

Schutz von Workloads auf Azure/AVS

NetApp Solutions

NetApp April 26, 2024

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

Inhalt

Schutz von Workloads auf Azure/AVS	1
Disaster Recovery mit ANF und JetStream	1
Disaster Recovery mit CVO und AVS (Storage mit Anbindung an den Gast)	. 14
TR-4955: Disaster Recovery with Azure NetApp Files (ANF) and Azure VMware Solution (AVS)	. 41
Verwenden von Veeam Replizierung und Azure NetApp Files-Datastore für die Disaster Recovery zu	
Azure VMware-Lösung	56

Schutz von Workloads auf Azure/AVS

Disaster Recovery mit ANF und JetStream

Disaster Recovery in die Cloud ist eine stabile und kostengünstige Möglichkeit zum Schutz der Workloads vor Standortausfällen und Datenbeschädigungen (z. B. Ransomware). Mithilfe des VMware VAIO Frameworks können VMware On-Premises-Workloads auf Azure Blob Storage und für die Recovery repliziert werden, was zu minimalen oder fast keinem Datenverlust und nahezu keinem RTO führt.

Jetstream DR kann verwendet werden, um die Workloads, die von On-Premises-Systemen auf AVS repliziert wurden, nahtlos wiederherzustellen. Insbesondere können sie auf Azure NetApp Files übertragen werden. Sie ermöglicht eine kostengünstige Disaster Recovery, da minimale Ressourcen am DR-Standort und kostengünstiger Cloud Storage genutzt werden. Jetstream DR automatisiert die Recovery auf ANF-Datastores über Azure Blob Storage. Jetstream DR stellt unabhängige VMs oder Gruppen zugehöriger VMs in der Infrastruktur des Recovery-Standorts entsprechend der Netzwerkzuordnung wieder her und sorgt für zeitpunktgenaue Recovery zur Sicherung von Ransomware.

Dieses Dokument vermittelt ein Verständnis der JetStream DR-Prinzipien des Betriebs und seiner Hauptkomponenten.

- 1. Installation der JetStream DR-Software im lokalen Datacenter
 - a. Laden Sie das JetStream DR-Software-Bundle aus Azure Marketplace (ZIP) herunter, und implementieren Sie das JetStream DR MSA (OVA) im dafür vorgesehenen Cluster.
 - b. Konfigurieren Sie das Cluster mit dem I/O-Filterpaket (JetStream VIB installieren).
 - c. Bereitstellen von Azure Blob (Azure Storage-Konto) in derselben Region wie das DR-AVS-Cluster
 - d. Implementierung von DRVA-Appliances und Zuweisung von Protokoll-Volumes (VMDK aus vorhandenem Datastore oder gemeinsam genutztem iSCSI-Storage)
 - e. Erstellen Sie geschützte Domänen (Gruppen zugehöriger VMs) und weisen Sie DRVAs und Azure Blob Storage/ANF zu.
 - f. Schutz starten.
- 2. Installieren Sie die JetStream DR-Software in der Private Cloud der Azure VMware Lösung.
 - a. Verwenden Sie den Befehl Ausführen, um JetStream DR zu installieren und zu konfigurieren.
 - b. Fügen Sie denselben Azure Blob-Container hinzu und entdecken Sie Domänen mithilfe der Option "Scan Domains".
 - c. Bereitstellung der erforderlichen DRVA-Appliances
 - d. Verwenden von verfügbaren vSAN oder ANF-Datastores für Replizierungsprotokolle erstellen
 - e. Importieren Sie geschützte Domänen und konfigurieren Sie RocVA (Recovery VA), um einen ANF-Datenspeicher für VM-Platzierungen zu verwenden.
 - f. Wählen Sie die entsprechende Failover-Option aus, und beginnen Sie mit der kontinuierlichen Wiederherstellung nach RTO-Domänen von nahezu null oder VMs.
- 3. Bei einem Notfall wird ein Failover zu Azure NetApp Files-Datastores am zugewiesenen AVS-DR-Standort ausgelöst.
- 4. Rufen Sie den geschützten Standort nach der Wiederherstellung des geschützten Standorts auf.bevor Sie beginnen, stellen Sie sicher, dass die Voraussetzungen wie in diesem angegeben erfüllt sind "Verlinken" Führen Sie außerdem das von JetStream Software zur Verfügung gestellte Bandwidth Testing Tool (BWT) aus, um die potenzielle Performance des Azure Blob Storage und dessen Replikationsbandbreite in Verbindung mit der JetStream DR-Software zu bewerten. Nachdem die Voraussetzungen, einschließlich Konnektivität, vorhanden sind, richten Sie JetStream DR für AVS von der ein und abonnieren Sie sie "Azure Marketplace". Nachdem das Software Bundle heruntergeladen wurde, fahren Sie mit dem oben beschriebenen Installationsvorgang fort.

Verwenden Sie beim Planen und Starten des Schutzes für eine große Anzahl von VMs (z. B. 100+) das Capacity Planning Tool (CPT) aus dem JetStream DR Automation Toolkit. Geben Sie eine Liste der VMs an, die zusammen mit ihren RTO- und Recovery-Gruppeneinstellungen geschützt werden sollen, und führen Sie dann das CPT aus.

CPT führt die folgenden Funktionen aus:

- Die Kombination von VMs in Sicherungsdomänen entsprechend ihrer RTO-Vorgaben.
- Die optimale Anzahl von DRVAs und deren Ressourcen festlegen.
- Schätzen der erforderlichen Replikationsbandbreite
- Ermittlung der Merkmale von Replikationsprotokollvolumes (Kapazität, Bandbreite usw.)

• Schätzung der erforderlichen Objekt-Storage-Kapazität und mehr



Die Anzahl und der Inhalt der Domänen hängen von den verschiedenen VM-Merkmalen ab, wie beispielsweise durchschnittlichen IOPS, Gesamtkapazität, Priorität (die Failover-Reihenfolge definiert), RTO und anderen.

Installation der JetStream DR im lokalen Datacenter

Die Jetstream DR-Software besteht aus drei Hauptkomponenten: Jetstream DR Management Server Virtual Appliance (MSA), DR Virtual Appliance (DRVA) und Host-Komponenten (I/O-Filterpakete). MSA wird verwendet, um Hostkomponenten auf dem Computing-Cluster zu installieren und zu konfigurieren und anschließend JetStream DR-Software zu verwalten. Die folgende Liste enthält eine ausführliche Beschreibung des Installationsprozesses:

- 1. Voraussetzungen prüfen.
- 2. Führen Sie das Capacity Planning Tool für Ressourcen- und Konfigurationsempfehlungen aus (optional, jedoch für Proof-of-Concept-Tests empfohlen).
- 3. Implementieren Sie JetStream DR MSA auf einem vSphere-Host im zugewiesenen Cluster.
- 4. Starten Sie das MSA-Produkt mit dem DNS-Namen in einem Browser.
- 5. Registrieren Sie den vCenter-Server mit dem MSA.um die Installation durchzuführen, führen Sie die folgenden detaillierten Schritte aus:
- Nachdem JetStream DR MSA implementiert und der vCenter Server registriert wurde, greifen Sie über den vSphere Web Client auf das JetStream DR Plug-in zu. Dazu können Sie im Datacenter > Configure > JetStream DR navigieren.

vm vSphere Client	Menu 🗸 🔍 Search in all	environments		C @~	Administrator@EHCDC.COM ~
□ □ □ → a300-vcsa.ehcdc.com	A300-DataCent	Pr ACTIONS ~ Figure Permissions Hosts & Clusters VMs Datastc	res Networks Updates		
 A300-Datacenter A300-Cluster a300-esxi02.eh 	 More Alarm Definitions Scheduled Tasks 	JebSbream DR Protected Domains Statistics Storage Sites Applia	nces Configurations Task Log		톝
a300-esxi03.en.	Network Protocol Pr	Site Details			Alarm Settings
a300-esxi05.eh	JetStream DR	vCenter Server Hostname 172.2	21.253.160		
ANFJSDR-MSA0		Management Appliance Hostname ANFJ	SDR-msa		
🔂 AuctionAppA0		Software Version 4.0.0	.443		
🖧 AuctionAppA2		Subscription ID 0000	0000-0000-0000-0000-000000000000 Configure	2	
🔂 AuctionAppA3		Tenant ID / Application ID - CC	mfigure		
AuctionAppB0		Application Secret + Cr	<u>infigure</u>		

7. Wählen Sie über die JetStream DR-Schnittstelle den entsprechenden Cluster aus.

ite Details							Alarm Sette
Center Server Hostname		172.21.253.160					
Aanagement Appliance Hostname loftware Version	Configure C	lusters					
iubscription ID enant ID / Application ID			1	Select All	Clear All	٩	
pplication Secret	Cluster	r Name 🔺	Datac	enter Name 🔺		_	
onfigured Clusters	M A300-CI	luster	A300-	DataCenter		^	
Configure Cluster							
] Cluster Name 🔺						~	Host Details 🔺
No cluster contigured				Ca	ancel	nfigure	
	-						

8. Konfigurieren Sie das Cluster mit dem I/O-Filterpaket.

	Add Storage Site
Storage Sites	
+ Add Storage Site Scan Domains	Dances Cér Tura 1
Name 🛦	Azure Blob Storage
No Storage Site configured.	
	Access Type *
	Key Access
	Storage Site Name (Provide a name to identify this Site) *
	ANFDemoblobrepo
Storage Site Details Alarms	
	Adure Blob Storage Account Name *
No storage site selected. Select a storage	Azure Blob Storage Account Key *
	······································
	Cancel Add Storage Site

- 9. Fügen Sie Azure Blob Storage am Recovery-Standort hinzu.
- 10. Stellen Sie eine DR Virtual Appliance (DRVA) über die Registerkarte Appliances bereit.



DRVAs können automatisch durch CPT erstellt werden. Für POC-Tests wird jedoch empfohlen, den DR-Zyklus manuell zu konfigurieren und auszuführen (Schutz starten > Failover > Failback).

JetStream DRVA ist eine virtuelle Appliance, die wichtige Funktionen bei der Datenreplizierung unterstützt. Ein geschützter Cluster muss mindestens eine DRVA enthalten, und normalerweise ist pro Host ein DRVA konfiguriert. Jeder DRVA kann mehrere geschützte Domänen verwalten.

Jet:Stream DR Protected Domains Statistics	Deploy New DR Virtual Appliance (DR	VA)			Ē
DRVAs (DR Virtual Appliances)	1. General 2. DRVA VI	M 3. DRVA Network	4. Summary		
+ 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	8			0
+ New Replication Log Volume	Memory Size	32GB			q
Disk Path Name 🔺	Management Network	VM_187		Details 🔺	
No DRVA selected. Select a DRVA to vi	Host(iofilter) to DRVA Data Network	VM_187			
	Replication Network to Object Store	VM_187			
	Replication Log Network	VM_187	~		\sim
		Cancel Back	Deploy		

In diesem Beispiel wurden vier DRVA's für 80 virtuelle Maschinen erstellt.

1. Erstellen Sie Protokoll-Volumes für jedes DRVA unter Verwendung von VMDK aus den verfügbaren Datastores oder unabhängigen, gemeinsam genutzten iSCSI-Speicherpools.

2. Erstellen Sie auf der Registerkarte geschützte Domänen die erforderliche Anzahl geschützter Domänen mithilfe von Informationen über die Azure Blob Storage-Site, die DRVA-Instanz und das Replikationsprotokoll. Eine geschützte Domäne definiert eine bestimmte VM oder einen Satz von VMs innerhalb des Clusters, die gemeinsam geschützt werden, und weist eine Prioritätsreihenfolge für Failover-/Failback-Vorgänge zu.

JetStream DR Protected Domains Statistics	Storage Sites Appliances Configu	urations Task Log		Ê
Select Protected Domain:	Create Protected Domain			+ Create
	1. General 2. f	Primary Site	3. Summary	
	Protected Domain Name	ANFPD001		
	Priority Level (Optional)	1		
	Total estimated data size to be protecte	d 1000GB		
	DR Virtual Appliance	ANFdemo001		
	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		
		Cancel Ba	ack Create	

3. Wählen Sie VMs aus, die Sie sichern möchten, und starten Sie den VM-Schutz der geschützten Domäne. Dies beginnt mit der Datenreplizierung zum zugewiesenen Blob-Store.

Vergewissern Sie sich, dass derselbe Sicherungsmodus für alle VMs in einer geschützten Domäne verwendet wird.



 (\mathbf{i})

Write Back(VMDK)-Modus kann eine höhere Performance bieten.

JetStream DR						Ê
Protected Domains Statistics Stor	age Sites Appliances	Configurations Task	Log			
Select Protected Domain: ANFPD001 S	tart Protection				reate 🛍 Delete	
Recoverable / Total VMs	rotection Mode for selected VMs Write-Back(VMDK)			٩		Edit Details
Replication Status	VM Name	- # of Disks	Protection Mode		ANFDemoblobrepo	^
Remaining Background Data	1	×			AL (172.21.253.160)	
Current DDO	AuctionAppA1	1	Write-Back(VMDK) v	^	0-DataCenter \ A300-Cluster	
Current RPO	AuctionAppB1	1	Write-Back(VMDK) V		0.00	*
Protected VMs Settings Ala	AuctionDB1	2	Write-Back(VMDK) v	ĵ		
	AuctionLB1	1	Write-Back(VMDK) V			
+ Start Protection	AuctionMSQ1	1	Write-Back(VMDK) v			Q
i Star Protection	AuctionNoSQL1	2	Write-Back(VMDK) v			
U VM Name ▲	AuctionWebA1	1	Write-Back(VMDK) V		kground Dat Details	
No VM is protected.	AuctionWebB1	1	Write-Back(VMDK) V	Ì		
	Client1	1	Write-Back(VMDK) V			
		0	····· - · · · · · · · · ·	~		
			Cancel Start Pr	otection		
			·			~

Vergewissern Sie sich, dass die Protokoll-Volumes für die Replizierung auf hochperformanten Storage



Failover Run Books können so konfiguriert werden, dass sie die VMs (namens Recovery Group) gruppieren, die Boot-Reihenfolge festlegen und die CPU-/Speichereinstellungen sowie die IP-Konfigurationen ändern.

Installieren Sie JetStream DR für AVS mit dem Befehl Run in einer Private Cloud der Azure VMware Lösung

Eine Best Practice für einen Recovery-Standort (AVS) ist die Erstellung eines Pilotlichtclusters mit drei Knoten im Voraus. Dadurch kann die Infrastruktur am Recovery-Standort vorkonfiguriert werden, einschließlich der folgenden Elemente:

- Netzwerkzielsegmente, Firewalls, Services wie DHCP und DNS usw.
- Installation von JetStream DR für AVS
- Konfiguration von ANF Volumes als Datastores und mehrJetStream DR unterstützt RTO-Modus von nahezu null für geschäftskritische Domänen. In diesen Domänen sollte der Ziel-Storage vorinstalliert sein. ANF ist in diesem Fall ein empfohlener Speichertyp.



Die Netzwerkkonfiguration einschließlich der Segmenterstellung sollte auf dem AVS-Cluster entsprechend den Anforderungen vor Ort konfiguriert werden.

Je nach SLA- und RTO-Anforderungen kann für einen kontinuierlichen Failover oder einen normalen (Standard-) Failover-Modus verwendet werden. Für eine RTO von nahezu null sollte am Recovery-Standort eine kontinuierliche Rehydrierung gestartet werden.

So installieren Sie JetStream DR für AVS auf einer privaten Cloud der Azure VMware-Lösung:

1. Wählen Sie im Azure-Portal die Azure VMware-Lösung aus, wählen Sie die Private Cloud aus und wählen Sie Ausführen Command > Packages > JSDR.Configuration.



Der CloudAdmin-Standardbenutzer in Azure VMware verfügt nicht über ausreichende Berechtigungen, um JetStream DR für AVS zu installieren. Die Azure VMware Lösung ermöglicht eine vereinfachte und automatisierte Installation von JetStream DR durch Aufrufen des Befehls Azure VMware Solution Run für JetStream DR.

Der folgende Screenshot zeigt die Installation mithilfe einer DHCP-basierten IP-Adresse.

Microsoft Azure	.P. South movietes	services, and door.(5+/)	🖬 🕼 🖓 🗇 🖓 niyazilinetapp.com 🧃
Home > ANFDataOus			Run command - Install-JetDRWithDHCP ×
ANFDataClus Run	command		The two local Conduct Dependencies (art) to write here BMK creates a here user assists
(P Seiech (Chit+))	🔘 Rehish 🔗 Teesback		Herated prolifyges to the user, deploys JetDr Management Server Appliance(MSA), registers vCenter to the JetDr MSA, configures cluster.
Access controls (UAM)	Packages Run execution status		Command parameters
Diagnose and solve problems	 Name 	Description	Angathi Wenty ()
Settings	 ISORConfiguration (274) Researching 	the to conjugation of address follows on Ad. See address follows in, to conserv	ProtectedCuster *
A Look	Disable-letDRfc+Dunter	This Crediet unconfigures a cluster but doesn't unmstall JetDR completely to other clusters	Cluster-1
H		polices.	Datastore * (j)
Manage	Unable-JetDNJ or/Duater	This Cindlet configures an additional cluster for protection. It installs vibs to all hosts in the	vsecDatadow
🔶 Connectivity	Install-SetOWARDERCP	This top level Cindlet Downloads JetDr bundle from MMS, creates a new user, assigns elevi	VMName* (3
Chatters		registers vCenter to the JetDr MSA, comfigures chaster.	Brigwa-ma
Identity	Install-JetDRGWthStates3P	This top level Cristlet Downloads JetDr bundle from MMS, creates a new user, assigns elevi registers vCenter to the JetDr MSA, configures cluster.	Date-1
 Storage (preview) 	Invole PrefightJetDSmital	This Cincillet checks and dopleys current state of the system it checks whether the minimal	- Credential ()
Placement policies		a nosts is the costler decase are conject, is there is an any if y will work the same name provid	Osemanie *1
+ Add-ons	Invole-Prefight/etDRUtomball	This Cindlet checks and dioplays current state of the system it checks whether the minimal 4 houts, if the cluster details are correct and if any VCenter is registered to the MGA.	root
Workload Maturchine	Device And	The true level Condient meaters a new user and one elevated multilenes to the user incoming	Password *
	N Manual IN Manual AND		<u>e</u>
*c septem	> motorowanayanex	EX COST O YOULDING BY BUT I WITH AND THE POLICE	HistHare 🕢
TT DHCP			antpoal-maa
Port manualing			Network 1 (j)
2MG O			DRSeg
Operation			Detain
Run command			Retain up bi

 Nachdem die JetStream DR f
ür AVS-Installation abgeschlossen ist, aktualisieren Sie den Browser. Um auf die JetStream DR-UI zuzugreifen, wechseln Sie zum SDDC Datacenter > Configure > JetStream DR.

Site Details						Alarm Set	tir
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	🛍 Unconfigure	🛠 Resolv	e Configure Iss	ue			
Cluster Name	Datacenter	Name 🔺	Status 🔺	Software Ver	sion 🔺	Host Details	jî,
Cluster-1	SDDC-Data	center	📀 Ok	4.0.2.132		Details	

 Fügen Sie über die JetStream DR-Schnittstelle das Azure Blob Storage-Konto hinzu, das zum Schutz des lokalen Clusters als Storage-Standort verwendet wurde, und führen Sie die Option Scan Domains aus.

	Protected Domain	Description	Recoverable V	VMs	Import			100	
SIL	ANFPD000	Protected Domain Tile0	20	20	Import	2	^		
ra	ANFPD001	-	20	20	Import				C
	ANFPD002	Protected Domain 02	20	20	Import				
	ANFPD003	Protected Domain Tile 03	20	20	Import		•		9
	<					>			
Si									
Sit									
ii C								~	

4. Nachdem die geschützten Domains importiert wurden, sollten DRVA-Appliances bereitgestellt werden. In diesem Beispiel wird mithilfe der JetStream DR-Benutzeroberfläche eine kontinuierliche Rehydrierung manuell vom Wiederherstellungsstandort gestartet.



Diese Schritte können auch mithilfe von CPT erstellten Plänen automatisiert werden.

- 5. Verwenden von verfügbaren vSAN oder ANF-Datastores für Replizierungsprotokolle erstellen
- 6. Importieren Sie die geschützten Domänen und konfigurieren Sie die Recovery VA, um den ANF-Datenspeicher für VM-Platzierungen zu verwenden.

ect Protected Domain:	Continuous Fai	lover Protected Dom	ain					🗊 Delete	=	More
de		0. Esilovor Sottings	Oh VIII Sottings	2 8000		4 DB Sattings	E Cummani			Deta
coverable / Total VMs	1. General	za. Fanover settings	20. VIVI Settings	5. Recu	very va	4. DR Settings	5. Summary	∧ reporec		1
	Protected Do	main Name		ANFPD002				253.160)		
	Datacenter			SDDC-Datac	enter					
	Cluster			Cluster-1						
	Resource Poo	ol (Optional)		2						
rotected VMs Setti	VM Folder (O	ptional)		-						
	Datastore			ANFRecoDS	J002					
	Internal Netw	ork		DRSeg						C
VM Name 🔺	External Repl	lication Network		DRSeg					Details	
AuctionAppA2	Management	Network		DRSeg					Details	-
AuctionAppB2	Storage Site			ANFDemoblo	breporec				Details	
AuctionDB2	DR Virtual Ap	pliance		ANFRecDRV	A003				Details	
AuctionLB2	Bonligation	on Ptorono		idoviedh				~	Details	
AuctionMSQ2					Cancel	Back	Continuous Failov	er	Details	

Stellen Sie sicher, dass DHCP für das ausgewählte Segment aktiviert ist und genügend IP-Adressen verfügbar sind. Dynamische IPs werden vorübergehend verwendet, während Domänen sich wiederherstellen. Jede wiederherzuckernde VM (einschließlich kontinuierlicher Rehydrierung) erfordert eine individuelle dynamische IP-Adresse. Nach Abschluss der Wiederherstellung wird die IP freigegeben und kann wiederverwendet werden.

7. Wählen Sie die entsprechende Failover-Option (Continuous Failover oder Failover) aus. In diesem Beispiel wird die kontinuierliche Rehydrierung (kontinuierliches Failover) ausgewählt.

Protected Domains	Statistic	s Stora	ge Sites	Appliances	Configuratio	ns	Task Log	8
Select Protected Do	main: ANF	D000 -	View all		+ Create		Delete	≡ More
Mode			Imported	Configura	tions		O Restore	
Recoverable / Total \	/Ms		20 / 20	Storage Si	te	Δ	→ Failover	
				Owner Site	3	REI	→ Continuo	us Failover
							→ Test Faile	over
Protected VMs	Settings	Alarms						
								q
VM Name 🔺			Protec	tion Status 🔺	P	rotectio	on Mode 🔺	Details
AuctionAppA0			Reco	overable	v	Vrite-Bac	ck(VMDK)	Details ^
AuctionAppB0			Reco	overable	v	vrite-Bac	k(VMDK)	Details

Failover/Failback Wird Durchgeführt

i.

1. Nachdem im geschützten Cluster der lokalen Umgebung ein Ausfall auftritt (ein teilweiser oder vollständiger Ausfall), lösen Sie den Failover aus.



CPT kann verwendet werden, um den Failover-Plan zur Wiederherstellung der VMs von Azure Blob Storage auf dem AVS Cluster Recovery-Standort auszuführen.

()

Nach dem Failover (zur kontinuierlichen oder standardmäßigen Wiederherstellung), wenn die geschützten VMs in AVS gestartet wurden, wird der Schutz automatisch fortgesetzt und JetStream DR repliziert ihre Daten weiterhin in den entsprechenden/Original-Containern im Azure Blob Storage.





In der Taskleiste wird der Status von Failover-Aktivitäten angezeigt.

2. Nach Abschluss der Aufgabe greifen Sie auf die wiederhergestellten VMs zu, und der Geschäftsbetrieb läuft normal weiter.

JetStream DR Protected Domains Sta	Continuous Rehydration Task Result			
Select Protected Domain:	A Task Completed Successfully			Delete E More
Mode	Protected Domain	ANEPD003		Eat Det
	VMs Recovery Status	Success		noblobreporec
Janlication Status	Total VMs Recovered	20		2 30 156 2)
Auguneanorr George	testFGP0 Status:			tenter \ Cluster-1
Remaining Background Data	Pre-script Execution Status	Not defined		
turrent RPO	Runbook Execution Status	Success		
	Post-script Execution Status	Not defined		
Protected VMs Setting	IS.			
+ Start Protection	-			٩
UM Name A				d D Details
AuctionAppA3				Details
AuctionApp83				Details
AuctionDB3				Details
AuctionLB3				Details
AuctionMSQ3			Dismiss	Details
AuctionNoSQL3	a recordinate	er on missionautymun	9. 00	Details

Wenn der primäre Standort wieder in Betrieb ist, kann ein Failback durchgeführt werden. Der VM-Schutz wird wieder aufgenommen und die Datenkonsistenz sollte überprüft werden.

 Wiederherstellung der lokalen Umgebung Je nach Art des Notfalleinfalls sind möglicherweise die Wiederherstellung und/oder Überprüfung der Konfiguration des geschützten Clusters erforderlich. Falls erforderlich, muss die JetStream DR-Software möglicherweise erneut installiert werden.



Hinweis: Der recovery_utility_prepare_failback Das im Automation Toolkit zur Verfügung gestellte Skript kann verwendet werden, um die ursprüngliche geschützte Site von veralteten VMs, Domäneninformationen usw. zu reinigen.

4. Greifen Sie auf die wiederhergestellte On-Premises-Umgebung zu, rufen Sie die Jetstream DR UI auf und wählen Sie die entsprechende geschützte Domäne aus. Nachdem der geschützte Standort für Failback bereit ist, wählen Sie die Failback-Option in der UI aus.

			+ Create	Delete	■More
ode	Running in Failover	Configurations		O Restore	
ctive Site	172.30.156.2	Storage Site	ANF	O Resume Continu	ous Rehydratic
ecoverable / Total VMs	20 / 20	Owner Site	REMOT	← Failback	
			1		
And a second sec					c
VM Name A	Protection Sta	itus 🛦 Protec	tion Mode A	Details	
AuctionAppA3	Recoverable	Write-E	ack(VMDK)	Details	
AuctionAppB3	Recoverable	write-e	ack(VMDK)	Details	
AUCTION DB3	Recoverable	Write-E	ack(VMDK)	Details	
AuctionLB3	Recoverable	Write-E	ack(VMDK)	Details	

Mit dem durch CPT generierten Failback-Plan kann außerdem die Rückgabe der VMs und ihrer Daten aus dem Objektspeicher in die ursprüngliche VMware Umgebung initiiert werden.

Geben Sie die maximale Verzögerung an, nachdem Sie die VMs am Recovery-Standort angehalten und am geschützten Standort neu gestartet haben. Diese Zeit umfasst das Abschließen der Replizierung nach dem Stoppen von Failover-VMs, die Zeit für die Bereinigung des Recovery-Standorts und die Zeit zur Wiederherstellung von VMs am geschützten Standort. Der von NetApp empfohlene Wert beträgt 10 Minuten.

Schließen Sie den Failback-Prozess ab, und bestätigen Sie anschließend die Wiederaufnahme des VM-Schutzes und der Datenkonsistenz.

Wiederherstellung Von Lösegeld-Waren

(i)

Die Wiederherstellung von Ransomware kann eine gewaltige Aufgabe sein. Insbesondere kann es für IT-Abteilungen schwierig sein, den sicheren Rückgabepunkt zu ermitteln und einmal festgestellt zu haben, wie sichergestellt werden kann, dass wiederhergestellte Workloads vor den erneuten Angriffen (vom Schlafen von Malware oder durch anfällige Anwendungen) geschützt sind.

Jetstream DR für AVS kann zusammen mit Azure NetApp Files Datastores diese Bedenken lösen, da Unternehmen eine Recovery von verfügbaren Zeitpunkten durchführen können, sodass Workloads bei Bedarf in einem funktionsfähigen, isolierten Netzwerk wiederhergestellt werden können. Durch Recovery können Applikationen funktionieren und miteinander kommunizieren, ohne dass sie dem Nord- Süd-Datenverkehr ausgesetzt werden. So erhalten Sicherheitsteams einen sicheren Ort, um forensische und andere notwendige Korrekturmaßnahmen durchzuführen.

JetStream DR									li)
Protected Domains S	tatistics Sto	orage Sites Apoliar	oces Configu	rations Task I	00			-	
Select Protected Domai	Failback Prote	ected Domain						Delete	≡More
Mode	1. General	2a. Failback Settings	2b. VM Settings	3. Recovery VA	4, DR 5) Settings	5. Summary		Edit Details
Active Site		1949 - 1947 - 1947 - 1947 - 1947 - 1947 - 1947 - 1947 - 1947 - 1947 - 1947 - 1947 - 1947 - 1947 - 1947 - 1947 -	1997-1997 - Constant Carlos -	2000 00 000 000 000 00 00 00 00 00 00 00		2000-000 -0 000	6-04-04-04-07	^ :po	^
Recoverable / Total VMs	Protected D	omain Name		ANFPD003				56.2.)	
	Failback Dat	tacenter		A300-DataCenter					
	Failback Clu	uster		A300-Cluster					×
Destanted Mile Se	Failback Re	source Pool		-				1000	
Protected VMS de	VM Folder (Optional)						1.000	
	Failback Dat	tastore		A300_NFS_DS02				- 200	0
VM Name A	Maximum D	elay After Stopping		60 Minutes					~
AuctionAppA3	Internal Net	work		VM_187					^
AuctionAppB3	External Re	plication Network		VM_187					
AuctionDB3	Managemer	nt Network		VM_187				~	
AuctionLB3					Cancel	Back	Failback		
AuctionMSQ3			Recoverab	le	Write-Back	VMDK)	Deta	105	
AuctionNoSQL3			Recoverab	le	Write-Back	VMDK)	Det	uls	~

Disaster Recovery mit CVO und AVS (Storage mit Anbindung an den Gast)

Überblick

Autoren: Ravi BCB und Niyaz Mohamed, NetApp

Disaster Recovery in die Cloud ist eine stabile und kostengünstige Möglichkeit zum Schutz von Workloads vor Standortausfällen und Datenbeschädigungen wie Ransomware. Mit NetApp SnapMirror können lokale VMware Workloads, die einen mit dem Gast verbundenen Storage verwenden, auf NetApp Cloud Volumes ONTAP in Azure repliziert werden. Dies bezieht sich auf Applikationsdaten, doch was ist mit den eigentlichen VMs selbst. Disaster Recovery sollte alle abhängigen Komponenten, einschließlich Virtual Machines, VMDKs, Applikationsdaten und mehr, abdecken. Zu diesem Zweck kann SnapMirror zusammen mit Jetstream verwendet werden, um Workloads, die von On-Premises zu Cloud Volumes ONTAP repliziert wurden, nahtlos wiederherzustellen und gleichzeitig vSAN Storage für VM-VMDKs zu verwenden.

Dieses Dokument bietet einen Schritt-für-Schritt-Ansatz zur Einrichtung und Durchführung von Disaster Recovery mit NetApp SnapMirror, JetStream und der Azure VMware Lösung (AVS).



Voraussetzungen

Dieses Dokument konzentriert sich auf den Gast-Storage für Applikationsdaten (auch als Gastsystem bekannt) und wir gehen davon aus, dass die On-Premises-Umgebung SnapCenter für applikationskonsistente Backups verwendet.



Dieses Dokument bezieht sich auf jede Backup- oder Recovery-Lösung eines Drittanbieters. Je nach der in der Umgebung verwendeten Lösung befolgen Sie Best Practices, um Backup-Richtlinien zu erstellen, die die SLAs des Unternehmens erfüllen.

Für die Konnektivität zwischen der On-Premises-Umgebung und dem virtuellen Azure-Netzwerk nutzen Sie die globale Express Route oder ein virtuelles WAN mit einem VPN-Gateway. Segmente sollten basierend auf dem lokalen VLAN-Design erstellt werden.



Es gibt mehrere Optionen, um On-Premises-Datacenter mit Azure zu verbinden, sodass wir nicht einen bestimmten Workflow in diesem Dokument beschreiben können. Die entsprechende On-Premises-zu-Azure-Konnektivitätsmethode finden Sie in der Azure-Dokumentation.

Implementieren der DR-Lösung

Übersicht Zur Lösungsimplementierung

- 1. Stellen Sie sicher, dass die Applikationsdaten mit SnapCenter zusammen mit den erforderlichen RPO-Anforderungen gesichert werden.
- 2. Stellen Sie mithilfe von Cloud Manager Cloud Volumes ONTAP mit der richtigen Instanzgröße innerhalb des entsprechenden Abonnements und des virtuellen Netzwerks bereit.
 - a. Konfiguration von SnapMirror für die entsprechenden Applikations-Volumes

- b. Aktualisieren Sie die Backup-Richtlinien in SnapCenter, um SnapMirror Updates nach den geplanten Aufgaben auszulösen.
- 3. Installieren Sie die JetStream DR-Software im lokalen Datacenter, und beginnen Sie mit dem Schutz für Virtual Machines.
- 4. Installieren Sie die JetStream DR-Software in der Private Cloud der Azure VMware Lösung.
- Bei einem Notfall können Sie die SnapMirror Beziehung mithilfe von Cloud Manager unterbrechen und das Failover von Virtual Machines zu Azure NetApp Files oder zu vSAN Datastores im vorgesehenen AVS-DR-Standort auslösen.
 - a. Schließen Sie die ISCSI-LUNs und NFS-Mounts für die Applikations-VMs wieder an.
- 6. Rufen Sie Failback auf den geschützten Standort auf, indem Sie SnapMirror nach der Wiederherstellung des primären Standorts erneut resynchronisieren.

Einzelheiten Zur Bereitstellung

Konfiguration von CVO auf Azure und Replizierung von Volumes zu CVO

Als ersten Schritt müssen Sie Cloud Volumes ONTAP auf Azure konfigurieren ("Verlinken") Und replizieren Sie die gewünschten Volumen zu Cloud Volumes ONTAP mit den gewünschten Frequenzen und Snapshot-Aufbewahrung.

Health Status 💠	Source Volume	Target Volume 8	Total Transfer Time 🔹	Status	Mirror State	Last Successful Transfer	6
0	gcsdrsqidb_sc46 ntaphci-a300e9u25	gcsdrsqldb_sc46_copy ANFCVODRDemo	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 AM 7.22 MiB	
\odot	gcsdrsqllog_sc46 ntaphci-a300e9u25	gcsdrsqilog_sc46_copy ANFCVODRDemo	16 seconds	idle	snapmirrored	May 6, 2022, 11:43:52 AM 130.69 KiB	•

Konfigurieren Sie AVS-Hosts und CVO-Datenzugriff

Zwei wichtige Faktoren, die bei der Implementierung des SDDC berücksichtigt werden müssen, sind die Größe des SDDC-Clusters in der Azure VMware Lösung und die Dauer des SDDC im Service. Diese beiden wichtigen Überlegungen für eine Disaster-Recovery-Lösung tragen zur Senkung der Gesamtbetriebskosten bei. Das SDDC kann mit nur drei Hosts eingerichtet sein und bis hin zu einem Cluster mit mehreren Hosts in einer umfassenden Implementierung.

Die Entscheidung für die Implementierung eines AVS-Clusters hängt in erster Linie von den RPO/RTO-Anforderungen ab. Mit der Azure VMware Lösung kann das SDDC bereits rechtzeitig zur Verfügung gestellt werden, um entweder für das Testen oder für ein tatsächliches Notfallereignis zu sorgen. Ein durch die Just-in-time-Implementierung implementierter SDDC spart ESXi Hostkosten, wenn Sie keine Katastrophe mehr haben. Diese Form der Implementierung wirkt sich jedoch auf das RTO um einige Stunden aus, während das SDDC bereitgestellt wird.

Am häufigsten implementiert wird die SDDC-Option in einem Pilot-Light-Modus, der immer aktiviert ist. Diese Option bietet einen kleinen Platzbedarf von drei Hosts, die immer verfügbar sind. Außerdem werden Recovery-Vorgänge durch eine Basis für Simulationsaktivitäten und Compliance-Prüfungen beschleunigt, sodass das Risiko einer operativen Abweichungen zwischen dem Produktions- und dem DR-Standort vermieden wird. Der Pilot-Light-Cluster kann bei Bedarf schnell auf das gewünschte Niveau skaliert werden, um tatsächliche DR-Ereignisse zu bewältigen.

Informationen zur Konfiguration des AVS SDDC (ob On-Demand oder im Pilot-Light-Modus) finden Sie unter "Implementieren und Konfigurieren der Virtualisierungsumgebung auf Azure". Überprüfen Sie als Voraussetzung, ob die Gast-VMs auf den AVS-Hosts nach dem Einrichten der Konnektivität Daten von Cloud Volumes ONTAP nutzen können.

Nach der ordnungsgemäßen Konfiguration von Cloud Volumes ONTAP und AVS beginnen Sie mit der Konfiguration des Jetstream zur Automatisierung der Wiederherstellung lokaler Workloads auf AVS (VMs mit Applikations-VMDKs und VMs mit in-Guest-Storage) mithilfe des VAIO Mechanismus und durch Nutzung von SnapMirror für Applikations-Volumes-Kopien auf Cloud Volumes ONTAP.

Die Jetstream DR-Software besteht aus drei Hauptkomponenten: Der JetStream DR Management Server Virtual Appliance (MSA), der DR Virtual Appliance (DRVA) und den Host-Komponenten (I/O-Filterpakete). Mit dem MSA-System werden Hostkomponenten auf dem Compute-Cluster installiert und konfiguriert und JetStream DR-Software verwaltet. Die Installation erfolgt wie folgt:

- 1. Voraussetzungen prüfen.
- 2. Nutzen Sie das Kapazitätsplanungs-Tool für Ressourcen- und Konfigurationsempfehlungen.
- 3. Implementieren Sie JetStream DR MSA auf jedem vSphere-Host im zugewiesenen Cluster.
- 4. Starten Sie das MSA-Produkt mit dem DNS-Namen in einem Browser.
- 5. Registrieren Sie den vCenter-Server mit dem MSA.
- Nachdem JetStream DR MSA implementiert und der vCenter Server registriert wurde, navigieren Sie zum JetStream DR Plug-in mit dem vSphere Web Client. Dazu können Sie im Datacenter > Configure > JetStream DR navigieren.
 - betetteam bit navigieren.



- 7. Führen Sie über die JetStream DR-Schnittstelle die folgenden Aufgaben aus:
 - a. Konfigurieren Sie das Cluster mit dem I/O-Filterpaket.

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	-0000-00000000001 <u>Configure</u>			
Tenant ID / Application ID	- Configure				
Application Secret	- <u>Configure</u>				
Configured Clusters	Configure Clusters				
Configure Cluster & Upgrade Unconfigure & Res		Select All	Clear All Q		٩
Cluster Name	Cluster Name	Datacenter Name		sion 🔺	Host Details 🔺
No cluster configured	A300-Cluster	A300-DataCenter	*		
		5			
		Cance	el Configure		

b. Fügen Sie den Azure Blob-Storage am Recovery-Standort hinzu.

Storage Sites		Add Storage Site	
+ Add Storage Site	Scan Domain I	Starage Ste Type *	
Name 🛦		Azure Blob Storage	
No Storage Site configured.			
3	5	Access Type *	
		Key Access	
		Storage Site Name (Provide a name to identify this Site) *	
		ANFDemoblobrepo	
Storage Site Details	Almeria		
).		Acure Bob Storage Account Name *	
		anfdrdemostor	
No storage site selected. S	elect a storage	Journ Rob Diverse Lermont Year *	
		Name skol oski dige Akadoli nev	

8. Stellen Sie die erforderliche Anzahl an DR Virtual Appliances (DRVAs) über die Registerkarte Appliances bereit.



Verwenden Sie das Kapazitätsplanungs-Tool, um die Anzahl der benötigten DRVAs zu ermitteln.

Jet:Stream DR Protected Domains Statistics Storage Sites App	liances Configurations	Task Log			E.
DRVAs (DR Virtual Appliances)					
+ Deprog New DRVA TUpgrade TUpconfigure					Q
Name A	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 🔺	



9. Erstellen Sie Protokoll-Volumes für jedes DRVA unter Verwendung der VMDK aus den verfügbaren Datenspeichern oder dem unabhängigen gemeinsamen iSCSI-Speicherpool.

JetStream DR								i i
Protected Domains	Statistics	Storage Sites	Appliances	Configurations	Task Log			
DRVAs (DR Virtual Ap	opliances)	La .						
+ Deploy New DRVA	t toppade	Dunconfigure						a
Name 🔺				Status A	Child Alarm 🔺	Software Version	Details A	
GCSDRPD001				Running	00	4.0.0.134	Detain	
+ New Replication Log V	folume 🛱 Un	contgune.						c
Disk Path Name				Status	Child Alarm	Size (available/total) 🔺	Details A	
idev/sdb				O Ok	0	179 88 GB / 200 GB	Details	
Replication Log Volu	me Details							

10. Erstellen Sie auf der Registerkarte geschützte Domänen die erforderliche Anzahl geschützter Domänen mithilfe von Informationen über die Azure Blob Storage-Site, die DRVA-Instanz und das Replikationsprotokoll. Eine geschützte Domäne definiert eine bestimmte VM oder einen Satz von Applikations-VMs innerhalb des Clusters, die gemeinsam gesichert werden und einer Prioritätsreihenfolge für Failover-/Failback-Vorgänge zugewiesen ist.

elect Protected Domain: * View all	Create Protected Domain				+ Create = Mo
	1. General 2.	Primary Site	J. Summary		
	Protected Domain Name	GCSDRPD_Demo01			
	Priority Level (Optional)				
	Description	Protection domain ANF			
	Total estimated data size to be protected	d 1000GB			
	DR Virtual Appliance	GCSDRPD001			
	Compression	Yes			
	Compression Level	Default		10	
	Normal GC Storage Overhead	50%			
	Maximum GC Storage Overhead	300%			
	Replication Log Storage	/dev/sdb			
	Papilication Log Size	50GR		*	



11. Wählen Sie die zu sichernden VMs aus und gruppieren Sie die VMs je nach Abhängigkeit in Applikationsgruppen. Anhand von Applikationsdefinitionen können Gruppen von VMs zu logischen Gruppen gruppiert werden, die ihre Boot-Aufträge, Boot-Verzögerungen und optionale Applikationsvalidierungen enthalten, die nach der Recovery ausgeführt werden können.



Vergewissern Sie sich, dass derselbe Sicherungsmodus für alle VMs in einer geschützten Domäne verwendet wird.

Write Back(VMDK)-Modus bietet eine höhere Performance.

elect Protected Domain: GCSDRPD_Demo01 *	VIE Star	1 Protection				+ Croate Delete = M
ecoverable / Total VMs					_	Edi I
epication Status	Pit	fection Mode for selected VMs 🔹			٩	
emaining Background Data	0	VM Name 🔺	# of Disks	Protection Mo	de	LOCAL (177,21,253,169)
	0	ElasticWebA2	1		×. *	Disabled
anean ro-D	0	ElasticWebA3	1			
Development VDB Carthorns Abarrow	0	ElasticWebB0	1		Ψ.	
Sentige Swarres	0	ElasticWebB1	Cit .		ω_	
+ Obert Berthauften		ElasticWebB2	1		10 A	
T-SHELFIGHUSSON		ElasticWebB3	3 1	Write Through	¥	
VM Name 🔺	2	GCS-DR-DC	1	Write-Through	* N	Background Data A Details
NO VM is producted	2	GCS-DR-LinVM01		Write-Through	 Int 	
	2	GCS-DR-SCA	1	Write-Through	~	
		GCS-DR-SQL01	1	White-Through	U	
	2	GCS-DR-WeVM01	.1	Write-Through	~	
		jss-drva-GCSDRPD001	2			
	0	PrimeClient	2		ν.	
		Standby0	1	With Through	¥	
	0	Standby1	.t		¥.,	
	0	Standby2	1.0		×1	
	0	Standby3				
		VMmark-Template01	10		×. •	
				Cancel	Start Protection	

12. Stellen Sie sicher, dass Replizierungs-Protokoll-Volumes auf hochperformanten Storage platziert werden.

elect Protected Domain: GCSDRPD_Demo01 .	Start Protection				+ Creato 🛢 Delete	
ecoverable / Total VMs	SUIT FIORCOOT			1		Las Der
epication Status	Write-Back(VMDK) •			٩	ANFORDemoFalloverSite	
emaining Background Data	VM Name 🔺	# of Disks	Protection Mode		LOCAL (172 21 253 160)	
	ElasticWebA2	1	Write Through	· . *	Destroyant	
anten 1620	ElasticWebA3	1	White Through	×		
And a second second	ElasticWebB0	1	vinite-Through	×.		
HURPERES VARS BEIDOGE ALLITE	ElasticWebS1	1	Witte-Through	¥.,		
tourse and	ElasticWebB2	1	Write-Through	1.		
T Start Procection	ElasticWeb63	1	Write-Through	10 a		
VM Name 🔺	GCS-DR-DC	1	Witte-Back(VMDH	9	Background Data Details	
No VM is protected.	GCS-DR-LivVM01	3	Write-Back(VMDH	Q 🗸		
	GCS-DR-SCA	1	Write-Back(VMDP	G 👻		
	GCS-DR-SQL01	1	Write-Back/VMDH	0 -		
	GCS-DR-WeVM01	31	Witte-Back(VMDR	0 🗸		
	int-diva-GCSDRPD001	2		× .		
	PrimeClient	2				
	Standby0	1	Wide Trendt	÷.		
	Standby1	1		- W.L.		
	Standby2	1	White Through	×		
	Standby3	1	Write Through	14.5		
	VMmark-Template01	1		 N (2) 		
			Cancel	Start Protection		
			and a standard and a	N		

13. Klicken Sie nach dem Abschluss auf Schutz für die geschützte Domäne starten. Damit wird die Datenreplizierung für die ausgewählten VMs auf den zugewiesenen Blob-Speicher gestartet.

Protected Domains Statistics Storage	Sites Appliances Configurat	ions Task Log			Running Tasks
elect Protected Domain: GCSDRPD_Demo0	1 • <u>View all</u>			+ (Start Protection (GCS-DR-SCA) 50%
ecoverable / Total VMs		0/5	Configurations		Start Protection (GCS-DR-Win 50%
eplication Status		ок	Storage Site	ANFDRDe	Start Protection (GCS-DR-Lin 50%
			Owner Site	LOCAL (172.2	
emaining Background Data		0 B	Datacenter \ Cluster	A300-DataCen	Stan Protection (GCS-DR-DC) 50%
irrent RPO			Point-in-time Recovery	Disabled	Start Protection (GCS-DR-SQ 50%
Protected VMs Settings Alarms					Configure VMDK Re Completed
+ Start Protection Start Protection					Configure VMDK Re Completed
Protected VMs Settings Alarms Start Protection VM Name	Protection Status	Replication St	atus 🔺 Protection Mode 🔺	Background Dr	Close
Protected VMs Settings Alarms	Protection Status O Initializing	Replication St	atus A Protection Mode A Write-Back(VMDK)	Background De	Configure VMDK Re_ Completed Ctose
	Protection Status Protection Status	Replication St	atus Protection Mode Write-Back(VMDK) Write-Back(VMDK)	Background Da	Configure VMDK Re Completed Cose
Protected VMs Settings Alarms Start Protection VM Name GCS-DR-DC GCS-DR-BCA	Protection Status Protection Status Initializing Initializing Initializing	Replication St - -	atus Protection Mode A Write-Back(VMDK) Write-Back(VMDK) Write-Back(VMDK)	Background De - -	Configure VMDK Re Completed Close Ita A Details Details Details Details
Protected VMs Settings Alarms + Start Protection VM Name ▲ GCS-DR-DC GCS-DR-SCA GCS-D	Protection Status Protection Status Initializing Init	Replication St - -	atus ▲ Protection Mode ▲ Write-Back(VMDK) Write-Back(VMDK) Write-Back(VMDK) Write-Back(VMDK)	Background Di - - -	Configure VMDK Re Completed Close ta A Details Details Details Details Details

14. Nach Abschluss der Replizierung wird der Sicherungsstatus der VM als wiederherstellbar markiert.

IEUSUREATT DR Protected Domains Statistics Stor	rage Sites Appliances Configuration:	i Task Log				l	
elect Protected Domain: GCSDRPD_De	mo01 👻 <u>View all</u>			+ Create	Delete	≡ More	
ecoverable / Total VMs		5/5	Configurations			Edit Detail	
eplication Status		OK	Storage Site	ANFDRDemoFaile	noFailoverSite		
		1.00	Owner Site	LOCAL (172.21.253.1	LOCAL (172 21 253 160)		
emaining Background Data		0 B	Datacenter \ Cluster	A300-DataCenter \ A300-Cluster			
urrent RPO		0s	Point-in-time Recovery	Disabled			
r tononia rine ocuniga: manna							
+ Start Protection	Protection Status	Replication Sta	tus 🔺 Protection Mode 🔺	Background Data	Details	٩	
Start Protection Mame GCS-DR-DC	Protection Status A	Replication Sta	tus Protection Mode Write-Back(VMDK)	Background Data 🔺 0 B	Details Details	٩	
Start Protection VM Name GCS-DR-DC GCS-DR-LinVM01	Protection Status A	Replication Sta	tus Protection Mode Write-Back(VMDK)	Background Data A 0 B 0 B	Details Details Details	٩	
Start Protection WN Name GCS-DR-DC GCS-DR-LinVW01 GCS-DR-SCA	Protection Status ▲ Recoverable Recoverable Recoverable	Replication Sta	tus Protection Mode Write-Back(VMDK) Write-Back(VMDK) Write-Back(VMDK)	Background Data A 0 B 0 B 0 B	Details Details Details Details	٩	
Start Protection Star Protection VM Name Gcs-DR-DC Gcs-DR-LinVM01 Gcs-DR-SCA GcS-DR-SCA	Protection Status Recoverable Recoverable Recoverable Recoverable Recoverable	Replication State	tus Protection Mode Write-Back(VMDK) Write-Back(VMDK) Write-Back(VMDK) Write-Back(VMDK)	Background Data A 0 B 0 B 0 B 0 B	Details Details Details Details Details	٩	

(i)

Failover-Runbooks können so konfiguriert werden, dass sie die VMs gruppieren (so genannte Recovery-Gruppe), die Boot-Reihenfolge festlegen und die CPU-/Speichereinstellungen zusammen mit den IP-Konfigurationen ändern.

15. Klicken Sie auf Einstellungen und dann auf den Link Runbook Configure, um die Runbook-Gruppe zu konfigurieren.

Protected Domains Statistics Storage Sites Appliances Configurations Task Log						
select Protected Domain: GCSDRPD_Demo01 View all			+ Create	Delete	≡ More	
Recoverable / Total VMs 5/5	Configurations				Edit Deta	
Replication Status	Storage Site	ANFDRDemoFailoverSite				
	Owner Site	LOCAL (172.21.253.160)				
Remaining Background Data 0 B	Datacenter \ Cluster	A300-0	ataCenter \ A300	Cluster		
Current RPO 0s	Point-in-time Recovery	Disable	ю			
O O Protected VMs Settings Alarms						
Failover Runbook Not Configured Configure						
Test Failover Runbook Not Configured Configure						
Faliback Runbook & Not Configured Configure						
Memory Setting Not Configured Configure						
GC Settings Configured Configure						
Concurrency Settings Not Configured Configure						

16. Klicken Sie auf die Schaltfläche Gruppe erstellen, um mit der Erstellung einer neuen Runbook-Gruppe zu beginnen.



Falls erforderlich, wenden Sie im unteren Teil des Bildschirms benutzerdefinierte Prescripts und Post-scripts an, um automatisch vor und nach dem Betrieb der Runbook-Gruppe auszuführen. Stellen Sie sicher, dass die Runbook-Skripte auf dem Management-Server residieren.

JetStream DR Protected Domains	Statistics Storage Sites A	Failover Runbook Settings			B
Select Protected Dom	ain: GCSDRPD_Demo01 * Vi	+ Create Group	Delete Group		+ Create Delete E More
Recoverable / Total VM	ts /	O Group Name	# of VM Power Off	Retain MAC	Edd Details
Replication Status		O 🗌 Independent VMs	5 -	·*:	ANFDRDemoFalloverSite
Remaining Background	1 Data				A300-DataCenter (A300-Cluster
Current RPO					Deabled
Protected VMs S	Settings Alarms	0 0			
Failover Runbook	Configured Details				
Test Fallover Runbook	Configured Details				
Failback Runbook	Configured Details				
Memory Setting	Not Configured Configure				
GC Settings	Configured Configure				
Concurrency Settings	Not Configured Configure				

17. Bearbeiten Sie die VM-Einstellungen nach Bedarf. Geben Sie die Parameter für die Wiederherstellung der VMs an, einschließlich der Boot-Sequenz, der Boot-Verzögerung (angegeben in Sekunden), der Anzahl der CPUs und der zuzuzuzuzuzuzuzuzuzuzuzuzuzuzuzuzuzu Boot-Sequenz der VMs, indem Sie auf die Pfeile nach oben oder unten klicken. Zur Aufbewahrung von MAC stehen auch Optionen zur Verfügung.

JebSbream DR Protected Domains Statistics Storage	Create Runbook Group									
Select Protected Domain: GCSDRPD_Demo	1. General	2. Select VM:	5	3. Edit V	M Settings		4. Summa	+ Create	E Oelicte	≡ More
Recommitte / Total Vills	Retain MAC		Power Of	f VMs			O Reset	*		
Replication Status	VM Name	Boot Sequence	Boot Delay	CPU	Memory	Script	NIC	#FDRDembFilloverSit		
Remaining Background Data	GCS-DR-WinVM01	17 4	0s	32	64 GB	Config	View	SalaCenter (A300-Cla		
Current RPO	GCS-DR-SCA	21 4	0s	4	16 GB	Config	Xiew	d		
Partition	GCS-DR-DC	3 11hr	0s	4	16 GB	Config	<u>View</u>			
Protected volts. Settings Aurmo	GCS-DR-LinVM01	414	0s	2	4 GB	Config	View			
	GCS-DR-SQL01	5†↓	05	4	8 GB	Config	View			
Test Failover Rumbook Configured Cellais Faiback Rumbook Configured Cellais Memory Setting Hist Configured Configured GC Settings Configured Configured Concurrency Settings Not Configured Configured	Osubie click on the cell	or click on the up/down	cicon to change v	Ca	ncel	Back	N	nt		

18. Statische IP-Adressen können manuell für die einzelnen VMs der Gruppe konfiguriert werden. Klicken Sie auf den Link "NIC-Ansicht" einer VM, um die IP-Adresseinstellungen manuell zu konfigurieren.

t Protected Domain: GCSDRPD_Demo	•										
	1 General	2 Salact VM		1 Edit M	A Settinos		4 Summary		+ Create	TO Delate	≡ Moru
	. Sanna	2. Select emi			e ocunigo		4. Summary	1			
	Retain MAC		Power On	VMS			O Reset		FORDemoFallo	entities.	
	VM Name	Boot Sequence	Boot Delay	CPU	Memory	Script	NIC				
	GCS-DR-WinVM01	1† ↓	0s	32	64 GB	Config	View ~			G Cluster:	
	GCS-DR-SCA	2↑↓	Qs	4	16 GB	Contig	VS				
	GCS-DR-LinVM01	37 4	0s	2	4 GB	Contig	View				
	GCS-DR-SOLOT	47 4	0s	4	8 GB	Config	View				
	GCS-DR-DC	51 4	0s.	4	16 GB	Config	View +				
Settinges Configured <u>Configured</u>											

19. Klicken Sie auf die Schaltfläche Konfigurieren, um die NIC-Einstellungen für die jeweiligen VMs zu speichern.

	Label	Network Name	Key	PCI Slot #	IP	
π.	Network adapter 1	VM_3510	4000	192	Configure	aiy
Re						
VM No						
GCS-E	Configu	re Static IP Address				1
GCSD						
GCS-C	172.21.2	54.185				
Cen C	о—о				_	
	Subret Mar	k-				
	200.200	255.0			- 11	
	Gateway *					
	172.21.2	54.1				
	200					
	172.30.1	53.20				
	UNS SU	tos			_	
					_	
		Reset	Can	cel Confi	gure	
					Close	Next
	GCSDRPD_Demo	neral Z. Select VMs	3. Edit VM s	intungs 4. Summ	+ Dante	
	Group N Number	ame of VMs	GCSRecovery 5		- FERDimoReland	
	Retain V Power C	M's MAC addresses IT VMs	true faise		Sincer II Aspens	
	Sector	p mangeung and boot sequence change with	be applied to both Fallover	and Failback runbook.		

Der Status der Failover- und Failback-Runbooks wird nun als konfiguriert aufgeführt. Failover- und Failback-Runbook-Gruppen werden paarweise erstellt, wobei dieselbe erste Gruppe von VMs und Einstellungen verwendet wird. Bei Bedarf können die Einstellungen einer Runbook-Gruppe individuell angepasst werden, indem Sie auf den entsprechenden Link Details klicken und Änderungen vornehmen.

QK

Eine Best Practice für einen Recovery-Standort (AVS) ist die Erstellung eines Pilotlichtclusters mit drei Knoten im Voraus. Dadurch kann die Infrastruktur am Recovery-Standort vorkonfiguriert werden, einschließlich:

- Netzwerkzielsegmente, Firewalls, Services wie DHCP und DNS usw.
- Installation von JetStream DR f
 ür AVS
- · Konfiguration von ANF-Volumes als Datastores und mehr

Jetstream DR unterstützt einen RTO-Modus von nahezu null für geschäftskritische Domänen. In diesen Domänen sollte der Ziel-Storage vorinstalliert sein. ANF ist in diesem Fall ein empfohlener Speichertyp.



Die Netzwerkkonfiguration einschließlich der Segmenterstellung sollte auf dem AVS-Cluster entsprechend den Anforderungen vor Ort konfiguriert werden.



Je nach SLA- und RTO-Anforderungen können Sie einen kontinuierlichen Failover oder einen normalen (Standard-) Failover-Modus verwenden. Bei einer RTO von nahezu null sollten Sie am Recovery-Standort mit der kontinuierlichen Rehydrierung beginnen.

1. Verwenden Sie den Befehl Ausführen, um JetStream DR für AVS auf einer privaten Cloud der Azure VMware-Lösung zu installieren. Wählen Sie im Azure-Portal zur Azure VMware-Lösung die Private Cloud aus und wählen Sie Ausführen Command > Packages > JSDR.Configuration.



Der CloudAdmin-Standardbenutzer der Azure VMware-Lösung verfügt nicht über ausreichende Berechtigungen, um JetStream DR für AVS zu installieren. Die Azure VMware Lösung ermöglicht eine vereinfachte und automatisierte Installation von JetStream DR durch Aufrufen des Befehls Azure VMware Solution Run für JetStream DR.

Der folgende Screenshot zeigt die Installation mithilfe einer DHCP-basierten IP-Adresse.

Microsoft Azure	P Statch resources	. services, and docs (G+/)	🗉 🕒 🖓 🗇 🔿 🖉 niyaz@netapp.com irrano.couo.twi
Home > ANFDataClus ANFDataClus Run	command -		Run command - Install-JetDRWithDHCP ×
A/S Private clood	🔘 Refresh 🛱 Feedback		This top level Cindlet Downloads JetDr bundle from MMS, creates a new user, assigns elevated privileges to the user, deploys JetDr Managenient Server Appliance/MSA), registers vCenter to the JetDr MSA, configures cluster.
 Access control (IAM) Tags 	Packages Run execution status		Command parameters
Diagnose and solve problems	v Name	Description	Begitterwithip () Due
Settings	 SOR Configuration (114) Powerser Internet In	nue to configuration at activities fortunes on AVS. See <u>information Schoors, ins</u> for support	PrintectedCluster * ()
Locks	Disable-JetDRForCluster	This Cmdlet unconfigures a cluster but doesn't uninstall JetDR completely so other clusters	Couter1
Hinane		porces.	stanDatastore
and the second se	Ematrie-SetCHD-orChuster	This Emdlet configures an adottonal ouster for protection. It installs vide to all hosts in the	Withame* (1)
Connectivity	Install-JetDRWithDHCP	This top level Condiet Downloads JetDr bundle from MMS, creates a new user, assigns elevi registers vCenter to the JetDr MSA, coefficients cluster.	anfjorat-moa
Clusters	Instatic Gropping Andrews	This the level Centlet Doundstate for the burnels from MMS creates a new user actions along	Cluster * ()
Identity	HILLING VIEL PROVIDED AND PROVIDANT PROVIDED AND PROVIDED AND PROVIDED AND PROVIDED AND PROVIDED AND PROVIDED AND PROVIDANT PROVIDED AND PROVIDANT PR	registers vCenter to the JetDr MSA, configures cluster.	Guster-1
Storage (preview)	Invoka-PreflightJetDRInitaB	This Endlet checks and displays current state of the system it checks whether the minimal	Credential ()
Placement policies		4 hosts, if the cluster details are correct, if there is already a VM with the same name provid	Username *
Add-oni	Invoke-PreflighttetDRUminstall	This Criticlet checks and displays current state of the system it checks whether the minimal	toot
	The second second	 rosts, in the bustler details are correct and if any vicence is registered to the work 	Pessword *
Vorkload Networking	Orwinstan-JetCHL	The top level Undet onlates a new user, assigns elevated privileges to the user, unconfigu	
Segments	> MicrosoftAVSManagement +147 y	rook ondiels för edministreter lever taks in meneging Azure VMMeet Soutisme	HostName 🕥
DHCP			anfpvaliensa
Port mirroring			Network* ()
ONS			DiSeg
operations			Details
Run command			Retain up to

2. Nachdem die JetStream DR für AVS-Installation abgeschlossen ist, aktualisieren Sie den Browser.

Um auf die JetStream DR-UI zuzugreifen, wechseln Sie zum SDDC Datacenter > Configure > JetStream DR.

Protected Domains	Statistics	Storage Site	es App	pliances	Configurations	Task Log	J	
Site Details							Alarm Sett	ting
vCenter Server Hostnar	me	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	Dunconfigure	🛠 Resolv	e Configure Iss	sue			C
Cluster Name		Datacenter	Name 🔺	Status 🛦	Software Ve	ersion 🛦	Host Details	
Cluster-1		SDDC-Data	center	🔮 Ok	4.0.2.132		Details	

- 3. Führen Sie über die JetStream DR-Schnittstelle die folgenden Aufgaben aus:
 - a. Fügen Sie das Azure Blob Storage-Konto hinzu, das zur Sicherung des lokalen Clusters als Storage-Standort verwendet wurde, und starten Sie dann die Option Scan Domains.
 - b. Wählen Sie im angezeigten Popup-Dialogfeld die zu importierende geschützte Domäne aus, und klicken Sie anschließend auf den Link Importieren.

JetStream DR Protected Domains Statistics Storage Sites	Available Protected Domain(s) For Import		E.
Storage Sites + Add Storage Site Name A AMFDemoclobinepore:	Protected Domain Description Recoverable V GCSDRPD_Demo01 Protection domain ANF 5	VMs Import 5 Imogg ^	ee Ellob Storage

4. Die Domäne wird zur Wiederherstellung importiert. Gehen Sie auf die Registerkarte geschützte Domänen und überprüfen Sie, ob die vorgesehene Domäne ausgewählt wurde, oder wählen Sie die gewünschte aus dem Menü geschützte Domäne auswählen aus. Eine Liste der wiederherstellbaren VMs in der geschützten Domäne wird angezeigt.

rotected Domains Statistics Storage Sites Appliance	s Configurations Task	Log			
elect Protected Domain: GCSDRPD_Demo01 👻 View all			+ Create	Delete	■More
lode	Imported	Configurations			Det
ecoverable / Total VMs	5/5	Storage Site	ANFDemoblobrep	orec	
		Owner Site			
Methodological a					c
VM Name 🔺	Protection Status	*	Protection Mode 🔺	Details	
GCS-DR-DC	Recoverable		Write-Back(VMDK)	<u>Details</u>	
GCS-DR-LinVM01	Recoverable		Write-Back(VMDK)	Details	
GCS-DR-SCA	C Recoverable		Write-Back(VMDK)	Details	
			Write-Back(VMDK)	Dataila	
GCS-DR-SQL01	Recoverable		inite back incred	Decana	

5. Nachdem die geschützten Domains importiert wurden, sollten DRVA-Appliances bereitgestellt werden.



Diese Schritte können auch mithilfe von CPT- erstellten Plänen automatisiert werden.

- 6. Verwenden von verfügbaren vSAN oder ANF-Datastores für Replizierungsprotokolle erstellen
- 7. Importieren Sie die geschützten Domänen und konfigurieren Sie die Recovery-VA, um einen ANF-Datenspeicher für VM-Platzierungen zu verwenden.

ect Protected Domain:	Continuous F	ailover Protected Dom	ain					Delete	=	More
de	1 General	22 Esilouer Settings	O VM Settings	1 Perc		A DR Settings	5 Summanı			Dela
coverable / Total VMs	i, General	za. ranover settings	zo, vin setuilija	s. neur	isely in	4, Dr. Settings	o. Summary	~ reporec		3
	Protected D	omain Name		ANFPD002				253 160)		
	Datacenter			SDDC-Datac	enter					
	Cluster			Cluster-1				1000		8
	Resource P	ool (Optional)						1000		
rotected VMs Sett	VM Folder (Optional)		*)						
	Datastore			ANFRecoDS	U002					
	Internal Net	twork		DRSeg						0
VM Name	External Re	plication Network		DRSeg					Details	1
AuctionAppA2	Manageme	nt Network		DRSeg				- 64	Destroite	- 1
AuctionAppb2	Storage Site			ANFDemoblobreporec					Outsile	
AuctionL/B2	DR Virtual Appliance			ANFRecDRV	A003				Details	
AuctionLB2	Donligation	I an Starsna		Mouladh				<u> </u>	Details	
AuctionM5G2					Cancel	Back	Continuous Failow	er	Denaits	

Stellen Sie sicher, dass DHCP für das ausgewählte Segment aktiviert ist und genügend IP-Adressen verfügbar sind. Dynamische IPs werden vorübergehend verwendet, während Domänen sich wiederherstellen. Jede wiederherzuckernde VM (einschließlich kontinuierlicher Rehydrierung) erfordert eine individuelle dynamische IP-Adresse. Nach Abschluss der Wiederherstellung wird die IP freigegeben und kann wiederverwendet werden.

8. Wählen Sie die entsprechende Failover-Option (Continuous Failover oder Failover) aus. In diesem Beispiel wird die kontinuierliche Rehydrierung (kontinuierliches Failover) ausgewählt.



Obwohl sich der kontinuierliche Failover- und Failover-Modus bei der Konfiguration unterscheiden, werden beide Failover-Modi mit den gleichen Schritten konfiguriert. Failover-Schritte werden als Reaktion auf ein Notfall konfiguriert und durchgeführt. Ein kontinuierlicher Failover kann jederzeit konfiguriert werden und dann im Hintergrund während des normalen Systembetriebs ausgeführt werden. Nach einem Zwischenfall wird der fortlaufende Failover abgeschlossen, sodass die Eigentümerschaft der geschützten VMs direkt auf den Recovery-Standort übertragen wird (RTO von nahezu null).

JebSbream DR Protected Domains Statistics Storage Sites Appliances	Configurations Task	Log			1
Select Protected Domain: GCSDRPD_Demo01 👻 View all			+ Create	Delete	■More
Mode	Imported	Configurations		O Restore	
Recoverable / Total VMs	5/5	Storage Site	ANFDemoblobrepor	→ Failover	
		Owner Site	REMOTE (172.21.253.1f	+ Continuous Fail	over.
				→ Test Failover	0
Protected VMs Settings Alarms O O					
					C
VM Name 🔺	Protection Status	•	Protection Mode 🔺	Details	
GCS-DR-DC	Recoverable		Write-Back(VMDK)	Details	^
GCS-DR-LinVM01	Recoverable		Write-Back(VMDK)	Details	
GCS-DR-SCA	Recoverable		Write-Back(VMDK)	Details	
GCS-DR-SQL01	Recoverable		Write-Back(VMDK)	Details	

Der kontinuierliche Failover-Prozess beginnt und der Fortschritt kann über die UI überwacht werden. Durch Klicken auf das blaue Symbol im Abschnitt "Aktueller Schritt" wird ein Popup-Fenster angezeigt, in dem Details zum aktuellen Schritt des Failover-Prozesses angezeigt werden.

Failover und Failback

1. Nach einem Ausfall im geschützten Cluster der lokalen Umgebung (teilweiser oder kompletter Ausfall) können Sie das Failover für VMs auslösen. Dazu verwenden Sie Jetstream, nachdem die SnapMirror Beziehung für die jeweiligen Applikations-Volumes unterbrochen wurde.



 (\mathbf{i})

Dieser Schritt kann zur Erleichterung des Recovery-Prozesses einfach automatisiert werden.

2. Greifen Sie auf die Jetstream UI auf dem AVS SDDC (Zielseite) zu und lösen Sie die Failover-Option aus, um den Failover abzuschließen. Die Taskleiste zeigt den Fortschritt für Failover-Aktivitäten an.

Im Dialogfeld, das beim Abschluss des Failover angezeigt wird, kann die Failover-Aufgabe als geplant oder als erzwungen angegeben werden.

Select Protected Domain: GCSDRPD_Demot	J1 💌 <u>View all</u>		+ Create OF	Nover	≡ Mor	
Mode	Continuous Rehydration in Progress	Configurations			Details	
Recoverable / Total VMs	4/4	Storage Site	ANFDemobiobreporec		-	
		Owner Site	REMOTE (172.21.253.160)			
Data (Processed/Known Remaining)	329.01 GB / 6.19 GB	Datacenter \ Cluster	SDDC-Datacenter \ Cluster-1			
Current Step	Recover VMs' data from Storage Site®	Point-in-time Recovery	Disabled		~	
					٩	
	Protection Status A		Protection Mode 🔺	Details		
VM Name 🔺			Write-Back(VMDK)	Details	-	
VM Name A GCS-DR-DC	@ Recoverable					
VM Name A GCS-DR-DC GCS-DR-LinVM01	Recoverable Recoverable		Write-Back(VMDK)	Details		
VM Name A GCS-DR-DC GCS-DR-Lin/M01 GCS-DR-SCA	© Recoverable © Recoverable © Recoverable		Write-Back(VMDK) Write-Back(VMDK)	Details		
VM Name ▲ GCS-DR-DC GCS-DR-Lin/M01 GCS-DR-SCA GCS-DR-SOL01	Recoverable Recoverable Recoverable Recoverable Recoverable		Write-Back(VMDK) Write-Back(VMDK) Write-Back(VMDK)	Details Details Details		

vin network mapping		
Protected VM Network A	Recovery VM Network	1
VM_3510	DRStretchSeg 👻	
0 0		γ.
Planned Failover		
Some VM's guest credential are requ	ired because of network configuration: Configure	

Erzwungenes Failover geht davon aus, dass auf den primären Standort nicht mehr zugegriffen werden kann und die Eigentümerschaft der geschützten Domäne direkt vom Recovery-Standort übernommen werden muss.

D	Force Failover of Protected Domain requested. Administrator consent is required!
	Complete ownership of this Protected Domain will be taken over by this Site. Are you sure you want to continue?

Network Mapping				
otected VM Network 🔺	Recovery VM Network			^
I_3510	DRStretchSeg		- ^	
0 0				
			v	~
her settings				
Planned Failover				
Force Failover				
ome VM's guest credential are requ	red because of network configuration:	Configure		

 Nachdem der kontinuierliche Failover abgeschlossen ist, wird eine Meldung angezeigt, die den Abschluss der Aufgabe bestätigt. Nach Abschluss der Aufgabe greifen Sie auf die wiederhergestellten VMs zu, um ISCSI- oder NFS-Sitzungen zu konfigurieren.

> Der Failover-Modus wird in Failover ausgeführt, und der Status der VM ist wiederherstellbar. Alle VMs der geschützten Domäne werden jetzt am Recovery-Standort in dem von den Failover-Runbook-Einstellungen angegebenen Zustand ausgeführt.

Um die Failover-Konfiguration und die Infrastruktur zu überprüfen, kann JetStream DR im Testmodus (Option Test Failover) betrieben werden, um die Wiederherstellung von Virtual Machines und deren Daten vom Objektspeicher in einer Test-Recovery-Umgebung zu beobachten. Wenn ein Failover-Verfahren im Testmodus ausgeführt wird, ähnelt sein Vorgang einem tatsächlichen Failover-Prozess.

 (\mathbf{i})

(i)

Protected Domains Statistics Stora	Continuous Rehydration Task Resu	nt	
Select Protected Domain: GCSDRPD002	Task Completed Successfully with	warnings	+ Create Delate Etitor
Node			Edt Da
	Protected Domain	GCSDRPD002	AVECVODR
Recoverative / total VMs	VMs Recovery Status	Success with warnings	0CAL/(17230456.2)
	Total VMs Recovered	4	DDC-Datacenter 1 Chutter 1
Plate almost The Sector and Plate	VM(s) with warning	2 <u>View</u>	reabled
Kemaining background bata	GCSRecovery03 Status:		
	Pre-script Execution Status	Not defined	
	Runbook Execution Status	O Success	
Protected VMs Settings Alarms	Post-script Execution Status	Not defined	
+ Start Protection			
VM Name A		~	ackground Data 🔺 Details
GCS-DR-SC45		14	8 Details
GCS-DR-SOL03			D Datails
GCSDR-W2K16-01			8 Details
UbuntuSrv001			B Detain

- 4. Sobald die Virtual Machines wiederhergestellt sind, wird Disaster Recovery für Storage auf dem Gast-Storage eingesetzt. Um diesen Prozess zu demonstrieren, wird SQL-Server in diesem Beispiel verwendet.
- 5. Melden Sie sich bei der wiederhergestellten SnapCenter-VM auf dem AVS SDDC an und aktivieren Sie den DR-Modus.
 - a. Greifen Sie über Browsern auf die SnapCenter-Benutzeroberfläche zu.

https://gcs-dr-sc46.gcsdc.com:8146/ D	- ≞× O gcs-dr-	-sc46.gcsdc.com ×
		etApp。。
Res _	SnapCente	er®
	Username	gcsdc\adminnimo
	Password	•••••
		Sign In

- b. Navigieren Sie auf der Seite Einstellungen zu Einstellungen > Globale Einstellungen > Disaster Recovery.
- c. Wählen Sie Disaster Recovery Aktivieren.
- d. Klicken Sie Auf Anwenden.

	letApp SnapC	enter®						•	-	9 -	SnapCenterAdmin	Sign Out
<		Global Settings	Policies	Users and Access	Roles	Credential	Software					
	Dashboard											
9	Resources	Global Settings	9									
۲	Monitor											
M	Reports	Hypervisor Settin	g1 0									~
	Hosts	Notification Serv	er Settings	0		0.0	r.					~
ł.	Storage Systems	Configuration Se	ttings 😗									~
華	Settings	Purge jobs Settin	gs O									~
▲	Alerts	Domain Settings	0									~
		CA Certificate Set	tings 🕕									~
		Disaster Recover										

e. Überprüfen Sie, ob der DR-Job aktiviert ist, indem Sie auf Überwachen > Jobs klicken.



Für das Storage Disaster Recovery sollte NetApp SnapCenter 4.6 oder höher verwendet werden. Frühere Versionen sollten applikationskonsistente Snapshots (replizierte mit SnapMirror) verwenden und ein manuelles Recovery ausführen, falls frühere Backups am Disaster Recovery-Standort wiederhergestellt werden müssen.

6. Stellen Sie sicher, dass die SnapMirror Beziehung beschädigt ist.

Canvas	Replication	Backup & Restore	Data Sense	File Cache	Compute	Sync All Service	rs (+9) ~			
Repli	cation									
		J Volume Re	lationships	9 4.78 Replicate	GiB d Capacity	0 Currently Tran	isterring	⊙ 3 Healthy	⊗ 0 Failed	
		3 Volume Relationships								٩٥
		Health Status 🗧	Source Volume	s Target V	olume a	ार्च्य Total Transfer Time ः	Status 🗟	Mirror State	E Lust Successful Transfer	0
		Ø	gcsdrsqldb_sc46 ntaphci-a300e9u25	gcsdrsql ANFCVO	fb_sc46_copy DRDemo	6 minutes 41 seconds	idle	broken-off	May 5, 2022, 12:08:34 PN 33.66 KiB	
		\odot	gcsdrsqlhld_sc46 ntaphci-a300e9u25	gcsdrsql ANFCVO	1ld_sc46_copy ORDemo	4 minutes 56 seconds	idle	broken-off	May 5, 2022, 12:09:15 PM 69.84 KiB	
		\odot	gcsdrsqllog_sc46 ntaphci-a300e9u25	gcsdrsq8 ANFCVD	og_sc46_copy DRDemo	10 minutes 18 seconds	idie	broken-aff	May 5. 2022, 12:08:34 PN 104.34 KiB	

7. Verbinden Sie die LUN aus Cloud Volumes ONTAP mit der wiederhergestellten SQL Gast-VM mit gleichen Laufwerksbuchstaben.

📅 Disk Managemer	nt						5 -1 3	×
File Action View	v Help							
🗢 🏟 🗊 👔 t	m 🗩 🕑 (F						
Volume	Layout	Туре	File System	Status	Capacity	Free Spa	% Free	
-	Simple	Basic	1 contract Contraction	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. Öffnen Sie den iSCSI-Initiator, löschen Sie die vorherige getrennte Sitzung und fügen Sie das neue Ziel zusammen mit Multipath für die replizierten Cloud Volumes ONTAP Volumes hinzu.

Targets	Discovery	Favorite Targets	Volumes and Devices	RADIUS	Configuration
Quick (Connect				
DNS na	ame of the ta	arget and then dick	Quick Connect.	Q	Jick Connect
Discourse					
Discove	ered targets				Refresh
Discove	ered targets			Status	Refresh
Name	ered targets	netapp:sn.547772c	cc47811ecbb62000	Status Connecte	Refresh d

9. Stellen Sie sicher, dass alle Laufwerke mit denselben Laufwerksbuchstaben verbunden sind, die vor DR verwendet wurden.



10. Starten Sie den MSSQL-Serverdienst neu.

rices (Local)	Services (Local)					_	
	SQL Server (MSSQLSERVER)	Name	Description	Statu	JS	Startup Type	Log
	10 million (10 mil	🖏 SQL Full-text Filter Daemon	Service to la	Runn	ning	Manual	NT
	Stop the service	SQL Server (MSSQLSERVER)	Provider rto	Rung	ning	Automatic	GCS
	Restart the service	SQL Server Agent (MSS)	Start	1	ning	Automatic	GCS
		SQL Server Browser	Stop	7	ning	Automatic	Loc
	Description	Q SQL Server CEIP service	Pause	if.	ning	Automatic	NT
	Provides storage, processing and	SQL Server Integration S	Resume	1	ning	Automatic	NT
	controlled access of data, and rapid	Q SQL Server Integration S	Restart	1	ning	Automatic	NT
	transaction processing.	SQL Server VSS Writer		1	ning	Automatic	Loc
		SSDP Discovery	All Tasks	>	ning	Manual	Loc
		State Repository Service	Refresh	1	ning	Manual	Loc
		Starsan Service	Descention			Manual Manual /Trin	Loc
		Storage Tierr Managem	rioperues			Manual (mg	Loc
		Superfetch	Help			Manual	Loc
		Sync Host df83a	This service	Runn	nina	Automatic (D	Loc
		System Event Notification S	Monitors sv	Runn	ning	Automatic	Loc v
		<					>

11. Stellen Sie sicher, dass die SQL-Ressourcen wieder online sind.



i.

Hängen Sie im Fall von NFS die Volumes mit dem Mount-Befehl an, und aktualisieren Sie die /etc/fstab Einträge.

An diesem Punkt können Betriebsabläufe ausgeführt werden und der Geschäftsbetrieb normal weiterläuft.



Am NSX-T-Ende kann ein separates, dediziertes Tier-1 Gateway zur Simulation von Failover-Szenarien erstellt werden. So ist sichergestellt, dass alle Workloads miteinander kommunizieren können, dass jedoch kein Traffic in die bzw. aus der Umgebung geleitet werden kann. So können alle Triage-, Containment- oder Härteaufgaben ohne das Risiko einer Kreuzkontamination durchgeführt werden. Dieser Vorgang ist außerhalb des Anwendungsbereichs dieses Dokuments, kann aber problemlos zur Simulation der Isolation durchgeführt werden.

Wenn der primäre Standort wieder in Betrieb ist, können Sie ein Failback durchführen. Die VM-Sicherung wird durch Jetstream fortgesetzt, und die SnapMirror Beziehung muss umgekehrt werden.

- Wiederherstellung der lokalen Umgebung Je nach Art des Notfalleinfalls sind möglicherweise die Wiederherstellung und/oder Überprüfung der Konfiguration des geschützten Clusters erforderlich. Falls erforderlich, muss die JetStream DR-Software möglicherweise erneut installiert werden.
- Greifen Sie auf die wiederhergestellte On-Premises-Umgebung zu, rufen Sie die Jetstream DR UI auf und wählen Sie die entsprechende geschützte Domäne aus. Nachdem der geschützte Standort für Failback bereit ist, wählen Sie die Failback-Option in der UI aus.



Mit dem CPT-generierten Failback-Plan kann außerdem die Rückgabe der VMs und ihrer Daten aus dem Objektspeicher in die ursprüngliche VMware Umgebung initiiert werden.

Protected Domains Statistics Storage Sites	Appliances 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		O Resume Continuous R	ehydration
Recoverable / Total VMs	4/4	Owner Site	REMOTE (172.3	+ Failback	
rotected VMs Settings Alarms	0 0				1
rotected VMs Settings Alarms	O O Protection Status		Protection Mode	Details	C
rolected VMs Settings Alarms	O O Protection Status © Recoverable		Protection Mode 🔺 Write-Back(VIMDK)	Details Details	a
rolected VMs Settings Alarms VM Name ▲ GCS-DR-LinVM01	O O Protection Status		Protection Mode ▲ Write-Back(MDK) Write-Back(VMDK)	Details Details Details	Q
rotected VMs Settings Alarms VM Name ▲ GCS-DR-DC GCS-DR-LinVM01 GCS-DR-SCA	O O Protection Status Protection Status Protection Status Protection Status Protection Status Protection Status		Protection Mode ▲ Write-Back(MDK) Write-Back(VMDK) Write-Back(VMDK)	Details Details Details Details	q
Trotected VMs Settings Alarms VM Name ▲ GCS-DR-LC GCS-DR-LinVM01 GCS-DR-SCA GCS-DR-SOL01	Protection Status Protection Status Recoverable Recoverable Recoverable Recoverable		Protection Mode ▲ Write-Back(VMDK) Write-Back(VMDK) Write-Back(VMDK) Write-Back(VMDK)	Details Details Details Details Details	Q

Geben Sie die maximale Verzögerung an, nachdem Sie die VMs am Recovery-Standort angehalten und am geschützten Standort neu gestartet haben. Die zum Abschluss dieses Prozesses erforderliche Zeit umfasst das Abschließen der Replizierung nach dem Stoppen von Failover-VMs, die zum Reinigen des Recovery-Standorts benötigte Zeit und die Zeit zur Wiederherstellung von VMs am geschützten Standort. NetApp empfiehlt 10 Minuten.

•		•	•			0
1. General	2a. Failback Settings	2b. VM Settings	3. Recovery VA	4. D	R Settings	5. Summary
Failback Da	itacenter		A300-DataCenter			
Failback Cl	uster		A300-Cluster			
Failback Re	source Pool		*			
VM Folder (Optional)					
Failback Da	itastore		A300_NFS_vMotion	1		
Maximum D	elay After Stopping		10 Minutes			
Internal Ret	work		VM_187			
External Re	plication Network		VM_187			
Manageme	nt Network		VM_187			
Storage Sit	e		ANFCVODR			
DR Virtual	Appliance		GCSDRVA002			
Replication	Log Storage		/dev/sdb			

3. Schließen Sie den Failback-Prozess ab, und bestätigen Sie anschließend die Wiederaufnahme des VM-Schutzes und der Datenkonsistenz.

(i)

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	Success	
Demaining Background Data	Total VMs Recovered	4	
Containing Procession of Conta	GCSRecovery03 Status:		
Current RPO	Pre-script Execution Status	Not defined	
	Runbook Execution Status	Success	
Protected VMs Settings Alarms	Post-script Execution Status	O Not defined	3

4. Nachdem die VMs wiederhergestellt wurden, trennen Sie den sekundären Storage vom Host und stellen eine Verbindung zum primären Storage her.

Health Status 🔅	Source Volume	191	Target Volume	91	Total Transfer Time 💠	Status	÷.	Mirror State	Ś.	Last Successful Transfer	
\odot	gcsdrsqldb_sc46 ntaphci-a300e9u25	14	gcsdrsqldb_sc46_copy ANFCVODRDemo		6 minutes 41 seconds	idle		broken-off		May 5. 2022. 12:08:34 PN 33.66 KiB	(
\odot	gcsdrsqlhld_sc46 ntaphci-a300e9u25		gcsdrsqlhld_sc46_copy ANFCVODRDemo		4 minutes 56 seconds	idle		broken-off		Information	
Ø	gcsdrsqllog_sc46 ntaphci=a300e9u25	(4)	gcsdrsqllog_sc46_copy ANFCVODRDemo	•	10 minutes 18 seconds	idle		broken-off		Resync Reverse Resync	
										Edit Schedule	
										Edit Max Transfer Rate	
										Delete	
3 Volume Re	lationships	Þ	6.54 GIB Replicated Capacity		0 Currently Trans	ferring	0	3 Healthy		€ O Failed	
J Volume Re	lationships	<u>م</u>	6.54 GIB Replicated Capacity		O Currently Trans	ferring	C	3 Healthy		O Failed	
Unter Relationships	lationships	₽	6.54 GIB Replicated Capacity Target Volume	*	O Currently Transl O Currently Transl O O O Total Transfer Time :	ferring	Ţ.	3 Healthy	*	Derece O Failed Last Successful Transfer	
Volume Re ume Relationships Health Status	Iationships Source Volume gcsdrsqldb_sc46 ntaphci-a300e9u25	•	6.54 GIB Replicated Capacity Target Volume gcsdrsqldb_sc46_copy ANFCVODRDemo	÷	O Currently Trans O Total Transfer Time + 19 seconds	ferring Status idle	₹	Mirror State	÷	Last Successful Transfer May 6, 2022, 11:03:00 AA 5.73 MIB.	
Volume Relationships	lationships Source Volume gcsdrsqldb_sc46 ntaphcl-a300e9u25 gcsdrsqlhld_sc46_copy ANFCVODRDemo	•	6.54 GIB Replicated Capacity Target Volume gcsdrsqldb_sc46_copy ANFCVODRDemo	•	O Currently Trans O Total Transfer Time : 19 seconds 1 minute 46 seconds	ferring Grant Control	€	Mirror State snapmirrored	•]	Derece 0 Failed Failed Last Successful Transfer May 6, 2022, 11:03:00 MA 5.73 MiB May 6, 2022, 11:01:39 AA May 6, 2022, 11:01:39 AA 800.76 MiB	

- 5. Starten Sie den MSSQL-Serverdienst neu.
- 6. Vergewissern Sie sich, dass die SQL-Ressourcen wieder online sind.



Für ein Failback auf den primären Storage sollten Sie sicherstellen, dass die Beziehungsrichtung vor dem Failover unverändert bleibt, indem Sie einen umgekehrten Resynchronisierungsvorgang durchführen.



i .

Um die Rollen des primären und sekundären Storage nach der umgekehrten Resynchronisierung beizubehalten, führen Sie den umgekehrten Resync-Vorgang erneut aus.

Dieser Prozess gilt für andere Applikationen wie Oracle, ähnliche Datenbankumgebungen und andere Applikationen, die mit Gast-vernetztem Storage verwenden.

Testen Sie wie immer die Schritte zur Wiederherstellung der kritischen Workloads, bevor Sie sie in die Produktionsumgebung portieren.

Vorteile dieser Lösung

- Nutzt die effiziente und ausfallsichere Replizierung von SnapMirror
- · Wiederherstellung zu beliebigen verfügbaren Zeitpunkten mit ONTAP Snapshot Aufbewahrung
- Eine vollständige Automatisierung steht für alle erforderlichen Schritte zur Wiederherstellung von Hunderten bis Tausenden von VMs zur Verfügung von den Schritten für Storage, Computing, Netzwerk und Applikationen.
- SnapCenter nutzt Klonmechanismen, die das replizierte Volume nicht ändern.
 - So wird das Risiko einer Beschädigung von Daten von Volumes und Snapshots vermieden.

- · Keine Replizierungsunterbrechungen während der DR-Test-Workflows
- Nutzung der DR-Daten f
 ür Workflows
 über DR hinaus, wie Entwicklung/Test, Sicherheitstests, Patchund Upgrade-Tests und Korrekturtests
- CPU- und RAM-Optimierung können die Cloud-Kosten senken, indem Recovery auf kleinere Computing-Cluster ermöglicht wird.

TR-4955: Disaster Recovery with Azure NetApp Files (ANF) and Azure VMware Solution (AVS)

Autor(en): Niyaz Mohamed, NetApp Solutions Engineering

Überblick

Disaster Recovery mit Replizierung auf Blockebene zwischen Regionen in der Cloud ist eine ausfallsichere und kostengünstige Möglichkeit, um Workloads vor Standortausfällen und Datenbeschädigung (z. B. Ransomware) zu schützen. Mit der regionsübergreifenden Volume-Replizierung über Azure NetApp Files (ANF) können VMware-Workloads, die auf einem AVS-Standort (Azure VMware Solution) mit Azure NetApp Files Volumes als NFS-Datastore auf dem primären AVS-Standort ausgeführt werden, auf einen designierten sekundären AVS-Standort in der Zielwiederherstellungsregion repliziert werden.

Disaster Recovery Orchestrator (DRO) (eine skriptbasierte Lösung mit einer Benutzeroberfläche) kann verwendet werden, um Workloads, die von einem AVS-SDDC zum anderen repliziert werden, nahtlos wiederherzustellen. DRO automatisiert die Recovery, indem Replikations-Peering gebrochen und das Ziel-Volume dann als Datastore gemountet wird. Dies geschieht durch VM-Registrierung in AVS, um Netzwerkzuordnungen direkt auf NSX-T (in allen AVS Private Clouds enthalten) zu ermöglichen.



Voraussetzungen und allgemeine Empfehlungen

- Vergewissern Sie sich, dass Sie die regionsübergreifende Replikation aktiviert haben, indem Sie Replikations-Peering erstellen. Siehe "Volume-Replizierung für Azure NetApp Files erstellen".
- Sie müssen ExpressRoute Global Reach zwischen den Private Clouds der Quell- und Ziellösung von Azure VMware konfigurieren.
- Sie müssen über einen Dienstprinzipal verfügen, der auf Ressourcen zugreifen kann.
- Die folgende Topologie wird unterstützt: Primärer AVS-Standort zum sekundären AVS-Standort.
- Konfigurieren Sie die "Replizierung" Planen Sie für jedes Volume entsprechend den Geschäftsanforderungen und der Datenänderungsrate ein.



Kaskadierung und Fan-in- und Fan-out-Topologien werden nicht unterstützt.

Erste Schritte

Implementieren Sie die Azure-VMware-Lösung

Der "Azure VMware Lösung" (AVS) ist ein Hybrid-Cloud-Service mit voll funktionsfähigen VMware SDDCs in einer Microsoft Azure Public Cloud. AVS ist eine Lösung eines Erstanbieters, die vollständig von Microsoft verwaltet und unterstützt wird und von VMware überprüft wurde, die eine Azure-Infrastruktur nutzt. Daher erhalten Kunden VMware ESXi für die Compute-Virtualisierung, vSAN für hyperkonvergenten Storage und NSX für Netzwerk und Sicherheit. Gleichzeitig profitieren sie von der globalen Präsenz und den erstklassigen Datacenter-Einrichtungen von Microsoft Azure sowie der Nähe zum umfassenden Ecosystem nativer Azure-Services und -Lösungen. Eine Kombination aus Azure VMware Solution SDDC und Azure NetApp Files bietet die beste Performance bei minimaler Netzwerklatenz.

Gehen Sie wie folgt vor, um eine AVS Private Cloud auf Azure zu konfigurieren "Verlinken" Zu NetApp-Dokumentation und in diesem "Verlinken" Für Microsoft-Dokumentation. Für DR-Zwecke kann eine Pilotumgebung mit minimaler Konfiguration verwendet werden. Dieses Setup enthält nur Kernkomponenten zur Unterstützung kritischer Applikationen. Es kann horizontal skalierbar sein und weitere Hosts aufbauen, um den Großteil der Auslastung bei einem Failover zu übernehmen.



In der ersten Version unterstützt DRO einen vorhandenen AVS SDDC-Cluster. Die Erstellung eines On-Demand SDDC wird in einer kommenden Version verfügbar sein.

Bereitstellung und Konfiguration von Azure NetApp Files

"Azure NetApp Dateien" Der hochperformante gemessene File-Storage-Service der Enterprise-Klasse. Befolgen Sie die hier beschriebenen Schritte "Verlinken" Die Bereitstellung und Konfiguration von Azure NetApp Files als NFS-Datastore zur Optimierung von AVS Private-Cloud-Implementierungen.

Volume-Replizierung für Datastore-Volumes mit Azure NetApp Files erstellen

Der erste Schritt besteht darin, regionsübergreifende Replikation für die gewünschten Datastore Volumes vom primären AVS-Standort zum sekundären AVS-Standort mit den entsprechenden Frequenzen und Aufbewahrungen einzurichten.

Home > Azure NetApp Files > WEANFAVSacct | Volumes > testrepIdemo (WEANFAVSacct/testcap/test testrepIdemo (WEANFAVSacct/testcap/testrepIdemo) | Replication * × 1 Search 🕐 Refresh ∧ Essentials JSON View 📅 🗏 Overview Activity log End point type : Source Destination : testrepidemo.copy Health status : Healthy Relationship status : Idle Access control (IAM) Mirror state : Mirrored Total progress : 2.13 GiB Tags

Befolgen Sie die hier beschriebenen Schritte "Verlinken" Zur Einrichtung einer regionsübergreifenden Replikation durch Erstellen von Replikations-Peering. Das Service-Level für den Zielkapazitätspool kann mit dem des Quell-Kapazitäts-Pools übereinstimmen. Für diesen speziellen Anwendungsfall können Sie jedoch das Standard-Service-Level und dann auswählen "Ändern Sie den Service-Level" Im Falle einer echten Katastrophe oder DR-Simulationen.



Eine regionsübergreifende Replikationsbeziehung ist Voraussetzung und muss zuvor erstellt werden.

DRO-Installation

Um mit DRO zu beginnen, verwenden Sie das Ubuntu-Betriebssystem auf der zugewiesenen virtuellen Azure-Maschine und stellen Sie sicher, dass Sie die Voraussetzungen erfüllen. Installieren Sie dann das Paket.

Voraussetzungen:

- Dienstprinzipal, das auf Ressourcen zugreifen kann.
- Stellen Sie sicher, dass entsprechende Konnektivität mit den SDDC Quell- und Ziel-Instanzen und den Azure NetApp Files Instanzen besteht.
- DNS-Auflösung sollte vorhanden sein, wenn Sie DNS-Namen verwenden. Verwenden Sie andernfalls die IP-Adressen für vCenter.

OS-Anforderungen:

- Ubuntu Focal 20.04 (LTS)die folgenden Pakete müssen auf der zugewiesenen virtuellen Agent-Maschine installiert werden:
- Docker
- Docker Komposition
- JqChange docker.sock Zu dieser neuen Berechtigung: sudo chmod 666 /var/run/docker.sock.



Der deploy.sh Skript führt alle erforderlichen Voraussetzungen aus.

Dies sind die Schritte:

1. Laden Sie das Installationspaket auf der angegebenen virtuellen Maschine herunter:

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



Der Agent muss in der sekundären AVS-Standortregion oder in der primären AVS-Standortregion in einer separaten AZ als dem SDDC installiert werden. 2. Entpacken Sie das Paket, führen Sie das Bereitstellungsskript aus, und geben Sie die Host-IP ein (z. B. 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. Greifen Sie mit den folgenden Anmeldedaten auf die UI zu:
 - Benutzername: admin
 - Kennwort: admin

NetApp	
Disaster Recovery Orchestrator Singlet Source with Guil Username	
Paissond	
toppin .	
	and the second sec

DRO-Konfiguration

Nachdem Azure NetApp Files und AVS ordnungsgemäß konfiguriert wurden, können Sie mit der Konfiguration von DRO beginnen, um die Wiederherstellung von Workloads vom primären AVS-Standort zum sekundären AVS-Standort zu automatisieren. NetApp empfiehlt, den DRO-Agent am sekundären AVS-Standort bereitzustellen und die ExpressRoute Gateway-Verbindung zu konfigurieren, damit der DRO-Agent über das Netzwerk mit den entsprechenden AVS- und Azure NetApp Files-Komponenten kommunizieren kann.

Der erste Schritt besteht darin, Anmeldeinformationen hinzuzufügen. FÜR DIE Erkennung von Azure NetApp Files und der Azure VMware-Lösung ist DIE DRO-Berechtigung erforderlich. Sie können einem Azure-Konto die erforderlichen Berechtigungen erteilen, indem Sie eine Azure Active Directory (AD)-Anwendung erstellen und einrichten und die Azure-Anmeldeinformationen erhalten, die DRO benötigt. Sie müssen den Service-Prinzipal an Ihr Azure-Abonnement binden und ihm eine benutzerdefinierte Rolle zuweisen, die über die entsprechenden erforderlichen Berechtigungen verfügt. Wenn Sie Quell- und Zielumgebungen hinzufügen, werden Sie aufgefordert, die Anmeldeinformationen auszuwählen, die dem Dienstprinzipal zugeordnet sind. Sie müssen diese Anmeldeinformationen zu DRO hinzufügen, bevor Sie auf Neuen Standort hinzufügen klicken können.

Um diesen Vorgang auszuführen, führen Sie die folgenden Schritte aus:

- 1. Öffnen Sie DRO in einem unterstützten Browser und verwenden Sie den Standardbenutzernamen und das Standardpasswort /admin/admin). Das Passwort kann nach der ersten Anmeldung mit der Option Passwort ändern zurückgesetzt werden.
- 2. Klicken Sie oben rechts auf der DRO-Konsole auf das Symbol **Einstellungen** und wählen Sie **Anmeldeinformationen** aus.
- 3. Klicken Sie auf Neue Anmeldedaten hinzufügen, und befolgen Sie die Schritte im Assistenten.
- 4. Geben Sie zum Definieren der Anmeldeinformationen Informationen über den Azure Active Directory-Dienstprinzipal ein, der die erforderlichen Berechtigungen gewährt:
 - Name der Anmeldeinformationen
 - Mandanten-ID
 - Client-ID
 - · Kundengeheimnis
 - · Abonnement-ID

Sie sollten diese Informationen bei der Erstellung der AD-Anwendung erfasst haben.

5. Bestätigen Sie die Details zu den neuen Anmeldeinformationen, und klicken Sie auf Credential hinzufügen.

NetApp Disaster Recovery Orchestrator 💊 Dashbo	ard Discover Resource Groups Replication Plans Job Monitoring	4 0 0 🗅
Add New Credential	Credentials Details	×
	Enter Credentials Details	
	Credential Name	
	Tenant Id	
	Client Id	
	Client Secret	
	Subscription Id	
	Add Credential	

Nachdem Sie die Anmeldedaten hinzugefügt haben, wird es Zeit, den primären und sekundären AVS-Standort (sowohl vCenter als auch das Azure NetApp Files-Speicherkonto) zu ermitteln und zu DRO hinzuzufügen. Gehen Sie wie folgt vor, um den Quell- und Zielstandort hinzuzufügen:

- 6. Gehen Sie auf die Registerkarte Entdecken.
- 7. Klicken Sie Auf Neue Site Hinzufügen.
- 8. Fügen Sie den folgenden primären AVS-Standort hinzu (in der Konsole als Quelle bezeichnet).
 - SDDC vCenter
 - Azure NetApp Files Storage Konto
- 9. Fügen Sie den folgenden sekundären AVS-Standort hinzu (in der Konsole als Ziel bezeichnet).

- SDDC vCenter
- Azure NetApp Files Storage Konto

NetApp Disaster Recovery Orchestrator A Dashboard Discover Resource Groups Replication Plans Job Monitoring	٥	?	9
Add New Site Of Site Type (2) Site Details (3) vCenter Details (3) storage Details			×
Site Type			
Source Destination			
Continue			

10. Fügen Sie Standortdetails hinzu, indem Sie auf **Quelle** klicken und einen freundlichen Standortnamen eingeben und den Konnektor auswählen. Klicken Sie dann auf **Weiter**.



Das Hinzufügen einer Quellwebsite wird zu Demonstrationszwecken in diesem Dokument behandelt.

- 11. Aktualisieren Sie die vCenter-Details. Wählen Sie dazu die Anmeldedaten, die Azure-Region und die Ressourcengruppe aus der Dropdown-Liste für das primäre AVS-SDDC aus.
- 12. DRO listet alle verfügbaren SDDCs innerhalb der Region auf. Wählen Sie die entsprechende Private-Cloud-URL aus der Dropdown-Liste aus.
- 13. Geben Sie das ein cloudadmin@vsphere.local Benutzeranmeldeinformationen. Auf diese kann über das Azure-Portal zugegriffen werden. Befolgen Sie die hier beschriebenen Schritte "Verlinken". Klicken Sie anschließend auf Weiter.

Add New Site	🕑 Site Type () Site Details (3) vCenter Details (4)	Storage Details	
		Source AVS Private Cloud		
	Select Credentials	Azure Region	Azure Resource Group	
	DemoCred -	West Europe 👻	ANFAVSVal2 +	
	Add New Credential (2			
		AVS Details		
	Web Clien	URL		
		ANFDataClus	·	
	Username		0	
	cloudad	min@vsphere.local		
	Password			
		•••••		
		Accept self-signed certificates		

- 14. Wählen Sie die Details zum Quell-Storge (ANF) aus, indem Sie die Azure Ressourcengruppe und das NetApp Konto auswählen.
- 15. Klicken Sie Auf **Site Erstellen**.

op Dis	saster Recovery Orchestrator 💊 🛛	Dashboard Discover Resource	e Groups Replication Plans	Job Monitoring			¢
	C 2	2 Centers 2 Storages	Site Type	1 Destination	Site Location 0 On Prem	Cloud.	
2	2 Sites					Q O Add New Site	
	Site Name	‡ Site Type 🖙 Lo	ocation 🔤 🛛 vCenter 🗘 🛛	Storage 😂 VM List	Discovery Status	Û.	
	DemoDest	Destination C	loud 1	1	 https://10.75.0.2/ 	⊘ Success	
	DemoSRC	Source C	loud 1	1 View VM List	• https://172.30.156.2/	⊘ Success	

Nach dem Hinzufügen führt DRO eine automatische Erkennung durch und zeigt die VMs an, die entsprechende regionsübergreifende Replikate vom Quellstandort zum Zielstandort haben. DRO erkennt automatisch die Netzwerke und Segmente, die von den VMs verwendet werden, und füllt diese aus.

tApp	Disaster Recovery Orchestrator	Deshboard Discover R	eseverce Groups Replication Plans Job	Monitoring			3
	Back						
			VM List Site: DemoSRC vCenter: https://172	30.156.2/			
	-			VM Protection			
	Cotas	tores	128 Virtual Machines	🧭 2 Protected	0 126 Unproteite	e	
	128 vm				٩	Create Resource Group	
	VM Name	2 We Status	1 VM State	Detatore	21 OV	C Memory (MD) C	
	HD5enth_251	O Not Protected	() Powered Cn	vianDatastore	8	8192	
	hci-fio-datastore-13984-0-1	0 Not Protected	Powesett Off	HCRstDS	я	65536	
	ICCA2005-WO-R1	O Not Protected	(b) Powered On	vianDataitose	8	14336	
	ICCA2005-NE-R1	0 Not Protected	() Powered On	vsanDataitore	1	3072	
	10CA2505-01-81	0 Not Protected	() Powered On	vianDatastiore	5	3072	
	HCX_Demo_05	9 Not Protected	Powered Dft	Demo002	1	2041	
	hci-nim-datastore-13964-0-1	0 Not Protected	() Fowered Off	HCItyIDS	24	49152	

Im nächsten Schritt werden die erforderlichen VMs als Ressourcengruppen in ihre funktionalen Gruppen gruppiert.

Ressourcen-Gruppierungen

Nachdem die Plattformen hinzugefügt wurden, gruppieren Sie die VMs, die Sie wiederherstellen möchten, in Ressourcengruppen. MIT DRO-Ressourcengruppen können Sie eine Gruppe abhängiger VMs zu logischen Gruppen gruppieren, die ihre Boot-Aufträge, Boot-Verzögerungen und optionale Applikationsvalidierungen enthalten, die bei der Wiederherstellung ausgeführt werden können.

Um Ressourcengruppen zu erstellen, klicken Sie auf den Menüpunkt Neue Ressourcengruppe erstellen.

1. Greifen Sie auf **Resource Grou*ps zu und klicken Sie auf *Neue Ressourcengruppe erstellen**.

🖬 NetApp	Disaster Recovery Orchestrator 💊	Dashboard Discover Resource Groups	Replication Plans Job Monitoring	٨	¢ ? ©
	Resource Group	C 1 Site	P 1 vCenter	2 Virtual Machines	
	1 Resource Group			Create New Resource Group	
	Resource Group Name	\$ Site Name		≂ i vM list i	
	DemoRG	DemoSRC	https://172.30.156.2/	View VM List	

- 2. Wählen Sie unter Neue Ressourcengruppe den Quellstandort aus dem Dropdown-Menü aus und klicken Sie auf **Erstellen**.
- 3. Geben Sie die Details der Ressourcengruppe ein und klicken Sie auf Weiter.
- 4. Wählen Sie über die Suchoption die entsprechenden VMs aus.
- 5. Wählen Sie für alle ausgewählten VMs die Optionen Boot Order und Boot Delay (s) aus. Legen Sie die Reihenfolge der Einschaltsequenz fest, indem Sie jede virtuelle Maschine auswählen und die Priorität für sie festlegen. Der Standardwert für alle virtuellen Maschinen ist 3. Folgende Optionen stehen zur Verfügung:

- · Die erste virtuelle Maschine, die eingeschaltet wird
- Standard
- · Die letzte virtuelle Maschine, die eingeschaltet werden muss

NetApp Disaster Recovery Orchestrator 🔌	Dashboard Disco		Replication Plans	Job Monitoring			¢ 0	9
Edit Resource Group		Resource Group Deta	ails 🕜 Select VMs	s 🚯 Boot order	and Delay			×
			Boot order an	d Delay				
	VM Name	Boot Order 💿		Boot Delay	(secs)			
	QALin1	3	12	0	12			
	QALin	3	10	0	[2]			

6. Klicken Sie Auf Ressourcengruppe Erstellen.

n NetApp	Disaster Recovery Orchestrator 💊 📔 D	ashboard Discover Resource G	roups Replication Plans Job Monitoring	A 3	¢ ? 2
	☑ 1		1 🔐 1	a 2	
	1 Resource Group		sne – v.enter	Q O Create New Resource Group	
	Resource Group Name	C Site Name	⇒ Source vCenter	≂ VM List	
	DemoRG	DemoSRC	https://172.30.156.2/	View VM List	

Replizierungspläne

Die Wiederherstellung von Applikationen im K-Fall ist unverzichtbar. Wählen Sie in der Dropdown-Liste die Quell- und Ziel-vCenter-Plattformen aus und wählen Sie die Ressourcengruppen aus, die in diesen Plan aufgenommen werden sollen. Außerdem berücksichtigen Sie die Gruppierung der wiederherzustellenden und hochzusteuenden Applikationen (z. B. Domain Controller, Tier-1, Tier-2 usw.). Pläne werden oft auch Blaupausen genannt. Um den Wiederherstellungsplan zu definieren, navigieren Sie zur Registerkarte Replikationsplan und klicken Sie auf **Neuer Replikationsplan**.

Gehen Sie wie folgt vor, um mit der Erstellung eines Replikationsplans zu beginnen:

1. Navigieren Sie zu **Replikationspläne** und klicken Sie auf **Neuen Replikationsplan erstellen**.

NetApp	Disaster Recovery	Orchestrator 💊 🕴 Dash	board Discover Resource C	iroups Replication Plans	Job Monitoring				•	?	(
	e 1		1	Source Details	<i>.</i>	Destination	Details	<i>.</i>			
	Rej	plication Plans	Resource Groups	Sites	vCenters	Sites		vCenters			
	1 Replication Plan						Q 9	Create New Replication Plan			
	Plan Name	C Active Site	Status	Compliance	Source Site		91	i i			
	DemoRP	⊘ Source	⊘ Active	Partially Healthy	DemoSRC	DemoDest	Res	ource Groups			

 Geben Sie im New Replication Plan einen Namen f
ür den Plan ein und f
ügen Sie Wiederherstellungszuordnungen hinzu, indem Sie den Quellstandort, das zugeh
örige vCenter, den Zielstandort und das zugeh
örige vCenter ausw
ählen.

NetApp Disaster Recovery Orchestrator	Dashboard Discover Resource Groups Replication	Plans Job Monitoring	4	٠	?	9
Create New Replication Plan	Replication Plan and Site Details (2) Select Resour	te Groups ③ Set Execution Order ④ Set VM Details				×
	Replicatio	n Plan Details				
	Plan Name	0				
	DemoRP					
	Recove	y Mapping				
	Source Site	Destination Site				
	DemoSRC +	DemoDest ~				
	Source vCenter	Destination vCenter 0				
	https://172.30.156.2/ ~	https://10.75.0.2/ +				
	Cluste	Mapping				
	Source Site Resource Destinat	ion Site Resource				
	Cluster-1	Cluster-1 + Add				
			6			
	Source Resource Destin	ation Resource				
	No Map	pings added!				
		Continue				

3. Nachdem die Wiederherstellungszuordnung abgeschlossen ist, wählen Sie die Option **Cluster Mapping** aus.

NetApp Disaster Recovery Orchestrator	Dashboard Discover Resource	Groups Replication Pla	ns Job Monitoring		â ở 9 Q
Create New Replication Plan	Replication Plan and Site Detail	s (2) Select Resource G	roups ③ Set Execution Order ④ Set VM Deta	ils	×
		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	/ *	https://10.75.0.2/	*	
		Cluster	Mapping		
	No mor	e Source/Destination clust	er resources available for mapping		
	Source Resource	Destination Re	source		
	Cluster-1	Cluster-1	Delete		
	È				
		Con	inue -		

- 4. Wählen Sie **Ressourcengruppendetails** und klicken Sie auf **Weiter**.
- 5. Legen Sie die Ausführungsreihenfolge für die Ressourcengruppe fest. Mit dieser Option können Sie die Reihenfolge der Vorgänge auswählen, wenn mehrere Ressourcengruppen vorhanden sind.
- 6. Stellen Sie anschließend die Netzwerkzuordnung auf das entsprechende Segment ein. Die Segmente sollten bereits auf dem sekundären AVS-Cluster bereitgestellt werden. Um die VMs diesen zuzuordnen, wählen Sie das entsprechende Segment aus.
- 7. Aufgrund der Auswahl der VMs werden automatisch Datastore-Zuordnungen ausgewählt.



Die regionsübergreifende Replikation (CRR) befindet sich auf Volume-Ebene. Daher werden alle VMs auf dem jeweiligen Volume auf das CRR-Ziel repliziert. Stellen Sie sicher, dass alle VMs ausgewählt werden, die Teil des Datenspeichers sind, da nur virtuelle Maschinen verarbeitet werden, die Teil des Replikationsplans sind.

NetApp Disaster Recovery Orchestrator	Dashboard Discover Resource	Groups Replication Plans Job	Monitoring			۵	?	۹
Create New Replication Plan	Replication Plan and Site Details	Select Resource Groups	Set Execution Order	(4) Set VM Details				×
		Replication Plan De	tails					
		Select Execution Ord	er					
	Resource Group Name		Execution Order	D				
	DemoRG		3					
		Notwork Mapping			1			
	No more	Source/Destination network resource	s available for mappi	ng				
	Source Resource	Destination Resource						
	SepSeg	SegDR		Delete				
	-	DataStore Mapping)		1			
	Source DataStore	Destination Volume						
	TestSrc01	gwc_ntap_acct/gwc_DRO_cp/testsr	c01copy					
		Previous Cont	ínue					

8. Unter VM-Details können Sie optional die Größe der CPU- und RAM-Parameter der VMs ändern. Das ist vor allem hilfreich, wenn Sie große Umgebungen auf kleinere Ziel-Cluster wiederherstellen oder DR-Tests durchführen, ohne eine 1:1-physische VMware-Infrastruktur bereitstellen zu müssen. Ändern Sie außerdem die Startreihenfolge und die Startverzögerung (s) für alle ausgewählten VMs in den Ressourcengruppen. Es gibt eine zusätzliche Option, um die Startreihenfolge zu ändern, wenn Änderungen an den Änderungen erforderlich sind, die Sie bei der Auswahl des Ressource- Gruppe-Startauftrags ausgewählt haben. Standardmäßig wird die während der Auswahl der Ressourcengruppe ausgewählte Startreihenfolge verwendet. Änderungen können jedoch in dieser Phase vorgenommen werden.

Replication Plan and Site Details	Select Resource G	0.00						
		roups Set Execu	tion Order	Set VM Details				
	VMI	Details						
/Ms					۹			
M Name	No. of CPUs	Memory (MB)	NIC/IP	Boot Order 👩 🖬 Override				
esource Group : DemoRG								
ALin1	1 🛛	1024 [2]	 Static Dynamic 	3	0			
ALin	4 [0]	1024 [0]	 Static Dynamic 	3	0			
			-					
		Previous	Previous Create Replication Plan	Previous Create Replication Plan	Previous Create Replication Plan	Previous Create Replication Plan	Previous Create Replication Plan	Previous Create Replication Plan

9. Klicken Sie auf **Create Replication Plan**.Nachdem der Replikationsplan erstellt wurde, können Sie die Failover-, Test-Failover- oder Migrationsoptionen je nach Ihren Anforderungen ausführen.

🗖 NetApp	Disaster Recovery O	Drchestrator 💊 📔 Dashboard	d Discover Resource (Groups Replication Plans	Job Monitoring				\$?	۹
	B 1 Rep	lication Plans	3 1 Resource Groups	Source Details	1 vCenters	Destination	n Details	2 1 vCenters		
	1 Replication Plan						۹٥	Create New Replication Plan		
	Plan Name	Active Site	Status	Compliance	Source Site		÷ I			
	CEMORP	() source	() Adme	A Partially reality	Demoske	Demotiest	Can	Pian Details	1	
								Edit Plan		
								Test Fallover		
								Migrate		
								Delete Plan		

Während der Failover- und Test-Failover-Optionen wird der aktuellste Snapshot verwendet, oder ein bestimmter Snapshot kann aus einem Point-in-Time-Snapshot ausgewählt werden. Die Point-in-Time-Option kann sehr vorteilhaft sein, wenn Sie vor einem Korruptionsereignis wie Ransomware stehen, wo die neuesten Replikate bereits kompromittiert oder verschlüsselt sind. DRO zeigt alle verfügbaren Zeitpunkte an.

	_	Source Details		Destination Details	
Replication Plans	Resource Groups	Sites 1	vCenters	T Sites	vCenters
	Testfailover Details			×	
Replication Plan	 Use latest snapshot () Select specific snapshot 	o		^ o	Create New Replication Pl
Plan Name 🗢 🗧 Active Site	Volume	0	Snapshot	÷.	I,
DemoRP 💮 Source	WEANFAVSacct/testcap/te	stsrc01	Select Snapshot	-	Resource Groups
			2023-04-28		
			2023-04-28T11:31:55.000Z - gwc_ntap		
			2023-04-28T11:21:54.000Z - gwc_ntap.		

Um Failover oder Test Failover mit der im Replikationsplan angegebenen Konfiguration auszulösen, können Sie auf **Failover** oder **Test Failover** klicken. Sie können den Replikationsplan im Aufgabenmenü überwachen.

Cloning volumes for test (in parallel)	
	0.7 Seconds 🕕
Mounting cloned volumes and creating datastores (in parallel)	0.9 Seconds 🕚
Registering VMs (in parallel)	0.1 Seconds 🕕

Nachdem der Failover ausgelöst wurde, können die wiederhergestellten Objekte im sekundären Standort AVS SDDC vCenter (VMs, Netzwerke und Datastores) erkannt werden. Standardmäßig werden die VMs im Workload-Ordner wiederhergestellt.

II NetApp	Disaster Recovery Orchestrat	tor 💊 Deckloard Discover	Resource Groups Replicate	on Plans Job Monitoring			¢ 0 0
	C 2 Sites	1 Resource Group	B 1 Replication	Pan 🗗	128 Protected VMs	0 J27 Ungerähreched	
	Environments Z Vistual Environments	2 Alef Storage Accounts	Topology Canvas			Immensive View ()	
	SDBC Summary	D 14 Neiders	Dv Nega, dt	muSRC 172.36 196.29	DemoCest reps./110.756.02		
	Datastores						
	Execution Jobs		Replication Plans			1	
	Ø 1 Tertal Solite	C 1 milliogense	Replication Plan DemoRP	Active State	Status		

Failback kann auf der Ebene des Replikationsplans ausgelöst werden. Im Falle eines Test-Failovers kann die Option zum Abreißen verwendet werden, um die Änderungen rückgängig zu machen und das neu erstellte Volume zu entfernen. Failbacks im Zusammenhang mit Failover sind ein zweistufiger Prozess. Wählen Sie den Replikationsplan aus und wählen Sie **Reverse Data Sync** aus.

Disaster Recovery Orche	estrator 💊 Dashboard	Discover Resource Group	s Replication Plar	s Job Monitoring		4
B 1 Replication	on Plans	1 Resource Groups	Source Details	vCenters	Destination Details	VCenters 1
1 Replication Plan					م	O Create New Replication Plan
Plan Name	© Active Site	Status	Compliance	Source Site	⇒ Destination Site 🔹	ц. — Ц
DemoRP	() Destination	Running In Failover Mod	G Healthy	DemoSRC	DemoDest	Resource Groups
						Plan Details
						Reverse Data Sync

Wenn dieser Schritt abgeschlossen ist, führen Sie ein Failback aus, um zum primären AVS-Standort zurückzukehren.

🖬 NetApp	Disaster Recovery Orchestrator 🔌 Dashboard Discover	Resource Groups Replication Plans Job Monitoring	ê ở O O
	B 1 Replication Plans Resource Gro	ups Source Details	Destination Details
	1 Replication Plan		Q O Create New Replication Plan
	Plan Name C Active Site Status DemoRP	Compliance Source Site 〒 Destinati ⊘ Healthy DemoSRC DemoDe	tt Resource Groups
			Plan Details Failback
III NetApp	Disaster Recovery Orchestrator 🦄 Dashtmani Discover	Resource Grings Replication Plans Job Monitoring	A O O O
	△ 2	B 1 B 128	Protected VMs
	The second secon		Producted Unproducted
	Environments 2 2 Virtual Environments ANF Ecoupy Accounts	Topology Canvas	Immentive View (3
	SDDC Summary		
	Clusters.	DenoSRC D https://172.30.156.3/ https:	moCent V10 75 0.2/
	∃ 12 Datastores ■ 12 Networks		
	Execution Jobs	Replication Plans	
	O 3 O 1 Tetal Jobs to Progress	Replication Rim Addust Site Demotifier Demotifier	Status O Attive

Über das Azure-Portal können wir sehen, dass der Zustand der Replizierung für die entsprechenden Volumes unterbrochen wurde, die dem AVS SDDC am sekundären Standort als Lese-/Schreib-Volumes zugeordnet

wurden. Beim Test-Failover weist DRO nicht das Ziel- oder Replikatvolume zu. Stattdessen wird ein neues Volume des erforderlichen regionsübergreifenden Replikations-Snapshots erstellt und das Volume als Datenspeicher bereitgestellt, wodurch zusätzliche physische Kapazität aus dem Kapazitäts-Pool verbraucht wird und sichergestellt wird, dass das Quell-Volume nicht geändert wird. Bemerkenswert ist, dass Replizierungsjobs während DR-Tests oder Triage Workflows fortgesetzt werden können. Darüber hinaus stellt dieser Prozess sicher, dass die Wiederherstellung bereinigt werden kann, ohne dass das Risiko besteht, dass das Replikat zerstört wird, wenn Fehler auftreten oder beschädigte Daten wiederhergestellt werden.

Recovery durch Ransomware

Die Wiederherstellung von Ransomware kann eine gewaltige Aufgabe sein. Insbesondere KANN es für IT-Abteilungen schwierig sein, den sicheren Rückgabepunkt zu bestimmen und, sobald dies festgelegt ist, zu gewährleisten, dass wiederhergestellte Workloads vor den wiederholten Angriffen geschützt werden (zum Beispiel vor dem Einschlafen von Malware oder durch anfällige Anwendungen).

DRO löst diese Probleme, indem es Unternehmen ermöglicht, Wiederherstellungen von beliebigen Zeitpunkten aus durchzuführen. Die Workloads werden dann in funktionsfähigen, aber isolierten Netzwerken wiederhergestellt, sodass Applikationen zwar funktionieren und miteinander kommunizieren können, aber keinem Nord-/Süd-Datenverkehr ausgesetzt sind. Dieser Prozess bietet Sicherheitsteams einen sicheren Ort, um forensische Analysen durchzuführen und versteckte oder schlafende Malware zu identifizieren.

Schlussfolgerung

Die Disaster-Recovery-Lösung Azure NetApp Files und Azure VMware bietet folgende Vorteile:

- · Effiziente und ausfallsichere regionsübergreifende Azure NetApp Files Replizierung
- Recovery zu einem beliebigen verfügbaren Point-in-Time mit Snapshot-Aufbewahrung.
- Automatisieren Sie alle erforderlichen Schritte zur Wiederherstellung von Hunderten bis Tausenden VMs aus den Validierungsschritten für Storage, Compute, Netzwerk und Applikationen.
- Workload Recovery nutzt den Prozess "Erstellung neuer Volumes aus den neuesten Snapshots", der das replizierte Volume nicht manipuliert.
- Vermeiden Sie das Risiko der Datenbeschädigung auf den Volumes oder Snapshots.
- · Keine Replizierungsunterbrechungen während DR-Test-Workflows
- Nutzen Sie DR-Daten und Cloud-Computing-Ressourcen für Workflows, die über DR hinausgehen, wie z. B. Entwicklungs-/Test, Sicherheitstests, Patch- und Upgrade-Tests oder Fehlerbehebungstests.
- Die CPU- und RAM-Optimierung kann dazu beitragen, Cloud-Kosten zu senken, indem eine Recovery auf kleinere Compute-Cluster ermöglicht wird.

Wo Sie weitere Informationen finden

Sehen Sie sich die folgenden Dokumente und/oder Websites an, um mehr über die in diesem Dokument beschriebenen Informationen zu erfahren:

Volume-Replizierung für Azure NetApp Files erstellen

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

• Regionsübergreifende Replizierung von Azure NetApp Files Volumes

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

• "Azure VMware Lösung"

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

• Implementieren und Konfigurieren der Virtualisierungsumgebung auf Azure

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

• Implementierung und Konfiguration der Azure-VMware-Lösung

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

Verwenden von Veeam Replizierung und Azure NetApp Files-Datastore für die Disaster Recovery zu Azure VMware-Lösung

Autor: Niyaz Mohamed - NetApp Solutions Engineering

Überblick

Azure NetApp Files Datastores (ANF) entkoppeln Storage von Computing und ermöglichen jedem Unternehmen die erforderliche Flexibilität, um Workloads in die Cloud zu verlagern. Sie bietet eine flexible, hochperformante Storage-Infrastruktur, die unabhängig von den Compute-Ressourcen skaliert werden kann. Azure NetApp Files Datastore vereinfacht und optimiert die Implementierung zusammen mit der Azure VMware Lösung (AVS) als Disaster-Recovery-Standort für lokale VMware Umgebungen.

Mit Volume-basierten Azure NetApp Files (ANF) NFS-Datastores können Daten mit jeder validierten Drittanbieterlösung, die VM-Replizierungsfunktionen bietet, aus On-Premises-Systemen repliziert werden. Durch das Hinzufügen von Azure NetApp Files-Datenspeichern kann eine kostenoptimierte Implementierung durchgeführt werden, anstatt eine SDDC-Lösung für Azure VMware mit einer enormen Anzahl an ESXi-Hosts für den Storage einzurichten. Dieser Ansatz wird als "Pilot Light Cluster" bezeichnet. Ein Pilot-Light-Cluster ist eine minimale AVS-Hostkonfiguration (3 AVS-Knoten) zusammen mit der Kapazität des Azure NetApp Files-Datenspeichers.

Ziel ist es, eine kostengünstige Infrastruktur mit allen Kernkomponenten für ein Failover zu erhalten. Ein Pilot-Light-Cluster kann horizontal skalieren und im Falle eines Failovers weitere AVS-Hosts bereitstellen. Sobald der Failover abgeschlossen und der normale Betrieb wiederhergestellt ist, kann das Pilot Light-Cluster wieder auf den kostengünstigen Betriebsmodus zurückskaliert werden.

Zweck dieses Dokuments

In diesem Artikel wird beschrieben, wie Sie Azure NetApp Files mit Veeam Backup and Replication die Disaster Recovery für lokale VMware-VMs auf (AVS) mithilfe der Veeam VM-Replizierungssoftware einrichten.

Veeam Backup & Replication ist eine Backup- und Replizierungsapplikation für virtuelle Umgebungen. Wenn virtuelle Maschinen repliziert werden, wird Veeam Backup & Replication von auf AVS repliziert, erstellt die Software eine exakte Kopie der VMs im nativen VMware vSphere-Format auf dem Ziel-AVS SDDC-Cluster. Veeam Backup & Replication hält die Kopie mit der ursprünglichen VM synchron. Die Replizierung bietet die beste Recovery Time Objective (RTO), da am DR-Standort eine gemountete Kopie einer VM in einem startfähigen Zustand ist.

Dieser Replizierungsmechanismus sorgt dafür, dass die Workloads bei einem Notfall schnell in einem AVS

SDDC gestartet werden können. Die Veeam Backup & Replication Software optimiert darüber hinaus die Datenübertragung zur Replizierung über WAN und für langsame Verbindungen. Außerdem werden doppelte Datenblöcke, keine Datenblöcke, Swap-Dateien und "ausgeschlossene VM Gast-OS-Dateien" herausgefiltert. Die Software komprimiert auch den Replikatverkehr. Um zu verhindern, dass Replikationsjobs die gesamte Netzwerkbandbreite verbrauchen, können WAN-Beschleuniger und Regeln zur Netzwerkdrosselung verwendet werden.

Der Replizierungsprozess in Veeam Backup & Replication ist auftraggesteuert, d. h. die Replizierung wird durch Konfiguration von Replizierungsjobs durchgeführt. Bei einem Ausfall kann ein Failover zur Wiederherstellung der VMs durch einen Failover auf die Replikatkopie ausgelöst werden. Wenn ein Failover durchgeführt wird, übernimmt eine replizierte VM die Rolle der ursprünglichen VM. Ein Failover kann auf den neuesten Status eines Replikats oder auf einen der bekannten Wiederherstellungspunkte erfolgen. Dies ermöglicht bei Bedarf eine Wiederherstellung nach Ransomware-Angriffen oder isolierte Tests. Veeam Backup & Replication bietet mehrere Optionen für unterschiedliche Disaster-Recovery-Szenarien.

[]

Lösungsimplementierung

Übergeordnete Schritte

- 1. Die Veeam Backup & Replication-Software wird in einer On-Premises-Umgebung mit entsprechender Netzwerkverbindung ausgeführt.
- 2. "Implementieren der Azure-VMware-Lösung (AVS)" Private Cloud und "Verbinden Sie Azure NetApp Files-Datastores" Auf Hosts der Azure-VMware-Lösung.

Für DR-Zwecke kann eine Pilot-Light-Umgebung mit minimaler Konfiguration verwendet werden. Bei einem Vorfall erfolgt ein Failover von VMs auf dieses Cluster, und es können weitere Nodes hinzugefügt werden).

- 3. Richten Sie den Replikationsjob ein, um VM-Replikate mit Veeam Backup and Replication zu erstellen.
- 4. Erstellen eines Failover-Plans und Durchführen eines Failover
- 5. Wechseln Sie zurück zu den Produktions-VMs, sobald der Notfall abgeschlossen und der primäre Standort eingerichtet ist.

Voraussetzungen für die Veeam VM Replication to AVS- und ANF-Datastores

- 1. Stellen Sie sicher, dass die Backup-VM von Veeam Backup & Replication sowohl mit den Quell- als auch den Ziel-AVS SDDC-Clustern verbunden ist.
- Der Backup-Server muss in der Lage sein, Kurznamen aufzulösen und eine Verbindung zu Quell- und ZielvCenter herzustellen.
- 3. Der Ziel-Azure NetApp Files-Datastore muss über genügend freien Speicherplatz für die VMDKs replizierter VMs verfügen.

Weitere Informationen finden Sie unter "Überlegungen und Einschränkungen" "Hier".

Einzelheiten Zur Bereitstellung

Veeam Backup & Replication nutzt VMware vSphere Snapshot-Funktionen/während der Replizierung fordert Veeam Backup & Replication VMware vSphere zur Erstellung eines VM-Snapshots an. Der VM-Snapshot ist die Point-in-Time-Kopie einer VM, die virtuelle Laufwerke, den Systemstatus, die Konfiguration und Metadaten umfasst. Veeam Backup & Replication verwendet den Snapshot als Datenquelle für die Replizierung.

Gehen Sie wie folgt vor, um VMs zu replizieren:

- 1. Öffnen Sie die Veeam Backup & Replication Console.
- 2. In der Home-Ansicht. Klicken Sie mit der rechten Maustaste auf den Knoten Jobs, und wählen Sie Replikationsjob > Virtuelle Maschine aus.
- 3. Geben Sie einen Jobnamen an, und aktivieren Sie das entsprechende Kontrollkästchen für die erweiterte Steuerung. Klicken Sie Auf Weiter.
 - Aktivieren Sie das Kontrollkästchen Replikat-Seeding, wenn die Bandbreite zwischen On-Premises und Azure eingeschränkt ist.

*Aktivieren Sie das Kontrollkästchen Network Remapping (für AVS SDDC-Standorte mit unterschiedlichen Netzwerken), wenn Segmente auf der Azure VMware-Lösung SDDC nicht mit denen auf lokalen Netzwerken übereinstimmen.

 Wenn sich das IP-Adressierungsschema am Produktionsstandort vor Ort vom Schema am Ziel-AVS-Standort unterscheidet, aktivieren Sie das Kontrollkästchen Replica RE-IP (für DR-Standorte mit unterschiedlichem IP-Adressierungsschema).

[]

4. Wählen Sie im Schritt Virtuelle Maschinen* die VMs aus, die auf einen Azure NetApp Files-Datastore repliziert werden sollen, der mit einem Azure VMware-Lösung SDDC verbunden ist. Die Virtual Machines können auf vSAN platziert werden, um die verfügbare vSAN Datastore-Kapazität zu füllen. In einem Pilotcluster wird die nutzbare Kapazität eines 3-Knoten-Clusters begrenzt. Die restlichen Daten lassen sich problemlos auf Azure NetApp Files Datenspeichern platzieren, um die VMs wiederherzustellen und das Cluster zu erweitern, um die CPU-/mem-Anforderungen zu erfüllen. Klicken Sie auf Hinzufügen, wählen Sie dann im Fenster Objekt hinzufügen die erforderlichen VMs oder VM-Container aus und klicken Sie auf Hinzufügen. Klicken Sie Auf Weiter.

[]

 Wählen Sie anschließend das Ziel als Azure VMware Solution SDDC Cluster/Host und den entsprechenden Ressourcen-Pool, VM-Ordner und FSX for ONTAP Datastore f
ür VM-Replikate aus. Klicken Sie anschließend auf Weiter.

[]

6. Erstellen Sie im nächsten Schritt die Zuordnung zwischen dem virtuellen Quell- und Zielnetzwerk nach Bedarf.

[]

- 7. Geben Sie im Schritt **Job-Einstellungen** das Backup-Repository an, in dem Metadaten für VM-Replikate, Aufbewahrungsrichtlinien usw. gespeichert werden.
- 8. Aktualisieren Sie die Proxy-Server **Source** und **Target** im Schritt **Data Transfer** und lassen Sie die Option **Automatic** (Standard) und halten Sie die Option **Direct** ausgewählt und klicken Sie auf **Next**.

9. Wählen Sie im Schritt **Gastverarbeitung** die Option **anwendungsorientierte Verarbeitung aktivieren** nach Bedarf aus. Klicken Sie Auf **Weiter**.

[]

10. Wählen Sie den Replikationszeitplan aus, um den Replikationsjob regelmäßig auszuführen.

[]

11. Überprüfen Sie im Schritt **Zusammenfassung** des Assistenten die Details des Replikationsjobs. Um den Job direkt nach dem Schließen des Assistenten zu starten, aktivieren Sie das Kontrollkästchen **Job ausführen, wenn ich auf Fertig stellen klicke**, andernfalls lassen Sie das Kontrollkästchen deaktiviert. Klicken Sie dann auf **Fertig stellen**, um den Assistenten zu schließen.

[]

Sobald der Replikationsjob gestartet wurde, werden die VMs mit dem angegebenen Suffix auf dem Ziel-AVS SDDC-Cluster/Host aufgefüllt.

[]

Weitere Informationen zur Veeam-Replizierung finden Sie unter "Funktionsweise Der Replikation"

Erstellen Sie nach Abschluss der ersten Replikation oder des Seeding den Failover-Plan. Mithilfe des Failover-Plans können Sie ein Failover für abhängige VMs einzeln oder als Gruppe automatisch durchführen. Der Failover-Plan ist das Modell für die Reihenfolge, in der die VMs verarbeitet werden, einschließlich der Boot-Verzögerungen. Der Failover-Plan trägt außerdem dazu bei, sicherzustellen, dass kritische abhängige VMs bereits laufen.

Um den Plan zu erstellen, navigieren Sie zum neuen Unterabschnitt **Replikate** und wählen Sie **Failover-Plan**. Wählen Sie die entsprechenden VMs aus. Veeam Backup & Replication sucht nach den nächstgelegenen Wiederherstellungspunkten zu diesem Zeitpunkt und verwendet diese, um VM-Replikate zu starten.



Der Failover-Plan kann nur hinzugefügt werden, wenn die erste Replikation abgeschlossen ist und sich die VM-Replikate im Bereitschaftszustand befinden.



Es können maximal 10 VMs gleichzeitig gestartet werden, wenn ein Failover-Plan ausgeführt wird



Während des Failover-Prozesses werden die Quell-VMs nicht ausgeschaltet

Um den Failover Plan zu erstellen, gehen Sie wie folgt vor:

1. In der Home-Ansicht. Klicken Sie mit der rechten Maustaste auf den Knoten Replikate, und wählen Sie Failover Plans > Failover Plan > VMware vSphere.

[]

 Geben Sie als nächstes einen Namen und eine Beschreibung für den Plan an. Pre- und Post-Failover-Skript können bei Bedarf hinzugefügt werden. Führen Sie beispielsweise ein Skript aus, um die VMs vor dem Starten der replizierten VMs herunterzufahren.

[]

3. Fügen Sie die VMs zum Plan hinzu und ändern Sie die VM-Startreihenfolge und die Boot-Verzögerungen, um die Applikationsabhängigkeiten zu erfüllen.

[]

Weitere Informationen zum Erstellen von Replikationsjobs finden Sie unter "Erstellen Von Replikationsjobs".

Schritt 3: Führen Sie den Failover-Plan aus

Bei einem Failover wird die Quell-VM am Produktionsstandort auf ihr Replikat am Disaster-Recovery-Standort umgeschaltet. Im Rahmen des Failover-Prozesses stellt Veeam Backup & Replication das VM-Replikat zum erforderlichen Wiederherstellungspunkt wieder her und verschiebt alle I/O-Aktivitäten von der Quell-VM auf das Replikat. Replikate können nicht nur im Notfall verwendet werden, sondern auch DR-Übungen simulieren. Während der Failover-Simulation bleibt die Quell-VM aktiv. Sobald alle erforderlichen Tests durchgeführt wurden, können Sie das Failover rückgängig machen und zum normalen Betrieb zurückkehren.



Stellen Sie sicher, dass die Netzwerksegmentierung vorhanden ist, um IP-Konflikte während des Failovers zu vermeiden.

Um den Failover-Plan zu starten, klicken Sie einfach auf die Registerkarte **Failover Plans** und klicken Sie mit der rechten Maustaste auf Ihren Failover-Plan. Wählen Sie ***Start**. Dabei wird ein Failover mit den neuesten Wiederherstellungspunkten der VM-Replikate durchgeführt. Um ein Failover zu bestimmten Wiederherstellungspunkten von VM-Replikaten durchzuführen, wählen Sie **Start to** aus.

[]

[]

Der Status des VM-Replikats ändert sich von "bereit" zu "Failover", und die VMs werden auf dem Ziel-Cluster/Host des SDDC der Azure VMware-Lösung (AVS) gestartet.

[]

Sobald der Failover abgeschlossen ist, ändert sich der Status der VMs in "Failover".

[]



Veeam Backup & Replication hält alle Replikationsaktivitäten für die Quell-VM an, bis das Replikat in den Bereitschaftszustand zurückkehrt.

Ausführliche Informationen zu Failover-Plänen finden Sie unter "Failover-Pläne".

Wenn der Failover-Plan ausgeführt wird, gilt er als Zwischenschritt und muss basierend auf den Anforderungen abgeschlossen werden. Folgende Optionen stehen zur Verfügung:

• Failback zur Produktion - Wechseln Sie zurück zur ursprünglichen VM und übertragen Sie alle Änderungen, die während des VM-Replikats auf die ursprüngliche VM ausgeführt wurden.



Wenn Sie ein Failback durchführen, werden die Änderungen nur übertragen, aber nicht veröffentlicht. Wählen Sie **commit Failback** (sobald die ursprüngliche VM wie erwartet funktioniert) oder Undo Failback, um zum VM-Replikat zurückzukehren, wenn die ursprüngliche VM nicht wie erwartet funktioniert.

- Rückgängigmachen des Failover Wechseln Sie zurück zur ursprünglichen VM und verwerfen Sie alle Änderungen, die während der Ausführung am VM-Replikat vorgenommen wurden.
- **Permanent Failover** Wechseln Sie dauerhaft von der ursprünglichen VM auf ein VM-Replikat und verwenden Sie dieses Replikat als ursprüngliche VM.

In dieser Demo wurde "Failback zur Produktion" gewählt. Failback auf die ursprüngliche VM wurde während des Zielschritts des Assistenten ausgewählt und das Kontrollkästchen "VM nach der Wiederherstellung einschalten" war aktiviert.

[]		
[]		
[]		
[]		

Failback-Commit ist eine der Möglichkeiten, den Failback-Vorgang abzuschließen. Wenn Failback durchgeführt wird, wird bestätigt, dass die an die zurückgeschickte VM (die Produktions-VM) gesendeten Änderungen wie erwartet funktionieren. Nach dem Commit-Vorgang setzt Veeam Backup & Replication die Replizierungsaktivitäten für die Produktions-VM fort.

Detaillierte Informationen zum Failback-Prozess finden Sie in der Veeam-Dokumentation für "Failover und Failback für die Replikation".

[]

Nach einem erfolgreichen Failback zur Produktion werden die VMs alle auf den ursprünglichen Produktionsstandort zurückgestellt.

[]

Schlussfolgerung

Mit der Datastore-Funktion von Azure NetApp Files können Veeam oder jedes beliebige validierte Drittanbieter-Tool eine kostengünstige DR-Lösung anbieten, indem Pilot-Light-Cluster eingesetzt werden, anstatt nur ein großes Cluster einzurichten, um VM-Replikate aufzunehmen. So wird ein maßgeschneiderter und individuell angepasster Disaster-Recovery-Plan effizient umgesetzt und vorhandene Backup-Produkte intern für DR wiederverwendet. So wird Cloud-basierte Disaster Recovery durch das Beenden von DR-Datacentern vor Ort möglich. Bei einem Ausfall kann ein Failover durch Klicken auf eine Schaltfläche oder bei einem Ausfall automatisch durchgeführt werden.

Wenn Sie mehr über diesen Prozess erfahren möchten, folgen Sie bitte dem detaillierten Video zum Rundgang.

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

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU "RESTRICTED RIGHTS": Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel "Rights in Technical Data – Noncommercial Items" in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.