated data size to be protected	1000GB			
Compression Yes Compression Level Default Normal GC Storage Overhead 50% Maximum GC Storage Overhead 300% Replication Log Storage /devisdb		DR Virtual Appliance	GCSDRPD001			
Compression Level Default Normal GC Storage Overhead 50% Maximum GC Storage Overhead 300% Replication Log Storage /devisdb		Compression	Yes			
Normal GC Storage Overhead 50% Maximum GC Storage Overhead 300% Replication Log Storage /dev/sdb		Compression Level	Default		-	
Maximum GC Storage Overhead 300% Replication Log Storage //devisdb		Normal GC Storage Overhead	50%			
Replication Log Storage //dev/sdb		Maximum GC Storage Overhead	300%			
		Replication Log Storage	/dev/sdb			
Penlication Los Size KAGB		Panlication Log Size	50GR		-	



11. Selezionare le macchine virtuali da proteggere e raggrupparle in gruppi di applicazioni in base alla dipendenza. Le definizioni delle applicazioni consentono di raggruppare set di macchine virtuali in gruppi logici che contengono i relativi ordini di avvio, ritardi di avvio e validazioni opzionali delle applicazioni che possono essere eseguite al momento del ripristino.



Assicurarsi di utilizzare la stessa modalità di protezione per tutte le macchine virtuali in un dominio protetto.

La modalità Write-Back (VMDK) offre performance superiori.

et Protected Domain, GCSDRPD_Demoul	Start Protection		+ Croate Deinte E Ma
coversible / Total VMs			East D
plication Status	Protection Mode for selected VMs 👻	٩	ANFERED AND AND AND AND AND AND AND AND AND AN
maining Background Data	VM Name 🔺	# of Disks Protection Mode	LOCAL (177.21.253.160-)
	ElasticWebA2	1 Witter Through St.	Thushed
tien HPO	ElasticWebA3	🕇 🛛 🗤 🗸 🗸	- Andrews
Sectorized VAIR Controls Attantos	ElasticWebB0	1 write Through 🗸 .	
Theorem With Security Committee	ElasticWebB1	t Write-Through 🗢 _	
A Start Ecologica Research	ElasticWebB2	 Write Through Sec. 	
Source Environment	ElasticWebB3	1 Write Through 😔	
VM Name A	GCS-DR-DC	1 Write-Through V	Background Data A Distails
No VM is producted	GCS-DR-LinVM01	1 Write-Through 🗸	
	CCS-DR-SCA	.1 Write-Through 😽	
	GCS-DR-SQL01	1 Write-Through V	
	GCS-DR-WnVM01	1 Write-Through 🗸	
	jss-drva-GCSDRPD001	2 Witte Through V.	
	PrimeClient	2 Write Through 🤟	
	Standby0	4 Write Through 😪 🖉	
	Standby1	t Wins Through 🗢	
	Standby2	1 Witter Thready 🖌 😪	
	Standby3	🐧 Write Through 😪 🖉	
	VMmark-Template01	1 Write Timough 🗸 🐨	
		Cancel Start Protection	

12. Assicurarsi che i volumi dei log di replica siano posizionati su uno storage dalle performance elevate.

ect Protected Domain: GCSDRPD_Demo01 -	Start Protection				+ Creato Dotete
coverable / Total VMs				1	Edd 1
plication Status	Write-Back(VMDK)			٩	ANFORDemoFallover5ite
maining Background Data	VM Name 🔺	# of Disks	Protection Mode		LOCAL (172,21,253,160)
	ElasticWebA2	1	Write-Through		The state of the s
	ElasticWebA3	1	White-Through		2000//20
And a second second	ElasticWebB0	1	white-Through v		
TORRELEC VARS SERIOGS AUGUME	ElasticWebS1	-1	Witte-Through		
and the second se	ElasticWebB2	1	With-Through		
STATI PTONECTION	ElasticWeb63	1	Write-Through		
VM Name 🔺	GCS-DR-DC	1	(White-Back/VMDK)	3	Background Data A Details
No VM is protected.	GCS-DR-LivVM01	1	Write-Back(VMDK) ~		
	C GCS-DR-SCA	1	Write-Back(VMDK)		
	GCS-DR-SQL01	1	Write-Back(VMDK)		
	GCS-DR-WeVM01	1	Write-Back(VMDK)		
	jttl-dtva-GCSDRPD001	2	Witte-Tricogt >		
	PrimeClient	2	With-Through v		
	Standby0	1	with Trends	S. U	
	Standby1	1	Wms-Through W		
	C Standby2	21	White Through		
	C Standby3	1	Write Through	S	
	VMmark-Template01	1	With Through	5 第二	
			Cancel Start P	rotection	
			and and	N	

13. Al termine dell'operazione, fare clic su Start Protection (Avvia protezione) per il dominio protetto. In questo modo viene avviata la replica dei dati per le macchine virtuali selezionate nell'archivio Blob designato.

Protected Domains Statistics Storage	e Sites Appliances Configurations Task	Log			Running Tasl	
elect Protected Domain: GCSDRPD_Demo	01 - <u>View all</u>			+ (Start Protection (GCS-DR-	SCA) 50%
ecoverable / Total VMs	i.	0/5 Configurati	ons		Start Protection (GCS-DR-	Win
eplication Status		OK Storage Site		ANFDRDe	Start Protection (GCS-DR-I	Lin 50%
		Owner Site		LOCAL (172.2	Start Protection (GCS.DR.)	001 50%
emaining Background Data		0 B Datacenter \	Cluster	A300-DataCen	Sian Protection (GCS-DR-	00) 50%
urrent RPO		Point-in-time	Recovery	Disabled	Start Protection (GCS-DR-	SQ. 50%
Protected VMs Settings Alarms					Configure VMDK Re Cor	mpleted 🔽
Protected VMs Settings Alarms + Start Protection Glop Protection				- 1	Configure VMDK Re Con	npleted 🔽
Protected VMs Settings Alarms Start Protection VM Name	Protection Status Replica	ition Status	Protection Mode	Background Da	Close Close	npleted 🔽
Settings Alarms Start Protection WN Name GCS-DR-DC	Protection Status Replice Initializing	tion Status 🔺	Protection Mode ▲ Write-Back(VMDK)	Background Da	Configure VMDK Re Con Close ta Details Details	npieted 🔽
Protected VMs Settings Alarms + Start Protection VM Name GCS-DR-DC GCS-DR-LinVM01	Protection Status Replica initializing - initializing -	ation Status 🔺	Protection Mode Write-Back(VMDK) Write-Back(VMDK)	Background Da	Configure VMDK Re Con Close ta A Details Details Details	npleted 🗹
	Protection Status Replica Initializing initializing initializing initializing	ation Status 🔺	Protection Mode Write-Back(VMDK) Write-Back(VMDK) Write-Back(VMDK)	Background Da - -	Configure VMDK Re Con Close ta A Details Details Details Details	npieted 🗹
Protected VMs Settings Alarms + Start Protection ○ VM Name ▲ ○ GCS-DR-DC ○ GCS-DR-LintVM01 ○ GCS-DR-SCA ○ GCS-DR-SOL01	Protection Status Replica Initializing Initializing Initializing Initializing Initializing Initializing	ation Status 🔺	Protection Mode Write-Back(VMDK) Write-Back(VMDK) Write-Back(VMDK) Write-Back(VMDK)	Background Da - -	Configure VMDK Re Con Close ta Details Details Details Details Details	npieted 🗹

14. Una volta completata la replica, lo stato di protezione della macchina virtuale viene contrassegnato come ripristinabile.

JebSbream DR Protected Domains Statistics Storage	Sites Appliances Configurat	ions Task Log				5
Select Protected Domain: GCSDRPD_Demo	h ▼ <u>View all</u>			+ Create	Delete	≡ More
Recoverable / Total VMs		5/5	Configurations			Edit Details
Replication Status		OK	Storage Site	ANFDRDemoFailo	verSite	
			Owner Site	LOCAL (172.21.253.16	(0	
Remaining Background Data		0 B	Datacenter \ Cluster	A300-DataCenter \ A30	0-Cluster	
Current RPO		05	Point-in-time Recovery	Disabled		
Protected VMs Settings Alarms + Start Protection III Stop Protection						100
						۹
VM Name A	Protection Status A	Replication Statu	us Protection Mode	Background Data 🔺	Details	۹
VM Name ▲ GCS-DR-DC	Protection Status A	C OK	US Protection Mode Write-Back(VMDK)	Background Data A 0 B	Details Details	۹.
VM Name ▲ GCS-DR-DC GCS-DR-LinVM01	Protection Status Recoverable Recoverable	Replication Statu OK OK	Vrite-Back(VMDK) Write-Back(VMDK) Write-Back(VMDK)	Background Data A 0 B 0 B	Details Details Details	٩
VM Name ▲ GCS-DR-DC GCS-DR-LinVM01 GCS-DR-SCA	Protection Status Recoverable Recoverable Recoverable Recoverable Recoverable	Peplication Statu OK OK OK	us Protection Mode Virite-Back(VMDK) Virite-Back(VMDK) Virite-Back(VMDK) Virite-Back(VMDK)	Background Data A 0 B 0 B 0 B	Details Details Details Details Details	â
VM Name GCS-DR-DC GCS-DR-LinVM01 GCS-DR-SCA GCS-DR-SQL01	Protection Status	Replication Statu O OK O OK O OK O OK	us ▲ Protection Mode ▲ Write-Back(VMDK) Write-Back(VMDK) Write-Back(VMDK) Write-Back(VMDK)	Background Data ▲ 0 B 0 B 0 B 0 B	Details Details Details Details Details Details	a

i

Le runbook di failover possono essere configurate per raggruppare le macchine virtuali (denominate gruppo di ripristino), impostare la sequenza dell'ordine di avvio e modificare le impostazioni della CPU/memoria insieme alle configurazioni IP.

15. Fare clic su Impostazioni, quindi sul collegamento Configura runbook per configurare il gruppo runbook.

Select Protected Domain: GCSDRPD_Demo01 - View all		+ Create	≡ More
Recoverable / Total VMs 5 / 5	Configurations		Edit Detail
Replication Status	Storage Site	ANFDRDemoFailoverSite	(a
	Owner Site	LOCAL (172 21 253 160)	
Remaining Background Data 0 B	Datacenter \ Cluster	A300-DataCenter \ A300-Cluster	
Current RPO 0s	Point-in-time Recovery	Disabled	
Protected VMs Settings Alarms			
Failover Runbook Not Configured Configure			
Test Failover Runbook Not Configured Configure			
Fallback Runbook 🔓 Not Configured Configure			
Memory Setting Not Configured Configure			
GC Settings Configured Configure			
Concurrency Settings Not Configured Configure			

16. Fare clic sul pulsante Create Group (Crea gruppo) per iniziare a creare un nuovo gruppo di runbook.

Se necessario, nella parte inferiore della schermata, applicare pre-script e post-script personalizzati da eseguire automaticamente prima e dopo l'operazione del gruppo di runbook. Assicurarsi che gli script Runbook risiedano sul server di gestione.

i

Jet/Stream DR Protected Domains Statistics Storage Site	Failover Runbook Settings		Ē
Select Protected Domain: GCSDRPD_Demo01	+ Create Group / Edit 1	Delate Group	+ Create Delete E More
Recoverable / Total VMs	O Group Name	# of VM Power Off Retain MAC	Edd Details
Replication Status	O 🗌 Independent VMs	5	ANFDRDemoFalloverSite
Remaining Background Data			A300-DataCenter (A300-Cluster
Current RPO			Disabled .
Protected VMs Settings Alarms	0 0		
Failover Runbook Configured Details			
Test Failover Runbook Configured Details			
Failback Runbook Configured Details			
Memory Setting Not Configured Configure			
GC Settings Configured Configure			
Concurrency Settings Not Configured Configure			

17. Modificare le impostazioni della macchina virtuale secondo necessità. Specificare i parametri per il ripristino delle macchine virtuali, tra cui la sequenza di avvio, il ritardo di avvio (specificato in secondi), il numero di CPU e la quantità di memoria da allocare. Modificare la sequenza di avvio delle macchine virtuali facendo clic sulle frecce verso l'alto o verso il basso. Sono inoltre disponibili opzioni per conservare MAC.

JebSbream DR Protected Domains Statistics Storage	Create Runbook Group										劉
Select Protected Domain: GCSDRPD_Damo	1. General	2. Select VM	s	3. Edit V	M Settings		4. Summ	iry	+ Create	E Oeliste	≡ More
Recoverable / Total VMs	Retain MAC		Power Of	f VMs			O Reset				
Replicitor Skins	VM Name	Boot Sequence	Boot Delay	CPU	Memory	Script	NIC				
Replaning Background Cata	GCS-DR-WinVM01	17 4	0s	32	64 GB	Config	View	-			
Communication of the second	GCS-DR-SCA	21 1	0s	4	16 GB	Config	View				
Cancell 1950	GCS-DR-DC	3 11m+	0s	4	16 GB	Config	View				
Protecting VUIs Settings Alarma	GCS-DR-LinVM01	41 4	0s	2	4 GB	Config	View				
	GCS-DR-SQL01	5† 4	0s	4	8 GB	Config	View				
Failback Rundbook Confoured Latas Failback Rundbook Microsoft Latas Memory Setting Not Confoured Confoured GC Settings Confoured Confoured Concurrency Settings Not Confoured Confoured				Ca	ncel	Back		iest			

18. Gli indirizzi IP statici possono essere configurati manualmente per le singole macchine virtuali del gruppo. Fare clic sul collegamento NIC View (visualizzazione NIC) di una macchina virtuale per configurare manualmente le impostazioni dell'indirizzo IP.

nain: GCSDRPD_Demo	1. General	2. Select VM:	5	3. Edit VI	A Settings		4. Summar	У	+ Creals	Delete	≡ Ak
Ma U	Retain MAC		Power Of	VMs			0.044				
			-				C Reset		VED RD anoF alloy	er folge	
A MARTINE AND A MARTINE	VM Name	Boot Sequence	Boot Delay	CPU	Memory	Script	NIC		21/1722125316		
d Loga	GCS-DR-WINVM01	11 4	05	32	64 68	Contro	35	- -	DataCenter I, A300	Chuster	
	GCS-DR-SCA	27 4	QS 0.	4	10 GB	Comp	Xight		at :		
	ace op sol Q	37 4	0s	4	4 GB	Contra	VIEW				
Sectiongs Alamma	GCS-DR-SQL01	47.4	05	*	808	Canling	XIRVI				

19. Fare clic sul pulsante Configure (Configura) per salvare le impostazioni NIC per le rispettive macchine virtuali.

	Label	Network Name	Key	PCI Slot #	IP	- 64
1.	Network adapter	1 VM_3510	4000	192	Configure	aix
Re						
VM NA						
GCS-E						
Ubum	Con	igure Static IP Addres	is			
GCSD	PAS	iness -				
GCS-E	172	21.254.185				
- OP	00					
	Subr	t Mask *				
	255	255.255.0				
	Gara	div *				
	172	21.254.1				
	DNS					
	172	30.153.20				
	DNS	Suffix				
					_	
		Reset	Cance	el Conf	igure	
			_			
					Close	Next
					1	
liktStream DR				_		
	entrinest interio	te Runbook Group			14700 I.I.	
		1. General Z. Select VM	s 3. Edit VM Set	ungs 4. Summ	-	
		lumber of VMs	5 true		PERDensfelduesta	
		ower Off VMs	faise		State and LANG Co.	
	No Anna	Group mangerstig and boot sequence change	will be applied to both Fallover and	ž Faliback runbook.		
		Success				

Lo stato dei runbook di failover e failback è ora elencato come configurato. I gruppi runbook di failover e failback vengono creati in coppie utilizzando lo stesso gruppo iniziale di macchine virtuali e impostazioni. Se necessario, le impostazioni di qualsiasi gruppo di runbook possono essere personalizzate singolarmente facendo clic sul relativo link Details (Dettagli) e apportando modifiche.

Una Best practice per un sito di recovery (AVS) consiste nella creazione anticipata di un cluster pilota a tre nodi. Ciò consente di preconfigurare l'infrastruttura del sito di ripristino, tra cui:

- Segmenti di rete di destinazione, firewall, servizi come DHCP e DNS e così via
- Installazione di JetStream DR per AVS
- · Configurazione dei volumi ANF come datastore e altro ancora

Jetstream DR supporta una modalità RTO quasi zero per i domini mission-critical. Per questi domini, lo storage di destinazione deve essere preinstallato. ANF è un tipo di storage consigliato in questo caso.



La configurazione di rete, inclusa la creazione di segmenti, deve essere configurata sul cluster AVS per soddisfare i requisiti on-premise.



A seconda dei requisiti SLA e RTO, è possibile utilizzare il failover continuo o la normale modalità di failover (standard). Per un RTO vicino allo zero, è necessario avviare una reidratazione continua nel sito di ripristino.

1. Per installare JetStream DR per AVS su un cloud privato Azure VMware Solution, utilizzare il comando Esegui. Dal portale Azure, accedere alla soluzione Azure VMware, selezionare il cloud privato e selezionare Esegui comando > pacchetti > Configurazione JSDR.



L'utente CloudAdmin predefinito di Azure VMware Solution non dispone di privilegi sufficienti per installare JetStream DR per AVS. Azure VMware Solution consente un'installazione semplificata e automatica del DR JetStream invocando il comando Azure VMware Solution Run per il DR JetStream.

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

Microsoft Azure	P Search resources, services, and docs (G+/)	🗈 🔂 🤌 🗇 🔗 niyaz@netapp.com 🧶
Home > ANFDataClus ANFDataClus Run ArS Private cloud	command –	Run command - Install-JetDRWithDHCP × This top level Cindlet Downloads JetDr tundle from MMS, creates a new user, assigns
Seatch (Ctrl+/) Access control (IAM)	Refresh R Feedback Packages Run execution status	elevated privileges to the user, deploys ArtDr Management Server Applance/MSA), registers vCente to the IntEC MSA, configures cluster. Command patameters
Tigs Diagnose and solve problems	V Name Description	RegisterWithp 💿
Settings	SOR Configuration 224 Powener Masse to simplicity at actives Software 345 see and easy Disuble- Int/DRFor/Cluster This Circlet unconfigures a duater but doesn't unit policies.	and and the Name of Annual Annua
Manage Connectivity	Estable-setCIRForCluster This Cindlet configures an additional duster for pro Initial-IetDRWithCIRCP This top level Cindlet Downloads JetDr bunche from contents of centre to the JetDr Addit Configure to the JetDr Addit	tection it installs uids to all hosts in the VARDame* O Antonie* O
Custers Clusters	Install-intDRWirtGtaticIP This top level Criticity and a set of the anti-intDRWirtGtaticIP This top level Criticity and the anti-intDRWirtGtaticIP ASA, configure clust	MMS, crosses a new user, stidigns eleve er.
Storage (preview) Placement policies Add cost	Invike-Prefight/eitDRinatall This Circlet checks and displays current state of the A hosts. If the locate details are correct, if there is a Invike-Prefight/eitDRUxinstall This Circlet checks and displays current state of the	system Tokeks whether the ensional Uperanne * uperanne
Workload Networking	4 hosts, if the cluster details are correct and if any V Uninstall letDR The top level Cmdlet creates a new user, assigns ele	Center is registered to the MSA Plastacid * winde privilleges to the user, unconfigu
Segments DHCP Fort mimoring	2 Microsoft.Arg.Managetterit, 4207 Wolve onlike to estimate we see in newspip Azer Winew S	ndm Hottane ⊙ antpodema Network * ⊙
O DNS		Ditiseg
Run command		Retain up to

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

W20 1955 100 Ac									
Site Details								Alarm Set	ti
vCenter Server Hostna	ne	172.30.1	56.2						
Management Appliance	Hostname	anfjsval-n	nsa						
Software Version		4.0.2.450	i.						
Subscription ID		- Config	ure						
Tenant ID / Application	ID	- Config	ure						
Application Secret		- Config	ure						
Configure Cluster	1 Upgrade	Duconfigure	🛠 Resolv	e Configure	Issue				
Cluster Name		Datacenter	Name 🔺	Status	A	Software Version	A	Host Details	5
Cluster-1		SDDC-Data	center	🕝 Ok		4.0.2.132		Details	

- 3. Dall'interfaccia DR JetStream, completare le seguenti attività:
 - a. Aggiungere l'account Azure Blob Storage utilizzato per proteggere il cluster on-premise come sito di storage, quindi eseguire l'opzione Scan Domains.
 - b. Nella finestra di dialogo a comparsa visualizzata, selezionare il dominio protetto da importare, quindi fare clic sul relativo collegamento Importa.



4. Il dominio viene importato per il ripristino. Accedere alla scheda Protected Domains (domini protetti) e verificare che sia stato selezionato il dominio desiderato oppure scegliere quello desiderato dal menu Select Protected Domain (Seleziona dominio protetto). Viene visualizzato un elenco delle macchine virtuali ripristinabili nel dominio protetto.

Jet/Stream DR Protected Domains Statistics Storage Sites Appliances Configurations	Task Log			l
Select Protected Domain: GCSDRPD_Demo01 View all		+ Create	Delete	≡More
Mode Impor	ted Configurations			Detail
Recoverable / Total VMs-	5/5 Storage Site Owner Site	ANFDemoblobre	porec	
Protected VMs Settings Alarms O O				
VM Name A Protection	Status 🔺	Protection Mode	Details	٩
GCS-DR-DC Ø Recover:	sble	Write-Back(VMDK)	Details	^
GCS-DR-LinVM01 Ø Recovera	able	Write-Back(VMDK)	Details	
GCS-DR-SCA Ø Recover:	able	Write-Back(VMDK)	Details	
GCS-DR-SQL01 ØRecovera	ible	Write-Back(VMDK)	Details	

5. Una volta importati i domini protetti, implementare le appliance DRVA.

 (\mathbf{i})

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

- 6. Creare volumi di log di replica utilizzando datastore vSAN o ANF disponibili.
- 7. Importare i domini protetti e configurare il VA di ripristino in modo che utilizzi un datastore ANF per il posizionamento delle macchine virtuali.

ect Protected Domain:	Continuous F	ailover Protected Dom	ain		_			Delete	=	More
de	1 Ceneral	0 Esilouar Sattings	O VM Settings	1 Per		A DR Settings	5 Summany			Dela
coverable / Total VMs	i. General	za. ranover settings	zo, vin setungs	s. nec	overy w	4. Dit antungs	o. ouninary	~ reporec		1
	Protected D	omain Name		ANFPD002				253,160)		
	Datacenter			SDDC-Data	center			100		
	Cluster			Cluster-1				1000		
rotected VMs Seth	Resource P	ool (Optional)						1000		
	VM Folder (Optional)		÷.,						
	Datastore			ANFRecoD	SU002			100		
	Internal Net	twork		DRSeg				100	-	
VM Name A	External Re	plication Network		DRSeg					Details	71
AuctionAppR2	Managemer	nt Network		DRSeg				1000	Dataile	
AuctionDB2	Storage Site	•		ANFDemob	lobreporec			1000	Dutaile	
Auction R2	DR Virtual A	ppliance		ANFRecDR	VA003				Detaile	
Auction/ISO2	Donlightion	I an Ctorsea		Mouladh				_	Dutails	
Aucuonworzz					Cancel	Back	Continuous Failov	er	Contraines	12

()

Assicurarsi che DHCP sia attivato sul segmento selezionato e che sia disponibile un numero sufficiente di IP. Gli IP dinamici vengono temporaneamente utilizzati durante il ripristino dei domini. Ogni macchina virtuale di ripristino (inclusa la reidratazione continua) richiede un IP dinamico individuale. Una volta completato il ripristino, l'IP viene rilasciato e può essere riutilizzato.

8. Selezionare l'opzione di failover appropriata (failover o failover continuo). In questo esempio, viene selezionata la reidratazione continua (failover continuo).

 (\mathbf{i})

Anche se le modalità di failover continuo e failover differiscono quando viene eseguita la configurazione, entrambe le modalità di failover vengono configurate utilizzando le stesse procedure. I passaggi di failover vengono configurati ed eseguiti insieme in risposta a un evento di emergenza. È possibile configurare il failover continuo in qualsiasi momento e consentire l'esecuzione in background durante il normale funzionamento del sistema. In seguito a un evento di emergenza, il failover continuo viene completato per trasferire immediatamente la proprietà delle macchine virtuali protette al sito di ripristino (RTO quasi nullo).

letStream DR Protected Domains Statistics Storage Sites Appliance	s Configurations Task	Log			
elect Protected Domain: GCSDRPD_Demo01 👻 View all			+ Create	Delete	≡ More
lode	Imported	Configurations		O Restore	
Recoverable / Total VMs	5/5	Storage Site	ANFDemoblobrepor	→ Failover	
		Owner Site	REMOTE (172.21.253.1f	→ Continuous Fai	lover.
				t commuters i di	G
Protected VMs Settings Alarms O O					
VM Name 🔺	Protection Status	*	Protection Mode 🔺	Details	
GCS-DR-DC	Recoverable		Write-Back(VMDK)	Details	
GCS-DR-LinVM01	O Recoverable		Write-Back(VMDK)	Details	
GCS-DR-SCA	C Recoverable		Write-Back(VMDK)	Details	
GCS-DR-SQL01	O Recoverable		Write-Back(VMDK)	Details	
CCS-DR-WeVII01	A Recoverable		Write Back(MDK)	Details	

Viene avviato il processo di failover continuo, che può essere monitorato dall'interfaccia utente. Facendo clic sull'icona blu nella sezione Current Step (fase corrente) viene visualizzata una finestra a comparsa che mostra i dettagli della fase corrente del processo di failover.

Failover e failover

In caso di disastro nel cluster protetto dell'ambiente on-premise (errore parziale o completo), è
possibile attivare il failover per le macchine virtuali utilizzando Jetstream dopo aver interrotto la
relazione SnapMirror per i rispettivi volumi applicativi.





Questo passaggio può essere facilmente automatizzato per facilitare il processo di recovery.

2. Accedere all'interfaccia utente Jetstream su AVS SDDC (lato destinazione) e attivare l'opzione di failover per completare il failover. La barra delle applicazioni mostra lo stato di avanzamento delle attività di failover.

Nella finestra di dialogo visualizzata al completamento del failover, è possibile specificare l'attività di failover come pianificata o presunta come forzata.

elect Protected Domain. GCSDRPD_Demod	1 View all		+ Create	O Failover	≡ Mor
Mode	Continuous Rehydration in Progress	Configurations			Details
Recoverable / Total VMs	4/4	Storage Site		rec	^
		Owner Site	REMOTE (172.21.253.1	160)	
Data (Processed/Known Remaining)	329.01 GB / 6.19 GB	Datacenter \ Cluster	SDDC-Datacenter \ Clu	ster-1	
Current Step	Recover VMs' data from Storage Site	Point-in-time Recovery	Disabled		~
VM Name	Protection Status		Protection Mode	Details	ų
	© Recoverable		Write-Back(VMDK)	Details	^
GCS-DR-DC	Recoverable		Write-Back(VMDK)	Details	
GCS-DR-LinVM01			Write-Back(VMDK)	Details	
GCS-DR-DC GCS-DR-LinVM01 GCS-DR-SCA	Recoverable				
GCS-DR-LinVM01 GCS-DR-SCA GCS-DR-SCA GCS-DR-SQL01	 Recoverable Recoverable 		Write-Back(VMDK)	Details	

an network mapping			
Protected VM Network 🔺	Recovery VM Network		3
VM_3510	DRStretchSeg	^	
0 0		v	Č.
Other Settings			
Lam, FOICE Failuyer			
40			

Il failover forzato presuppone che il sito primario non sia più accessibile e che la proprietà del dominio protetto debba essere direttamente assunta dal sito di ripristino.

Force Failover	r of Protected Domai	in requested. Adminis	trator consent is
Complete own	nership of this Prote	cted Domain will be ta	aken over by this
Site.			
Are you sure y	ou want to continue	?	
		0	Contrast.
	Force Failover required Complete own Site. Are you sure y	Force Failover of Protected Domai required! Complete ownership of this Prote Site. Are you sure you want to continue	Force Failover of Protected Domain requested. Adminis required! Complete ownership of this Protected Domain will be to Site. Are you sure you want to continue?

in network mapping					
Protected VM Network 🔺	Recovery VM Network				^
/M_3510	DRStretchSeg		•	^	
0 0					
				~	~
ther Settings					
Planned Failover					
Force Failover					
Sama VIII's quast cradeatial are rear	ired because of network configuration	Continues			
	med because of network configuration.	Configure			

3. Una volta completato il failover continuo, viene visualizzato un messaggio che conferma il completamento dell'attività. Al termine dell'attività, accedere alle macchine virtuali ripristinate per configurare le sessioni ISCSI o NFS.

La modalità di failover diventa in esecuzione in failover e lo stato della macchina virtuale è ripristinabile. Tutte le macchine virtuali del dominio protetto sono ora in esecuzione nel sito di ripristino nello stato specificato dalle impostazioni del runbook di failover.

Per verificare la configurazione e l'infrastruttura di failover, è possibile utilizzare JetStream DR in modalità test (opzione Test failover) per osservare il ripristino delle macchine virtuali e dei relativi dati dall'archivio di oggetti in un ambiente di test recovery. Quando una procedura di failover viene eseguita in modalità test, il suo funzionamento assomiglia a un processo di failover effettivo.

 (\mathbf{i})

(i)

JebSbream DR Protected Domains Statistics Stora	Continuous Rehydration Task Resu	n	
Select Protected Domain: GCSDRPD002	Task Completed Successfully with	warnings	+ Create B Delete = More
Mode	<u> </u>		Edit Option
HORON I 122220 000 HE 227 (41194)	Protected Domain	GCSDRPD002	MECHODR
rescoverance / rome vives	VMs Recovery Status	Success with warnings	DCAL:/ 172:30:458:23
	Total VMs Recovered	4	DDC-Datacenter (Duster, 1
Parallel Control (1999) International Parallel	VM(s) with warning	2 <u>View</u>	enabled
Kemaining background bata	GCSRecovery03 Status:		100000
	Pre-script Execution Status	Not defined	
	Runbook Execution Status	Success	
Protected VMs Settings Atarms	Post-script Execution Status	Not defined	
+ Start Protection			c
VM Name A		~	ackground Data 🔺 Details
GCS-DR-SC45		2	e Details
GCS-DR-SOL03			B Details
GCSDR-W2K16-01			8 Detaits
UbuntuSrv001			B Dataita

- 4. Una volta ripristinate le macchine virtuali, utilizzare il disaster recovery dello storage per lo storage inguest. Per dimostrare questo processo, in questo esempio viene utilizzato SQL Server.
- 5. Accedere alla macchina virtuale SnapCenter recuperata su AVS SDDC e attivare la modalità DR.
 - a. Accedere all'interfaccia utente di SnapCenter utilizzando il browserN.

A https://gcs-dr-sc46.gcsdc.com:8146/	→ A × O gcs-dr-	sc46.gcsdc.com ×
	N N	etApp。。
	SnapCente	er®
	Username	gcsdc\adrųjnnimo
	Password	•••••
diskinger states in		Sign In

- b. Nella pagina Settings (Impostazioni), accedere a Settings (Impostazioni) > Global Settings (Impostazioni globali) > Disaster Recovery (Ripristino di emergenza).
- c. Selezionare Enable Disaster Recovery (attiva ripristino di emergenza).
- d. Fare clic su Applica.

	letApp SnapC	enter®						•	-	9 -	SnapCenterAdmin	Sign Out
<		Global Settings	Policies	Users and Access	Roles	Credential	Software					
	Dashboard											
9	Resources	Global Settings	9									
۲	Monitor											
ai	Reports	Hypervisor Settin	gs O									~
*	Hosts	Notification Serv	er Settings	0		0.0)					~
ł.	Storage Systems	Configuration Se	ttings 😗									~
華	Settings	Purge jobs Settin	gs O									~
▲	Alerts	Domain Settings	0									~
		CA Certificate Set	ttings 🕕									~
		Disaster Recover	y o									

e. Verificare che il processo DR sia attivato facendo clic su Monitor > Jobs (Monitor > processi).



Per il disaster recovery dello storage è necessario utilizzare NetApp SnapCenter 4.6 o versione successiva. Per le versioni precedenti, è necessario utilizzare snapshot coerenti con l'applicazione (replicati utilizzando SnapMirror) e eseguire il ripristino manuale nel caso in cui i backup precedenti debbano essere ripristinati nel sito di disaster recovery.

6. Verificare che la relazione di SnapMirror non sia più stabilita.

Canvas	Replication	Backup & Restore	Data Sense	File Cache	Compute	Sync All Service	s (+9) ~			
Repli	cation									
		J Volume Re	lationships	2 4.7	8 GIB ted Capacity	0 Currently Trans	sterring	3 Healthy	⊗ 0 Failed	
		3 Volume Relationships								a c
		Health Status 🔹	Source Volume	= Target	Volume =	Total Transfer Time ÷	Status 🐨	Mirror State	Last Successful Transfer	0
		Health Status +	Source Volume gcsdrsqldb_sc46 ntaphci-a300e9u25	i Target gcsdrsc ANFCVI K	Volume = Idb_sc46_copy ODRDemo	Total Transfer Time + 6 minutes 41 seconds	Status 👻	Mirror State	Lust Successful Transfer May 5, 2022, 12:08:34 PN 33.66 KiB	•
		Health Status +	Source Volume gcsdrsqldb_sc45 ntaphci-a300e9u25 gcsdrsqlhid_sc46 ntaphci-a300e9u25	s Target gcsdrsc ANFCVI ¢ gcsdrsc ANFCVI ¢	Volume 2 Idb_sc46_copy ODRDemo 2hid_sc46_copy ODRDemo >	Total Transfer Time 5 6 minutes 41 seconds 4 minutes 56 seconds	Status 👻 idle idle	Mirror State broken-off broken-off	3 Last Successful Transfer May 5, 2022, 12:08:34 Ph 33.66 KIB May 5, 2022, 12:09:15 Ph 69.84 KIB	•

7. Collegare il LUN da Cloud Volumes ONTAP alla macchina virtuale SQL guest recuperata con le stesse lettere di unità.
| 📅 Disk Manageme | nt | | | | | | 3 77 3 | | × |
|------------------|-----------|-------|--------------------------|------------|----------|----------|-------------------|---|---|
| File Action View | v Help | | | | | | | | |
| 🗢 🔿 🖂 🖬 | m 🗩 🕑 (| | | | | | | | |
| Volume | Layout | Туре | File System | Status | Capacity | Free Spa | % Free | 1 | |
| - | Simple | Basic | 1 contract of a contract | Healthy (R | 450 MB | 450 MB | 100 % | | |
| - | Simple | Basic | | Healthy (E | 99 MB | 99 MB | 100 % | | |
| - (C:) | Simple | Basic | NTFS | Healthy (B | 89.45 GB | 67.03 GB | 75 % | | |
| BACKUP (G:) | Simple | Basic | NTFS | Healthy (P | 9.97 GB | 9.92 GB | 99 % | | |
| - DATA (E:) | Simple | Basic | NTFS | Healthy (P | 24.88 GB | 24.57 GB | 99 % | | |
| - LOG (F:) | Simple | Basic | NTFS | Healthy (P | 9.97 GB | 8.93 GB | 90 % | | |
| | | | | | 0 | 0 | | | |

8. Aprire iSCSI Initiator, cancellare la sessione disconnessa precedente e aggiungere la nuova destinazione insieme al multipath per i volumi Cloud Volumes ONTAP replicati.

- Si init		illes			
Targets	Discovery	Favorite Targets	Volumes and Devices	RADIUS	Configuration
Quick (To disc DNS na	Connect cover and log ame of the to	g on to a target usin arget and then dick	ng a basic connection, ty Quick Connect.	ype the IP	address or
Discove	ered targets				Refresh
Name	1			Status	
2010/07/2	992-08.com.	netapp:sn.547772c	cc47811ecbb62000	Connecte	d
ign. 1				······································	

9. Assicurarsi che tutti i dischi siano collegati utilizzando le stesse lettere di unità utilizzate prima del DR.



10. Riavviare il servizio del server MSSQL.

⊨ → 🖂 🖾 	🗟 🛃 🔣 📷 🕨 🔳 💵 🕨					
Services (Local)	Services (Local)					
	SQL Server (MSSQLSERVER)	Name	Description	Status	Startup Type	Log '
		🖏 SQL Full-text Filter Daemon	Service to la	Running	Manual	NT
	Stop the service	SQL Server (MSSQLSERVER)	Provider do	Running	g Automatic	GCS
	Restart the service	SQL Server Agent (MSS)	Start	ning	g Automatic	GCS
		SQL Server Browser	Stop	ning	a Automatic	Loc
	Description	SQL Server CEIP service	Pause	ning	g Automatic	NT
	Provides storage processing and	SQL Server Integration S	Resume	ning	g Automatic	NT
	controlled access of data, and rapid	SQL Server Integration S	Restart	ning	a Automatic	NT
	transaction processing.	🧠 SQL Server VSS Writer	url'au	ning	g Automatic	Loc
		SSDP Discovery	All Tasks	> nînç	Manual	Loc
		State Repository Service	Refresh	ning	g Manual	Loc
		🗟 Still Image Acquisition E	Nerrean		Manual	Loc
		Carl Storage Service	Properties		Manual (Trig	Loc
		Storage Tiers Managem	Help		Manual	Loc
		Charles Superfetch	riep		Manual	Loc
		🔍 Sync Host_df83a	This service	Running	Automatic (D	Loc
		System Event Notification S	Monitors sy	Running	g Automatic	Loc
		<				>

11. Assicurarsi che le risorse SQL siano nuovamente in linea.



÷.

Nel caso di NFS, collegare i volumi utilizzando il comando mount e aggiornare /etc/fstab voci.

A questo punto, è possibile eseguire le operazioni e continuare normalmente il business.

Sull'estremità NSX-T, è possibile creare un gateway Tier-1 dedicato separato per simulare scenari di failover. Ciò garantisce che tutti i carichi di lavoro possano comunicare tra loro, ma che nessun traffico possa essere instradato all'interno o all'esterno dell'ambiente, in modo che qualsiasi attività di triage, contenimento o protezione avanzata possa essere eseguita senza rischi di contaminazione incrociata. Questa operazione non rientra nell'ambito del presente documento, ma può essere facilmente eseguita per simulare l'isolamento.

Una volta che il sito primario è stato nuovamente operativo, è possibile eseguire il failback. La protezione delle macchine virtuali viene ripristinata da Jetstream e la relazione SnapMirror deve essere invertita.

- 1. Ripristinare l'ambiente on-premise. A seconda del tipo di incidente, potrebbe essere necessario ripristinare e/o verificare la configurazione del cluster protetto. Se necessario, potrebbe essere necessario reinstallare il software DR JetStream.
- 2. Accedere all'ambiente on-premise ripristinato, accedere all'interfaccia utente DR Jetstream e selezionare il dominio protetto appropriato. Una volta che il sito protetto è pronto per il failback, selezionare l'opzione failover nell'interfaccia utente.



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

Protected Domains Statistics Storage Sites Appliar	ices Configurations Task L	og			
Select Protected Domain: GCSDRPD_Demo01 💌 View all			+ Create	Telete	■ More
Mode	Running in Failover	Configurations		O Restore	
Active Site	172.30.156.2	Storage Site	ANFCVODR	O Resume Continuous R	ehydration
Recoverable / Total VMs	414	Owner Site	REMOTE (172.3	← Fallback	
		1			
Protected VMs Settings Alarms O O					
VM Name	Protection Status		Protection Mode 🔺	Details	a
Orotected VMs Settings Alarms O O VM Name ▲ GCS-DR-DC GCS-DR-DC	Protection Status		Protection Mode Write-Back(VMDK)	Details Details	٩
VM Name ▲ GCS-DR-DC GCS-DR-LinVM01	Protection Status Recoverable Recoverable		Protection Mode Write-Back(VMDK) Write-Back(VMDK)	Details <u>Details</u> <u>Details</u>	Q
Protected VMs Settings Alarms O O VM Name ▲ GCS-DR-DC GCS-DR-LinVM01 GCS-DR-SCA	Protection Status Recoverable Recoverable Recoverable		Protection Mode Write-Back(VMDK) Write-Back(VMDK) Write-Back(VMDK)	Details Details Details Details	q
Protected VMs Settings Alarms O O VM Name GCS-DR-DC GCS-DR-LinVM01 GCS-DR-SGA GCS-DR-SGL01	Protection Status © Recoverable © Recoverable © Recoverable © Recoverable		Protection Mode Write-Back(VIIDK) Write-Back(VIIDK) Write-Back(VIIDK) Write-Back(VIIDK)	Details Details Details Details Details	q

Specificare il ritardo massimo dopo la pausa delle macchine virtuali nel sito di ripristino e il riavvio nel sito protetto. Il tempo necessario per completare questo processo include il completamento della replica dopo l'arresto delle macchine virtuali di failover, il tempo necessario per pulire il sito di ripristino e il tempo necessario per ricreare le macchine virtuali nel sito protetto. NetApp consiglia 10 minuti.

•		•	•			0
. General	2a. Failback Settings	2b. VM Settings	3. Recovery VA	4. DR 5	lettings	5. Summary
Failback Da	tacenter		A300-DataCenter			
Failback Cl	uster		A300-Cluster			
Failback Re	source Pool					
VM Folder (Optional)					
Failback Da	tastore		A300_NFS_vMotion			
Maximum D	elay After Stopping		10 Minutes			
Internal Net	wolk		VM_187			
External Re	plication Network		VM_187			
Managemen	nt Network		VM_187			
Storage Site	e		ANFCVODR			
DR Virtual A	Appliance		GCSDRVA002			
Replication	Log Storage		/dev/sdb			

3. Completare il processo di failback e confermare la ripresa della protezione delle macchine virtuali e la coerenza dei dati.

(;)

JetStream DR Protected Domains Statistics Storage S	Failback Task Result		
Select Protected Domain: GCSDRPD002 *	Task Completed Successfully		
Recoverable / Total VMs	Protected Domain	GCSDRPD002	
Replication Status	VMs Recovery Status	O Success	
Remaining Background Data	Total VMs Recovered	4	
remaining beinground bere	GCSRecovery03 Status:		
Current RPO	Pre-script Execution Status	O Not defined	
	Runbook Execution Status	Success	
Protected VMs Settings Alarms	Post-script Execution Status	Not defined	6

4. Una volta ripristinate le macchine virtuali, scollegare lo storage secondario dall'host e connettersi allo storage primario.

Health Status 🔅	Source Volume	e i jerges			(News) (Addition (News) (1993)	Status	1811	Alternational and a second second	80	Last successful transfer	1
\odot	gcsdrsqldb_sc46 ntaphci-a300e9u25	gcsdrs ANFCV	qldb_sc46_coj 'ODRDemo	oy •	6 minutes 41 seconds	idle		broken-off		May 5. 2022. 12:08:34 PN 33.66 KiB	(
\odot	gcsdrsqlhld_sc46 ntaphci-a300e9u25	gcsdrs ANFCV	qlhld_sc46_co ′ODRDemo	ру	4 minutes 56 seconds	idle		broken-off		Information	
0	gcsdrsqllog_sc46 ntaphci-a300e9u25	e gcsdrs ANFCV	qllog_sc46_co ′ODRDemo	Þy	10 minutes 18 seconds	idle		broken-off		Resync Reverse Resync	
										Edit Schedule	
										Edit Max Transfer Rate	
										Delete	
3 Volume Re	elationships	6.5 Replica	4 GIB ated Capacity		0 Currently Trans	ferring	0	3 Healthy		Ø 0 Failed	
Jolume Re	elationships	6.5 Replica	4 GiB Ited Capacity		O Currently Trans	ferring	0	3 Healthy		O Failed	
Volume Relationships	elationships	6.5 Replica	4 GIB Ited Capacity		0 Currently Trans	ferring	0	3 Healthy		Outer O Failed	
Ume Relationships Health Status :	elationships	6.5 Replica Target gcsdrs ANFCV	4 GIB ated Capacity Volume qldb_sc46_cop VORDemo	e]	O Currently Trans Currently Trans	ferring Status idle	⊘ ₹	Mirror State	*	Last Successful Transfer May 6, 2022, 11:03:0 AA 5.73 MiB	
Volume Relationships Health Status :	elationships Source Volume gcsdrsqldb_sc46 ntaphci-a300e9u25 gcsdrsqlhld_sc46_copy ANFEVVODRDemo	G.5 Replica Target gcsdrs ANFCV gcsdrs ntapho	4 GIB ted Capacity Volume qldb_sc46_cop ODRDemo qlhld_sc46 ci-a300e9u25	¢]	O Currently Trans O O Currently Trans O O Total Transfer Time I minute 46 seconds	ferring Status idle idle	₹	3 Healthy Mirror State snapmirrored	•	O Failed Last Successful Transfer May 6, 2022, 11:03:0 Ah 5.73 MiB May 6, 2022, 11:01:39 Ah 800.76 MiB	

- 5. Riavviare il servizio del server MSSQL.
- 6. Verificare che le risorse SQL siano nuovamente in linea.



Per eseguire il failback allo storage primario, assicurarsi che la direzione della relazione rimanga la stessa di prima del failover eseguendo un'operazione di risincronizzazione inversa.



i.

Per mantenere i ruoli dello storage primario e secondario dopo l'operazione di risincronizzazione inversa, eseguire nuovamente l'operazione di risincronizzazione inversa.

Questo processo è applicabile ad altre applicazioni come Oracle, ad altri tipi di database simili e ad altre applicazioni che utilizzano lo storage connesso al guest.

Come sempre, verifica le fasi necessarie per il ripristino dei carichi di lavoro critici prima di portarli in produzione.

Vantaggi di questa soluzione

- Utilizza la replica efficiente e resiliente di SnapMirror.
- Effettua il ripristino in qualsiasi punto disponibile in tempo con la conservazione delle snapshot di ONTAP.
- È disponibile un'automazione completa per tutte le fasi necessarie per il ripristino di centinaia o migliaia di macchine virtuali, dalle fasi di convalida di storage, calcolo, rete e applicazioni.
- SnapCenter utilizza meccanismi di cloning che non modificano il volume replicato.
 - In questo modo si evita il rischio di corruzione dei dati per volumi e snapshot.
 - Evita le interruzioni di replica durante i flussi di lavoro dei test di DR.

- Sfrutta i dati di DR per flussi di lavoro oltre il DR, come sviluppo/test, test di sicurezza, test di patch e upgrade e test di correzione.
- L'ottimizzazione della CPU e della RAM può contribuire a ridurre i costi del cloud consentendo il ripristino di cluster di calcolo più piccoli.

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

Autore: Niyaz Mohamed, NetApp Solutions Engineering

Panoramica

Il disaster recovery che utilizza la replica a livello di blocco tra regioni all'interno del cloud è un metodo resiliente e conveniente per proteggere i carichi di lavoro da interruzioni del sito ed eventi di corruzione dei dati (ad esempio ransomware). Con la replica dei volumi Azure NetApp Files (ANF) cross-region, i carichi di lavoro VMware eseguiti su un sito SDDC Azure VMware Solution (AVS) utilizzando i volumi Azure NetApp Files come datastore NFS sul sito AVS primario possono essere replicati in un sito AVS secondario designato nella regione di recupero di destinazione.

Disaster Recovery Orchestrator (DRO) (una soluzione basata su script con un'interfaccia utente) può essere utilizzato per ripristinare senza problemi i carichi di lavoro replicati da un SDDC AVS a un altro. DRO automatizza il recovery interrompendo il peering delle repliche e montando il volume di destinazione come datastore, attraverso la registrazione delle macchine virtuali in AVS, sulle mappature di rete direttamente su NSX-T (incluso con tutti i cloud privati AVS).



Prerequisiti e raccomandazioni generali

• Verificare di aver attivato la replica tra regioni creando il peering delle repliche. Vedere "Creare la replica di un volume per Azure NetApp Files".

- È necessario configurare ExpressRoute Global Reach tra i cloud privati Azure VMware Solution di origine e di destinazione.
- È necessario disporre di un service principal in grado di accedere alle risorse.
- È supportata la seguente topologia: Dal sito AVS primario al sito AVS secondario.
- Configurare "replica" pianifica ciascun volume in modo appropriato in base alle esigenze aziendali e al tasso di cambiamento dei dati.



Non sono supportate topologie a cascata e fan-in e fan-out.

Per iniziare

Implementare la soluzione VMware Azure

Il "Soluzione VMware Azure" (AVS) è un servizio di cloud ibrido che fornisce SDDC VMware completamente funzionali all'interno di un cloud pubblico Microsoft Azure. AVS è una soluzione di prima parte 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 lo storage iperconvergente e NSX per il networking e la sicurezza, il tutto sfruttando la presenza globale di Microsoft Azure, le strutture di data center leader di settore e la vicinanza al ricco ecosistema di servizi e soluzioni Azure native. Una combinazione di SDDC e Azure NetApp Files per la soluzione VMware Azure offre le migliori performance con una latenza di rete minima.

Per configurare un cloud privato AVS su Azure, seguire la procedura descritta in questa sezione "collegamento" Per la documentazione NetApp e in questo "collegamento" Per la documentazione Microsoft. Un ambiente pilota con configurazione minima può essere utilizzato per scopi di DR. Questa configurazione contiene solo i componenti principali per supportare le applicazioni critiche e può scalare e generare più host per sostenere la maggior parte del carico in caso di failover.



Nella versione iniziale, DRO supporta un cluster SDDC AVS esistente. La creazione di SDDC on-demand sarà disponibile in una release imminente.

Provisioning e configurazione di Azure NetApp Files

"Azure NetApp Files" è un servizio di file storage misurato di livello enterprise dalle performance elevate. Seguire la procedura descritta in questa sezione "collegamento" Eseguire il provisioning e la configurazione di Azure NetApp Files come datastore NFS per ottimizzare le implementazioni di cloud privato AVS.

Creazione di replica di volumi per i volumi datastore basati su file di Azure NetApp

Il primo passaggio consiste nell'impostare la replica cross-region per i volumi del datastore desiderati dal sito primario AVS al sito secondario AVS con le frequenze e le ritention appropriate.

Home > Azure NetApp Files > WEANFAVSacct Volumes > testrepidemo (WEANFAVSacct/testcap/testrepidemo)								
»		IFAVSacct/testcap/testrepIdemo) Replication 🙁 😁			×			
	. ⊘ Search ≪	🕐 Refresh						
100	Cverview	∧ Essentials		JSON	View			
	Activity log	End point type : Source	Destination : ter	strepidemo_copy				
3=	Access control (IAM)	Health status : Healthy	Relationship status : Idl	le				
•	🔷 Tags	Mirror state : Mirrored	Total progress : 2.1	13 GiB				

Seguire la procedura descritta in questa sezione "collegamento" per impostare la replica tra regioni creando il peering delle repliche. 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 di utilizzo specifico, è possibile selezionare il livello di servizio standard, quindi "modificare il livello di servizio" In caso di disastro reale o di simulazioni di DR.



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

Installazione DRO

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

Prerequisiti:

- Service Principal in grado di accedere alle risorse.
- Assicurarsi che esista una connettività appropriata alle istanze SDDC e Azure NetApp Files di origine e destinazione.
- Se si utilizzano i nomi DNS, la risoluzione DNS deve essere effettiva. 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 comporre
- 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 nell'area del sito AVS secondario o nell'area del sito AVS primario in un AZ separato da SDDC.

2. Decomprimere il pacchetto, eseguire lo script di implementazione e immettere 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. Accedere all'interfaccia utente utilizzando le seguenti credenziali:
 - Nome utente: admin

• Password: admin

■ NetApp	
Object Recovery Orchestrator Ender Sector and Gal Vernam Prisonal Login Login	

Configurazione DRO

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

Il primo passaggio consiste nell'aggiungere credenziali. DRO richiede l'autorizzazione per scoprire Azure NetApp Files e la soluzione VMware Azure. È possibile concedere le autorizzazioni richieste 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 del servizio all'abbonamento Azure e assegnargli un ruolo personalizzato con le autorizzazioni necessarie pertinenti. Quando si aggiungono ambienti di origine e di destinazione, viene richiesto di selezionare le credenziali associate all'entità del servizio. È necessario aggiungere queste credenziali a DRO prima di fare clic su Add New Site (Aggiungi nuovo sito).

Per eseguire questa operazione, attenersi alla seguente procedura:

- Aprire DRO in un browser supportato e utilizzare il nome utente e la password predefiniti /admin/admin). La password può essere reimpostata dopo il primo accesso utilizzando l'opzione Change Password (Modifica password).
- 2. Nella parte superiore destra della console DRO, fare clic sull'icona **Impostazioni** e selezionare **credenziali**.
- 3. Fare clic su Add New Credential (Aggiungi nuova credenziale) e seguire la procedura guidata.
- 4. Per definire le credenziali, immettere le informazioni relative all'entità del servizio Azure Active Directory che concede le autorizzazioni richieste:
 - Nome della credenziale
 - ID tenant
 - ID client

- · Segreto del client
- · ID abbonamento

Queste informazioni dovrebbero essere state acquisite al momento della creazione dell'applicazione ad.

5. Confermare i dettagli relativi alle nuove credenziali e fare clic su Add Credential (Aggiungi credenziale).

NetApp Disaster Recovery Orchestrator 🂊 Dashboard Discover	Resource Groups Replication Plans Job Monitoring	4 🌣 🛛 🔍
Add New Credential	Credentials Details	×
	Enter Credentials Details	
	Credential Name]
	Client Id 🕘]
	Client Secret	
	Subscription Id	
		J
	Add Credential	

Dopo aver aggiunto le credenziali, è il momento di individuare e aggiungere i siti AVS primari e secondari (sia vCenter che l'account storage Azure NetApp Files) a DRO. Per aggiungere il sito di origine e di destinazione, attenersi alla seguente procedura:

- 6. Accedere alla scheda Discover.
- 7. Fare clic su **Aggiungi nuovo sito**.
- 8. Aggiungere il seguente sito AVS primario (indicato come origine nella console).
 - VCenter SDDC
 - Account storage Azure NetApp Files
- 9. Aggiungere il seguente sito AVS secondario (indicato come destinazione nella console).
 - VCenter SDDC
 - Account storage Azure NetApp Files

RetApp Disaster Recovery Orchestrator 🂊 Dashb	oard Discover Resource Groups Replication Plans Job Monitoring	4	¢ (?	9
Add New Site	 Site Type Site Details VCenter Details Storage Details 			×
	Site Type			
	Source Destination			
	Continue			

10. Aggiungere i dettagli del sito facendo clic su **Source (origine)**, immettendo un nome descrittivo del sito e selezionando il connettore. Quindi fare clic su **continua**.



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

- 11. Aggiorna i dettagli di vCenter. A tale scopo, selezionare le credenziali, l'area Azure e il gruppo di risorse dal menu a discesa per l'AVS SDDC primario.
- 12. IL DRO elenca tutti gli SDDC disponibili all'interno della regione. Selezionare l'URL del cloud privato designato dal menu a discesa.
- 13. Inserire il cloudadmin@vsphere.local credenziali dell'utente. È possibile accedervi dal portale Azure. Seguire la procedura indicata in questo "collegamento". Al termine, fare clic su **Continue** (continua).

NetApp Disaster Recovery Orchestrator	Dashboard Discover Resource Grou	ps Replication Plans Job Monitoring	i ()	ê 🌣 😗 😩
Add New Site	🕑 Site Type 🛛 🕢) Site Details (3) vCenter Details (4) Storage Details	×
		Source AVS Private Cloud		
	Select Credentials	Azure Region O West Europe +	Azure Resource Group	
		AVS Details		
	Web Client	ANFDataClus	•	
	Username	nin@vsphere.local	•	
	Password	••••		
		Accept self-signed certificates		
		Previous Continue		

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

15. Fare clic su Create Site (Crea sito).

n NetApp	Disaster Recovery Orchestrator 💊 📔 Dashboard	Discover Resource Grou	ups Replication Plans	Job Monitoring		8	¢ 0 2
	C 2 Sites 2 vCenters	E 2 Storages	Site Type	2 1 Destination	Site Location	Cloud 2	
	2 sites					Q D Add New Site	l L
	Site Name	≎ Site Type = 〒 Locatio	n 〒 vCenter ≎ Stora	age ≎ VM List	Discovery Status	() ()	
	DemoDest	Destination Cloud	1 1		 https://10.75.0.2/ 	⊘ Success	
	DemoSRC	Source Cloud	1 1	(View VM List	 https://172.30.156.2/ 	⊙ Success	

Una volta aggiunto, DRO esegue il rilevamento automatico e visualizza le macchine virtuali con repliche tra regioni corrispondenti dal sito di origine al sito di destinazione. DRO rileva automaticamente le reti e i segmenti utilizzati dalle macchine virtuali e li popola.

n NetApp	Disaster Recovery Orchestrator	S Dashboard Discover R	source Groups Replication Plans Job	Monitoring		A Ø 0	۹
	Back		VM List				
			Site: DemoSRC vCenter: https://17	2.30.156.2/			
			1.000	VM Protection			
	7 Data	Mores	128 Virtual Machines	🥑 2. Protected	0 126 Unprotected		
	128 vm				Q 9	eate Resource Group	
	VM Mare	2 1. MM Status	VM State	DataStore	tiou :	Memory (MB)	
	HDSenth_2.5.1	0 Not Protected	() Powered On	vianDatastore	.8	8192	
	hci-fio-datastore-13984-0-1	0 Not Protected	Powered Off	HOtstDS	12	65536	
	ICCA2005-WD-R1	O Not Protected	(b) Powered On	wanDataitore	8	14336	
	10GA2005-NE-R1	0 Not Protected	() Powered On	vianDataitore	1	3072	
	ICCA2005-01-81	0 Not Protected	() Powered On	vianDatastore	8	3072	
	HCK_Demo_05	0 Not Protected	Dewered Dff	Demo002	1	2048	
	hci-nim-datastore-13564-0-1	10 Not Protected	() Fowered Off	HORIDS	24	49152	

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

Raggruppamenti di risorse

Una volta aggiunte le piattaforme, raggruppare le macchine virtuali che si desidera ripristinare in gruppi di risorse. I gruppi di risorse DRO consentono di raggruppare un set di macchine virtuali dipendenti in gruppi logici che contengono i relativi ordini di avvio, ritardi di avvio e validazioni opzionali 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. Accedere a **Resource Grou*ps e fare clic su *Create New Resource Group** (Crea nuovo gruppo di risorse).

n NetApp	Disaster Recovery Orchestrator 💊 🗌	Dashboard Discover Resource Groups	Replication Plans Job Monitoring		¢ ? 2
				C 2	
	Resource Group	Site	VCenter	Virtual Machines	
	1 Resource Group			Q O Create New Resource Group	
	Resource Group Name	\$ Site Name	⇒ Source vCenter	≂ VM List	
	DemoRG	DemoSRC	https://172.30.156.2/	View VM List	

- 2. In New Resource Group (nuovo gruppo di risorse), selezionare il sito di origine dal menu a discesa e fare clic su **Create** (Crea).
- 3. Fornire i dettagli del gruppo di risorse e fare clic su continua.
- 4. Selezionare le macchine virtuali appropriate utilizzando l'opzione di ricerca.
- 5. Selezionare Boot Order (Ordine di avvio) e Boot Delay (sec) per tutte le macchine virtuali selezionate. Impostare l'ordine della sequenza di accensione selezionando ciascuna macchina virtuale e impostando la relativa priorità. Il valore predefinito per tutte le macchine virtuali è 3. Le opzioni sono le seguenti:
 - · La prima macchina virtuale ad accenderlo
 - Predefinito
 - · L'ultima macchina virtuale ad accenderlo

NetApp Disaster Recovery Orchestrate	or 💊 Dashboard Di		Replication Plans	Job Monitoring			•	?
Edit Resource Group		Resource Group Det	ails 🕜 Select VM:	s 🚯 Boot order	and Delay			
			Boot order an	d Delay				
	VM Name	Boot Order 📀		Boot Delay	(secs)			
	QALin1	3	10	0	12			
	QALin	3	10	0	[0]			

6. Fare clic su Crea gruppo di risorse.

Disaste	er Recovery Orchestrator 💊 📔	Dashboard Disc	over Resource Groups R	eplication Plans Job Monitoring	4	\$
	Resource Group		1 Site	C 1 _{vCenter}	C 2 Virtual Machines	
1 Re	source Group				Q D Create New Resource Group	
Res	source Group Name	019	te Name	≂ Source vCenter	≂ VM List	

Piani di replica

È necessario disporre di un piano per il ripristino delle applicazioni in caso di disastro. Selezionare le piattaforme vCenter di origine e di destinazione dall'elenco 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, Tier-1, Tier-2 e così via). I piani sono spesso chiamati anche blueprint. Per definire il piano di ripristino, accedere alla scheda Replication Plan (piano di replica) e fare clic su **New**

Replication Plan (nuovo piano di replica).

Per iniziare a creare un piano di replica, attenersi alla seguente procedura:

1. Selezionare **Replication Plans** (piani di replica) e fare clic su **Create New Replication Plan** (Crea nuovo piano di replica

etApp	Disaster Recovery (Orchestrator 🗞 🕴 Dashb	oard Discover Resource (roups Replication Plans	Job Monitoring				۹	¢	8
	8 1			Source Details	- 1 -	Destinatio	n Details	<i>a</i> .			
	Rep	olication Plans	Resource Groups	Sites	vCenters	Sites 1		vCenters			
	1 Replication Plan						م٥	Create New Replication Pl	lan		
	Plan Name	C Active Site	Status	Compliance	Source Site	· ⇒ Destination 5ite	÷(Ĵ.			
	DemoRP	⊘ Source	 Active 	A Partially Healthy	DemoSRC	DemoDest	Resou	irce Groups			

 In New Replication Plan, fornire un nome per il piano e aggiungere i mapping di ripristino selezionando Source Site (Sito di origine), Associated vCenter (vCenter associato), Destination Site (Sito di destinazione) e Associated vCenter (vCenter associato).

NetApp Disaster Recovery Orchestrator	Dashboard Discover Resource Group	s Replication P	lans Job Monitoring	ĺ.		۵	٥	?	9
Create New Replication Plan	Replication Plan and Site Details	2 Select Resource	Groups ③ Set Executi	on Order (4) S	Set VM Details				×
		Replication	Plan Details						
	Plan Name				0				
	DemoRP								
		Recovery	Mapping						
	Source Site	0	Destination Site		0				
	DemoSRC	*		DemoDest	*				
	Source vCenter	0	Destination vCenter		0				
	https://172.30.156.2/	*	htt	ps://10.75.0.2/	*				
		Cluster	Mapping						
	Source Site Resource	O Destinatio	n Site Resource	.0					
	Cluster-1	•	Cluster-1	*	Add				
	Source Resource	Destinat	tion Resource						
		No Mappi	ngs added!						
		6	ontinue						

3. Una volta completata la mappatura di ripristino, selezionare Cluster Mapping (mappatura cluster).

Create New Replication Plan	Replication Plan and Site D	Petails (2) Select Resource	Groups 3 Set Execution Order	4 Set VM Details			
		Replication	Plan Details				
	Plan Name				0		
	DemoRP						
		Recover	/ Mapping				
	Source Site	0	Destination Site		0		
	DemoSR		DemoDest		-		
	Source vCenter	0	Destination vCenter		0		
	https://172.30	156.2/ +	https://10.75.0.2	ν	•		
		Cluster	Mapping				
	No	more Source/Destination clus	ter resources available for mapping				
	Source Resource	Destination R	esource				
	Cluster-1	Cluster-1		Delete			

- 4. Selezionare **Dettagli gruppo di risorse** e fare clic su **continua**.
- 5. Impostare l'ordine di esecuzione per il gruppo di risorse. Questa opzione consente di selezionare la sequenza di operazioni quando esistono più gruppi di risorse.
- Al termine, impostare la mappatura di rete sul segmento appropriato. I segmenti devono essere già sottoposti a provisioning sul cluster AVS secondario e, per mappare le macchine virtuali su di essi, selezionare il segmento appropriato.
- 7. I mapping degli archivi dati vengono selezionati automaticamente in base alla selezione delle macchine virtuali.



La replica cross-region (CRR) è a livello di volume. Pertanto, tutte le macchine virtuali che risiedono sul rispettivo volume vengono replicate nella destinazione CRR. Assicurarsi di selezionare tutte le macchine virtuali che fanno parte del datastore, in quanto vengono elaborate solo le macchine virtuali che fanno parte del piano di replica.

NetApp Disaster Recovery Orchestrator	Dashboard Discover Resource C	Groups Replication Plans Job N	Aonitoring	4	۰ ب	•
Create New Replication Plan	Replication Plan and Site Details	Select Resource Groups 3	Set Execution Order ④ Set VM Details			×
		Replication Plan Det	ails			
		Select Execution Orde	r			
	Resource Group Name		Execution Order 👔			
	DemoRG		3 [0]			
	2	Network Mapping				
	No more	Source/Destination network resources	available for mapping			
	Source Resource	Destination Resource				
	SepSeg	SegDR	Delete			
		DataStore Mapping				
	Source DataStore	Destination Volume				
	TestSrc01	gwc_ntap_acct/gwc_DRO_cp/testsrci	О1сору			
		Previous Contin	nae			

8. In VM details (Dettagli VM), è possibile ridimensionare i parametri della CPU e della RAM delle macchine virtuali. Questo può essere molto utile quando si ripristinano ambienti di grandi dimensioni in cluster di destinazione più piccoli o quando si eseguono test di DR senza dover eseguire il provisioning di un'infrastruttura fisica VMware uno a uno. Inoltre, modificare l'ordine di avvio e il ritardo di avvio (sec) per tutte le macchine virtuali selezionate nei gruppi di risorse. Esiste un'opzione aggiuntiva per modificare l'ordine di avvio se sono necessarie modifiche da ciò che è stato 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 in questa fase è possibile eseguire qualsiasi modifica.

NetApp	Disaster Recovery Orchestrator 🗞	Dashboard Discover Resourc	e Groups Replication	n Plans Job Monitoring	1			۵	٥	?	9
	Create New Replication Plan	Replication Plan and Site Details	s 🕢 Select Resource	e Groups 🕜 Set Exect	ution Order	Set VM Details					×
			VN	/ Details							
		2 vms					۹				
		VM Name	No. of CPUs	Memory (MB)	NIC/IP	Boot Order 🕢					
		Resource Group : DemoRG			1						
		QALin1	1 [3]	1024 [3]	 Static Dynamic 	3	0				
		QALin	4 [0]	1024 [0]	 Static Dynamic 	3	0				
			Previous	Create Replication Plan							

9. Fare clic su **Create Replication Plan** (Crea piano di replica). Una volta creato il piano di replica, è possibile eseguire il failover, il failover di test o le opzioni di migrazione in base ai requisiti.

	plication Plans	Resource Groups	Source Details	2 1 vCenters	Destination	Details	2 1 VCenters
1 Replication Plan						۹٥	Create New Replication Plan
Plan Name							Ĵ.
DemoRP	⊘ Source	 Active 	A Partially Healthy	DemoSRC	DemoDest	Resour	ce Groups
							Plan Details
							Edit Plan
							Fallover
							Test Failover

Durante le opzioni di failover e test di 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

vantaggiosa se si sta affrontando un evento di corruzione come ransomware, in cui le repliche più recenti sono già compromesse o crittografate. DRO mostra tutti i tempi di rilevazione disponibili.

1 mm		Source Details		Destination Details		
Replication Plans	Resource Groups	Sites 1	vCenters	Sites 1		VCenters
	Testfailover Details			×		
1 Replication Plan	 Use latest snapshot ① Select specific snapshot ① 			^	Q D	Create New Replication Plan
Plan Name 🗢 Active Site	Volume		Snapshot		ί¢.	₿.
DemoRP 📀 Source	WEANFAVSacct/testcap/tests	src01	Select Snapshöt	-	Res	ource Groups
			2023-04-28			
			2023-04-28T11:31:55.000Z - gwc_ntap			
			2023-04-28T11:21:54.000Z - gwc ntap			

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

tApp Disaster	Recovery Orchestrator 💊 Dashboard Discover Resource Groups Replication Plans Job Monitoring		
Back			
	Test Failover Steps		
	Replication Plan: DemoRP		
~	Cloning volumes for test (in parallel)	Success 0.7 Seconds (D
~	Mounting cloned volumes and creating datastores (in parallel)	Success 0.9 Seconds (D
~	Registering VMs (in parallel)	Success 0.1 Seconds (D
~	Powering on VMs in protection group - DemoRG - in target (in parallel)	Success 0.1 Seconds (D

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

C 2 Sites	1 Resource Group	B 1 Replication P	lan 🗗	Protected VMs 128 9 1 Ms Protected	0 127 Ungentriched
Enviroisments	B 2	Topology Canvas			Immeniye Vew ()
SDOC Summary	Ref Storings Accounts	Dente	SRC 3.11162	DemoCect republic 2	
12 Datastores		_			
Encuriori Jobsi		Replication Plans			1
1 Testal Solar	C1 m Property	Replication Plan	Adve Sta	Statue	

Il failback può essere attivato a livello di piano di replica. In caso di failover di test, l'opzione di strappo può essere utilizzata per eseguire il rollback delle modifiche e rimuovere il volume appena creato. I fallback relativi al failover sono un processo in due fasi. Selezionare il piano di replica e selezionare **Reverse Data Sync**.

etApp	Disaster Recovery Orche	estrator 💊 📔 Dashboard	Discover Resource Group	Replication Plan	Job Monitoring				2
				Source Details		Destination Details			
	B 1 Replication	on Plans	1 Resource Groups	1 Sites	vCenters	Sites 1	Centers		
								-	
	1 Replication Plan		l Ginter I	Compliance	Course Cite	Q	O Create New Replication Plan		
	DemoRP	(7) Destination	Running In Failover Mod-	() Healthy	DemoSRC	DemoDest	Resource Groups		
							Plan Details		
							Raverse Data Sync		

Al termine di questa fase, attivare il failback per tornare al sito AVS primario.

Арр	Disaster Recovery Orchestrator 💊	Dashboard Discover Resource	ce Groups Replication Plan	i Job Monitoring		٨	¢ ?	9
			Source Details		Destination Details			
	B 1 Replication Plans	Resource Groups	1 Sites	2 1 vCenters	Sites 1	vCenters		
	1 Replication Plan	and the second second			Q	Create New Replication Plan		
	Plan Name C Active 5	tination Active	Compliance	Demo58C	⇒ Destination Site	Resource Groups		
		0	0			Pian Details		
						Failback		

C 2 Stes	1 Rassburge Group	Replacition Plan	128 Protected VMs	127 Umprofacted
Invironments		Topólogy Canvas		Immenive View 🗗
2 virtual transments	2 And Storage Accounts			
SDDC Summary				
Chatters	D 14 Folders	DemoSRC. Hege/r172.30.156.2/	DemoDest https://10.75.0.2/	
12 Datastores	9 12 Networks			
Execution Jobs		Replication Plans		
01	01	Replication Pan Acts	e Sile Sales	

Dal portale Azure, possiamo vedere che lo stato di salute della replica è stato interrotto per i volumi appropriati che sono stati mappati al sito secondario AVS SDDC come volumi di lettura/scrittura. Durante il failover di test, DRO non esegue il mapping del volume di destinazione o di replica. Al contrario, crea un nuovo volume dello snapshot di replica cross-region richiesto ed espone il volume come 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 replica possono continuare durante i test di 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 ripristino di dati corrotti.

Recovery ransomware

Il ripristino dal ransomware può essere un compito scoraggiante. In particolare, può essere difficile per le organizzazioni IT individuare il punto di ritorno sicuro e, una volta stabilito, come garantire che i carichi di lavoro recuperati siano protetti dagli attacchi che si verificano (ad esempio, da malware in sospensione o attraverso applicazioni vulnerabili).

DRO risolve questi problemi consentendo alle organizzazioni di eseguire il ripristino da qualsiasi point-in-time disponibile. I carichi di lavoro vengono quindi ripristinati in reti funzionali ma isolate, in modo che le applicazioni possano funzionare e comunicare tra loro, ma non siano esposte al traffico nord-sud. Questo processo offre ai team di sicurezza un luogo sicuro per condurre indagini legali e identificare eventuali malware nascosti o inattivi.

Conclusione

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

- Sfrutta una replica Azure NetApp Files cross-region efficiente e resiliente.
- Ripristino a qualsiasi point-in-time disponibile con la conservazione degli snapshot.
- Automatizzare completamente tutte le fasi necessarie per ripristinare da centinaia a migliaia di macchine virtuali dalle fasi di convalida di storage, calcolo, rete e applicazioni.
- Il recupero del workload sfrutta il processo "Create new volumes from the most recent snapshot" (Crea nuovi volumi dalle snapshot più recenti), che non manipola il volume replicato.

- Evitare qualsiasi rischio di corruzione dei dati sui volumi o sugli snapshot.
- Evita le interruzioni della replica durante i flussi di lavoro dei test di DR.
- Sfrutta i dati di DR e le risorse di calcolo del cloud per i flussi di lavoro che vanno oltre il DR, come sviluppo/test, test di sicurezza, test di patch e upgrade e test di correzione.
- L'ottimizzazione della CPU e della RAM può contribuire a ridurre i costi del cloud consentendo il ripristino a cluster di calcolo più piccoli.

Dove trovare ulteriori informazioni

Per ulteriori informazioni sulle informazioni descritte in questo documento, consultare i seguenti documenti e/o siti Web:

Creare la replica di un volume per Azure NetApp Files

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

• Replica cross-region di volumi Azure NetApp Files

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

• "Soluzione VMware Azure"

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

• Implementare e configurare l'ambiente di virtualizzazione su Azure

"https://docs.netapp.com/us-en/netapp-solutions/ehc/azure-setup.html"

• Implementare e configurare Azure VMware Solution

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

Utilizzo di Veeam Replication e datastore Azure NetApp Files per il disaster recovery nella soluzione Azure VMware

Autore: Niyaz Mohamed - Ingegneria di soluzioni di NetApp

Panoramica

I datastore Azure NetApp Files (ANF) separano lo storage dal calcolo e liberano la flessibilità necessaria a qualsiasi organizzazione per portare i propri workload nel cloud. Offre ai clienti un'infrastruttura storage flessibile e dalle performance elevate, che scala in modo indipendente dalle risorse di calcolo. Le dimensioni del datastore di Azure NetApp Files semplificano e ottimizzano l'implementazione insieme alla soluzione Azure VMware (AVS) come sito di disaster recovery per gli ambienti VMware on-premise.

I datastore NFS basati su volume Azure NetApp Files (ANF) possono essere utilizzati per replicare i dati onpremise utilizzando qualsiasi soluzione di terze parti validata che offre funzionalità di replica delle VM. Aggiungendo datastore Azure NetApp Files, potrai ottimizzare i costi dell'implementazione rispetto a una soluzione SDDC Azure VMware con un'enorme quantità di host ESXi per ospitare lo storage. Questo approccio è chiamato "quadro spie pilota". Un cluster di spie pilota è una configurazione host AVS minima (3 nodi AVS) insieme alla capacità del datastore Azure NetApp Files. L'obiettivo è mantenere un'infrastruttura a basso costo con tutti i componenti principali per gestire il failover. Un cluster di spie pilota può scalare in orizzontale e fornire più host AVS se si verifica un failover. Inoltre, una volta completato il failover e ripristinate le normali operazioni, il cluster di spie può scalare di nuovo alla modalità operativa a basso costo.

Finalità del presente documento

Questo articolo descrive come utilizzare il datastore Azure NetApp Files con Veeam Backup e la replica per configurare il disaster recovery per le VM VMware on-premise su (AVS) utilizzando la funzionalità software di replica Veeam VM.

Veeam Backup & Replication è un'applicazione di backup e replica per ambienti virtuali. Quando le macchine virtuali vengono replicate, Veeam Backup & Replication viene replicato da AVS, il software crea una copia esatta delle VM nel formato VMware vSphere nativo sul cluster SDDC AVS di destinazione. Veeam Backup & Replication manterrà la copia sincronizzata con la VM originale. La replica offre il miglior recovery time objective (RTO) essendo presente una copia montata di una macchina virtuale nel sito di DR in uno stato ready-to-start.

Questo meccanismo di replica garantisce che i carichi di lavoro possano avviarsi rapidamente in un AVS SDDC in caso di evento di emergenza. Il software Veeam Backup & Replication ottimizza anche la trasmissione del traffico per la replica su WAN e le connessioni lente. Inoltre, filtra anche blocchi di dati duplicati, zero blocchi di dati, file swap e "file OS guest di macchine virtuali esclusi". Il software comprime anche il traffico di replica. Per evitare che i processi di replica consumino l'intera larghezza di banda della rete, è possibile utilizzare acceleratori WAN e regole di limitazione della rete.

Il processo di replica in Veeam Backup & Replication è basato sul processo, il che significa che la replica viene eseguita configurando i processi di replica. In caso di evento di emergenza, è possibile attivare il failover per ripristinare le macchine virtuali con failover sulla copia di replica. Una volta eseguito il failover, una VM replicata assume il ruolo della VM originale. Il failover può essere eseguito allo stato più recente di una replica o a uno dei suoi punti di ripristino noti. Ciò abilita recovery dal ransomware o test isolati, se necessario. Veeam Backup & Replication offre diverse opzioni per gestire diversi scenari di disaster recovery.

[]

Implementazione della soluzione

Gradini di alto livello

- 1. Il software Veeam Backup and Replication è in esecuzione in un ambiente on-premise con appropriata connettività di rete.
- 2. "Implementa la soluzione Azure VMware (AVS)" cloud privato e. "Collegare i datastore Azure NetApp Files" Agli host della soluzione Azure VMware.

Un ambiente pilota configurato con una configurazione minima può essere utilizzato per scopi di DR. In caso di incidente, è possibile eseguire il failover delle macchine virtuali su questo cluster e aggiungere nodi.

- 3. Impostare il processo di replica per creare repliche VM utilizzando Veeam Backup and Replication.
- 4. Creazione di un piano di failover ed esecuzione di un failover.
- 5. Tornare alle macchine virtuali di produzione una volta che l'evento di disastro è completo e il sito primario è attivo.

Prerequisiti per la replica della macchina virtuale Veeam nei datastore AVS e ANF

- 1. Assicurarsi che la VM di backup di Veeam Backup & Replication sia connessa all'origine e ai cluster SDDC AVS di destinazione.
- 2. Il server di backup deve essere in grado di risolvere i nomi brevi e di connettersi ai centri virtuali di origine e di destinazione.
- 3. Il datastore Azure NetApp Files di destinazione deve avere spazio libero sufficiente per archiviare VMDK di macchine virtuali replicate.

Per ulteriori informazioni, fare riferimento a "considerazioni e limitazioni" "qui".

Dettagli sull'implementazione

Veeam Backup & Replication sfrutta le funzionalità snapshot di VMware vSphere/durante la replica, Veeam Backup & Replication richiede a VMware vSphere la creazione di una snapshot delle VM. Lo snapshot della VM è la copia point-in-time di una VM che include dischi virtuali, stato del sistema, configurazione e metadati. Veeam Backup & Replication utilizza la snapshot come origine dei dati per la replica.

Per replicare le VM, attenersi alla seguente procedura:

- 1. Apri la Veeam Backup & Replication Console.
- 2. Nella vista Home. Fare clic con il pulsante destro del mouse sul nodo processi e selezionare processo di replica > macchina virtuale.
- 3. Specificare un nome di lavoro e selezionare la casella di controllo controllo avanzata appropriata. Fare clic su Avanti.
 - Selezionare la casella di controllo Replica seeding se la connettività tra on-premise e Azure ha limitato la larghezza di banda.

*Selezionare la casella di controllo Network remapping (per i siti AVS SDDC con reti diverse) se i segmenti della soluzione Azure VMware SDDC non corrispondono a quelli delle reti dei siti in sede.

 Se lo schema di indirizzamento IP nel sito di produzione locale differisce dallo schema nel sito AVS di destinazione, selezionare la casella di controllo Replica re-IP (per siti DR con schema di indirizzamento IP diverso).

[]

4. Selezionare le VM da replicare nel datastore Azure NetApp Files collegato a un SDDC della soluzione Azure VMware nel passaggio macchine virtuali*. Le macchine virtuali possono essere posizionate su vSAN per riempire la capacità del datastore vSAN disponibile. In un cluster spia pilota, la capacità utilizzabile di un cluster a 3 nodi sarà limitata. Il resto dei dati può essere posizionato facilmente nei datastore Azure NetApp Files, in modo che sia possibile ripristinare le macchine virtuali e espandere il cluster per soddisfare i requisiti di CPU/mem. Fare clic su Aggiungi, quindi nella finestra Aggiungi oggetto selezionare le VM o i contenitori VM necessari e fare clic su Aggiungi. Fare clic su Avanti.

[]

 Quindi, seleziona la destinazione come cluster/host SDDC della soluzione Azure VMware e il pool di risorse, la cartella VM e il datastore FSX per le repliche delle VM di ONTAP. Quindi fare clic su Avanti.

[]

6. Nel passaggio successivo, creare la mappatura tra la rete virtuale di origine e di destinazione secondo necessità.

[]

- 7. Nel passaggio **Impostazioni processo**, specificare il repository di backup che memorizzerà i metadati per le repliche della VM, i criteri di conservazione e così via.
- Aggiornare i server proxy Source e Target nel passo trasferimento dati e lasciare selezionata l'opzione Automatic (impostazione predefinita) e mantenere l'opzione Direct (diretto) e fare clic su Next (Avanti).

9. Nel passaggio elaborazione guest, selezionare attiva elaborazione in base alle esigenze dell'applicazione. Fare clic su Avanti.

[]

10. Scegliere la pianificazione di replica per eseguire regolarmente il processo di replica.

[]

11. Nel passo **Riepilogo** della procedura guidata, esaminare i dettagli del processo di replica. Per avviare il lavoro subito dopo la chiusura della procedura guidata, selezionare la casella di controllo **Esegui il lavoro quando si fa clic su fine**, altrimenti lasciare deselezionata la casella di controllo. Quindi fare clic su **fine** per chiudere la procedura guidata.

[]

Una volta avviato il processo di replica, le macchine virtuali con il suffisso specificato verranno popolate nel cluster/host AVS SDDC di destinazione.

[]

Per ulteriori informazioni sulla replica Veeam, fare riferimento "Come funziona la replica"

Una volta completata la replica o il seeding iniziale, creare il piano di failover. Il piano di failover consente di eseguire automaticamente il failover per le VM dipendenti una alla volta o come gruppo. Il piano di failover è il modello per l'ordine in cui le macchine virtuali vengono elaborate, inclusi i ritardi di avvio. Il piano di failover aiuta inoltre a garantire che le VM dipendenti da fattori critici siano già in esecuzione.

Per creare il piano, passare alla nuova sottosezione chiamata **repliche** e selezionare **piano di failover**. Scegliere le VM appropriate. Veeam Backup & Replication cercherà i punti di ripristino più vicini a questo punto nel tempo e li utilizzerà per avviare le repliche della VM.



Il piano di failover può essere aggiunto solo una volta completata la replica iniziale e le repliche della VM sono nello stato Pronta.



Il numero massimo di VM che possono essere avviate contemporaneamente quando si esegue un piano di failover è 10



Durante il processo di failover, le macchine virtuali di origine non verranno spente

Per creare il piano di failover, procedere come segue:

1. Nella vista Home. Fare clic con il pulsante destro del mouse sul nodo repliche e selezionare piani di failover > piano di failover > VMware vSphere.

[]

2. Fornire quindi un nome e una descrizione del piano. Gli script pre e post-failover possono essere aggiunti secondo necessità. Ad esempio, eseguire uno script per arrestare le macchine virtuali prima di avviare le macchine virtuali replicate.

[]

3. Aggiungere le VM al piano e modificare l'ordine di avvio delle VM e i ritardi di avvio per soddisfare le dipendenze delle applicazioni.

[]

Per ulteriori informazioni sulla creazione di processi di replica, fare riferimento a. "Creazione di processi di replica".

Passaggio 3: Eseguire il piano di failover

Durante il failover, la macchina virtuale di origine nel sito di produzione viene commutata alla replica nel sito di disaster recovery. Come parte del processo di failover, Veeam Backup & Replication ripristina la replica della VM al punto di ripristino richiesto e sposta tutte le attività di i/o dalla VM di origine alla replica. Le repliche possono essere utilizzate non solo in caso di disastro, ma anche per simulare esercitazioni sul DR. Durante la simulazione del failover, la VM di origine rimane in esecuzione. Una volta eseguiti tutti i test necessari, è possibile annullare il failover e tornare alla normale operatività.



Assicurarsi che la segmentazione della rete sia attiva per evitare conflitti IP durante il failover.

Per avviare il piano di failover, è sufficiente fare clic sulla scheda **piani di failover** e fare clic con il pulsante destro del mouse sul piano di failover. Selezionare ***Avvia**. Il failover viene eseguito utilizzando gli ultimi punti di ripristino delle repliche della VM. Per eseguire il failover su punti di ripristino specifici delle repliche della VM, selezionare **Avvia**.

[]

[]

Lo stato della replica della macchina virtuale cambia da Pronto a failover e le macchine virtuali vengono avviate sul cluster/host SDDC di Azure VMware Solution (AVS) di destinazione.

[]

Una volta completato il failover, lo stato delle macchine virtuali passa a "failover".

[]



Veeam Backup & Replication interrompe tutte le attività di replica per la VM di origine fino a quando la replica non viene riportata allo stato Ready.

Per informazioni dettagliate sui piani di failover, consultare "Piani di failover".

Quando il piano di failover è in esecuzione, viene considerato come una fase intermedia e deve essere finalizzato in base al requisito. Le opzioni includono:

• Failback to Production - consente di tornare alla VM originale e di trasferire tutte le modifiche apportate durante l'esecuzione della replica della VM alla VM originale.



Quando si esegue il failback, le modifiche vengono solo trasferite ma non pubblicate. Scegliere **commit failback** (una volta che la VM originale è confermata per funzionare come previsto) o Annulla failback per tornare alla replica della VM se la VM originale non funziona come previsto.

- **Annulla failover** consente di tornare alla VM originale e di ignorare tutte le modifiche apportate alla replica della VM durante l'esecuzione.
- **Failover permanente** consente di passare in modo permanente dalla VM originale a una replica della VM e di utilizzare questa replica come VM originale.

In questa demo, è stato scelto il failback in produzione. Il failback alla macchina virtuale originale è stato selezionato durante la fase di destinazione della procedura guidata ed è stata attivata la casella di controllo "accensione della macchina virtuale dopo il ripristino".

[]	
[]	
[]	
[]	

Il commit di failback è uno dei modi per finalizzare l'operazione di failback. Quando il failback viene eseguito, conferma che le modifiche inviate alla VM che ha avuto esito negativo (la VM di produzione) funzionano come previsto. Dopo l'operazione di commit, Veeam Backup & Replication riprende le attività di replica per la VM di produzione.

Per informazioni dettagliate sul processo di failback, fare riferimento alla documentazione Veeam per "Failover e failback per la replica".

[]

Una volta eseguito il failback in produzione, le macchine virtuali vengono tutte ripristinate nel sito di produzione originale.

[]

Conclusione

La funzionalità datastore di Azure NetApp Files consente a Veeam o a qualsiasi tool validato di terze parti di fornire una soluzione di DR a basso costo sfruttando i cluster leggeri pilota, anziché standar in un cluster grande solo per le repliche delle VM. Ciò fornisce un modo efficace per gestire un piano di disaster recovery personalizzato e su misura e riutilizzare i prodotti di backup esistenti in sede per il disaster recovery, consentendo il disaster recovery basato sul cloud in uscita dai data center di DR on-premise. È possibile eseguire il failover facendo clic su un pulsante in caso di emergenza o eseguendo il failover automatico in caso

di emergenza.

Per ulteriori informazioni su questo processo, segui il video dettagliato.

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=2855e0d5-97e7-430f-944a-b061015e9278

Migrazione dei carichi di lavoro su Azure/AVS

TR-4940: Migrazione dei carichi di lavoro al datastore Azure NetApp Files con VMware HCX - Guida rapida

Autore: NetApp Solutions Engineering

Panoramica: Migrazione di macchine virtuali con VMware HCX, datastore Azure NetApp Files e soluzione VMware Azure

Uno dei casi di utilizzo più comuni per la soluzione VMware Azure e il datastore Azure NetApp Files è la migrazione dei carichi di lavoro VMware. VMware HCX è un'opzione preferita e offre vari meccanismi di migrazione per spostare macchine virtuali (VM) on-premise e i relativi dati negli archivi dati Azure NetApp Files.

VMware HCX è principalmente una piattaforma di migrazione progettata per semplificare la migrazione delle applicazioni, il ribilanciamento dei carichi di lavoro e persino la business continuity tra i cloud. È incluso come parte di Azure VMware Solution Private Cloud e offre diversi modi per migrare i workload e può essere utilizzato per le operazioni di disaster recovery (DR).

Questo documento fornisce istruzioni dettagliate per il provisioning del datastore Azure NetApp Files, seguito dal download, dall'implementazione e dalla configurazione di VMware HCX, inclusi tutti i componenti principali in sede e il lato soluzione VMware Azure, tra cui interconnessione, estensione di rete e ottimizzazione WAN per l'abilitazione di vari meccanismi di migrazione delle macchine virtuali.



VMware HCX funziona con qualsiasi tipo di datastore poiché la migrazione è a livello di VM. Pertanto, questo documento è valido per i clienti NetApp esistenti e non, che intendono implementare la soluzione Azure NetApp Files con Azure VMware per un'implementazione cloud VMware conveniente. Questo elenco fornisce i passaggi di alto livello necessari per installare e configurare HCX Cloud Manager sul lato cloud di Azure e installare HCX Connector on-premise:

- 1. Installare HCX attraverso il portale Azure.
- 2. Scaricare e implementare IL programma di installazione DI HCX Connector Open Virtualization Appliance (OVA) nel server VMware vCenter on-premise.
- 3. Attivare HCX con la chiave di licenza.
- 4. Associare il connettore VMware HCX on-premise con Azure VMware Solution HCX Cloud Manager.
- 5. Configurare il profilo di rete, il profilo di calcolo e la mesh del servizio.
- 6. (Facoltativo) eseguire l'estensione di rete per evitare il re-IP durante le migrazioni.
- 7. Verificare lo stato dell'appliance e assicurarsi che sia possibile eseguire la migrazione.
- 8. Migrare i carichi di lavoro delle macchine virtuali.

Prerequisiti

Prima di iniziare, assicurarsi che siano soddisfatti i seguenti prerequisiti. Per ulteriori informazioni, consulta questa sezione "collegamento". Una volta soddisfatti i prerequisiti, inclusa la connettività, configurare e attivare HCX generando la chiave di licenza dal portale Azure VMware Solution. Una volta scaricato il programma di installazione di OVA, procedere con la procedura di installazione come descritto di seguito.



HCX Advanced è l'opzione predefinita e VMware HCX Enterprise Edition è disponibile anche attraverso un ticket di supporto e supportato senza costi aggiuntivi.

- Utilizza un data center software-defined (SDDC) esistente per la soluzione Azure VMware o crea un cloud privato utilizzando questo "Link NetApp" o questo "Collegamento Microsoft".
- La migrazione delle macchine virtuali e dei dati associati dal data center abilitato VMware vSphere on-premise richiede la connettività di rete dal data center all'ambiente SDDC. Prima di migrare i carichi di lavoro, "Configurare una connessione VPN sito-sito o di accesso globale Express Route" tra l'ambiente on-premise e il rispettivo cloud privato.
- Il percorso di rete dall'ambiente VMware vCenter Server on-premise al cloud privato Azure VMware Solution deve supportare la migrazione delle macchine virtuali utilizzando vMotion.
- Assicurarsi di aver selezionato il necessario "porte e regole del firewall" Sono consentiti per il traffico vMotion tra vCenter Server on-premise e vCenter SDDC. Nel cloud privato, il routing sulla rete vMotion è configurato per impostazione predefinita.
- Il volume NFS di Azure NetApp Files deve essere montato come datastore nella soluzione VMware di Azure. Seguire i passaggi descritti in questa sezione "collegamento" Per collegare datastore Azure NetApp Files agli host delle soluzioni VMware Azure.

Architettura di alto livello



Implementazione della soluzione

Seguire la serie di passaggi per completare l'implementazione di questa soluzione:

Per eseguire l'installazione, attenersi alla seguente procedura:

- 1. Accedi al portale Azure e accedi al cloud privato Azure VMware Solution.
- 2. Selezionare il cloud privato appropriato e accedere ai componenti aggiuntivi. Per eseguire questa operazione, accedere a **Gestisci > componenti aggiuntivi**.
- 3. Nella sezione HCX workload Mobility, fare clic su Get Started (inizia subito).



1. Selezionare l'opzione Accetto i termini e le condizioni e fare clic su attiva e implementa.



L'implementazione predefinita è HCX Advanced. Aprire una richiesta di supporto per attivare l'edizione Enterprise.



L'implementazione richiede da 25 a 30 minuti circa.



Fase 2: Implementazione dell'OVA del programma di installazione nel server vCenter on-premise

Affinché il connettore on-premise si connetta a HCX Manager in Azure VMware Solution, assicurarsi che le porte firewall appropriate siano aperte nell'ambiente on-premise.

Per scaricare e installare HCX Connector nel server vCenter on-premise, attenersi alla seguente procedura:

 Dal portale Azure, accedere alla soluzione VMware Azure, selezionare il cloud privato, quindi selezionare Gestisci > componenti aggiuntivi > migrazione utilizzando HCX e copiare IL portale HCX Cloud Manager per scaricare il file OVA.

Utilizzare le credenziali utente predefinite di CloudAdmin per accedere al portale HCX.



1. Dopo aver effettuato l'accesso al portale HCX con cloudadmin@vsphere.local utilizzando il jumphost, accedere a Administration > System Updates e fare clic su Request Download link.



i.

Scaricare o copiare il collegamento a OVA e incollarlo in un browser per avviare il processo di download del file OVA di VMware HCX Connector da implementare sul server vCenter on-premise.

vm VMware HCX							C	Ø~ ≡~	cloudadmin
Oashboard Infrastructure Ste Pairing Sinterconnect Services Compute Network Extension Migration Disaster Recovery	System Upd Pair your remote da Pair your remote da Pair your remote da Cocal HCX Coisce ree upbala	ates							
Administration Administration System Updates A Troubleshopting	Current Version	System Name		Status	info	System T Type	NSX Version T	VC Version T	Copy To Clipboarit
Audit Logs	O E4330	hcx. cloud	IVS-azure.co.		٩	HCX Ooud	312.0017883600	7.0.3.10234570	3
Support								Numb	er of Applances
	* ERENTE HCX								
	Current Version	System Name	 T Status 	info		System Type	· ·	Copy To Clipboard	
				8					
								0000	0.000 2

1. Una volta scaricato l'OVA, implementarlo nell'ambiente VMware vSphere on-premise utilizzando l'opzione **Deploy OVF Template**.

😑 vSphere Client	Q	C & American generations generations	#~ © ©>
	* III A300-Cluster	O1 Excritions	-
	Deploy OVF Template	Select an OVF template ×	
- B ANDONICH	1 Select an OVF template	Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.	Phe.
1 A200-00	2. Select a name and folder	Our	
E 1000-m	3 Select a compute resource		
G AD#_HC	4 - Perview details	UPEDAD FILES VMware-HCX-Connector-E: dva	
1 G ANFORM	5 Select storage		
- G HOLDH	 Ready to complete 		
(B HCH			
(3 HO) /5 HO			
D HOL			
(B. 100)			
15 HOL (3 HOL)		CANCEL NEXT	
(D +10x)		exemption increased of restman attraction and an operation of the operatio	-
18 HOU	noteo_34		N 40101(412 8
A Recent Tasks	Alactica C.		

1. Inserire tutte le informazioni richieste per l'implementazione di OVA, fare clic su **Avanti**, quindi fare clic su **fine** per implementare l'OVA di VMware HCX Connector.



Accendere l'appliance virtuale manualmente.

Per istruzioni dettagliate, consultare "Guida utente di VMware HCX".

Dopo aver implementato VMware HCX Connector OVA on-premise e avviato l'appliance, completare la seguente procedura per attivare HCX Connector. Generare la chiave di licenza dal portale Azure VMware Solution e attivarla in VMware HCX Manager.

- 1. Dal portale Azure, accedere alla soluzione VMware Azure, selezionare il cloud privato e selezionare **Gestisci > componenti aggiuntivi > migrazione con HCX**.
- 2. In **Connect with on-premise using HCX keys** (connessione con chiavi HCX on-premise), fare clic su **Add** (Aggiungi) e copiare la chiave di attivazione.





Per ciascun connettore HCX on-premise implementato è necessaria una chiave separata.

1. Accedere a VMware HCX Manager on-premise all'indirizzo "https://hcxmanagerIP:9443" utilizzando le credenziali di amministratore.



Utilizzare la password definita durante l'implementazione di OVA.

1. Nella licenza, inserire la chiave copiata dal passaggio 3 e fare clic su Activate (attiva).



Il connettore HCX on-premise deve disporre di accesso a Internet.

- 1. In **posizione del data center**, fornire la posizione più vicina per l'installazione di VMware HCX Manager on-premise. Fare clic su **continua**.
- 2. In Nome sistema, aggiornare il nome e fare clic su continua.
- 3. Fare clic su Sì, continua.
- In Connect your vCenter, fornire il nome di dominio completo (FQDN) o l'indirizzo IP di vCenter Server e le credenziali appropriate, quindi fare clic su Continue (continua).



Utilizzare l'FQDN per evitare problemi di connettività in un secondo momento.
1. In **Configure SSO/PSC** (Configura SSO/PSC*), fornire l'indirizzo FQDN o IP del Platform Services Controller e fare clic su **Continue** (continua).



Immettere l'indirizzo IP o il nome FQDN di VMware vCenter Server.

- 1. Verificare che le informazioni immesse siano corrette e fare clic su Restart (Riavvia).
- 2. Dopo il riavvio dei servizi, vCenter Server viene visualizzato in verde nella pagina visualizzata. VCenter Server e SSO devono disporre dei parametri di configurazione appropriati, che devono essere gli stessi della pagina precedente.



Questo processo richiede circa 10 - 20 minuti e l'aggiunta del plug-in al server vCenter.

vm HCX Manager	Dashboard	Applance Summary	Configuration	Administration		ţ	₩ 72.21.254.157	Version: 4.410 Type: Connector	admin
VMware-HCX FODN: IP Address: Version: Uptime: Current Time:	-440 VMware-HCX-440 172.2 4.4.1.0 20 days, 21 hours, Tuesday, 13 Septe	Xehcdc.com 9 minutes mber 2022 07:44:11 PM UT(:		0 0	CPU Used 1407 MHZ Memory Used 9691 MB Storage Used 290		Free 688 MHZ Capacity 2095 MHZ Free 2316 MB Capacity 12008 MB Free 980 Capacity 1276	67% 81% 23%
NSX			vCenter https://a300-vc	sa01.ehcdc.com	• h	SSO https://a300-vcsa01.ehcdc.com	n		
MANAGE			MANAGE			MANAGE			

Fase 4: Associazione on-premise di VMware HCX Connector con Azure VMware Solution HCX Cloud Manager

Dopo aver installato HCX Connector sia in sede che in Azure VMware Solution, configurare VMware HCX Connector on-premise per Azure VMware Solution Private Cloud aggiungendo l'accoppiamento. Per configurare l'associazione del sito, attenersi alla seguente procedura:

1. Per creare una coppia di siti tra l'ambiente vCenter on-premise e Azure VMware Solution SDDC, accedere a vCenter Server on-premise e al nuovo plug-in HCX vSphere Web Client.

≡ vSphere (Dient Q								C a	ら Administratore日に	ICCOM ~	9	3
Shortcuts													
Inventories													
([])	ð		Ø	11	8	000		(Sp)		(٢		
Hosts and Clusters	VMs and Templates	Storage	Networking	Content Libraries	Global Inventory Lists	Workload Management	SnapCenter Plug-in for VMware VSphere	Cloud Provider Migration		Site Recovery	нсх	1	
Monitoring													
圁		CB,	5	Ep.	\diamond								
Task Console	Event Console	VM Costomization Specifications	VM Storage Policies	Host Profiles	Lifecycle Manager	ONTAP tools							
Administratio	n												
Q													
Licensing													

1. In Infrastructure (infrastruttura), fare clic su Add a Site Pairing (Aggiungi associazione sito).



Immettere l'URL o l'indirizzo IP di Azure VMware Solution HCX Cloud Manager e le credenziali per il ruolo CloudAdmin per l'accesso al cloud privato.

e → O	08.	# • https://w300-vcsal	11.ehcdc.com/ui/app/plup	n/com.vmware.hybridity/com.vmware.h	or.sitePairing			0 =
😑 vSphere Client C								
HCX C Destroyed	8	Site Pairing					C 100.4.5	TEDAIDIGE
Six Parkog S	~		Connect to F Remote HCK URL Usemane Password	Remote Site https://172. cloudsdmin@vsphere.local	CONNECT	ava azuro com-		
1. Fare clic su	ı Conr	nect (Conne	etti).					



Il connettore VMware HCX deve essere in grado di instradare all'indirizzo IP DI HCX Cloud Manager tramite la porta 443.

1. Una volta creata l'associazione, l'associazione del sito appena configurata è disponibile nella dashboard HCX.

	< .	Cite Delui	20					
x Dashboard		Site Pairi	ng			C ADD A S	ITE PAIR	ING
Stee Pairing Subsconnect Le: Transport Analytics invices Network Extension Migration Disaster Recovery ystem	~	Ø EDIT COL	VMware-HCX-440 Phttps://172.21.254.157.443 Raleigh 1 Interconnect(s) NNECTION DISCONNECT	→	Incx.8ebf3b0b7ddf4cc08e3f85.westeurope.avs.azure cloud	.com-		
Administration		Ø EDIT CO	VMware-HCX-440 Phttps://T72.21.254.157.443 Raileigh 1 Interconnect(s) NNECTION DISCONNECT	→	HCX			

Fase 5: Configurare il profilo di rete, il profilo di calcolo e la mesh del servizio

L'appliance di servizio VMware HCX Interconnect offre funzionalità di replica e migrazione basata su vMotion su Internet e connessioni private al sito di destinazione. L'interconnessione offre crittografia, progettazione del traffico e mobilità delle macchine virtuali. Per creare un'appliance di servizio Interconnect, attenersi alla seguente procedura:

 In Infrastructure (infrastruttura), selezionare Interconnect > Multi-Site Service Mesh > Compute Profiles > Create Compute Profile (interconnessione > Mesh servizio multi-sito > profili di calcolo > Crea profilo di calcolo





 Una volta creato il profilo di calcolo, creare i profili di rete selezionando Multi-Site Service Mesh > Network Profiles > Create Network Profile (Mesh servizio multi-sito > profili di rete > Crea profilo di rete).

Il profilo di rete definisce un intervallo di indirizzi IP e reti utilizzati DA HCX per le proprie appliance virtuali.



i

Questa operazione richiede due o più indirizzi IP. Questi indirizzi IP vengono assegnati dalla rete di gestione alle appliance di interconnessione.

	<								
CX Dashboard nfrastructure O Site Pairing Interconnect	×	Mutt-Site Service Mesh Compute Profiles Service Mesh	Notwork Profiles Sentin	el Management			Q. C. CREATE N	ETWORK P	ROFILI
Transport Analytics ervices Migration Migration Missater Recovery ystem & Administration So Administration	* *	VM_3510 Network Details Backing: VM_3510 show more	MTU 9000	P Pools P Ranges 172.21.254.80 - 172.21.254.95	IP Usage(Used/Total) 4/ 16	Prefix Length 24	Gateway 172.21.254.230		
		EOIT DELETE							

- 1. A questo punto, i profili di calcolo e di rete sono stati creati correttamente.
- 2. Creare la mesh del servizio selezionando la scheda **Mesh del servizio** all'interno dell'opzione **Interconnect** e selezionando i siti SDDC on-premise e Azure.
- 3. Service Mesh specifica una coppia di profili di rete e di calcolo locale e remoto.



Nell'ambito di questo processo, le appliance HCX vengono implementate e configurate automaticamente sui siti di origine e di destinazione per creare un fabric di trasporto sicuro.

$\leftarrow \rightarrow \ G$	0 &	• https://a300-voia01.ehodccom/ui/app/plugin/com/vmware.hybridity/com/vmware.hoc.hybridConnect			⊚ ≡
\equiv vSphere Client	Q		C	3	0~
HCX Dashboard Infrastructure Site Pairing Interconnect Transport Analytics Services	~	Interconnect Mutb-Site Service Mesh Compute Profiles Service Mesh Network Profiles Sentinel Management ICC007		E MESH	Î
Network Extension Migration Disaster Recovery System & Administration & Support	×	New version for service mesh applances is available. Click on Update Applances to upgrade to latest. Size Paring WWware- HCX:440 ® Raingh Incidemo O Amsterdam Norter APPLIANCES New APPLIANCES Resync EQUIDATE UPDATE APPLIANCES New APPLIANCES Resync EQUIDATE		>	

1. Questa è la fase finale della configurazione. Il completamento dell'implementazione richiede circa 30 minuti. Una volta configurata la mesh del servizio, l'ambiente è pronto con i tunnel IPSec creati correttamente per migrare le macchine virtuali del carico di lavoro.

5390 (10-9240) (1926)	-	_			_				- 1 Sec. 10.		1942
viphere Clent Q									C 24	uluinen coccoli -	
e/baet	1	nterconr meteter	sect.								
the Parrieg		Conjule Pure	e brockier eestide. brockier								_
Tampion AAAAss		+)	CC007 ~							CON SERVIC	rene
**	9 L	Arapping	Bythinger Glave								
elsesre fotarisien											
Joanter Recovery			Australia News T	a desenance travel	(* 440 mm		fund inte	Darrente Versitier	Average research		
n Abrahastarian Lazarri	×	0.1	00007-0-0 40 3594995-0024-002-0025-00256-00266 Аканания 3300-0026690 Жинере 3300-0026-002	NO -CE COMPANY	112-204.80		۲	443.0			
		0.2	COUTINE AND	49 coares	722/248	annen (San ()	۲	6420	*** 📼		
			00001-Initi-A we A4017149-Mile-Anke attale-A0284A4495bolt Nationale A2700-2012(2010) Stamage A2002-2012(2010)	C manage				1490	NA.		
											-
		Applano	es on hox filebritb0b7ddf4cc08e1t85 westeurope avs.	kzuni com-cloud		d' Address				Law.	-
		.0007-0	220- #0):	80	1C) mainin	1222.30 (0 000000000000000000000000000000000				444	ð
		<00007 vi	14	63	+Civer bit	1230 1844 mmdartar				44.0	(P
		KCODOT W	oin:	1.000						- 734	

Fase 6: Migrazione dei carichi di lavoro

I carichi di lavoro possono essere migrati bidirezionalmente tra gli SDDC on-premise e Azure utilizzando varie tecnologie di migrazione VMware HCX. Le VM possono essere spostate da e verso le entità attivate da VMware HCX utilizzando diverse tecnologie di migrazione, come LA migrazione in blocco HCX, HCX vMotion, HCX Cold Migration, HCX Replication Assisted vMotion (disponibile con HCX Enterprise Edition) e HCX OS Assisted Migration (disponibile con HCX Enterprise Edition).

Per ulteriori informazioni sui vari meccanismi di migrazione HCX, vedere "Tipi di migrazione VMware HCX".

Migrazione in massa

In questa sezione viene descritto in dettaglio il meccanismo di migrazione in blocco. Durante una migrazione in blocco, LA funzionalità di migrazione in blocco di HCX utilizza vSphere Replication per migrare i file disco ricreando la macchina virtuale sull'istanza di destinazione di vSphere HCX.

Per avviare migrazioni di macchine virtuali in blocco, attenersi alla seguente procedura:

1. Accedere alla scheda **Migrate** in **servizi > migrazione**.

$\leftrightarrow \rightarrow \ C$	0 & ≓	https://x300-vcsa01.ehodc.com/wi/ap	p/plugin/con	normwanishyt	aridity/com.v	inwarie, he	ocmigraționold				<u></u> ± ≡
\equiv vSphere Client (٦.							C a	Administrator@EHCD	ссом ч 🛛 🕲	0
HCX Dashboard Infrastructure	×	Migration	vent	12 MIGRATI		6				Bideth	
C Ste Pairing		Neme	v	Ma/ Storage/	Memory/ CPS	ē.)	Progress	Start	End	Status	
Services	~	-									
Network Extension		1									_
Migration		✓ ∎a300-vcsa01.ehcdc.	com →	172.30.	156.2						
Custom		> 2022-09-26 09:00 FLJVU		4 2	08 2.0	1	Migration Complete	2	. .		
2n Ariministration		> 2022-09-26 08:35 8XMTM		1 2	GB 2.05	1	Migration Complete				
@ Support	-	> 2022-09-18 16:21 ERC20	CITATIO	2 4	GB 4 G8	2	@ Draft	¥			
		> MG-18cbce94 / Sep 16	1000	5 10	GB 10 G	6	Migration Complete	12.44 AU Sep 10			
		> MG-04abdeell / Sep 16	Real Coly	1 2	GB 2.03	1	Migration Complete	12.25 AM	5		
		> MG-ef7374dd / Sep 10	1000	1 2	GB 2 G	1	Migration Complete	12:11 Att	*		
		> MG-d2of93ef/Sep 14	1-1-17	5 10	08 10 G	i 5	Stagration Complete	02.05 mm	4		
		> MG-99fecac8 / Sep 14	Hant Day	1 2	69/ 20	1	Migration Complète	11.02 AM	×		
		> MG-548618cb/ Sep 14	Have Soly)	1 2	08 2.0	1	Stagration Complete	10.04 AM	*		
		> MG-dd475274 (Sep 12	auton)	2 4	GØ / 4 G	2	Migration Complete	12.25 PM			

- 1. Nella sezione **connessione sito remoto**, selezionare la connessione del sito remoto e selezionare l'origine e la destinazione. In questo esempio, la destinazione è Azure VMware Solution SDDC HCX endpoint.
- Fare clic su Select VM for Migration (Seleziona VM per la migrazione Questo fornisce un elenco di tutte le macchine virtuali on-premise. Selezionare le macchine virtuali in base all'espressione match:value e fare clic su Add (Aggiungi).
- Nella sezione Transfer and Placement (trasferimento e posizionamento), aggiornare i campi obbligatori (Cluster, Storage, Destination e Network), incluso il profilo di migrazione, quindi fare clic su Validate (convalida).

					Select VMs for Migration
 Transfer and Placement: 	This is	a migrating to ANF datastore			N.
Duster-1	9	G Datasbure02 (((11)((11)))	9	Bok Migradion	÷
C) (Soeofy Destination Follow)		B) Same format as source	×	(Optional Switchover Schedule)	0
Saltchover					
P APPENDED FOR THE FULL					
Extended Options:					
Extended Options:					
Extended Options: (Brian MAC)					
Extended Option: (#rtan MAC)					8
Extended Options: Cartain MMC More High abor.	4	isk / Memory / vCPU		Migration Info	a.
Extended Options: Extended Options: Centure MMC M for Hegration S Demo_HOC_BlackI	0	104 / Memory / vCPU 2 08 : 2 08 : 1 vCPU		Migration Into	8
Extended Options: Extended Options: Options MAC Options Automatical System Some_HCX_Build1 Some_HCX_Build2	0	184 / Memory / vCPU 208 - 208 - 1 vCPU 208 - 208 - 1 vCPU		Migration Into Bulk Migration Bulk Migration	Q.
	0	268 / Memory / VCPU 268 268 100 268 268 100 268 268 100 268 268 100 268 268 100		Migration Into Bulk Migration Bulk Migration Bulk Migration	Q.
Extended Options: Extended Options: Brius MAC M for Highelin Demo, HCC, Buildol Demo, HCC, Buildol Demo, HCC, Buildol Demo, HCC, Buildol Demo, HCC, Buildol	0 0 0	198 / Memory / vCP0 2 68 2 68 1 vCP0		Migration Info Buil Migration Buil Migration Buil Migration Duil Migration	ġ.

1. Al termine dei controlli di convalida, fare clic su **Go** per avviare la migrazione.

+ + C	0 & # musical	N-read	n wheekdown/v	and a state of the		manda	- Service of								\$		σ.	£ 15
😑 vSphere Cik	ent Q													C	& sense of processos	-	9	•
HCX O Dashboard Infrastructure	× •	Mig	tracking 1	E Marágement	17 MERATE)@0		UPCH	ίπ.							8		
C Ste Parry & Harconnect 10 Transport Analytic		0	Higrating V	м		Shirape? H	emory/ CPUs		Propries			Start	* End	15	Status ;			-
Services			a100.00	sa01 ebcdr. co	m 472-301	156.2												
System Se Admensionation	÷	0	Dema HCA	Jack15 gl=cot.cos Bak14	0	29	0 200	1	Hipping.			291 Hot 6(7 Sea 14			Perichanal stated			1
Q Support			> Dome_HCR	percocioni (MARI) percocioni		20	0 2.58	ŧ	37% Name Sorts	******	******	2 21 Aug 14			Transfer Started			
			Dens_HCA	(MAS2 (6)-001 0101	-	30	0 260	*	Marshop.	*******	*******	205 PM 607 Bag 74			Building stated			
		0	Dama_HOX	gérezet sonr "Mobue gérezet son	_	19	0 2.00	,	O Wgulan Co	ngilile	******	144 14 1102 Aut 821 Pee 14	11.10 AM-851 Pap-14	3	Migration completed			
v Becent Tasks	Alarma																	-
Tau Nate	Y Target	. 7	Matus	-e ¥	Gietalia	. 7	ndator		¥.	Donund ¥ Ewi	Stat Tate		Completion Time	â	* Senat			
Bulk Migration	(D. Dens, HDC, Buildo .			345.0	Transfer Started		Americhato	00	KODC DÓM	0.ma	08/14/20	22.2.05 TLP54			hybridity-manager			
Bulk Migration	(D Dens, HCK, Build)			05.0	Transfer Started		American	00	KDC.00M	0.05	08/14/203	22.2:03 11 994			hybrioty-manager			
Buk Mgrabon	D Denie HCK_BURD2			0.40	Transfer Starteg		American	00	CDC COM	0.00	09/14/203	17,205mPM			mybridity-manager			
Bulk Migration	(2 DANK, HOX, BARDS			53.0	Transfer Martinit		Administrato	40	KOC COM	0.8%	09/14/203	22, 2:05 11 244			trybratty-manager			
Buik Migration	Dens, HOK, Builde		-	225 0	Transfer Started		American	00	KOC COM	0.04	08/14/203	22.2.05 TI PH			hybrioty-manager			

Durante questa migrazione, viene creato un disco segnaposto nel datastore Azure NetApp Files specificato all'interno del vCenter di destinazione per consentire la replica dei dati del disco VM di origine nei dischi segnaposto. L'HBR viene attivato per una sincronizzazione completa con la destinazione e, una volta completata la linea di base, viene eseguita una sincronizzazione incrementale in base al ciclo RPO (Recovery Point Objective). Una volta completata la sincronizzazione completa/incrementale, lo switchover viene attivato automaticamente, a meno che non venga impostata una pianificazione specifica.

1. Una volta completata la migrazione, validare la stessa accedendo al vCenter SDDC di destinazione.

(i)

e + 0 0	Q A # mosit	terina sylarismoni Dalatti makkater	-2543473+5643-1000-43	10408-015115240	Non-Arts		¢	0 2 1
\equiv vSphere Client Q							C & involvement local v	.0
C B SCC Connector	DatastoreO2 I Across Summery Monter Configure Victor Matshare VM Templates	Permissions Files Hosts	vies.					
								114
Constantorect	VMs on ANF datastore after migra	tion			Constant March 1	1. Marketing	y Demo.	hood
Datashoved)	VMs on ANF datastore after migra	State (State	Produced Space	Used Space	nut ON	Tread Mann	v Demo	HUOR H
Contractor Contractor Contractor	VMs on ANF datastore after migra	Bon State 1 Solar Possibilition / N Disconting On	Produced Series	Verifiques Pagigr MB	mult OPU 0 HQ	Had Men 204 Mill 200 Mill	* <u>Owno</u>	luorul
Contractived Contractived Contractived mercer S2000005-000. Sourcestanteee	VMs on ANF datastore after migra	Note 1 State Plasmad Cn / N Plasmad Cn / N Plasmad Cn / N	Producted Space proval 2.08 proval 2.08 proval 2.08	246.87 MB 246.87 MB 751.24 MB 755.46 MB	0 HQ 0 HQ 0 HQ	Peak Mars 2014 MB 2010 MB 2010 MB	* <u>Dem</u>	ucul
Contractived Contractived Contractived merclaretaretaretaretaretaretaretaretaretaret	VMc on ANF datastore after migra - terre - 1 & Center, HCL, Bakdt - 1 & Center, HCL, Bakdt	Bos Ender Finder Piperend On	Protocol Series Innai 208 Innai 208 Innai 208 Innai 208	546 8944 246,87 MB 75124 MB 755 A6 MB 76122 MB	0 HQ 0 HQ 0 HQ 0 HQ 0 HQ	1964 Mars 2824 MB 280 MB 255 MB 255 MB	* <u>Orm</u>	URUE

Per ulteriori e dettagliate informazioni sulle varie opzioni di migrazione e su come migrare i carichi di lavoro da una soluzione VMware on-premise a Azure utilizzando HCX, vedere "Guida utente di VMware HCX".

Per ulteriori informazioni su questo processo, guarda il seguente video:

Migrazione dei carichi di lavoro con HCX

Ecco una schermata dell'opzione HCX vMotion.

< + C	O & at insulat	00-visie01ahodszem/	وساريق والمراجع	ب المحاولة والدوار المحدث		riputerald.	5							¢	e	3
😑 VSphere Client	٩												C		0	
HCX Destcord Interfacture	~	Migration = Tracking	E Maragement	(p minut)	e 0	1 68	000	_				(A.S.).	_		8	
C the ranky		C Higratero	VM.	-	through/h	Aerrory/ ONA	Papers				Sat	, Dal		Thefas		-
Derives © tacterph Exteriors Montantia	~	i														
Disaster Recovery			csa01ehcdc.co	en	62											
)versen		C > Denu_HC	Vilution	-	24	200	30% Sec. 5	in.	0	•101 ad inte	11.52 or 10 ⁺¹		_	Abdust Transfer IS Program		_
Chargerst		D > Down HC	Could allow		24	a 206	OHIN	at Car	giala		1204 Margar	NO VE ANALYS Data VY	18 anys	Migration (completion)		
		(1) MCX, Phot	un_47	-	20	2.08	(OHysh	in Cor	shele		1225 Pecasor Inc 12	1231 Person	12.000	lighter consider		
		0,000,000	int, 94	-	25	8 218	() Myse	HOM	and a		12.25 Hickory Mail 10	1235-44807 Bea 10		Register comprise		
		(1) HX./90	10,15		20	208	(Otherie	is Cor	ciele .		1217 Hot#21 Sec 13	12,24 (%c02) (%c12)	1.000	Nigration completed		
		□ > #O_0ee	6,28 -ga +cm cove		24	2.00	() Migrati	es Ope	unite .		12.01 mic451 (nor 1)	12:07 marater Sec 19	7.nie	Mignitus completed		
· Recent Tasks	darms.															
Task Rame	farget	* suni	+ ®	Drien	*	adator.		٠	Garant . W	Start Type	*	Comparison Type		* been		
Recordpare vertail mach.	Dens, HOL VMator	Compart	ed.	Reconfiguring Virtual	Marin.	EHCOC COM	device also		5.84	09/14/202	2,105717	09/94/2022 101	20.55 AM	abob-woadtahustc.com		
Arower entral inaction ()	de Democritics, vMillion	Comput	e0			EHEDC.COM/	division alter		4.004	09/14/300	3,103958	294/54/2023.301	20.58 AM	e300-wiseOlematic com		
Bellesh while methics 5.	@ Dere, KCK, Vikings	Completion (ed.			EHCOC COM;	denest after		6.94	09/94/202	0.00333.	06/14/2022 11:0	23.33 AM	a000-wysel7telentr.com		
-(hethardh tolet strelige kys	172 21254 00	S Compart	10			EHEOCCOM	April No.		3.86	09/34/303	2,110433 .	06/4/2022,110	NA 53 AM	a300-scsal01atustcicum		

Per ulteriori informazioni su questo processo, guarda il seguente video:

HCX vMotion

Assicurarsi che sia disponibile una larghezza di banda sufficiente per gestire la migrazione.



Il datastore ANF di destinazione deve disporre di spazio sufficiente per gestire la migrazione.

Conclusione

Sia che tu stia prendendo come riferimento il cloud all-cloud o ibrido e i dati che risiedono su storage di

qualsiasi tipo/vendor in on-premise, Azure NetApp Files e HCX offrono eccellenti opzioni per implementare e migrare i carichi di lavoro delle applicazioni, riducendo al contempo il TCO rendendo i requisiti dei dati perfetti a livello applicativo. Qualunque sia il caso d'utilizzo, scegli la soluzione VMware Azure insieme a Azure NetApp Files per una rapida realizzazione dei vantaggi del cloud, un'infrastruttura coerente e operazioni su cloud multipli e on-premise, portabilità bidirezionale dei carichi di lavoro e capacità e performance di livello Enterprise. Si tratta degli stessi processi e procedure familiari utilizzati per connettere lo storage e migrare le macchine virtuali utilizzando VMware vSphere Replication, VMware vMotion o persino la copia del file di rete (NFC).

Punti da asporto

I punti chiave di questo documento includono:

- Ora puoi utilizzare Azure NetApp Files come datastore su Azure VMware Solution SDDC.
- È possibile migrare facilmente i dati da un datastore on-premise a un datastore Azure NetApp Files.
- È possibile espandere e ridurre facilmente il datastore Azure NetApp Files per soddisfare i requisiti di capacità e performance durante l'attività di migrazione.

Dove trovare ulteriori informazioni

Per ulteriori informazioni sulle informazioni descritte in questo documento, fare riferimento ai seguenti collegamenti Web:

• Documentazione della soluzione VMware Azure

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

• Documentazione Azure NetApp Files

"https://docs.microsoft.com/en-us/azure/azure-netapp-files/"

• Guida utente di VMware HCX

"https://docs.vmware.com/en/VMware-HCX/4.4/hcx-user-guide/GUID-BFD7E194-CFE5-4259-B74B-991B26A51758.html"

Disponibilità regionale: Datastore NFS supplementare per ANF

La disponibilità di datastore NFS supplementari su Azure / AVS è definita da Microsoft. Innanzitutto, è necessario determinare se AVS e ANF sono disponibili in una regione specifica. Quindi, è necessario determinare se il datastore NFS supplementare ANF è supportato in quella regione.

- Verificare la disponibilità di AVS e ANF "qui".
- Verificare la disponibilità del datastore NFS supplementare ANF "qui".

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEQUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina http://www.netapp.com/TM sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.