

# Protection des workloads dans Azure/AVS

**NetApp Solutions** 

NetApp April 26, 2024

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

# Sommaire

Protection des workloads dans Azure/AVS	1
Reprise après incident avec ANF et JetStream	1
Reprise après incident avec CVO et AVS (stockage connecté à l'invité)	14
Tr-4955 : reprise d'activité avec Azure NetApp Files (ANF) et solution Azure VMware (AVS)	41
Utilisation de la réplication Veeam et du datastore Azure NetApp Files pour la reprise après incident ve	rs
la solution Azure VMware	56

# Protection des workloads dans Azure/AVS

# Reprise après incident avec ANF et JetStream

La reprise d'activité dans le cloud est une solution résiliente et économique de protection des workloads contre les pannes sur site et la corruption des données, par exemple, par ransomware. Grâce à la structure VMware VAIO, les charges de travail VMware sur site peuvent être répliquées vers le stockage Azure Blob et récupérées. Vous bénéficiez ainsi d'une perte de données minimale, voire quasi nulle.

Jetstream DR peut être utilisé pour restaurer de manière transparente les workloads répliqués depuis les sites vers AVS, et plus particulièrement vers Azure NetApp Files. Il permet une reprise d'activité économique en utilisant peu de ressources sur le site de reprise d'activité et un stockage cloud économique. Jetstream DR automatise la restauration vers les datastores ANF via Azure Blob Storage. Jetstream DR restaure les ordinateurs virtuels ou groupes de serveurs virtuels indépendants dans l'infrastructure de site de restauration en fonction du mappage du réseau et assure une restauration instantanée pour la protection par ransomware.

Ce document présente les principes JetStream DR des opérations et de ses principaux composants.

- 1. Installez le logiciel JetStream DR dans le data Center sur site.
  - a. Téléchargez le pack logiciel JetStream DR depuis Azure Marketplace (ZIP) et déployez JetStream DR MSA (OVA) dans le cluster désigné.
  - b. Configurez le cluster à l'aide du package filtre d'E/S (installez JetStream VIB).
  - c. Provisionnez Azure Blob (Azure Storage Account) dans la même région que le cluster AVS pour la reprise après incident.
  - d. Déployer des appliances DRVA et attribuer des volumes de journaux de réplication (VMDK à partir d'un datastore existant ou d'un stockage iSCSI partagé).
  - e. Créez des domaines protégés (groupes de machines virtuelles associées) et attribuez des DRVAs et Azure Blob Storage/ANF.
  - f. Démarrer la protection.
- 2. Installez le logiciel JetStream DR dans le cloud privé Azure VMware solution.
  - a. Utilisez la commande Exécuter pour installer et configurer JetStream DR.
  - b. Ajoutez le même conteneur Azure Blob et découvrez les domaines à l'aide de l'option Scan Domains.
  - c. Déployer les appareils DRVA requis.
  - d. Créez des volumes du journal de réplication à l'aide des datastores VSAN ou ANF disponibles.
  - e. Importez des domaines protégés et configurez RocVA (Recovery va) pour utiliser le datastore ANF dans le cadre du placement de VM.
  - f. Sélectionnez l'option de basculement appropriée et démarrez la réhydratation continue pour les domaines ou les machines virtuelles RTO proches de zéro.
- 3. En cas d'incident, déclenchez le basculement vers les datastores Azure NetApp Files sur le site AVS dédié à la reprise après incident.
- 4. Appelez le rétablissement vers le site protégé après la récupération du site protégé.avant de commencer, assurez-vous que les conditions préalables sont remplies comme indiqué dans le présent document "lien" De plus, exécutez l'outil de test de bande passante (BWT) fourni par JetStream Software pour évaluer les performances potentielles du stockage Azure Blob et de sa bande passante de réplication lorsqu'il est utilisé avec le logiciel JetStream DR. Une fois les conditions requises, y compris la connectivité, mises en place, configurez et abonnez-vous à JetStream DR pour AVS à partir du "Azure Marketplace". Une fois le pack logiciel téléchargé, procédez au processus d'installation décrit ci-dessus.

Lors de la planification et du démarrage de la protection pour un grand nombre de machines virtuelles (par exemple, 100+), utilisez l'outil de planification des capacités (CPT) du kit d'outils JetStream DR Automation. Fournissez une liste des machines virtuelles à protéger avec leurs préférences RTO et de groupes de récupération, puis exécutez CPT.

CPT effectue les fonctions suivantes :

- Combinaison des machines virtuelles dans des domaines de protection selon leur objectif de durée de restauration.
- Définir le nombre optimal de DRVAS et leurs ressources.
- Estimation de la bande passante de réplication requise.

- L'identification des caractéristiques du volume du journal de réplication (capacité, bande passante, etc.)
- Estimation de la capacité de stockage objet requise, etc.



Le nombre et le contenu des domaines prescrits dépendent de diverses caractéristiques des VM, telles que les IOPS moyennes, la capacité totale, la priorité (qui définit l'ordre de basculement), RTO et autres.

## Installer JetStream DR dans le data Center sur site

Le logiciel Jetstream DR est constitué de trois composants principaux : le serveur virtuel Jetstream DR Management Server (MSA), le dispositif virtuel DR (DRVA) et les composants hôtes (packages de filtres d'E/S). MSA est utilisé pour installer et configurer des composants hôtes sur le cluster de calcul, puis pour administrer le logiciel JetStream DR. La liste suivante fournit une description générale du processus d'installation :

- 1. Vérifier les prérequis.
- 2. Exécutez l'outil de planification de la capacité pour obtenir des recommandations en matière de ressources et de configuration (facultatif, mais recommandé pour les essais de validation).
- 3. Déployez JetStream DR MSA sur un hôte vSphere du cluster désigné.
- 4. Lancez le MSA à l'aide de son nom DNS dans un navigateur.
- 5. Enregistrez le serveur vCenter avec MSA.pour effectuer l'installation, procédez comme suit :
- 6. Après le déploiement de JetStream DR MSA et l'enregistrement du serveur vCenter, accédez au plug-in JetStream DR à l'aide du client Web vSphere. Pour ce faire, accédez à Datacenter > configurer > JetStream DR.

vm vSphere Client	Menu 🗸 🛛 📿 Search in all	environments		C ② ~ Administrator@EHCDC.COM ~ G
□ □ ● 9 → a300-vcsa.ehcdc.com	A300-DataCent	er ACTIONS - nfigure Permissions Hosts & Clust	ers VMs Datastores Networks Updates	
<ul> <li>A300-DataCenter</li> <li>A300-Cluster</li> <li>a300-esxi02.eh</li> </ul>	<ul> <li>More         Alarm Definitions         Scheduled Tasks     </li> </ul>	JetiStiream DR Protected Domains Statistics S	storage Sites Appliances Configurations Task Log	۴.
a300-esxi03.en	Network Protocol Pr	Site Details		Alarm Settings
a300-esxi05.eh	JetStream DR	vCenter Server Hostname	172.21.253.160	
ANFJSDR-MSA0		Management Appliance Hostname	ANFJSDR-msa	
🔂 AuctionAppA0		Software Version	4.0.0.443	
AuctionAppA2		Subscription ID	00000000-0000-0000-0000-000000000001 Configur	re l
AuctionAppA3		Tenant ID / Application ID	- Configure	
AuctionAppB0		Application Secret	- Configure	

7. Dans l'interface JetStream DR, sélectionnez le cluster approprié.

VCenter Server Hostname     172.21:253:160       Management Appliance Hostname     VCENTROL       Software Version     Configure Clusters       Subscription ID     Select All     Clear All       Application Secret     O atacenter Name A       Configured Clusters     A300-Cluster						
Management Appliance Hostname Software Version Subscription ID Tenant ID / Application ID Application Secret Configured Clusters Configured Clusters	ver Hostname	172.21.253.160				
Software Version Configure Clusters Subscription ID Penant ID / Application ID Application Secret Cluster Name A Datacenter Name A Configured Clusters Cluster A300-Cluster A300-Cluster Cluster A300-Cluster A300-Cluster Cluster A300-Cluster A3	t Appliance Hostname	ANT 1000				
Subscription ID     Select All     Clear All     Q       Image: Cluster Name A     Datacenter Name A       Image: Cluster Select All     Clear All     Q	rsion	Configure Clusters				
Image: Cluster Name A     Datacenter Name A       Image: Cluster Name A     Datacenter Name A       Image: Cluster Name A     A300-Cluster       Image: Cluster Name A     A300-Cluster	D					
Image: splication Secret     Image: splication Secret     Image: splication Secret       Image: splication Secret     Image: splication Secret       Image: splication Secret     A300-Cluster       Image: splication Secret     A300-Cluster       Image: splication Secret     A300-Cluster       Image: splication Secret     Image: splication Secret       Image: splication Secret     A300-Cluster       Image: splication Secret     Image: splication Secret	pplication ID		Select All	Clear All	ų	
onfigured Clusters	Secret	🗹 Cluster Name 🛦	Datacenter Name 🔺		_	
oningured clusters	Cluster	A300-Cluster	A300-DataCenter		^	
	Glusters					
Configure Cluster * Upprade 1	Cluster Digrade d					
Cluster Name 🔺 📉 Host Details 🔺	Name A				~	Host Details 🔺
No cluster configured Cancel Configure	ontigured		c	ancel Cor	nfigure	

8. Configurez le cluster avec le package de filtre d'E/S.

Protected Domains Statistics	Storage Sites Appliances Configurations Task Log	
Storage Sites	Add Storage Site	
+ Add Storage Site		
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		
	Acure Blob Storage Account Name * anfdrdemostor	
No storage site selected. Select a storage		Ī
	Acure Blob Storage Account Key *	
	Cancel Add Storage Site	

- 9. Ajoutez un stockage Azure Blob Storage situé sur le site de reprise.
- 10. Déployez une appliance DR virtuelle (DRVA) depuis l'onglet Appliances.



Les DRVAS peuvent être créés automatiquement par CPT, mais pour les tests POC, nous vous recommandons de configurer et d'exécuter manuellement le cycle de reprise après incident (démarrer la protection > basculement > retour arrière).

JetStream DRVA est une appliance virtuelle qui facilite les principales fonctions du processus de réplication des données. Un cluster protégé doit contenir au moins un DRVA et, en général, un DRVA est configuré par hôte. Chaque DRVA peut gérer plusieurs domaines protégés.

JetStream DR Protected Domains Statistics	Deploy New DR Virtual Appliance (D	RVA)		Ē
DRVAs (DR Virtual Appliances)	1. General 2. DRVA	VM 3. DRVA Network	4. Summary	
+ Deploy New DRVA	Name	ANFdemo001	^	ų
Name 🔺	Description (Optional)			Details 🔺
No DR Virtual Appliance configured.	Datacenter	A300-DataCenter		
	Cluster	A300-Cluster		
	Resource Pool (Optional)	-		
	VM Folder (Optional)	-		~
Replication Log Volume	Datastore	A300_NFS_DS04		
	Number Of CPUs	8		0
+ New Replication Log Volume	Memory Size	32GB		ų
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	~	~
		Cancel Back	Deploy	

Dans cet exemple, quatre DRVA ont été créés pour 80 machines virtuelles.

1. Créez des volumes de journal de réplication pour chaque DRVA à l'aide de VMDK provenant des datastores disponibles ou des pools de stockage iSCSI partagés indépendants.

2. À partir de l'onglet domaines protégés, créez le nombre requis de domaines protégés à l'aide des informations concernant le site Azure Blob Storage, l'instance DRVA et le journal de réplication. Un domaine protégé définit un ordinateur virtuel ou un ensemble de serveurs virtuels dans le cluster qui sont protégés ensemble et se voit attribuer un ordre de priorité pour les opérations de basculement/retour arrière.

JetStream DR Protected Domains Statistics	Storage Sites Appliances Configur	ations Task Log		
Select Protected Domain:	Create Protected Domain		+ Create = Mor	e
	1. General 2. Pr	imary Site     3. Sumr	mary	
	Protected Domain Name	ANFPD001	^	
	Priority Level (Optional)	1		
	Total estimated data size to be protected	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 Back	Create	

 Sélectionnez les machines virtuelles que vous souhaitez protéger et démarrez la protection des machines virtuelles du domaine protégé. La réplication des données commence alors dans le magasin d'objets blob désigné.

Vérifier que le même mode de protection est utilisé pour toutes les VM d'un domaine protégé.



Le mode Write- Back (VMDK) peut offrir de meilleures performances.

JetStream DR Protected Domains Statistics St	orage Sites Appliances	Configurations Task	Log			
Select Protected Domain: ANFPD001	Start Protection				reate 🗊 Delete	
Recoverable / Total VMs	Protection Mode for selected VMs			0		Edit Details
Replication Status	VM Name ▲	# of Disks	Protection Mode	4	ANFDemoblobrepo	^
Remaining Background Data	1	×			0-DataCenter \ A300-Cluster \	
Current RPO	AuctionAppA1	1	Write-Back(VMDK) v	^	bled	~
	AuctionAppB1	1	Write-Back(VMDK) v			
Protected VMs Settings Ala	AuctionDB1	2	Write-Back(VMDK) v			
	AuctionLB1	1	Write-Back(VMDK) V			
+ Start Protection	AuctionMSQ1	1	Write-Back(VMDK) V			Q
	AuctionNoSQL1	2	Write-Back(VMDK) v			
U VM Name ▲	AuctionWebA1	1	Write-Back(VMDK) V		ground Dat Details	
No VM is protected.	AuctionWebB1	1	Write-Back(VMDK) V			
	Client1	1	Write-Back(VMDK) V			
	- neonei	0	(	~		
			Cancel Start Pro	otection		
						~

Vérifier que les volumes des journaux de réplication sont placés sur un stockage haute performance.



Les guides d'exécution de basculement peuvent être configurés pour regrouper les VM (appelés groupes de récupération), définir l'ordre de démarrage et modifier les paramètres CPU/mémoire avec les configurations IP.

# Installez JetStream DR pour AVS dans un cloud privé Azure VMware solution à l'aide de la commande Exécuter

Il est recommandé de créer à l'avance un cluster Pilot-light à trois nœuds sur le site de récupération (AVS). L'infrastructure du site de reprise peut ainsi être préconfigurée, incluant les éléments suivants :

- Segments de réseau de destination, pare-feu, services comme DHCP et DNS, etc.
- Installation de JetStream DR pour AVS
- La configuration des volumes ANF en tant que datastores, et moreJetStream DR prend en charge le mode RTO quasi-nul pour les domaines stratégiques. Pour ces domaines, le stockage de destination doit être préinstallé. ANF est un type de stockage recommandé dans ce cas.



La configuration réseau comprenant la création de segments doit être configurée sur le cluster AVS afin de répondre aux exigences sur site.

Selon les exigences des niveaux de service et de l'objectif RTO, il est possible d'utiliser un mode de basculement continu ou standard. Pour un RTO proche de zéro, la réhydratation continue doit être mise sur le site de reprise.

Pour installer JetStream DR pour AVS sur un cloud privé Azure VMware solution, procédez comme suit :

1. Depuis le portail Azure, accédez à la solution Azure VMware, sélectionnez le cloud privé et sélectionnez Exécuter la commande > packages > JSDR.Configuration.



L'utilisateur CloudAdmin par défaut dans Azure VMware solution ne dispose pas des privilèges suffisants pour installer JetStream DR pour AVS. Azure VMware solution permet une installation simplifiée et automatisée de JetStream DR en appelant la commande Azure VMware solution Run pour JetStream DR.

La capture d'écran suivante montre l'installation à l'aide d'une adresse IP DHCP.

Microsoft Azure	South move	ter, service, and door.05+/V	🖬 🕼 🖓 🛞 🖉 niyazilandapp.com 🧃
Home > ANFOataClus			Run command - Install-JetDRWithDHCP ×
ANFDataClus   Run	command		The two local Conduct December in PD becaute here DBM control a base tax animal
P Search (Ch1+)) ∈	O Refresh R Freedback		relevanted previdinges to the user, deploys Jetth Management Server Appliance/MEA), registers vCenter to the JetDr MSA, configures cluster.
Access control (AM)	Packages Run execution status		Command parameters
Ø bigs			Becichie Within
Diagnose and solve problems	<ul> <li>Name</li> </ul>	Description	The line
Settings	v Kitk Conference 224 Burnet	Maria in contraction of address before an Add for address before the support	ProtectiveCuster *
	Durable left River's star	This Previat according and a factor but special converted LaDP conversional so other character	Outer1
A 1008		polos.	Datastore * (i)
Manage	Drable-Jet010 orCuster	This Cridiet configures an additional duster for protection. It installs vibs to all hosts in the	vsarDatastore
Connectivity	Install, Methodological Press	This tractional Constiller Downloads setTe transitio from MMS creation a new over attained ele-	VMName* ()
B Chatters		registers vCenter to the JetDr MSA, configures cluster.	antjuval-msa
	Install-JetDWWerdcasch	This top level Cindlet Downloads JetDr bundle from MMS, creates a new user, assigns elev-	Cluster * 😳
Di Identity		registers vCenter to the JetDr MSA, configures cluster.	Oute-1
<ul> <li>Storage (preview)</li> </ul>	Involve PrefightietDSimital	This Circlet checks and displays current state of the system it checks whether the minimal	- Credential ()
E Placement policies		4 boots if the cluster details are correct, if there is already a VM with the same name provid	Otername 5
+ Add-pm	Invoice PrefightletDRUmmtall	This Crititet checks and displays current state of the system it checks whether the minimal A host of the checks and details are correct and if any Vicenter is corrected to the MCA	root
distant and the second second	A DESCRIPTION OF A DESC	4 Loose is the provid memory and coulder more and Architely in Memory on the Architely	Password *
Workload Networking	Unerthall ArtDit	The top level Cindlet orbites a new user, assignt elevated philleges to the user, uncortigu	
< Segments	> Microsoft/WS/Management +Lst	wroat ond als for administration over lasts in managing Abre VMMee Southors	HastName ()
TT DHCF			anfoval-mua
Port manoring			Network 1 (j)
0.015			DRSep
			25722
Operation			Cetam
🗮 Run command 🔶 👻			Retain up to

 Une fois l'installation de JetStream DR pour AVS terminée, actualisez le navigateur. Pour accéder à l'interface de reprise après incident JetStream, allez dans SDDC Datacenter > configurer > JetStream DR.

	s storage site	s App		onngurations	IdSK LUU	9	-
Site Details						Alarm Set	tin
vCenter Server Hostname	172.30.15	6.2					
Management Appliance Hostname	anfjsval-m	isa					
Software Version	4.0.2.450						
Subscription ID	- <u>Configu</u>	lre					
Tenant ID / Application ID	- Configu	ure					
Application Secret	- Configu	ire					
Configure Cluster	Unconfigure	🛠 Resolv	e Configure Issue	9			1
Cluster Name	Datacenter	Name 🔺	Status 🔺	Software Ve	rsion 🔺	Host Details	2
Cluster-1	SDDC-Data	center	📀 Ok	4.0.2.132		Details	

3. À partir de l'interface JetStream DR, ajoutez le compte Azure Blob Storage utilisé pour protéger le cluster sur site en tant que site de stockage, puis exécutez l'option Scan Domains.

JetStre	Available Protected	Domain(s) For Import							
	Protected Domain	Description	Recoverable V	VMs	Import			^	-
Storage Sit	ANFPD000	Protected Domain Tile0	20	20	Import		^		
+ Add Stora	ANFPD001	-	20	20	Import			18	Q
Name A	ANFPD002	Protected Domain 02	20	20	Import			18	
ANFDemoble	ANFPD003	Protected Domain Tile 03	20	20	Import		~		^
	<					>		127	
									~
Storage Si									
Storage Ac								<b>,</b>	
Use SSL									
Used Space					Clo	se			
Lised Space A	larm	Disabled Configure	Alarm						

4. Une fois les domaines protégés importés, déployez les appareils DRVA. Dans cet exemple, la réhydratation continue est lancée manuellement à partir du site de restauration à l'aide de l'interface utilisateur JetStream DR.



Ces étapes peuvent également être automatisées à l'aide de plans créés par CPT.

- 5. Créez des volumes du journal de réplication à l'aide des datastores VSAN ou ANF disponibles.
- 6. Importez les domaines protégés et configurez le va de restauration de manière à utiliser le datastore ANF pour le positionnement des VM.

ect Protected Domain:	Continuous Fa	ilover Protected Dom	ain					Delete	=	More
de	•	•	•			•				De
coverable / Total VMs	1. General	2a. Failover Settings	2b. VM Settings	3. Reco	very VA	4. DR Settings	5. Summary	reporec		
	Protected D	omain Name		ANEPD002				253.160 )		
	Datacenter			SDDC-Datac	enter			1000		
	Cluster			Cluster-1				1000		
	Resource Po	ool (Optional)		2				1000		
rotected VMs Setti	VM Folder (	Optional)		-				1000		
	Datastore			ANFRecoDS	J002			100		
	Internal Net	work		DRSeg				1000		
VM Name 🔺	External Rep	blication Network		DRSeg				1.000	Details	
AuctionAppA2	Managemen	t Network		DRSeg				- 200	Details	
AuctionAppB2	Storage Site			ANFDemoblo	breporec				Details	
AuctionDB2	DR Virtual A	opliance		ANFRecDRV	4003				Details	
AuctionLB2	<b>Banliastian</b>	on Ptorono		idoviedh			6	~	Details	
AuctionMSQ2					Cancel	Back	Continuous Failov	er	Details	

Assurez-vous que DHCP est activé sur le segment sélectionné et qu'un nombre suffisant d'adresses IP est disponible. Des adresses IP dynamiques sont utilisées temporairement pendant la restauration des domaines. Chaque machine virtuelle de restauration (y compris la réhydratation continue) requiert une adresse IP dynamique individuelle. Une fois la récupération terminée, le IP est libéré et peut être réutilisé.

7. Sélectionnez l'option de basculement appropriée (basculement continu ou basculement). Dans cet exemple, la réhydratation continue (basculement continu) est sélectionnée.

Protected Domains St	atistics Stor	age Sites	Appliances	Configuration	ons	Task Log	-
Select Protected Domain:	ANFPD000 -	View all		+ Create	1	Delete	≡ Mor
Mode		Imported	Configura	ations		O Restore	
Recoverable / Total VMs		20 / 20	Storage Si	te	1	→ Failover	
			Owner Site	3	REN	→ Continuo	us Failove
						→ Test Faild	over
Protected VMs Settin	ngs Alarms						
							1
VM Name 🔺		Protec	tion Status 🔺	F	rotectio	on Mode 🔺	Details
AuctionAppA0		Rec	overable	N	Vrite-Bac	ck(VMDK)	Details
AuctionAppR0		O Rec	overable	1	Nrite-Bar		Dotaile

# Exécution du basculement/retour arrière

( **i** )

1. Après un incident se produit dans le cluster protégé de l'environnement sur site (défaillance partielle ou complète), déclencher le basculement.



CPT peut être utilisé pour exécuter le plan de basculement pour restaurer les machines virtuelles à partir d'Azure Blob Storage vers le site de restauration du cluster AVS.

**i** 

Après le basculement (pour la réhydratation en continu ou standard) lorsque les machines virtuelles protégées ont été lancées dans AVS, la protection reprend automatiquement et la reprise après incident JetStream continue de répliquer leurs données dans les conteneurs appropriés/originaux dans Azure Blob Storage.

Jet/Stream DR Protected Domains Statu	Complete Continuous Fallov	ver for Protected Domain ANFPD003			13
Select Protected Domain: Al	VM Network Mapping			O Fallover	I More
Province Statement	Protected VM Network A	Recovery VM Network	^		
Alodon 1	VM_3510	DRSeg *	^		
Receiverable / Total VMs				nobiobroporec	(A)
Real Property lies and the second sec				72.21.253 150 )	
Liata (Processed/Known Rem)	Force Failover			penter \ Cluster-1	
Current Ship					¥.
Protocled VMs Settings	Force Fail required Complete Are you su	over of Protected Domain requested. Administrator consent is ownership of this Protected Domain will be taken over by this Site. ure you want to continue?	~ ~		_
	Other S	Cancei Confirm			4
Austonanoaa	Planumenter			Jetails Mitsis	
AurthonAboRt	Force Failover			and a second	
Auroonliks					
Austion D3				Million .	
Australianta				The second	
Automatical Dirac					
		Cancel	lete Failover		



La barre des tâches affiche la progression des activités de basculement.

2. Une fois la tâche terminée, accédez aux machines virtuelles récupérées et l'entreprise continue d'être opérationnelle normalement.

Jet/Stream DR Protected Domains Statis	Continuous Rehydration Task Result				Ē
Select Protected Domain: Al	Task Completed Successfully			T Delete	≡ More
Mode	Sectorial Comple	ANERDOOD		E	dt Detais
Recoverable / Total VMs	Vite Recovery Status	ANF FDUGS		nobiobreporec	^
	Total VMs Decovered	20		2 30 156 2 )	
Replication Status	testECR0 Status	20		tenter \ Cluster-1	
Remaining Background Data	Pre-script Execution Status	Not defined			
Current RPO	Runbook Execution Status	Success			~
	Post-script Execution Status	Not defined			
Protected VMs Settings					
+ Start Protection					Q
VM Name A				d D Details	
AuctionAppA3				Details	~
AuctionApp83				Details	
AuctionDB3				Details	
AuctionLB3				Details	
AuctionMSQ3			Dismiss	Details	
AuctionNoSQL3	ar rocoverance	work mechanism	uny ua	Details	×

Une fois que le site primaire est à nouveau opérationnel, le retour arrière peut être effectué. La protection des machines virtuelles est reprise et la cohérence des données doit être vérifiée.

3. Restaurer l'environnement sur site. Selon le type d'incident, il peut être nécessaire de restaurer et/ou de vérifier la configuration du cluster protégé. Si nécessaire, il peut être nécessaire de réinstaller le logiciel JetStream DR.



Remarque : le recovery\_utility\_prepare\_failback Le script fourni dans le kit d'automatisation peut être utilisé pour nettoyer le site protégé d'origine de toutes les machines virtuelles obsolètes, des informations de domaine, etc.

4. Accédez à l'environnement sur site restauré, accédez à l'interface utilisateur Jetstream DR et sélectionnez le domaine protégé approprié. Une fois que le site protégé est prêt à être restauré, sélectionnez l'option de retour arrière dans l'interface utilisateur.

Select Protected Domain: ANFPD003 -	View all		+ Create	Delete	■More
Node	Running in Failover	Configurations		O Restore	
Active Site	172.30.156.2	Storage Site	ANF	O Resume Continu	ibus. Rehýdratic
Recoverable / Total VMs	20 / 20	Owner Site	REMOT	Failback	
Protected VMs Settings Alarms					
Protected VMs Settings Alarms					c
VM Name A	Protection Sta	tus A Protection	Mode 🔺	Details	c
VM Name A AuctionAppA3 AuctionAppB3	Protection Sta	tus ▲ Protection Write-Back Write-Back	(VMDK)	Details Details	c ,
VM Name ▲         Alarms           AuctionAppA3         AuctionApp83           AuctionDB3         AuctionDB3	Protection Sta © Recoverable © Recoverable © Recoverable © Recoverable	tus A Protection Write-Back Write-Back Write-Back	VMDK)	Details Details Details Details	, ,
VM Name     Settings     Alarms       VM Name     AuctionAppA3       AuctionAppB3     AuctionDB3       AuctionLB3	Protection Sta © Recoverable © Recoverable © Recoverable © Recoverable © Recoverable	tus ▲ Protection Write-Back Write-Back Write-Back Write-Back Write-Back	Mode           (VMDK)           (VMDK)           (VMDK)           (VMDK)	Details Details Details Details Details	c ,
Protected VMs Settings Alarms VM Name ▲ AuctionAppA3 AuctionApp83 AuctionDB3 AuctionLB3 AuctionMSQ3	Protection Sta Recoverable Recoverable Recoverable Recoverable Recoverable Recoverable Recoverable Recoverable	tus ▲ Protection Write-Back Write-Back Write-Back Write-Back Write-Back Write-Back	Mode	Details Details Details Details Details Details Details	ć

Le plan de restauration généré par CPT peut également être utilisé pour initier le retour des VM et de leurs données du magasin d'objets vers l'environnement VMware d'origine.

Spécifier le délai maximal après la mise en pause des VM dans le site de reprise et leur redémarrage sur le site protégé. Cette durée comprend l'exécution de la réplication après l'arrêt des machines virtuelles de basculement, la propreté du site de restauration et la recréation des machines virtuelles sur le site protégé. La valeur recommandée par NetApp est de 10 minutes.

Exécuter le processus de retour arrière, puis confirmer la reprise de la protection des machines virtuelles et de la cohérence des données.

# Récupération de Rantomeware

 $(\mathbf{i})$ 

(i)

Récupérer des données suite à un ransomware peut être une tâche extrêmement fastidieuse. En particulier, il peut être difficile pour les services IT de déterminer le point de retour sûr et, une fois déterminé, de garantir la protection des charges de travail récupérées contre les attaques se reproduisant (contre les programmes malveillants en veille ou à l'aide d'applications vulnérables).

Jetstream DR pour AVS avec les datastores Azure NetApp Files peut résoudre ces problèmes en permettant aux entreprises de récupérer les données à partir de points disponibles dans le temps, de sorte que les charges de travail soient récupérées sur un réseau fonctionnel et isolé si nécessaire. La récupération permet aux applications de fonctionner et de communiquer entre elles sans les exposer au trafic nord- sud, offrant ainsi aux équipes de sécurité un endroit sûr pour effectuer des analyses et autres corrections nécessaires.

JetStream DR Protected Domains	statistics Stor	ane Sites Anoliar	ces Coofiau	rations Task I	00				ß
Select Protected Domai	Failback Protec	ted Domain						Delete	≡ More
Mode	0 1. General	2a. Failback Settings	2b. VM Settings	3. Recovery VA	4. DR	Settings	5. Summary		Edit Details
Active Site								^ tpo	^
Recoverable / Total VMs	Protected Dor	main Name		ANFPD003				06.2.)	
	Failback Data	center		A300-DataCenter					
	Failback Clust	ter		A300-Cluster					
Protoclard Mile So	Failback Reso	ource Pool		2					
Piblicieu vivis de	VM Folder (O	ptional)							
	Failback Data	store		A300_NFS_DS02				- 200	0
VM Name A	Maximum Del	ay After Stopping		60 Minutes					~
AuctionAppA3	Internal Netwo	ork		VM_187					^
AuctionAppB3	External Repl	ication Network		VM_187					
AuctionDB3	Management	Network		VM_187				~	
AuctionLB3					Cancel	Back	Failback		
AuctionMSQ3	9		Recoverab	le	Write-Back	(VMDK)	Deta	105	
AuctionNoSQL3			Recoverab	le	Write-Back	(VMDK)	Deta	ills	~

# Reprise après incident avec CVO et AVS (stockage connecté à l'invité)

# Présentation

Auteurs : Ravi BCB et Niyaz Mohamed, NetApp

La reprise d'activité dans le cloud est une solution résiliente et économique qui protège les charges de travail contre les pannes sur site et la corruption des données, comme les attaques par ransomware. NetApp SnapMirror permet de répliquer les charges de travail VMware sur site utilisant un stockage connecté à l'invité vers NetApp Cloud Volumes ONTAP exécuté dans Azure. Il s'agit aussi des données applicatives, mais qu'en est-il des machines virtuelles elles-mêmes ? La reprise sur incident doit couvrir tous les composants dépendants, notamment les machines virtuelles, les VMDK ou les données d'application. Pour ce faire, SnapMirror et Jetstream peuvent être utilisés pour restaurer de manière transparente les charges de travail répliquées sur site vers Cloud Volumes ONTAP tout en utilisant le stockage VSAN pour les VMDK de VM.

Ce document présente une approche détaillée de la configuration et des performances de la reprise après incident à l'aide de NetApp SnapMirror, JetStream et d'Azure VMware solution (AVS).



# Hypothèses

Ce document est axé sur le stockage invité pour les données d'applications (également appelé « invité connecté »), et nous supposons que l'environnement sur site utilise SnapCenter pour assurer des sauvegardes cohérentes au niveau des applications.



Ce document s'applique à toute solution de sauvegarde et de restauration tierce. En fonction de la solution utilisée dans l'environnement, suivez les bonnes pratiques pour créer des stratégies de sauvegarde conformes aux SLA de l'entreprise.

Pour la connectivité entre l'environnement sur site et le réseau virtuel Azure, utilisez la voie express à portée globale ou un WAN virtuel avec une passerelle VPN. Les segments doivent être créés en fonction de la conception VLAN sur site.



Plusieurs options de connexion des data centers sur site à Azure restent disponibles. Ainsi, nous ne pouvons pas présenter un workflow spécifique dans ce document. Pour en savoir plus sur la méthode de connectivité, consultez la documentation Azure.

# Déploiement de la solution de reprise d'activité

## Présentation du déploiement de la solution

- 1. Assurez-vous que les données applicatives sont sauvegardées à l'aide de SnapCenter avec les exigences de RPO requises.
- 2. Provisionnez Cloud Volumes ONTAP avec la taille d'instance appropriée à l'aide de Cloud Manager dans l'abonnement et le réseau virtuel appropriés.
  - a. Configurer SnapMirror pour les volumes applicatifs concernés.

- b. Mettez à jour les règles de sauvegarde dans SnapCenter pour déclencher des mises à jour SnapMirror après les tâches planifiées.
- 3. Installez le logiciel JetStream DR dans le data Center sur site et commencez à protéger les machines virtuelles.
- 4. Installez le logiciel JetStream DR dans le cloud privé Azure VMware solution.
- 5. En cas d'incident, interrompre la relation SnapMirror avec Cloud Manager et déclencher le basculement des machines virtuelles vers des datastores Azure NetApp Files ou VSAN sur le site AVS dédié.
  - a. Reconnectez les LUN ISCSI et les montages NFS pour les machines virtuelles d'applications.
- 6. Annulez le rétablissement du site protégé après la restauration du site primaire.

#### Détails du déploiement

#### Configurez CVO pour Azure et répliquez les volumes dans CVO

La première étape consiste à configurer Cloud Volumes ONTAP sur Azure ("Lien") Et répliquez les volumes souhaités dans Cloud Volumes ONTAP avec les fréquences et les instantanés souhaités.

Health Status 💠	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful Transfer	(
0	gcsdrsqldb_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	
$\odot$	gcsdrsgilog_sc46 ntaphci-a300e9u25	gcsdrsqilog_sc46_copy ANFCVODRDemo	16 seconds	idle	snapmirrored	May 6, 2022, 11:43:52 AA 130.69 KiB	

#### Configurez l'accès aux données des hôtes AVS et CVO

Deux facteurs importants à prendre en compte lors du déploiement d'un SDDC sont la taille du cluster SDDC dans la solution Azure VMware et le délai de conservation d'un SDDC. Ces deux considérations clés à prendre en compte dans une solution de reprise sur incident permettent de réduire les coûts d'exploitation globaux. Le SDDC peut héberger jusqu'à trois hôtes, tout comme un cluster multi-hôtes dans un déploiement à grande échelle.

La décision de déployer un cluster AVS se base principalement sur les exigences en matière de RPO/RTO. Avec la solution Azure VMware, le SDDC peut être provisionné dans le temps en préparation des tests ou d'un incident. Un SDDC déployé juste à temps fait gagner des coûts d'hôtes ESXi lorsque vous ne traitez pas d'incident. Néanmoins, ce type de déploiement affecte le RTO de quelques heures lors du provisionnement du SDDC.

L'option la plus courante consiste à faire fonctionner le SDDC en mode de fonctionnement toujours actif avec un voyant allumé. Cette option réduit l'empreinte de trois hôtes disponibles en continu et accélère les opérations de reprise en fournissant une base en cours d'exécution pour les activités de simulation et les vérifications de conformité, ce qui évite le risque de dérive opérationnelle entre les sites de production et de reprise. Le cluster de lampe témoin peut être rapidement étendu au niveau souhaité si nécessaire pour gérer un événement de reprise après incident réel.

Pour configurer AVS (qu'il s'agit de IT à la demande ou en mode témoin lumineux), voir "Déploiement et configuration de l'environnement de virtualisation sur Azure". Avant cela, vérifiez que les machines virtuelles invitées résidant sur les hôtes AVS peuvent consommer des données depuis Cloud Volumes ONTAP une fois la connectivité établie.

Une fois que Cloud Volumes ONTAP et AVS ont été correctement configurés, commencez par configurer Jetstream pour automatiser la restauration des charges de travail sur site vers AVS (machines virtuelles avec VMDK des applications et machines virtuelles avec stockage « Guest ») à l'aide du mécanisme VAIO et en exploitant SnapMirror pour les copies de volumes d'applications vers Cloud Volumes ONTAP.

Le logiciel Jetstream DR est constitué de trois composants principaux : le serveur virtuel JetStream DR Management Server (MSA), le dispositif virtuel DR (DRVA) et les composants hôtes (packages de filtres E/S). MSA est utilisé pour installer et configurer des composants hôtes sur le cluster de calcul, puis pour administrer le logiciel JetStream DR. La procédure d'installation est la suivante :

- 1. Vérifiez les prérequis.
- 2. Exécutez l'outil de planification de la capacité pour obtenir des recommandations en matière de ressources et de configuration.
- 3. Déployez JetStream DR MSA sur chaque hôte vSphere du cluster désigné.
- 4. Lancez le MSA à l'aide de son nom DNS dans un navigateur.
- 5. Enregistrez le serveur vCenter avec MSA.
- Après le déploiement de JetStream DR MSA et l'enregistrement du serveur vCenter, accédez au plug-in JetStream DR avec le client Web vSphere. Pour ce faire, accédez à Datacenter > configurer > JetStream DR.



- 7. À partir de l'interface JetStream DR, effectuez les tâches suivantes :
  - a. Configurez le cluster avec le package de filtre d'E/S.

JetStream DR				fi.
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	00000000-0000-000	00-0000-000000000001 Configure		
Tenant ID / Application ID	- <u>Configure</u>			
Application Secret	- <u>Configure</u>			
Configured Clusters	Configure Clusters			
Configure Cluster 1 Upgrade 1 Unconfigure 1 Res		Select All Clear All C	a,	٩
Cluster Name	Cluster Name	Datacenter Name	sion 🔺	Host Defails 🔺
No cluster configured	A300-Cluster	A300-DataCenter	*	
		Cancel Configu	ure	

b. Ajoutez le stockage Azure Blob situé sur le site de reprise.

Storage Sites	Add Storage Site	
+ Add Storage Site	Strate Sta Ture *	
Name A	Azure Blob Storage	
No Storage Site configured.		
	Access Type *	
	Ney ALCOS	
	Storage Site Name (Provide a name to identify this Site) *	
	ANFDemoblobrepo	
Storage Site Details Alarma	Agure Bob Storage Account Name *	
	anfdrdemostor	
No storage site selected. Select a storage		
	Ature Bob Storage Account Key*	

8. Déployez le nombre requis d'appliances virtuelles de reprise sur incident (DR) dans l'onglet appliances.



Utiliser l'outil de planification de la capacité pour estimer le nombre d'ACR requis.

letStream DR Protected Domains St	atistics	Storage Sites	Appliances	Configurations	Task Log			Ē
DRVAs (DR Virtual Applia	nces)				200 200 All 1993			
+ Deproy New DRVA	Ipgrade	0 Unconfigure						۹
Name 🔺				Status 🔺	Child Alarm 🔺	Software Version 🔺	Details 🔺	
No DR Virtual Appliance contig	jured.							
Replication Log volume								
+ New Replication Log Volum	e Un	configure						q
Disk Path Name 🔺				Status	Child Alarm 🔺	Size (available/total)	Details 🔺	
No DRVA selected. Select a D	RVA to view	v replication log volume	s.					

Protected Domains	Statistics	Storage Sites	Deploy New DR Virtua	I Appliance (DRVA)					
DRVAs (DR Virtual A	ppliances)		1. General	2. DRVA VM	3. DRVA Network	4. Summary			
+ Deploy New DRVA	t Upprade	ti Lincontigura	Name		GCSDRPD001		1		Q
Name A			Description (Optional	0	Protected Domain for VMs with	ANF and JS		Details A	
No DR Virtual Appliance	configured.		Datacenter		A300-DataCenter				
	100.00400.000		Cluster		A300-Cluster				
			Resource Pool (Optio	inal)					
			VM Folder (Optional)						
Peplication Los Valu		-	Datastore		A300_NFS_vMotion				
Replication Log volu	and the second second	_	Number Of CPUs		8				
+ MH Replication Log	vourre Stinco	ent/gune	Memory Size		32GB				Q
Disk Path Name			Management Network	(	VM_187			Details 🔺	
No DRVA selected Sele	et a DRVA to view	replication los volum	Host(iofilter) to DRVA	Data Network	VM_187				
			Replication Network	to Object Store	VM_187		_		
			Replication Log Netw	ork	VM_187				
					Cancel Back				

9. Créez des volumes de journal de réplication pour chaque DRVA à l'aide du VMDK provenant des datastores disponibles ou du pool de stockage iSCSI partagé indépendant.

Protected Domains	Statistics	Storage Sites	Appliances	Configurations	Task Log			
DRVAs (DR Virtual Ap	opliances)	HE						
+ Deploy New DRVA	t uppade	D Unconfigure						C
Name 🔺				Status 🔺	Child Alarm 🔺	Software Version 🔺	Details 🔺	
GCSDRPD001				Running	00	4.0.0.134	Details	
+ New Replication Log V	Aolume 🛙 🕮 Uri	cantaure.						c
Disk Path Name				Status	Child Alarm	Size (available/total) 🔺	Details A	
idev/sdb				O Ok	<b>0</b> 0	179 88 GB / 200 GB	Detats	
Replication Log Volu	me Details							

10. À partir de l'onglet domaines protégés, créez le nombre requis de domaines protégés à l'aide des informations concernant le site Azure Blob Storage, l'instance DRVA et le journal de réplication. Un domaine protégé définit un ordinateur virtuel ou un ensemble de VM d'applications spécifiques au sein du cluster, qui sont protégés ensemble et ont un ordre de priorité pour les opérations de basculement/retour arrière.

I. General     2. Primary Site     3. Summary       Protected Domain Name     GCSDRPD_Demo01       Priority Level (Optional)     -       Description     Protection domain ANF       Total estimated data size to be protected     1000GB       DR Virtual Appliance     GCSDRPD001       Compression Level     Default       Normal GC Storage Overhead     300%       Replication Log Storage     /dev/sdb	elect Protected Domain: * View all	Create Protected Domain			+ Create = Mg
Protected Domain NameGCSDRPD_Demo01Priority Level (Optional)-DescriptionProtection domain ANFTotal estimated data size to be protected1000GBDR Virtual ApplianceGCSDRPD001CompressionYesCompression LevelDefaultNormal GC Storage Overhead50%Maximum GC Storage Overhead300%Replication Log Storage/dev/sdb		1. General 2.	Primary Site	J. Summary	
Priority Level (Optional)-DescriptionProtection domain ANFTotal estimated data size to be protected1000GBDR Virtual ApplianceGCSDRPD01Compression LevelDefaultNormal GC Storage Overhead50%Maximum GC Storage Overhead300%Replication Log Storageidev/sdb		Protected Domain Name	GCSDRPD_Demo01		
DescriptionProtection domain ANFTotal estimated data size to be protected1000GBDR Virtual ApplianceGCSDRPD001Compression LevelDefaultNormal GC Storage Overhead50%Maximum GC Storage Overhead30%Replication Log Storageidevis/b		Priority Level (Optional)			
Total estimated data size to be protected     1000GB       DR Virtual Appliance     GCSDRPD001       Compression     Yes       Compression Level     Default       Normal GC Storage Overhead     50%       Maximum GC Storage Overhead     300%       Replication Log Storage     /devistb		Description	Protection domain ANF		
DR Virtual Appliance     GCSDRPD001       Compression     Yes       Compression Level     Default       Normal GC Storage Overhead     50%       Maximum GC Storage Overhead     300%       Replication Log Storage     /devisdb		Total estimated data size to be protected	1000GB		
Compression     Yes       Compression Level     Default       Normal GC Storage Overhead     50%       Maximum GC Storage Overhead     300%       Replication Log Storage     /dev/sdb		DR Virtual Appliance	GCSDRPD001		
Compression Level     Default       Normal GC Storage Overhead     50%       Maximum GC Storage Overhead     300%       Replication Log Storage     /dev/sdb		Compression	Yes		
Normal GC Storage Overhead     50%       Maximum GC Storage Overhead     300%       Replication Log Storage     /devis/db		Compression Level	Default		
Maximum GC Storage Overhead 300% Replication Log Storage /devisidb		Normal GC Storage Overhead	50%		
Replication Log Storage /devis@		Maximum GC Storage Overhead	300%		
		Replication Log Storage	/dev/sdb		
Panlication Los Size 50/08		Panlication I on Size	500 P		



11. Sélectionnez les VM à protéger et regroupez-les dans des groupes d'applications en fonction de la dépendance. Les définitions d'application vous permettent de regrouper des jeux de machines virtuelles en groupes logiques contenant leurs ordres de démarrage, leurs retards de démarrage et les validations d'applications en option qui peuvent être exécutées à la reprise.



Assurez-vous que le même mode de protection est utilisé pour toutes les machines virtuelles d'un domaine protégé.

Le mode Write-Back (VMDK) offre de meilleures performances.

elect Protected Domain: GCSDRPD_Demo01 *	Start Protectio	on .				+ Create	Delata = bio
ecoverable / Total VMs							Eas D
epication Status	Protection Mod	e for poinched VMg 🔍			q		nesan
emaining Background Data	VM Name		# of Disks	Protection Mod	10	LOCAL ( 172 21 253 16	51
	ElasticWe	bA2	1		× . *	Thubbed	-Constant
area ees	ElasticWe	bA3	1		~		
Development Aller	ElasticWe	680	1		Ψ.		
Produced with Secondar Owning	<ul> <li>ElasticWe</li> </ul>	bB1	it.		÷.,		
+ Otart Brothardina (# Taran Damastan)	ElasticWe	682	18		w .		
T SHELFIOLOGO	ElasticWe	bB3	./ <b>T</b>	Write Through	w		
VM Name 🔺	GCS-DR-	DC	1	Write-Through	- N	Background Data 🔺	Debils
NO VM is producted	C GCS-DR-	LinVM01	4	Write-Through	~ ~		
	GCS-DR-	SCA	.1	Write-Through	~		
	GCS-DR-	SQL01	.4	Write-Through	~		
	GCS-DR-	WittVM01	1	Write-Through	~		
	🔲 jas-drva-C	ICSDRPD001	2		19 A		
	PrimeCile	est	2				
	Standby0		1	Write Through	¥		
	Standby1		1		w.,		
	Standby?				¥1.		
	Standby3		1		× .		
	VMmark-1	Template01	1		M. 4		
				Cancel	Start Protection		

12. Assurez-vous que les volumes des journaux de réplication sont placés sur un stockage haute performance.

	Start Protection				
				1	Edi De
ication Status	Write-Back(VMDK) •			٩	ANFORDemoFalloverSite
wining Background Data	VM Name 🔺	# of Disks	Protection Mode		LOCAL (172,21,253,169.)
	ElasticWebA2	1	Write Through	10 C	Destroyed
numes:	ElasticWebA3	1	White Through	2.	- 8150 MA
Automatical Continues Advances	ElasticWebB0	1	white-Through	¥.	
Selling Selling	ElasticWebS1	1	Write-Through	ν,	
Charl Data man	ElasticWebB2	1	Wrbi-Through	¥.	
Start Processor	ElasticWeb63	1	Write-Through	9	
VM Name 🔺	gcs-bR-bC	1	White-Back(VMDK)	~	Bockground Data A Details
to VM is protected.	GCS-DR-LinVM01	3	Write-Back(VMDK)	~	
	GCS-DR-SCA	1	Write-Back(VMDK)	*	
	GCS-DR-SQL01	1	Write-Back(VMDK)	~	
	GCS-DR-WeVM01	31	Write-Back(VMDK)	~	
	jst-dva-GCSDRPD001	2		N.S.	
	PrimeClient	2		× .	
	C Standby0	1	winter Through	Ý.	
	Standby1	1		21	
	Standby2	1	White Through	10 A	
	Standby3	1	Write-Through	10	
	VMmark-Template01	1		10.00	
			1 10000 1 1 AV	( Distanting )	

13. Une fois que vous avez terminé, cliquez sur Démarrer la protection du domaine protégé. La réplication des données démarre pour les machines virtuelles sélectionnées vers le magasin de objets blob désigné.

JeuSuream Dri Protected Domains Statistics Stora	ge Sites Appliances Configurations T	Task Log		1	Running Tasks	
elect Protected Domain: GCSDRPD_Dem	o01 ▼ <u>View all</u>			+ (	Start Protection (GCS-DR-SCA) 5	0%
Recoverable / Total VMs		0/5	Configurations		Start Protection (GCS-DR-Win 5	0%
Replication Status		ок	Storage Site	ANFDRDe	Start Protection (GCS-DR-Lin 5	0%
			Owner Site	LOCAL ( 172.2	Ored Destanting (DOD DD DD)	-
Remaining Background Data		0 B	Datacenter \ Cluster	A300-DataCen	Statt Protection (GCS-DR-DC) 5	10.20
Current RPO			Point-in-time Recovery	Disabled	Start Protection (GCS-DR-SQ 5	0%
					Configure VMDK Re Completed	<b>V</b>
Protected VMs         Settings         Alarms           + Start Protection         III Stop Protection					Close	ų
Protected VMs     Settings Alarms     Start Protection     VM Name	Protection Status 🔺 Re	eplication Sta	itus 🔺 Protection Mode 🔺	Background Da	Close	ų
Protected VMs Settings Alarms  + Start Protection VM Name GCS-DR-DC	Protection Status ▲ Re Ø Initializing	eplication Sta	tus  Protection Mode  Write-Back(VMDK)	Background Da	Close ta A Details Details	ų
Protected VMs     Settings:     Alarms       + Start Protection     It Stop Protection       V M Name ▲       GCS-DR-DC       GCS-DR-LinVM01	Protection Status  Protection Status O Initializing O Initializing -	eplication Sta	tus ▲ Protection Mode ▲ Write-Back(VMDK) Write-Back(VMDK)	Background Da -	Close ta A Details Dataits Dataits	ų
Protected VMs Settings Alarms  + Start Protection  VM Name ▲  GCS-DR-DC  GCS-DR-SCA	Protection Status  Protection Status Protection Status Protection	eplication Sta	tus Protection Mode Write-Back(VMDK) Write-Back(VMDK) Write-Back(VMDK)	Background Da - -	Close ta A Details Details Details Details	ų
Protected VMs Settings Alarms  + Start Protection  VM Name  GCS-DR-DC GCS-DR-LinVM01 GCS-DR-SCA GCS-DR-SC01	Protection Status A Re Initializing - Initializing - Initializing - Initializing -	eplication Sta	tus ▲ Protection Mode ▲ Write-Back(VMDK) Write-Back(VMDK) Write-Back(VMDK) Write-Back(VMDK)	Background Da - - -	Ckose ta  Oetalis Detalis Detalis Detalis Detalis Detalis Detalis Detalis	ų

14. Une fois la réplication terminée, l'état de protection de la VM est marqué comme récupérable.

rotected Domains Statistics Storage	e Sites Appliances Configurat	ions Task Log				l
elect Protected Domain: GCSDRPD_Demo	01 ▼ <u>View all</u>			+ Create	Delete	≡ More
ecoverable / Total VMs		5/5	Configurations			Edit Detail
eplication Status		ок	Storage Site	ANFDRDemoFallo	verSite	
		1000	Owner Site	LOCAL ( 172.21.253.16	50.)	
emaining Background Data		0 B	Datacenter \ Cluster	A300-DataCenter \ A30	0-Cluster	
urrent RPO		0s	Point-in-time Recovery	Disabled		
Protected VMs Settings Alarms						
Protected VMs Settings: Alarms  + Start Protection  VM Name	Protection Status 🔺	Replication Sta	tus 🔺 Protection Mode 🔺	Background Data 🔺	Details	٩
Protected VMs Settings Alarms  + Start Protection  VM Name  GCS-DR-DC	Protection Status 🔺	Replication Sta	tus ▲ Protection Mode ▲ Write-Back(VMDK)	Background Data 🔺 0 B	Details Details	٩
Protected VMs Settings: Alarms   Start Protection VM Name 4  GCS-DR-DC GCS-DR-LinVM01	Protection Status 🔺 🛛 Recoverable 🖉 Recoverable	Replication Sta	tus Protection Mode A Write-Back(VMDK) Write-Back(VMDK)	Background Date 🔺 0 B 0 B	Details Details Details	٩
	Profection Status ▲ © Recoverable © Recoverable @ Recoverable	Replication Sta	tus Protection Mode Virite-Back(VMDK) Write-Back(VMDK) Write-Back(VMDK)	Background Data A 0 B 0 B 0 B	Details Details Details Details	٩
Protected VMs Settings Alarms     Start Protection     VM Name ▲     GCS-DR-DC     GCS-DR-SCA     GCS-DR-SCA     GCS-DR-SCA	Protection Status ▲ © Recoverable © Recoverable © Recoverable © Recoverable	Replication Sta OK OK OK OK	tus ▲ Protection Mode ▲ Write-Back(VMDK) Write-Back(VMDK) Write-Back(VMDK) Write-Back(VMDK)	Background Data ▲ 0 B 0 B 0 B 0 B	Details Details Details Details Details	٩

(

Les runbooks de basculement peuvent être configurés pour regrouper les VM (appelé groupe de reprise), définir l'ordre de démarrage et modifier les paramètres CPU/mémoire avec les configurations IP.

15. Cliquez sur Paramètres, puis sur le lien Runbook Configure pour configurer le groupe Runbook.

		( states				
select Protected Domain: GCSDRPD_Demoon • View all		+ Create	Delete	= More		
Recoverable / Total VMs 57	Configurations			Edit Detai		
Replication Status	Storage Site	ANFDRDemoFail	overSite	1		
	Owner Site	LOCAL ( 172.21.253.160 )				
Remaining Background Data 0 B	Datacenter \ Cluster	A300-DataCenter \ A3	00-Cluster			
Current RPO	Point-in-time Recovery	Disabled				
0.0						
Protected VMs Settings Alarms						
Failover Runbook Not Configured Configure						
Test Failover Runbook Not Configured Configure						
Fallback Runbook 🔓 Not Configured Configure						
Memory Setting Not Configured Configure						
GC Settings Configured Configure						
Concurrency Settings Not Configured Configure						

16. Cliquez sur le bouton Créer un groupe pour commencer à créer un nouveau groupe de runbook.



Si nécessaire, dans la partie inférieure de l'écran, appliquez des pré-scripts personnalisés et des post-scripts pour s'exécuter automatiquement avant et après l'opération du groupe Runbook. Assurez-vous que les scripts Runbook résident sur le serveur de gestion.

JebSbream DR Protected Domains Statistics Storage Sites	Failover Runbook Settings				圕
Select Protected Domain: GCSDRPD_Demo01 *	+ Create Group	Delete Group		+ Create Delete	
Recoverable / Total VMs	O Sroup Name	# of VM Power Off	Retain MAC	Edd Det	Alt
Replication Status	O 🗌 Independent VMs	5 -		ANFDRDemoFalloverSite	-
Remaining Background Data				A300-DataCenter ( A300-Cluster	
Current RPO				Disabled	
Protected VIMs Settings Alarms	0 0				
Failover Runbook Configured Details					
Test Failover Runbook Configured Details					
Fallback Runbook Configured Details					
Memory Setting Not Configured Configured					
GC Settings Configured Configure					
Concurrency Settings Not Configured Configures					

17. Modifiez les paramètres de la machine virtuelle selon vos besoins. Spécifier les paramètres de restauration des VM, y compris la séquence de démarrage, le délai de démarrage (spécifié en secondes), le nombre de CPU et la quantité de mémoire à allouer. Modifier la séquence de démarrage des machines virtuelles en cliquant sur les flèches vers le haut ou vers le bas. Des options sont également fournies pour conserver MAC.

JebSbream DR Protected Domains Statistics Stored	Create Runbook Group										
Select Protected Domain: GCSDRPD_Demo	1. General	2. Select VM		3. Edit V	M Settings		4. Summ	arv	+ Create	III Delitte	≡ Mort
Recommine / Toble VMs	Retain MAC		Power Of	f VMs			O Recet				
Replacion Status	VM Name	Boot Sequence	Boot Delay	CPU	Memory	Script	NIC		FDRDembFlidev	erSite	
Rephining Baskground Cinta	GCS-DR-WinVM01	17 1	0s	32	64 GB	Config	View		And a start a stor		
Commun TIDO	GCS-DR-SCA	21 4	0s	4	16 GB	Config	View		receiver a second		
CHIRGIN 1990	GCS-DR-DC	3 11h-1	0s	4	16 GB	Config	View				
Destadant with Settlene Arenne	GCS-DR-LinVM01	41 4	0s	2	4 GB	Config	View				
FIGURE FIRE OFFERE	GCS-DR-SQL01	5↑↓	05	4	8 GB	Config	View	*			
Fallback Runbook Configured Editals Memory Setting Hits Configured Cooldage GC Settings Configured Cooldage Concurrency Settings Not Configured Cooldage				Са	ncel	Back		Next			

18. Les adresses IP statiques peuvent être configurées manuellement pour les machines virtuelles individuelles du groupe. Cliquez sur le lien vue NIC d'une machine virtuelle pour configurer manuellement ses paramètres d'adresse IP.

Protected Domains	Statistics Storag	Create Runbook Group										
Select Protected Dom	ain: GCSDRPD_Demo	1 General	2 Select VM		1 Edit V	Settinos		4 Summary		+ Create	Delete	≣ Moru
	6 T	The second second			(186	a octango			-			
		Norden minis			- ¥ 1952			O Reset		FORDemoFallow	ATS Re	
		VM Name	Boot Sequence	Boot Delay	CPU	Memory	Script	NIC		172 21 253 16		
	Duta	GCS-DR-WinVM01	1↑↓	0s	32	64 GB	Config	Vigw		DataCenter's A30	Chister:	
		GCS-DR-SCA	2↑↓	Qs	4	16 GB	Contig	View		(t)		
		GCS-DR-LinVM01	31 1	0s	2	4 GB	Config	View				
	kenings Alanna	GCS-DR-SQL01	41 1	0s	4	8 GB	Config	View				
	Same and the second second	GCS-DR-DC	5† J	0s	4	16 GB	Config	Xiew -				
Coscumency Settings	Compared Carthaus											
					Car	ncel	Back	Ne	đ			

19. Cliquez sur le bouton configurer pour enregistrer les paramètres NIC pour les machines virtuelles respectives.

	Label	Network Name	Key	PCI Slot #	IP	
<b>1</b>	Network adapter	1 VM_3510	4006	192	Configure	aty
Re						
						and the second
VM No						
GCS-E	Con	figure Static IP Addres	s			
Ubunt						
GCSD	PA	dress *				
66.9-6	172	21.254.185				
Van	0-0					
	Subr	et Mask *				
	255	255.255.0				
	Gana	way *				
	172	.21.254.1				
	DNS	-				
	172	.30.153.20				
		0.00				
	UN	s anus.				
		N 20 POW				
		Reset	Can	cel Confi	gure	
				5		
					Close	Next
					1	
NAMES OF TAXABLE PARTY.			110			
	Subries Horap	ate Runbook Group				
	ain: GCSDRPD_Demo	1. General Z. Select VM	S. Edit VM S	Settings 4. Summa	te Owner (	
		Group Name	GCSRecovery		-	
	dish.	Number of VMs Retain VM's MAC addresses	5 trué		1197221253 100 1	
		Power Off VMs	false		1	
		oroup manguing and boot sequence change	will be applied to both Fallover a	and Failback runbook.		

L'état des runbooks de basculement et de retour arrière est désormais répertorié comme configuré. Les groupes de runbooks de basculement et de retour arrière sont créés par paires en utilisant le même groupe initial de machines virtuelles et de paramètres. Si nécessaire, les paramètres d'un groupe de runbook peuvent être personnalisés individuellement en cliquant sur son lien Détails respectifs et en

QK

Il est recommandé de créer à l'avance un cluster Pilot-light à trois nœuds sur le site de récupération (AVS). L'infrastructure du site de reprise peut ainsi être préconfigurée, notamment :

- · Segments de réseau de destination, pare-feu, services comme DHCP et DNS, etc
- Installation de JetStream DR pour AVS
- · Configuration des volumes ANF comme datastore et plus encore

Jetstream DR prend en charge un mode RTO proche de zéro pour les domaines stratégiques. Pour ces domaines, le stockage de destination doit être préinstallé. ANF est un type de stockage recommandé dans ce cas.



La configuration réseau comprenant la création de segments doit être configurée sur le cluster AVS afin de répondre aux exigences sur site.



Selon les exigences des contrats de niveau de service et de durée de restauration, vous pouvez utiliser un mode de basculement continu ou standard. Pour un RTO proche de zéro, vous devez commencer la réhydratation continue sur le site de restauration.

1. Pour installer JetStream DR pour AVS sur un cloud privé Azure VMware solution, utilisez la commande Exécuter. Depuis le portail Azure, accédez à la solution VMware Azure, sélectionnez le cloud privé et sélectionnez Exécuter la commande > packages > JSDR.Configuration.



L'utilisateur CloudAdmin par défaut de la solution Azure VMware ne dispose pas des privilèges suffisants pour installer JetStream DR pour AVS. La solution Azure VMware permet une installation simplifiée et automatisée de JetStream DR en appelant la commande Azure VMware solution Run pour JetStream DR.

La capture d'écran suivante montre l'installation à l'aide d'une adresse IP DHCP.

Storage       Automation	Microsoft Azure	JP Search resour	ces, services, and docs (G+/)	🗈 😂 🖓 🗇 🗇 🕫 niyaz@netapp.com 🧕
As Areas control (AM)     Such (Chick)     Access control (AM)     Such (Chick)     Suc	Home > ANFDataClus			Run command - Install-JetDRWithDHCP ×
P Starth (Cht - ) <ul> <li>March MAN</li> <li>Togs</li> <li>Dogs and Store products</li> <li>Starting</li> <li>Dogs and Store products</li> <li>Starting</li> <li>Name</li> <li>Docifytion</li> <li>Store Control (Anth)</li> <li>Store Control (Control (Anth)</li> <li>Store Control (Control (Cont</li></ul>	ANFDataClus   Run	command —		This top local Credial Descriptuits left's fundate from MMC creates a page user assors
A Access control (MAK) Fackages Run execution status: A locus control (MAK) Fackages Run execution status: Name Description Setting: Conscription: Storage and solve problems: Setting: Conscription: Conscripti	🔎 Seatch (Citt+/) =	C Refresh 🛱 Feedback		elevated privileges to the user, deploys JetDr Management Server Appliance(MSA), registers vCenter to the JetDr MSA, configures duster.
✓       Name       Decription         ✓       Name       Decription         ✓       SDR_Configuration 12:8       Freewood interfactor interfacto	Access control (IAM)	Packages Run execution status		Command parameters
Settings <ul> <li>BORConfiguration 334</li> <li>Neverent feature to simplation at discense to 46. Ner galaxets tables tables</li></ul>	Diagnose and solve problems	<ul> <li>Name</li> </ul>	Description	RegisterWithip () True
▲ Locks       Disable-leftDS/orDate:       This Christer so duster but doesn't uninitial liefDA completely so other cluster         ▲ Locks       Disable-leftDS/orDate:       This Christer so duster but doesn't uninitial liefDA completely so other cluster         ▲ Conscritivity       Erable-leftDS/orDate:       This Christer So maked setD for christer to the left MAS configures a new user, assigns to the left MAS configures duster.       Disable-leftDS/orDate:       Disable-leftDS/orDate:         ▲ Conscritivity       Instat-leftDS/orDate:       This to pleved Christe Downloads setD for bundle from MAS, contess a new user, assigns to the left MAS configures duster.       Disable-leftDS/orDate:       Mame *       Disable-leftDS/orDate:         ▲ Boornent policies       Inscent-PrelightLeftDR/minutal       This Christer to the left MAS configures duster.       Disable-leftDS/orDate:       Disable-leftDS/orDate:         ▲ Boornent policies       Inscent-PrelightLeftDR/minutal       This Christer to the left MAS configures duster.       Disable-leftDS/orDate:       Disable-leftDS/orDate:         ▲ Add oni:       Uperstatel leftDR       This Christer contest a new user, assigns elevated privilenges to the later.       Disable-leftDS/orDate:       Disable-leftDS/orDate:         ▲ Post:       Uperstatel leftDR       This Christer contest a new user, assigns elevated privilenges to the later.       Disable-leftDS/orDate:       Disable-leftDS/orDate:         ▲ Post:       Uperstatel leftDR       This Christer	Settings	<ul> <li>ISDR Configuration (224) Powerner</li> </ul>	Masule to contrauration at lettimore Software on 205 See <u>information Software, ins</u> for subject	ProtectedCluster * (j)
Vock     police.       Manage     Endet = deCRG inclusted management       © connectivity     Instatil-indCRW/indCHAP       © connectivity     Inscale-indCRW/indCHAP       © conne     Inscale-indCRW/indCHAP	0 toda	Disable-letDRForCluster	This Cmdlet unconfigures a cluster but doesn't uninstall letDR completely so other clusters	Outer-1
Minage       Enable-MEDIGEO/Later       This Cindlet configures an addocinal duster for protection. It easts his bits to all hosts in the       semiDitative         © Connectivity       Instal-leiDRWindCakcO       This top level Cindlet Configures dustas.       This top level Cindlet Configures dustas.       Windle Hosts in the         © Lotrers       Instal-leiDRWindCakcO       This top level Cindlet Configures dustas.       This top level Cin	E was		policies.	Detestore * 🕢
Connectivity Install-iedDRWindStakCP This top level Gndiet Dounloads JerD Founde from MAES, creates a new user, satights is install-iedDRWindStakCP Install-iedDRWindStakCP This top level Gndiet Dounloads JerD Founde from MAES, creates a new user, satights is install-iedDRWindStakCP Install-iedDRWindStakCP This top level Gndiet Dounloads JerD Founde from MAES, creates a new user, satights is install-iedDRWindStakCP Install-iedDRWindStakCP This top level Gndiet Dounloads JerD Founde from MAES, creates a new user, satights is install-iedDRWindStakCP Install-iedDRWindStakCP This top level Gndiet Dounloads JerD Founde from MAES, creates a new user, satights is install-iedDRWindStakCP Inscene PreligiteidDRenstal This Creater is the JerD FW MAE, configures durate is selend and display current tate of the system it theids shelther the invition of A hosts. If the clutter details are correct, if their is selend and violation grame tate of the system it registers to the MED. Worklaad Networking Unitable iedDR Unitable iedDR This top level Gndiet cortex a new user, satight elevel and isolation cortex. If their is selend and violation grame tate of the system it registers to the MED. Worklaad Networking Unitable iedDR This top level Gndiet cortex a new user, satight elevel and if any Vionter is registered to the MED. MococortulySManagement 4:887 Worklaad Networking Worklaad Networking Vincture is the install iedDR/WindStakCP The top level Gndiet cortex a new user, satight elevel and with the same and provide the install iedDR/WindStakCP NococortulySManagement 4:887 Worklaad Networking Unitable iedDR NococortulySManagement 4:887 Worklaad Networking Unitable iedDR NococortulySManagement 4:887 Worklaad Networking Unitable iedDR NococortulySManagement 4:887 Worklaad Networking <p< td=""><td>Manage</td><td>Enable-JetORForCluster</td><td>This Condiet configures an additional duster for protection. It installs vibs to all hosts in the</td><td>vsanDatastore</td></p<>	Manage	Enable-JetORForCluster	This Condiet configures an additional duster for protection. It installs vibs to all hosts in the	vsanDatastore
Custors       registers (center to the Arth ASA configues cluster.         Is dentry       Instat-set/DRW/m6tatioP       This top level (mile Low/M6SA subb subb toucle from MAS, creates a new user, subjes e (custor)       Custors         Storage (serview)       Instat-set/DRW/m6tatioP       This top level (mile Low/M6SA subb subb toucle from MAS, creates a new user, subjes e (custor)       Custors       Custors         B bioment policies       Inscie Prelighted/DRW/m6tatioP       This Credit cluster details are correct. If there dustor details are correct, and if any VCenter is registered to the MSA       Custors       Custors         Workaad Networking       Uonstats/set/DR       This Credit creates a new user, subjes e cluster       Inscie Prelighted/DR/minutal       This Credit creates a new user, subjes e cluster       Custors       Inscie Prelighted/DR/minutal       Previous (custor)       Custors       Inscie Prelighted/DR/minutal       Custor (custor)       Custors	Connectivity	Install-JetDRWathDHCP	This top level Crediet Downloads JetDr trundle from MMS, creates a new user, assions elev-	VMName* ()
Install-indDRWindtatedP     This ippeed finale Dewords suffic bundle from MMS proteins a new user, assigns eight registers vicenter is to be JerDr MSA configure duster.     Duster* 0       Storage ipperiend     Inscke-PrelightietDRWindtatedP     This ingelied index and digings current take of the system it decks whither the initiation of the decks and digings current take of the system it decks whither the initiation of the system it decks whither the unit initiation of the system it decks whither the initiation of the system it decks whither the initiation of the system it decks whither the unit initiation of the system it decks whither the initiation of the system it decks	Cutters	20	registers vCenter to the JetDr MSA, configures cluster.	anfjsval-msa
Sorage [prevent]     Sora		Install-JetDRW/@6taticJP	This top level Cmtilet Downloads JetDr bundle from MMS, creates a new user, assigns elevi	Cluster* ()
Storage [steried]       Incke-PreligiteIdER.netal       The Condet doda and displays ourmet take of the system in the doda whether the neineral A hosts. If the cluster details are correct, if there is sheap? a VM with the same name provide in the doda and displays ourmet take of the system in the dods whether the neineral A hosts. If the cluster details are correct, if there is sheap? a VM with the same name provide in the dod and displays ourmet take of the system in the dods whether the neineral A hosts. If the cluster details are correct, if there is sheap? a VM with the same name provide in the dod and displays ourmet take of the system in the dods whether the neineral A hosts. If the cluster details are correct, all there is sheap? a VM with the same name provide in the dod and displays ourmet take of the system in the dods whether the neineral A hosts. If the cluster details are correct, all there is sheap? a VM with the same name provide in the dod and displays ourmet take of the system in the dods whether the neineral A hosts. If the cluster details are correct, all there is sheap? A VM with the same name provide in the dod and displays ourmet take of the system in the dods whether the neineral A hosts. If the cluster details are correct, all there is sheap? A vertice of the dod and displays ourmet take of the system in the dods whether the neineral A hosts. If the cluster details are correct and if any VCenter is registered to the MGA.	- spentity		registers vCenter to the JetDr MSA, configures cluster.	Outer-1
Becoment policies     A note.     A n	Storage (preview)	Invoka-PreflightletDRInutall	This Cridlet checks and displays current state of the system it checks whether the minimal	Credential ()
Add on:     Invoke-PreligitedDRUbrestall     The Cordet check and Digits current take of the system it checks whether the minimul     Anotat, if the colds and Digits current take of the system it checks whether the minimul     Anotat, if the colds and Digits current take of the system it checks whether the minimul     Anotat, if the colds and Digits current take of the system it checks whether the minimul     Anotat, if the colds and Digits current take of the system it checks whether the minimul     Anotat, if the colds and Digits current take of the system it checks whether the minimul     Cold     Colds     Segments     Monoport.ArS Management, 4500     Versus current take of the system it checks whether the minimul     Colds     Dick     Colds	Placement policies		4 hosts, if the cluster details are correct, if there is already a VM with the same name provic	Username *
Verklaad Networking     Usinstali ketDR     The top level Credies in revules as revules as in revules to it is reverse in revules as in revules as in revules to it is reverse in reverse in revules as in revules as in revules as in reverse i	+ Add-oni	Invola-PreflightletDRUwinstall	This Cindlet checks and displays current state of the system it checks whether the minimal A basis of the cluster details are conset and if any Wester's resistance to the MSA	toot
Worklaad Networking         UmittabilitER         The top level Cindlet consists in new later, sagans elevated priviliteges to the user, unconfige         Immuno			<ul> <li>Costa, in one costate design are context and in any inclusion in registrers to ane mum</li> </ul>	Password *
September     September	Workload Networking	Uninstall-letDR	The top level Gridlet creates a new user, assigns elevated privileges to the user, unconfigu-	
Im DRCP     imfgruiti-ma       Im Port meroring     Network * ①       Im Port meroring     Network * ①       Im Port meroring     DRG       Im Port meroring     Dreas       Im Port meroring     Breas up to	Segments	> MicrosoftAVSManagement +147	Versus ondets for estillativities even taxs in managing Azure VMMane Souttans	HostName ()
IP Fort minoring     Network * ③       ONS     DRSeg       Operations     Dreals       Reserved     Retain up to	T DHOP			anfpval msa
DNS         DRSeg           Operations         Declass           Per sections         Britain up to	Port minoring			Network*
Operations Details Retain up to	O DNS			DRSeg
Retain up to	Operations			Details
	- Due commend			Retain up to

2. Une fois l'installation de JetStream DR pour AVS terminée, actualisez le navigateur. Pour accéder à l'interface de reprise après incident JetStream, allez dans SDDC Datacenter > configurer > JetStream

rotected Domains	Statistics	Storage Site	es Ap	pliances	Configurations	Task Log	a	
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						
Subscription ID		- Config	ure					
Tenant ID / Application	ID	- Config	ure					
Application Secret		- Config	ure					
Configure Cluster	1 Upgrade	Duconfigure	* Resolv	e Configure Iss	ue			C
Cluster Name		Datacenter	Name 🔺	Status 🔺	Software Ve	ersion 🛦	Host Details	
Cluster-1		SDDC-Data	center	🔮 Ok	4.0.2.132		Details	

- 3. À partir de l'interface JetStream DR, effectuez les tâches suivantes :
  - a. Ajoutez le compte Azure Blob Storage qui a été utilisé pour protéger le cluster sur site en tant que site de stockage, puis exécutez l'option Scan Domains.
  - b. Dans la boîte de dialogue qui s'affiche, sélectionnez le domaine protégé à importer, puis cliquez sur son lien Importer.

JebSbream DR Protected Domains Statistics Storage Sites	Available Protected Domain(s) For Import	E
Storage Sites + Add Storage Site Name A WiFDemobilobreporec	Protected Domain         Description         Recoverable V         VMs         Import           GCSDRPD_Demo01         Protection domain ANF         5         5         Import	es Blob Storage

4. Le domaine est importé pour la récupération. Accédez à l'onglet domaines protégés et vérifiez que le domaine prévu a été sélectionné ou choisissez le domaine souhaité dans le menu Sélectionner un domaine protégé. La liste des VM récupérables du domaine protégé s'affiche.

letStream DR Protected Domains Statistics Storage Sites Appliances	Configurations Task	Log			
elect Protected Domain: GCSDRPD_Demo01 👻 View all			+ Create	Delete	≡More
lode	Imported	Configurations			Deta
Recoverable / Total VMs	5/5	Storage Site Owner Site	ANFDemoblobrepore	ec	
VII Name	Protection Status		Protection Mode	Details	c
GCS-DR-DC	@ Recoverable		Write-Back(VMDK)	Details	
GCS-DR-LinVM01	O Recoverable		Write-Back(VMDK)	Details	
GCS-DR-SCA	C Recoverable		Write-Back(VMDK)	Details	
GCS-DR-SQL01	Recoverable		Write-Back(VMDK)	Details	

5. Une fois les domaines protégés importés, déployez les appareils DRVA.

DR.



Ces étapes peuvent également être automatisées à l'aide de plans créés par CPT.

- 6. Créez des volumes du journal de réplication à l'aide des datastores VSAN ou ANF disponibles.
- 7. Importez les domaines protégés et configurez le va de restauration de manière à utiliser un datastore ANF pour le positionnement des VM.

ect Protected Domain:	Continuous Failover Protected Domain				Delete	=	More
đe	Capacal 22 Exilouer Settings 25 VM Setting		A DR Settings	5 Summary			Dela
coverable / Total VMs	i, Seiteran za, Fanover Setungs zo, vin Setur	gs s. necosery sk	4. Dr. settings	o. Summary	~ reporec		
	Protected Domain Name	ANFPD002			253.160)		
	Datacenter	SDDC-Datacenter					
	Cluster	Cluster-1			1.000		
	Resource Pool (Optional)				1000		
rotected VMs Setti	VM Folder (Optional)	*)			1.000		
	Datastore	ANFRecoDSU002					
	Internal Network	DRSeg					C
VM Name A	External Replication Network	DRSeg			1000	Details	73
Ансполярряг	Management Network	DRSeg			1.000	L/Stimits	
AuctionAppb2	Storage Site	ANFDemoblobreporec				Details	
AuctionDB2	DR Virtual Appliance	ANFRecDRVA003				Delans	
AuctionLB2	Bonlinstian Lan Storano	Moundaith			<u> </u>	Details	
AuctionMSQ2		Cancel	Back	Continuous Failow	er	Details	

Assurez-vous que DHCP est activé sur le segment sélectionné et qu'un nombre suffisant d'adresses IP est disponible. Des adresses IP dynamiques sont utilisées temporairement pendant la restauration des domaines. Chaque machine virtuelle de restauration (y compris la réhydratation continue) requiert une adresse IP dynamique individuelle. Une fois la récupération terminée, le IP est libéré et peut être réutilisé.

8. Sélectionnez l'option de basculement appropriée (basculement continu ou basculement). Dans cet exemple, la réhydratation continue (basculement continu) est sélectionnée.



Bien que les modes de basculement et de basculement continu diffèrent lorsque la configuration est effectuée, les deux modes de basculement sont configurés à l'aide des mêmes étapes. Les étapes de basculement sont configurées et effectuées ensemble en cas d'incident. Le basculement continu peut être configuré à tout moment, puis s'exécuter en arrière-plan pendant le fonctionnement normal du système. Après un incident, un basculement continu est effectué pour transférer immédiatement la propriété des machines virtuelles protégées vers le site de reprise (RTO quasi nul).

let/Stream DR Protected Domains Statistics Storage Sites Appliances Com	ligurations Task	Log			
elect Protected Domain: GCSDRPD_Demo01 👻 View all			+ Create	Delete	■More
lode	Imported	Configurations		O Restore	
Recoverable / Total VMs	5/5	Storage Site	ANFDemoblobrepor	→ Failover	
		Owner Site	REMOTE ( 172.21.253.1)	+ Continuous Fail	Inver.
					G
Protected VMs Settings Alarms O O					
	2000/02/02/02/07			0230200	
VM Name A	Protection Status		Write Rack/WDK	Details	
GCS-DR-J INVM01	Recoverable		Write-Back/VMDK)	Details	
GCS-DR-SCA	Recoverable		Write-Back(VMDK)	Details	
CCS.DR.90101	Pacevarable		Write-Back/VMDK)	Details	
GOG-DR-GOLD1	C recoverable		A R A FEM - BARBARIA & BITLEFT & C	the substances	

Le processus de basculement continu démarre et sa progression peut être surveillée dans l'interface utilisateur. Un clic sur l'icône bleue dans la section Etape actuelle permet d'afficher une fenêtre contextuelle affichant les détails de l'étape en cours du processus de basculement.

1. Après un incident se produit dans le cluster protégé de l'environnement sur site (défaillance partielle ou complète), vous pouvez déclencher le basculement pour les machines virtuelles à l'aide de Jetstream après avoir déclenché la relation SnapMirror pour les volumes d'application respectifs.

	Volume	e Relationships	4.78 GIB Replicated Capacity	0 Currently Tran	sterring	S Healthy	S O Falled	
	3 Volume Relationshi	ips						90
	Health Status	: Source Volume	Target Volume	0—0 Total Transfer Time 1	Status	🐨 🛛 Mirror State	Last Successful Transfer	•
	0	gcsdrsqldb_sc46 ntaphci-a300e9u25	gcsdrsqldb_sc46_copy ANFCVODRDemo	6 minutes 41 seconds	idle	snapmirrored	May 5, 2022, 12:08:34 P% 33.66 Ki8	
	0	gcsdrsq/hld_sc46 ntaphci-a300e9u25	gcsdrsqlhid_sc46_copy ANFCVODRDemo	4 minutes 56 seconds	idle	snapmirrored	Information	
	0	gcsdrsqllog_sc46 ntaphci-a300e9u25	gcsdrsqllog_sc46_copy ANECVODRDemo	10 minutes 18 seconds	idle	snapmirrored	Break Reverse Resync	
	¢		. ,				Edit Schedule	
							Edit Max Transfer Rate	
							Undate	
							opuere	
							Delete	
anvas Replication	om Backup & Resto	ore Data Sense	File Cache Compute	Sync All Service	es (+9) ~	-	Delete	
Canvas Replicati	on Backup & Resto	ore Data Sense e Relationships	File Cache Compute	Sync All Service	es (+9) V	i Battiy	Delete	
anvas Replication	Backup & Resto	ore Data Sense e Relationships	File Cache Compute	Sync All Service	es (+9) v	S Healthy	Delete Delete O Failed	Q
anvas Replication	Backup & Resto Backup & Resto 3 Volume Relationsh Health Status	ore Data Sense e Relationships	File Cache     Compute       4.78     GIB       Replicated Capacity       Break Relationship       Are you sure that you want 1       'gcsdrsqldb_sc46_copy'?	Sync All Service	es (+9) v resferring	3 Healthy	Delete           Delete           Image: Delete	Q (
Canvas Replication	Backup & Resto Backup & Resto Volume 3 Volume Relationsh Health Status	e Relationships	File Cache     Compute       4.78     GIB       Replicated Capacity       Break Relationship       Are you sure that you want 1       "gcsdrsqldb_sc46_copy"?	Sync All Service	es (+9) v nsferring	Bigging States and Sta	Delete Delete  Last Successful Transfer May 5, 2022, 12:08:34 PM 33.66 KIB	Q ( •
anvas Replicati	Backup & Resto Backup & Resto S Volume Relationsh Health Status ©	e Relationships	File Cache     Compute       4.78     GIB       Replicated Capacity       Break Relationship       Are you sure that you want 1       "gcsdrsqldb_sc46_copy"?	Symc All Service	es (+9) v nsferring	3       Healthy       Idb_3c46" and       d       Cancel	• Operation           Delete           • Delete           • Operation           • Operation <td>Q ( •</td>	Q ( •

(i)

Cette étape peut facilement être automatisée afin de faciliter le processus de reprise.

 Accédez à l'interface utilisateur Jetstream sur AVS SDDC (côté destination) et activez l'option de basculement pour terminer le basculement. La barre des tâches affiche la progression des activités de basculement.

Dans la boîte de dialogue qui s'affiche lors de la fin du basculement, la tâche de basculement peut être spécifiée comme planifié ou supposée être forcée.

elect Protected Domain: GCSDRPD_Demo01	View all		+ Create	O Freilover	≡ Mor
Mode	Continuous Rehydration in Progress	Configurations			Details
Recoverable / Total VMs	4/4	Storage Site		porec	^
		Owner Site	REMOTE ( 172.21.25	3.160)	
Data (Processed/Known Remaining)	329.01 GB / 6.19 GB	Datacenter \ Cluster	SDDC-Datacenter \ C	Cluster-1	
Current Step	Recover VMs' data from Storage Site()	Point-in-time Recovery	Disabled		~
VM Name	Protection Status		Protection Mode	Details	ų
GCS-DR-DC	Recoverable		Write-Back(VMDK)	Details	~
GCS-DR-LinVM01	Recoverable		Write-Back(VMDK)	Details	
GCS-DR-SCA	Recoverable		Write-Back(VMDK)	Detaits	
GCS-DR-SQL01	Recoverable		Write-Back(VMDK)	Details	
			and the second second second second second second	these buildings and the second s	

Protected VM Network A	Recovery VM Network		
VM_3510	DRStretchSeg	<u> </u>	
0 0		v	8
Other Settings			
Force Failover			
Some VM's guest credential are require	ed because of network configuration: Configure		

Le basculement forcé suppose que le site principal n'est plus accessible et que la propriété du domaine protégé devrait être directement assumée par le site de reprise.

Ð	Force Failover of Protected Do required! Complete ownership of this Pr	main requested. Adminis otected Domain will be t	trator consent is aken over by this
	Are you sure you want to contir	nue?	
		Cancel	Confirm

M Network Mapping				
rotected VM Network 🔺	Recovery VM Network			^
M_3510	DRStretchSeg	•	^	
0 0			~	2
her Settings				
Planned Failover				
Force Failover				
		engenee 1		
COME STATE PURCH CREASING THE FAMILY	ired because of network configuration: C	onfigure		

3. Une fois le basculement continu terminé, un message confirmant la fin de la tâche s'affiche. Une fois la tâche terminée, accédez aux VM récupérées pour configurer les sessions ISCSI ou NFS.

Le mode de basculement passe en mode d'exécution en basculement et l'état de la VM peut être récupérable. Toutes les machines virtuelles du domaine protégé sont à présent exécutées sur le site de reprise, dans l'état spécifié par les paramètres de runbook de basculement.

 $(\mathbf{i})$ 

 $(\mathbf{i})$ 

Pour vérifier la configuration et l'infrastructure de basculement, JetStream DR peut être utilisé en mode test (option Test Failover) afin d'observer la récupération des machines virtuelles et de leurs données à partir du magasin d'objets dans un environnement de restauration de test. Lorsqu'une procédure de basculement est exécutée en mode test, son fonctionnement ressemble à un processus de basculement réel.

Jet/Stream DR Protected Domains Statistics Stora	Continuous Rehydration Task Resu	it	B
Select Protected Domain: GCSDRPD002	Task Completed Successfully with	warnings.	+ Create Toniate Estore
Recoverable / Total VMs	Protected Domain	GCSDRPD002	ANFEVODR
The second	VMs Recovery Status	<ul> <li>Success with warnings</li> </ul>	OCAL (17230.1562)
Replication Stalus	Total VMs Recovered	4	DDC-Datacenter \ Cluster-1
Remaining Background Data	VM(s) with warning	2 <u>View</u>	esabled
Concession of the second se	GCSRecovery03 Status:		
Current RPD	Pre-script Execution Status	Not defined	×
	Runbook Execution Status	O Success	
Protected VMs Settings Atarms	Post-script Execution Status	Not defined	
+ Start Protection			٩
VII Name 🔺		N	ackground Data 🔺 Details
GCS-DR-SC46		48	8 Details
GCS-DR-SOL03			B Details
GCSDR-W2K16-01			8 Detaits
UbuntuSrv001			B Details

- 4. Une fois les machines virtuelles restaurées, utilisez la reprise après incident du stockage pour le stockage invité. Pour démontrer ce processus, SQL Server est utilisé dans cet exemple.
- 5. Connectez-vous à la machine virtuelle SnapCenter récupérée sur AVS SDDC et activez le mode DR.
  - a. Accédez à l'interface utilisateur SnapCenter à l'aide du navigateur.

Define the style of the set of th	- ≜× O gcs-dr-	sc46.gcsdc.com ×
		otAnn
	SnapCente	erapp <sub>°°</sub>
	Username	gcsdc\adminnimo
Ree - de x	Password	Sign In

- b. Dans la page Paramètres, accédez à Paramètres > Paramètres globaux > reprise après incident.
- c. Sélectionnez Activer la reprise après incident.
- d. Cliquez sur appliquer.

G	🐵 🖪 https://gcs-	ar-sc45.gcsdc.com/8146/Administ D = 🖨 C 🖪 SnepCenter 🗙 🔞 🛱 SnepCenter	0
	NetApp Snap(	Eenter® 🖉 🚱 🔹 🚱 🔹 🔒 🖉 🖉	ut
<		Global Settings Policies Users and Access Roles Credential Software	
	Dashboard		
۲	Resources	Global Settings	
۲	Monitor		
<b>a</b>	Reports	Hypervisor Settings 0	~
*	Hosts	Notification Server Settings 0 O .O	~
20	Storage Systems	Configuration Settings 0	~
#	Settings	Purge Jobs Settings	~
▲	Alerts	Domain Settings	~
		CA Certificate Settings 0	~
		Disaster Recovery 0	~
		Enable Disaster Recovery Apply	

e. Vérifiez si la tâche DR est activée en cliquant sur Monitor > Jobs.



NetApp SnapCenter 4.6 ou version ultérieure doit être utilisé pour la reprise après incident du stockage. Pour les versions précédentes, des snapshots cohérents avec les applications (répliqués à l'aide de SnapMirror) doivent être utilisés. Il convient également d'exécuter une restauration manuelle si les sauvegardes précédentes doivent être restaurées sur le site de reprise après incident.

6. S'assurer que la relation SnapMirror est rompue.

Canvas	Replication	Backup & Restore	Data Sense	File Cache	Compute	Sync All Services	s (+9) ~			
Repli	cation									
		Volume Rel	lationships	2.78 Replicated	GIB d Capacity	O Currently Trans	ferring	3 Healthy	S 0 Failed	
	3	3 Volume Relationships								Q C
	3	8 Volume Relationships Health Status 🔹	Source Volume	5 Target Vo	lume i l	⊙—10 Total Transfer Time ÷	Status 😤	Mirror State	+ Last Successful Transfer	۹.c •
		8 Volume Relationships Health Status :	Source Volume gcsdrsqldb_sc46 ntaphci-a300e9u25	<ul> <li>Target Vo gesdrsqld ANFCVOD</li> </ul>	lumo : b_sc46_copy RDemo	C-D Total Transfer Time = 6 minutes 41 seconds	Status 👻	Mirror State broken-off	÷ Lust Successful Transfer May 5, 2022, 12:08:34 PA 33.66 KIB	۹.0 •
	3	Volume Relationships	Source Volume gcsdrsqldb_sc46 ntaphci-a300e9u25 gcsdrsqlhld_sc46 ntaphci-a300e9u25	2 Target Vo gcsdrsqld ANFCVOD K gcsdrsqlh ANFCVOD	ttime 2 b. sc46_copy JRDemo 3 Id_sc46_copy JRDemo 3	C = 0 Total Transfer Time = 1 6 minutes 41 seconds 4 minutes 56 seconds	Status ♥ idle	Mirror State broken-off broken-off	East Successful Transfer           May 5, 2022, 12:08:34 PA           33.66 KIB           May 5, 2022, 12:09:15 PA           69.84 KIB	Q (0 ●

7. Reliez le LUN de Cloud Volumes ONTAP à la machine virtuelle hôte SQL récupérée à l'aide des mêmes lettres de disque.

📅 Disk Manageme	nt						0 <del>7-1</del> 0	×
File Action View	v Help							
🗢 🔿 🖂 🖬	m   🗩 🕑 (							
Volume	Layout	Туре	File System	Status	Capacity	Free Spa	% Free	
-	Simple	Basic	1 contract of a contract	Healthy (R	450 MB	450 MB	100 %	
-	Simple	Basic		Healthy (E	99 MB	99 MB	100 %	
- (C:)	Simple	Basic	NTFS	Healthy (B	89.45 GB	67.03 GB	75 %	
BACKUP (G:)	Simple	Basic	NTFS	Healthy (P	9.97 GB	9.92 GB	99 %	
- DATA (E:)	Simple	Basic	NTFS	Healthy (P	24.88 GB	24.57 GB	99 %	
- LOG (F:)	Simple	Basic	NTFS	Healthy (P	9.97 GB	8.93 GB	90 %	
					0	0		

8. Ouvrez l'initiateur iSCSI, effacez la session précédente déconnectée et ajoutez la nouvelle cible avec les chemins d'accès multiples pour les volumes Cloud Volumes ONTAP répliqués.

Targets	Discourse	Councillo Torrado	Values and Daviese	DADTUC	Configuration
raiges	Discovery	Favorite l'argets	volumes and Devices	RADIUS	Configuration
Quick C	Connect				
DNS na	ame of the ta	arget and then click	Quick Connect.		
raiger				Q	sick Connect
Discove	ered targets			Q	Jick Connect
Discove	ered targets			Q	ick Connect Refresh
Discove	ered targets			Status	ick Connect Refresh
Discove Name	ered targets	netapp:sn.547772c	cc47811ecbb62000	Que Status Connecte	Refresh

9. Assurez-vous que tous les disques sont connectés à l'aide des mêmes lettres que celles utilisées avant la reprise sur incident.



10. Redémarrez le service serveur MSSQL.

Action View	Help					
iervices (Local)	Services (Local)					
	SQL Server (MSSQLSERVER)	Name	Description	Status	Startup Type	Log ^
		SQL Full-text Filter Daemon	Service to la	Running	Manual	NT
	Stop the service	SQL Server (MSSQLSERVER)	Provider etc	Running	Automatic	GCS
	Restart the service	Q SQL Server Agent (MSS	Start	ning	Automatic	GCS
		SQL Server Browser	Stop	ning	Automatic	Loc
		SQL Server CEIP service	Pause	ning	Automatic	NT
	Provides storage processing and	🖏 SQL Server Integration S	Resume	ning	Automatic	NT
	controlled access of data, and rapid	SQL Server Integration S	Restart	ning	Automatic	NT
	transaction processing.	SQL Server VSS Writer	url'au	ning	Automatic	Loc
		SSDP Discovery	All Tasks	> nîng	Manual	Loc
		State Repository Service	Refresh	ning	Manual	Loc
		Still Image Acquisition E			Manual	Loc
		Storage Service	Properties		Manual (Trig	Loc
		Storage Tiers Managem	Help		Manual	Loc
		Superfetch			Manual	Loc
		Sync Host_df83a	This service	Running	Automatic (D	Loc
		System Event Notification S	Monitors sy	Running	Automatic	Loc v
		<b>`</b>				,

11. Assurez-vous que les ressources SQL sont de nouveau en ligne.

 $(\mathbf{i})$ 

O - O   12 - 12 - 22 ■ 2   20 M	New Query 🛢 இ இ இ இ இ \$ பி இ   7 - C -   図   -   5 Execute ■ ✔ 82 目目 82 82 11 回 画 ப   3 3   -E 王   10 -
Object Explorer <ul> <li></li></ul>	SQLQuery1.sql - GDC\adminnimo (66)) + X /***** Script for SelectTopNRows command from SSMS ******/ ESELECT TOP (1000) [Id] ,[Name] ,[Price] FROM [CarDB].[dbo].[Cars] 0 0
External Tables	100 % -
Graph Tables	I Results I Messages
<ul> <li></li></ul>	Id         Name         Price           1         1         Car-1         1000           2         2         Car-2         2000           3         3         Car-3         3000           4         4         Car-4         4000           5         5         Car-5         5000

Dans le cas d'un système NFS, reliez les volumes à l'aide de la commande mount et mettez à jour le /etc/fstab entrées.

À ce stade, le fonctionnement de l'entreprise peut se faire et son activité se poursuit normalement.



Sur la fin NSX-T, il est possible de créer une passerelle de niveau 1 dédiée distincte pour simuler des scénarios de basculement. Cela permet de s'assurer que toutes les charges de travail peuvent communiquer les unes avec les autres, mais qu'aucun trafic ne peut être acheminé depuis et vers l'environnement, de manière à ce que les tâches de triage, de confinement ou de durcissement puissent être effectuées sans risque de contamination croisée. Cette opération est hors du champ d'application de ce document, mais elle peut être facilement réalisée pour simuler l'isolement.

Une fois que le site primaire est de nouveau opérationnel, vous pouvez effectuer le rétablissement. La protection de machine virtuelle est reprise par Jetstream et la relation SnapMirror doit être inversée.

- 1. Restaurer l'environnement sur site. Selon le type d'incident, il peut être nécessaire de restaurer et/ou de vérifier la configuration du cluster protégé. Si nécessaire, il peut être nécessaire de réinstaller le logiciel JetStream DR.
- 2. Accédez à l'environnement sur site restauré, accédez à l'interface utilisateur Jetstream DR et sélectionnez le domaine protégé approprié. Une fois que le site protégé est prêt à être restauré, sélectionnez l'option de retour arrière dans l'interface utilisateur.



Le plan de restauration généré par CPT peut également être utilisé pour initier le retour des VM et de leurs données du magasin d'objets vers l'environnement VMware d'origine.

JetStream DR Protected Domains Statistics Storage Sites Appliances	Configurations Task L	og		Ê
Select Protected Domain: GCSDRPD_Demo01 • View all			+ Create	Delete E More
Mode	Running in Failover	Configurations		O Restore
Active Site	172.30.156.2	Storage Site	ANFCVODR	O Resume Continuous Rehydration
Recoverable / Total VMs	414	Owner Site REMOTE (172.3 + Faliback		
				v
Protected VMs Settings Alarms O O				
				Q
VM Name 🔺	Protection Status	<b>A</b>	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
GCS-DR-WinVM01	Recoverable		Write-Back(VMDK)	Details

Préciser le délai maximal après la mise en pause des VM dans le site de reprise, puis leur redémarrage sur le site protégé. Le temps nécessaire à l'exécution de ce processus comprend l'achèvement de la réplication après l'arrêt des VM de basculement, le temps nécessaire pour nettoyer le site de reprise et le temps nécessaire pour recréer les VM sur le site protégé. NetApp recommande 10 minutes.

•	•	•	•			•
. General	2a. Failback Settings	2b. VM Settings	3. Recovery VA	4. DR	Settings	5. Summary
Failback Da	tacenter		A300-DataCenter			
Failback Clu	uster		A300-Cluster			
Failback Re	source Pool					
VM Folder (	Optional)					
Failback Da	tastore		A300_NFS_vMotion			
Maximum D	elay After Stopping		10 Minutes			
Internal Net	wohk		VM_187			
External Re	plication Network		VM_187			
Managemen	nt Network		VM_187			
Storage Site	9		ANFCVODR			
DR Virtual A	ppliance		GCSDRVA002			
Replication	Log Storage		/dev/sdb			

3. Suivre le processus de retour arrière, puis confirmer la reprise de la protection des machines virtuelles et la cohérence des données.

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

4. Une fois les machines virtuelles restaurées, déconnectez le stockage secondaire de l'hôte et connectez-vous au stockage primaire.

9	gcsdrsqldb_sc46 ntaphci-a300e9u25	19	gcsdrsqldb_sc46_copy ANFCVODRDemo	6 minutes 41 seconds	idle	broken-off	May 5. 2022. 12:08:34 PN 33.66 KiB
9	gcsdrsqlhld_sc46 ntaphci-a300e9u25		gcsdrsqlhld_sc46_copy ANFCVODRDemo	4 minutes 56 seconds	idle	broken-off	Information
୭	gcsdrsqllog_sc46 ntaphci-a300e9u25	1	gcsdrsqllog_sc46_copy ANFCVODRDemo	10 minutes 18 seconds	idle	broken-off	Resync
							Edit Schedule
							Edit Max Transfer Rate
							Delete

Volume Re	lationships	6.54 GiB Replicated Capacity	Currently Tran	sferring	S Healthy	S O Failed	
Volume Relationships			0 0				Q (
Health Status 🔹	Source Volume 🔹	Target Volume +	Total Transfer Time 🗧	Status		+ Last Successful Transfer	•
$\odot$	gcsdrsqldb_sc46 ntaphcl-a300e9u25	gcsdrsqldb_sc46_copy ANFCVODRDemo	19 seconds	idle	snapmirrored	May 6. 2022, 11:03:00AN 5.73 MiB	
0	gcsdrsqlhld_sc46_copy ANFCVODRDemo	gcsdrsqlhld_sc46 ntaphci-a300e9u25	1 minute 46 seconds	idle	snapmirrored	May 6, 2022, 11:01:39 AN 800.76 MiB	
$\odot$	gcsdrsqllog_sc46 ntaphcl-a300e9u25	gcsdrsqllog_sc46_copy ANFCVODRDemo	51 seconds	idle	snapmirrored	May 6, 2022, 11:03:15 AN 785.8 MiB	

- 5. Redémarrez le service serveur MSSQL.
- 6. Vérifiez que les ressources SQL sont de nouveau en ligne.



Pour revenir au stockage primaire, veillez à ce que la direction de la relation reste la même qu'avant le basculement en effectuant une opération de resynchronisation inverse.

Pour conserver les rôles de stockage primaire et secondaire après l'opération de resynchronisation inverse, effectuez à nouveau l'opération de resynchronisation inverse.

i .

Ce processus s'applique à d'autres applications telles qu'Oracle, des versions similaires des bases de données et à toutes les autres applications qui utilisent un système de stockage connecté par l'invité.

Comme toujours, testez les étapes de récupération des charges de travail critiques avant de les porter en production.

# Avantages de cette solution

- Utilise la réplication efficace et résiliente de SnapMirror.
- Restauration des points disponibles à temps avec la conservation des snapshots de ONTAP.
- Une automatisation complète est disponible pour toutes les étapes nécessaires à la restauration de centaines de milliers de machines virtuelles, depuis les étapes de validation du stockage, du calcul, du réseau et des applications.
- SnapCenter utilise des mécanismes de clonage qui ne modifient pas le volume répliqué.
  - Cela permet d'éviter le risque de corruption des données pour les volumes et les snapshots.
  - · Evite les interruptions de réplication pendant les workflows de test de reprise après incident
  - Optimise les données de reprise après incident pour les flux de travail autres que la reprise après incident, comme le développement/test, les tests de sécurité, les tests de correctifs et de mise à niveau, et les tests de résolution des problèmes.
- L'optimisation du processeur et de la RAM permet de réduire les coûts liés au cloud en permettant la restauration sur des clusters de calcul plus petits.

# Tr-4955 : reprise d'activité avec Azure NetApp Files (ANF) et solution Azure VMware (AVS)

Auteur(s) : Niyaz Mohamed, ingénierie des solutions NetApp

# Présentation

La reprise d'activité avec réplication au niveau des blocs entre les régions dans le cloud est un moyen résilient et économique de protéger les workloads contre les pannes sur site et les corruptions de données (par exemple, les ransomwares). Avec la réplication de volume inter-régions Azure NetApp Files (ANF), les workloads VMware s'exécutant sur un site SDDC Azure VMware solution (AVS) avec des volumes Azure NetApp Files en tant que datastore NFS sur le site AVS principal peuvent être répliqués sur un site AVS secondaire désigné dans la région de restauration cible.

L'orchestrateur de reprise après incident (DRO) (une solution basée sur des scripts avec interface utilisateur) peut être utilisé pour restaurer de manière fluide les workloads répliqués depuis un SDDC AVS. DRO automatise la restauration en rompant le peering de réplication, puis en montant le volume de destination en tant que datastore, via l'enregistrement de machine virtuelle vers AVS, en passant par les mappages du réseau directement sur NSX-T (inclus avec tous les clouds privés AVS).



### Conditions préalables et recommandations générales

- Vérifiez que vous avez activé la réplication entre les régions en créant le peering de réplication. Voir "Création d'une réplication de volume pour Azure NetApp Files".
- Vous devez configurer ExpressRoute Global Reach entre les clouds privés de la solution Azure VMware source et cible.
- · Vous devez disposer d'une entité de service pouvant accéder aux ressources.
- La topologie suivante est prise en charge : du site AVS principal au site AVS secondaire.
- Configurer le "la réplication" planifiez chaque volume de manière appropriée en fonction des besoins de l'entreprise et du taux de changement des données.



Les topologies en cascade, « Fan-In » et « Fan-Out » ne sont pas prises en charge.

## Pour commencer

#### Déployez la solution Azure VMware

Le "Solution Azure VMware" (AVS) est un service de cloud hybride qui fournit des data centers complets VMware dans un cloud public Microsoft Azure. AVS est une solution première entièrement gérée et prise en charge par Microsoft, puis vérifiée par VMware qui utilise l'infrastructure Azure. Par conséquent, les clients bénéficient de VMware ESXi pour la virtualisation du calcul, de VSAN pour le stockage hyperconvergé et de NSX pour la mise en réseau et la sécurité, tout en exploitant la présence mondiale de Microsoft Azure, les installations de data Center de pointe et la proximité du riche écosystème de services et de solutions Azure natifs. La combinaison d'Azure VMware solution SDDC et d'Azure NetApp Files offre les meilleures performances et une latence réseau minimale.

Pour configurer un cloud privé AVS sur Azure, suivez la procédure décrite dans cette section "lien" Pour la documentation NetApp et dans ce document "lien" Pour la documentation Microsoft. Un environnement de

pilote léger configuré avec une configuration minimale peut être utilisé à des fins de reprise sur incident. Cette configuration ne contient que des composants de base pour prendre en charge les applications stratégiques, et elle peut évoluer horizontalement et générer plus d'hôtes pour prendre la charge en bloc en cas de basculement.



Dans la version initiale, DRO prend en charge un cluster SDDC existant. La création d'un SDDC à la demande sera disponible dans une prochaine version.

#### Provisionner et configurer Azure NetApp Files

"Azure NetApp Files" service de stockage de fichiers haute performance et mesuré. Suivez les étapes de cette procédure "lien" Pour provisionner et configurer Azure NetApp Files en tant que datastore NFS afin d'optimiser les déploiements de cloud privé AVS.

#### Créez une réplication de volume pour les volumes de datastore Azure NetApp Files

La première étape consiste à configurer la réplication interrégionale pour les volumes de datastore souhaités du site principal AVS vers le site secondaire AVS avec les fréquences et les rétentions appropriées.

Ho	ome > Azure NetApp Files > WEANFAVS	acct   Volumes > testrepIdemo (WEANFAVSacct/testcap/testrepIdemo)				
»	testrepidemo (WE	ANFAVSacct/testcap/testrepIdemo)   Replication	\$			×
D	P Search «	🕐 Refresh				
100	Noverview	↑ Essentials				JSON View
	Activity log	End point type : Source	3	Destination	: testrepidemo.copy	
3=	Access control (IAM)	Health status : Healthy	1	Relationship status	i : Idle	
•	Tags	Mirror state : Mirrored	3	Total progress	: 2.13 GiB	

Suivez les étapes de cette procédure "lien" pour configurer la réplication entre les régions en créant le peering de réplication. Le niveau de service du pool de capacité de destination peut correspondre à celui du pool de capacité source. Toutefois, pour ce cas d'utilisation spécifique, vous pouvez sélectionner le niveau de service standard, puis "modifier le niveau de service" En cas d'incident réel ou de simulations de reprise sur incident.

Une relation de réplication entre régions est un prérequis et doit être créée au préalable.

## Installation de DRO

Pour commencer avec DRO, utilisez le système d'exploitation Ubuntu sur la machine virtuelle Azure désignée et assurez-vous de respecter les conditions préalables. Installez ensuite le package.

#### Conditions préalables :

- Principal de service pouvant accéder aux ressources.
- Assurez-vous qu'une connectivité appropriée existe aux instances source et de destination du SDDC et du Azure NetApp Files.
- La résolution DNS doit être en place si vous utilisez des noms DNS. Sinon, utilisez les adresses IP pour vCenter.

#### Système d'exploitation requis :

- Ubuntu focal 20.04 (LTS)les paquets suivants doivent être installés sur la machine virtuelle de l'agent désignée :
- Docker

- · Docker- compose
- JqModifier docker.sock à cette nouvelle autorisation : sudo chmod 666 /var/run/docker.sock.



Le deploy.sh le script exécute toutes les conditions préalables requises.

Les étapes sont les suivantes :

1. Téléchargez le package d'installation sur la machine virtuelle désignée :

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



L'agent doit être installé dans la région du site AVS secondaire ou dans la région du site AVS principal dans une zone de disponibilité autre que le SDDC.

2. Décompressez le package, exécutez le script de déploiement et entrez l'adresse IP de l'hôte (par exemple, 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. Accédez à l'interface utilisateur à l'aide des informations d'identification suivantes :
  - Nom d'utilisateur : admin
  - Mot de passe : admin

■ NetApp	
Disaster Recovery Orchestrator     Grand Eductor extr Gal  Verman  Pesseord  Education  Educat	

# **Configuration DRO**

Une fois que Azure NetApp Files et AVS ont été correctement configurés, vous pouvez commencer à configurer DRO afin d'automatiser la restauration des workloads du site AVS principal vers le site AVS secondaire. NetApp recommande de déployer l'agent DRO sur le site AVS secondaire et de configurer la connexion de passerelle ExpressRoute de sorte que l'agent DRO puisse communiquer via le réseau avec les composants AVS et Azure NetApp Files appropriés.

La première étape consiste à ajouter des informations d'identification. DRO nécessite l'autorisation de découvrir Azure NetApp Files et la solution Azure VMware. Vous pouvez accorder les autorisations requises à un compte Azure en créant et en configurant une application Azure Active Directory (AD) et en obtenant les identifiants Azure dont DRO a besoin. Vous devez lier l'entité de service à votre abonnement Azure et lui attribuer un rôle personnalisé disposant des autorisations requises appropriées. Lorsque vous ajoutez des environnements source et de destination, vous êtes invité à sélectionner les informations d'identification associées à l'entité de service. Vous devez ajouter ces informations d'identification à DRO avant de cliquer sur Ajouter un nouveau site.

Pour effectuer cette opération, procédez comme suit :

- Ouvrez DRO dans un navigateur pris en charge et utilisez le nom d'utilisateur et le mot de passe par défaut /admin/admin). Le mot de passe peut être réinitialisé après la première connexion à l'aide de l'option Modifier le mot de passe.
- 2. Dans le coin supérieur droit de la console DRO, cliquez sur l'icône Settings et sélectionnez Credentials.
- 3. Cliquez sur Ajouter une nouvelle information d'identification et suivez les étapes de l'assistant.
- 4. Pour définir les informations d'identification, entrez les informations relatives au principal du service Azure Active Directory qui accorde les autorisations requises :
  - Nom d'identification
  - · ID locataire
  - ID client
  - Secret client
  - · ID d'abonnement

Vous devez avoir capturé ces informations lorsque vous avez créé l'application AD.

5. Confirmez les détails des nouvelles informations d'identification et cliquez sur Ajouter une information d'identification.

Add New Credential	Credentials Details	
	Enter Credentials Details	
	Credential Name	
	Tenant Id	
	Client Id	
	Client Secret	
	Subscription Id	

Après avoir ajouté les identifiants, il est temps de découvrir et d'ajouter les sites AVS principaux et secondaires (à la fois vCenter et le compte de stockage Azure NetApp Files) à DRO. Pour ajouter le site source et le site de destination, procédez comme suit :

- 6. Accédez à l'onglet **Discover**.
- 7. Cliquez sur Ajouter un nouveau site.
- 8. Ajoutez le site AVS principal suivant (désigné comme **Source** dans la console).
  - VCenter SDDC
  - · Compte de stockage Azure NetApp Files
- 9. Ajoutez le site AVS secondaire suivant (désigné comme destination dans la console).
  - VCenter SDDC
  - Compte de stockage Azure NetApp Files

Resource Groups   Replication Plans   Job Monitoring       Resource Groups   Replication Plans   Job Monitoring	🌲 🌣 😨 🛎
Add New Site 1 Site Type 2 Site Details 3 vCenter Details 3 Storage Details	×
Site Type	
Source Destination	
Continue	

10. Ajoutez les détails du site en cliquant sur **Source**, en saisissant un nom de site convivial, puis sélectionnez le connecteur. Cliquez ensuite sur **Continuer**.



À des fins de démonstration, l'ajout d'un site source est abordé dans ce document.

- 11. Mettez à jour les détails de vCenter. Pour ce faire, sélectionnez les informations d'identification, la région Azure et le groupe de ressources dans le menu déroulant du SDDC AVS principal.
- 12. DRO répertorie tous les SDDC disponibles dans la région. Sélectionnez l'URL de cloud privé désignée dans la liste déroulante.
- 13. Entrez le cloudadmin@vsphere.local informations d'identification de l'utilisateur. Vous pouvez y accéder depuis le portail Azure. Suivez les étapes mentionnées dans ce document "lien". Une fois terminé, cliquez sur **Continuer**.

NetApp Disaster Recovery Orchestrator	Dashboard   Discover   Resource Grou	ups   Replication Plans   Job Monitoring	ΞŤε.	ê 🌣 🕄 😩
Add New Site	🕑 Site Type 📿	) Site Details (3) vCenter Details (4)	) Storage Details	x
		Source AVS Private Cloud		
4	Select Credentials	Azure Region	Azure Resource Group	
	DemoCred -	West Europe +	ANFAVSVal2 v	
	<b></b>	AVS Details		
	Web Client	ANEDataClus		
	Username	nin@vsphere.local		
	Password			
		Accept self-signed certificates		
		Previous Continue		

- 14. Sélectionnez le groupe de ressources Azure et le compte NetApp dans les détails du stockage source (ANF).
- 15. Cliquez sur Créer un site.

Disaster Recovery Orchestrator 💊   Dashboard   Discover   Resour	ce Groups   Replication Plans   Job Monitoring	۵
	Site Type Site Location	
Sites Centers Storages	Source Destination On Prem	Cloud
2 sites		Q 🕤 Add New Site
Site Name	Location 🛛 😤   vCenter 🗘   Storage 🗘   VM List   Discovery Status	1
DemoDest Destination	Cloud 1 1 • https://10.75.0.2/	⊙ Success

Une fois ajouté, DRO effectue une détection automatique et affiche les VM qui ont des répliques inter-régions correspondantes du site source au site de destination. DRO détecte automatiquement les réseaux et les segments utilisés par les machines virtuelles et les remplit.

Disaster Recovery Orchestrator	Sectore R	esewarke Groups   Replication Plans   Job	Monitoring		<b>A O</b>
Back					
		VM List Site: DemoSRC   vCenter: https://172	30.1562/		
			VM Protection		
CP 7	Mores	128 Virtual Machines	2 Protected	0 126 Unprotected	
128 vm				Q	Create Resource Group
WM Name	2   VM Status	1 VM Stille	DutaStore	e i au	C Memory (M0) C
HD5enth,2.5.1	O Not Protected	Dewered On	vianDatastore	3	8192
hci-fio-datastore-13984-0-1	0 Not Protected	Powered Off	HCitstD5	32	65536
ICCA2005-WO-R1	O Not Protected	(5) Powered On	vianDataitore	8	34336
ICCA2005-NE-R1	0 Not Protected	() Powered On	vianDatastore		3072
ICCA2005-01-81	0 Not Protected	() Powered Gn	stanDatastore	8	3072
HCX_Damo_05	9 Not Protected	Dewered Off	Demo002	1	2048
hci-nim-datastore-13964-0-1	0 Not-Protected	() Fowered Off	HCItyIDS	24	49152

L'étape suivante consiste à regrouper les VM requises dans leurs groupes fonctionnels en tant que groupes de ressources.

### **Regroupements de ressources**

Une fois les plates-formes ajoutées, regroupez les VM que vous souhaitez restaurer en groupes de ressources. Les groupes de ressources DRO vous permettent de regrouper un ensemble de VM dépendants en groupes logiques contenant leurs ordres de démarrage, leurs délais de démarrage et les validations d'applications facultatives qui peuvent être exécutées lors de la récupération.

Pour commencer à créer des groupes de ressources, cliquez sur l'élément de menu **Créer un nouveau** groupe de ressources.

1. Accédez à Resource Grou\*ps et cliquez sur \*Create New Resource Group.

n NetApp	Disaster Recovery Orchestrator 💊 🗌	Dashboard   Discover   Resource Groups   Rep	dication Plans Job Monitoring	٨	¢? 2
	<b>1</b>	1	<b>a</b> 1	長 2	
	Resource Group	Site	vCenter	Virtual Machines	
	1 Resource Group			Q O Create New Resource Group	
	Resource Group Name	\$   Site Name	· ⇒   Source vCenter	⇒   VM List	
	DemoRG	DemoSRC	https://172.30.156.2/	View VM List	

- 2. Sous Nouveau groupe de ressources, sélectionnez le site source dans la liste déroulante et cliquez sur **Créer**.
- 3. Fournissez les détails du groupe de ressources et cliquez sur **Continuer**.
- 4. Sélectionnez les machines virtuelles appropriées à l'aide de l'option de recherche.
- Sélectionnez Boot Order et Boot Delay (sec) pour toutes les machines virtuelles sélectionnées.
   Définissez l'ordre de la séquence de mise sous tension en sélectionnant chaque machine virtuelle et en

définissant sa priorité. La valeur par défaut pour toutes les machines virtuelles est 3. Les options sont les suivantes :

- Première machine virtuelle à mettre sous tension
- Valeur par défaut
- Dernière machine virtuelle à mettre sous tension

🗖 NetApp	Disaster Recovery Orchestrator 💊 🛛	Dashboard Disco	ver   Resource Groups   Re	plication Plans   Job	Monitoring		ê 🔅	•	
	Edit Resource Group		Resource Group Details	Select VMs	Boot order and De	lay			
			Во	ot order and De	lay				
		VM Name	Boot Order 🕘		Boot Delay (secs)				
		QALin1	3	10	0				
		QALin	3	10	0	0			

6. Cliquez sur Créer un groupe de ressources.

n NetApp	Disaster Recovery Orchestrator 💊	Dashboard Discover Resource Groups	Replication Plans Job Monitoring	<b>A</b> :	¢ ? 2
	1 Resource Group	☐ 1 Site	1 vCenter	2 Virtual Machines	
	1 Resource Group			Create New Resource Group	
	Resource Group Name	Site Name	≂   Source vCenter	≂ I VM Est I	
	DemoRG	DemoSRC	https://172.30.156.2/	View VM List	

#### Plans de réplication

En cas d'incident, vous devez disposer d'un plan de restauration des applications. Sélectionnez les plateformes vCenter source et cible dans la liste déroulante, choisissez les groupes de ressources à inclure dans ce plan, ainsi que le regroupement des méthodes de restauration et de mise sous tension des applications (par exemple, contrôleurs de domaine, niveau 1, niveau 2, etc.). Les plans sont souvent appelés plans. Pour définir le plan de reprise, accédez à l'onglet Replication Plan, puis cliquez sur **Nouveau plan de réplication**.

Pour commencer à créer un plan de réplication, procédez comme suit :

1. Naviguez jusqu'à plans de réplication et cliquez sur Créer un nouveau plan de réplication.

NetApp	Disaster Recovery Orchestrator 💊 Dashboard Discover Resource Groups Replication Plans Job Monitoring								
	民 1	B 1 Replication Plans		Source Details		Destination Details			
	Rej	plication Plans	Resource Groups	Sites	vCenters	Sites	vCenters		
	1 Replication Plan						Q 🧿 Create New Re	plication Plan	
	Plan Name	C Active Site	Status	Compliance	Source Site		÷	1	
	DemoRP	Source	<ul> <li>Active</li> </ul>	A Partially Healthy	DemoSRC	DemoDest	Resource Groups		

 Sur le Nouveau plan de réplication, indiquez un nom pour le plan et ajoutez des mappages de récupération en sélectionnant le site source, le vCenter associé, le site de destination et le vCenter associé.

NetApp Disaster Recovery Orchestrator	Dashboard Discover Resource Groups Replication	n Plans   Job Monitoring	A 🌣 🕲 😩
Create New Replication Plan	Replication Plan and Site Details     (2) Select Resor	x	
	Replicatio	n Plan Details	
	Plan Name	0	
	DemoRP		
	Recov	ry Mapping	
	Source Site	Destination Site	
	DemoSRC +	DemoDest -	
	Source vCenter	Destination vCenter	
	https://172.30.156.2/ +	https://10.75.0.2/	
	Clust	r Mapping	
	Source Site Resource Destin	tion Site Resource	
	Cluxeri		
	Source Resource Desti	nation Resource	
	No Ma	ppings added!	
		Continue	

3. Une fois le mappage de récupération terminé, sélectionnez **Cluster Mapping**.

NetApp Disaster Recovery Orchestrator	Dashboard Discover Resource	Groups   Replication Pla	ns   Job Monitoring				٠	?	۹
Create New Replication Plan	(1) Replication Plan and Site Details	<li>Select Resource G</li>	roups ③ Set Execution Order ④ Set VM Details						×
		Replication	Plan Details						
	Plan Name			0					
	DemoRP								
		Recovery	Mapping						
	Source Site	ource Site O Destination Site O							
	DemoSRC		DemoDest	*					
	Source vCenter	0	Destination vCenter	0					
	https://172.30.156.2/	*	https://10.75.0.2/	*					
		Cluster	Mapping		N .				
	No more	e Source/Destination clust	er resources available for mapping						
	Source Resource	Destination Re	source						
	Cluster-1	Cluster-1	Delete						
		Con	tinue						

- 4. Sélectionnez Détails du groupe de ressources et cliquez sur Continuer.
- 5. Définissez l'ordre d'exécution du groupe de ressources. Cette option vous permet de sélectionner la séquence d'opérations lorsqu'il existe plusieurs groupes de ressources.
- 6. Une fois l'opération terminée, définissez le mappage réseau sur le segment approprié. Les segments doivent déjà être provisionnés sur le cluster AVS secondaire et, pour mapper les VM vers ceux-ci, sélectionnez le segment approprié.
- 7. Les mappages de datastores sont sélectionnés automatiquement en fonction de la sélection de machines virtuelles.



La réplication interrégionale (CRR) se situe au niveau du volume. Par conséquent, toutes les VM résidant sur le volume respectif sont répliquées vers la destination CRR. Assurezvous de sélectionner toutes les machines virtuelles qui font partie du datastore, car seules les machines virtuelles qui font partie du plan de réplication sont traitées.

NetApp Disaster Recovery Orchestrator 🔌	Dashboard Discover Resource C	Sroups Replication Plans Job N	lonitoring		۵ ۵	?	۹
Create New Replication Plan	Replication Plan and Site Details	Select Resource Groups 3	Set Execution Order	(4) Set VM Details			×
		Replication Plan Det	ails				
		Select Execution Orde	r				
	Resource Group Name		Execution Order				
	DemoRG		3				
		Network Mapping					
	No more	Source/Destination network resources	available for mappir	Ig			
	Source Resource	Destination Resource					
	SepSeg	SegDR		Delete			
		DataStore Mapping					
	Source DataStore	Destination Volume					
	TestSrc01	gwc_ntap_acct/gwc_DRO_cp/testsrc0	Лсору				
		Previous	ue				

8. Sous VM details, vous pouvez éventuellement redimensionner les paramètres CPU et RAM des VM. Cela peut s'avérer très utile lorsque vous récupérez de grands environnements sur des clusters cibles plus petits ou lorsque vous effectuez des tests de reprise après incident sans avoir à provisionner une infrastructure VMware physique individuelle. Modifiez également l'ordre de démarrage et le délai de démarrage (s) pour toutes les machines virtuelles sélectionnées dans les groupes de ressources. Il existe une option supplémentaire pour modifier l'ordre de démarrage si des modifications sont requises par rapport à ce que vous avez sélectionné lors de la sélection de l'ordre de démarrage ressource-groupe. Par défaut, l'ordre de démarrage sélectionné lors de la sélection de groupe de ressources est utilisé, mais toutes les modifications peuvent être effectuées à ce stade.

NetApp	Disaster Recovery Orchestrator 💊	Dashboard Discover Re	source Groups   Replicatio	n Plans   Job Monitoring	i (I			۵	٠	?	9
	Create New Replication Plan	Replication Plan and Site D	letails 🕜 Select Resource	ce Groups 🕢 Set Exec	ution Order	Set VM Details					×
			VI	M Details							
		2 vms				٩					
		VM Name	No. of CPUs	Memory (MB)	NIC/IP	Boot Order ) Override					
		Resource Group : DemoRG			-						
		QALin1	1 0	1024 [3]	O Static O Dynamic	3 0					
		QALin	4 10	1024 [0]	<ul> <li>Static</li> <li>Dynamic</li> </ul>	3 0					
							-				
			Previous	Create Replication Plan							

9. Cliquez sur **Créer un plan de réplication**.une fois le plan de réplication créé, vous pouvez utiliser les options de basculement, de basculement ou de migration selon vos besoins.

Disaster Recovery C	Drchestrator 🗞 📔 Dashboar	d   Discover   Resource (	Froups   Replication Plans	Job Monitoring				۰	0	٩
B 1 Rep	lication Plans	2 1 Resource Groups	Source Details	VCenters	Destination Sites 1	n Details	2 1 VCenters			
1 Replication Plan						Q 0	Create New Replication Plan			
Plan Name	C Active Site	Status	Compliance	Source Site		÷ I				
DemoRP	( Source	( Active	Partially Healthy	DemoSRC	DemoDest	Res	Plan Details		1	
							Edit Plan			
							Fallover Test Fallover			
							Migrate			
							Run Compliance Delete Plan			
	Disaster Recovery ( 1 Replication Plan Plan Name DemoRP	Disaster Recovery Orchestrator  Parkboar	Disaster Recovery Orchestrator       Dashbard       Discover       Resource of the source of the s	Disaster Recovery Orchestrator       Dashbard       Discover       Resource Groups       Source Details         Image: Source Details       Image: Source Groups       Image: Source Details       Image: Source Details       Image: Source Details         Image: Replication Plans       Image: Source Groups       Image: Source Groups       Image: Source Details       Image: Source Details         Image: Replication Plans       Image: Source Groups       Image: Source Groups       Image: Source Groups       Image: Source Groups         Image: Replication Plans       Image: Source Groups       Image: Source Groups       Image: Source Groups       Image: Source Groups         Image: Replication Plans       Image: Source Groups       Image: Source Groups       Image: Source Groups       Image: Source Groups         Image: Replication Plans       Image: Source Groups       Image: Source Groups       Image: Source Groups       Image: Source Groups         Image: Replication Plans       Image: Source Groups         Image: Replication Plans       Image: Source Groups       Image: Source Groups       Image: Source Groups       Image: Source Groups         Image: Replication Plans       Image: Source Groups       Image: Source Groups       Image: Source Groups       Image: Source Groups	Disaster Recovery Orchestrator       Dashboard       Discover       Resource Groups       Replication Plans       Job Monitoring         Image: Source Details         Image: Replication Plans       Image: Source Groups       Image: Source Details       Image: Sou	Disaster Recovery Orchestrator       Dashboard       Discover       Resource Groups       Replication Plans       Job Monitoring         Image: Source Details       Image: Source Orealis       Image: Source Orealis	Disaster Recovery Orchestrator in Bashoard Discover Resource Groups Replication Plans Details Teplication Plans Details Teplication Plans Details Detai	Disaster Recovery Orchestrator     Disaster Recovery Orchestrator     Disaster Recovery Orchestrator     Source Details     Source Details     Desination Plans     Periodion Plans     Source Oroups     Source Details     Detailer     Desination Plans     Periodion Plans     Source Oroups     Source Details     Detailer     Detailer     Periodion Plans     Periodion Plans     Source Oroups     Source Details     Detailer     Periodion Plans     Periodion Plans     Source Oroups     Source Details     Periodion Plans     Periodion Plans <td>Disaster Recovery Orchestrator Datower Network (excendence) Application Rians     Source Details     In replication Rians     In replication Rians     In replication Rians     Source Details     In replication Rians     In replication Rians     Source Details     In replication Rians     In replication Rians     Source Details     In replication Rians     Source Brians     Compliance     Source S</td> <td></td>	Disaster Recovery Orchestrator Datower Network (excendence) Application Rians     Source Details     In replication Rians     In replication Rians     In replication Rians     Source Details     In replication Rians     In replication Rians     Source Details     In replication Rians     In replication Rians     Source Details     In replication Rians     Source Brians     Compliance     Source S	

Au cours des options de basculement et de test, le snapshot le plus récent est utilisé ou un snapshot spécifique peut être sélectionné à partir d'un snapshot instantané. L'option instantanée peut être très avantageuse si vous êtes confronté à une situation de corruption, comme les ransomwares, où les réplicas les plus récents sont déjà compromis ou chiffrés. DRO affiche tous les points temporels disponibles.

		Source Details		Destination	n Details	
Replication Plans	Resource Groups	Sites	vCenters	Sites 1		VCenters
	Testfailover Details			×		
1 Replication Plan	<ul> <li>Use latest snapshot ()</li> <li>Select specific snapshot ()</li> </ul>			^	Q 9	Create New Replication Plan
Plan Name 🗢 🗧 Active Site	Volume		Snapshot		¢I	<u>ķ</u>
DemoRP 💮 Source	WEANFAVSacct/testcap/testsro	01	Select Snapshot		Reso	ource Groups
			2023-04-28	-		
			2023-04-28T11:31:55.000Z - gwc_ntap	-		
			2023-04-28T11:21:54.000Z - gwc_ntap.			

Pour déclencher le basculement ou tester le basculement avec la configuration spécifiée dans le plan de réplication, vous pouvez cliquer sur **basculement** ou **Test basculement**. Vous pouvez contrôler le plan de réplication dans le menu des tâches.

Back			
	Test Failover Steps Replication Plan: DemoRP		
~	Cloning volumes for test (in parallel)	⊘ Success	0.7 Seconds 🕕
~	Mounting cloned volumes and creating datastores (in parallet)	⊙ Success	0.9 Seconds 🛈
~	Registering VMs (in parallel)	⊙ Success	0.1 Seconds 🕕
~	Powering on VMs in protection group - DemoRG - in target (in parallel)	Success	0.1 Seconds ()

Une fois le basculement déclenché, les éléments récupérés sont visibles sur le site secondaire AVS SDDC vCenter (VM, réseaux et datastores). Par défaut, les machines virtuelles sont restaurées dans le dossier Workload.

II NetApp	Disaster Recovery Orchestra	tor 🔌   Decklaurd   Discover	Researce Groups   Replication	on Plans   Job Monitoring			٠	¢ 0 0
	C 2 Sites	1 Resource Group	B 1 Replication	Plan	128	T Protected	0 127 Ungrateched	
	Environments 2 Votual Environments	2 Alef Storige Accounts	Topology Canvas			-	Immersive View 🖉	
	SDOC Summary	D 14 Feiders	D Next	SRC 172 38 156 27	DemoCest tegs./18.75.6.2/	)		
	Datastores							
	Execution Jobs		Replication Plans					
	Ø 1 Tertal Soliti	C 1 su Propessi	Replication Flam DemoRP	Active Site	Clates	Fallover Mode		

La restauration peut être déclenchée au niveau du plan de réplication. En cas de basculement de test, l'option de démontage peut être utilisée pour annuler les modifications et supprimer le nouveau volume créé. Les retours arrière liés au basculement sont un processus en deux étapes. Sélectionnez le plan de réplication et sélectionnez **Inverser la synchronisation des données**.

Source Details       Destination Details         Image: splication Plans       Image: splication Plans         Image: splication Plans       Image: splication Plans	Image: Source Details     Image: Source Details       Image: Image	vCenters	Destination Details	Create New Replication Plan
I Replication Plan     Q O     Create New Replication Plan       Plan Name     C Active Site     Status     Compiliance     Source Site     T     I       DemoRP     O Destination     Running In Failover Modi O Healthy     DemoSRC     DemoDest     Resource Groups     Cmail	1 Replication Plan Plan Name: \$   Active Site:   Status   Compliance		Q 0	Create New Replication Plan
Plan Name     Compliance     Source Site     Image: Compliance       DemoRP     Image: Compliance     Source Site     Image: Compliance       DemoRP     Image: Compliance     Source Site     Image: Compliance	Plan Name C Active Site Status Compliance			
	DemoRP (O) Destination (I) Running In Failover Mode (I) Healthy	Source Site 국 Desti	estination Site C	

Une fois cette étape terminée, déclenchez la restauration pour revenir au site AVS principal.

tApp Disaste	r Recovery Orchestrat	or 💊   Dashboard	Discover Resource Gro	ups Replication Plans	Job Monitoring		<b>A</b> - 4	¢ ? (	9
				Source Details		Destination Details			
	B 1 Replication Pla	ins	1 Resource Groups	1 Sites	vCenters	Contraction 1 Sites	vCenters		
<b>1</b> Rej	plication Plan					Q (	Create New Replication Plan		
Plan	n Name 🗘 🕴	Active Site	Status	Compliance	Source Site 🛛 👻	Destination Site 0	3		
Den	noRP	© Destination	Active	<ul> <li>Healthy</li> </ul>	DemoSRC	DemoDest	Resource Groups		
							Plan Details	-	
							Failback		



Depuis le portail Azure, nous constatons que l'état de la réplication a été rompu pour les volumes appropriés mappés au SDDC AVS du site secondaire en tant que volumes de lecture/écriture. Pendant le basculement de test, DRO ne mappe pas le volume de destination ou de réplica. Elle crée un nouveau volume du snapshot de

réplication interrégionale requis et expose le volume en tant que datastore, ce qui consomme de la capacité physique supplémentaire du pool de capacité et garantit que le volume source n'est pas modifié. Les tâches de réplication peuvent notamment se poursuivre pendant les tests de reprise d'activité ou les workflows de hiérarchisation. De plus, ce processus permet de s'assurer que la restauration peut être nettoyée sans risque de destruction de la réplique si des erreurs se produisent ou si des données corrompues sont récupérées.

#### Restauration par ransomware

Récupérer des données suite à un ransomware peut être une tâche extrêmement fastidieuse. Plus précisément, il peut être difficile pour les services IT de déterminer le point de retour sûr et, une fois déterminé, comment s'assurer que les charges de travail restaurées sont protégées contre les attaques qui se produisent (par exemple, suite à un malware en sommeil ou à des applications vulnérables).

La DRO répond à ces préoccupations en permettant aux entreprises de récupérer leurs données à partir d'un point de disponibilité dans le temps. Les charges de travail sont ensuite restaurées sur des réseaux fonctionnels mais isolés, de sorte que les applications puissent fonctionner et communiquer les unes avec les autres, sans toutefois être exposées au trafic nord-sud. Ce processus permet aux équipes de sécurité d'effectuer des analyses et d'identifier tout malware caché ou endormi.

# Conclusion

La solution de reprise d'activité Azure NetApp Files et Azure VMware offre les avantages suivants :

- Exploitez la réplication interrégionale Azure NetApp Files efficace et résiliente.
- Restaurez vos données à un point dans le temps grâce à la conservation des copies Snapshot.
- Automatisez entièrement toutes les étapes requises pour restaurer des centaines, voire des milliers de machines virtuelles à partir des étapes de validation du stockage, du calcul, du réseau et des applications.
- La restauration des charges de travail repose sur le processus de « création de nouveaux volumes à partir des snapshots les plus récents », qui ne manipule pas le volume répliqué.
- Évitez tout risque de corruption des données sur les volumes ou les snapshots.
- Évitez les interruptions de réplication lors des workflows de test de reprise après incident.
- Exploitez les données de reprise d'activité et les ressources de calcul cloud pour les workflows en dehors de la reprise d'activité, tels que le développement/test, les tests de sécurité, les tests de correctifs et de mise à niveau, et les tests de correction.
- L'optimisation des processeurs et de la RAM peut contribuer à réduire les coûts du cloud en permettant la restauration vers des clusters de calcul plus petits.

### Où trouver des informations complémentaires

Pour en savoir plus sur les informations données dans ce livre blanc, consultez ces documents et/ou sites web

• Création d'une réplication de volume pour Azure NetApp Files

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

Réplication entre les régions de volumes Azure NetApp Files

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

• "Solution Azure VMware"

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

• Déploiement et configuration de l'environnement de virtualisation sur Azure

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

• Déploiement et configuration de la solution Azure VMware

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

# Utilisation de la réplication Veeam et du datastore Azure NetApp Files pour la reprise après incident vers la solution Azure VMware

Auteur: Niyaz Mohamed - NetApp Solutions Engineering

# **Présentation**

Les datastores Azure NetApp Files (ANF) dissocient le stockage du calcul et libèrent la flexibilité requise pour que les entreprises puissent migrer leurs workloads vers le cloud. Elle fournit aux clients une infrastructure de stockage haute performance flexible capable d'évoluer indépendamment des ressources de calcul. Le datastore Azure NetApp Files simplifie et optimise le déploiement en parallèle d'Azure VMware solution (AVS) en tant que site de reprise d'activité pour les environnements VMware sur site.

Les datastores NFS basés sur volumes Azure NetApp Files (ANF) peuvent être utilisés pour répliquer les données depuis un environnement sur site à l'aide d'une solution tierce validée qui offre une fonctionnalité de réplication de machine virtuelle. En ajoutant des datastores Azure NetApp Files, il permettra un déploiement plus économique que la création d'un SDDC avec une solution Azure VMware avec un nombre considérable d'hôtes ESXi pour prendre en charge le stockage. Cette approche est appelée « groupe de témoins lumineux ». Un cluster pilote léger est une configuration hôte AVS minimale (3 nœuds AVS) avec la capacité de datastore Azure NetApp Files.

L'objectif est de maintenir une infrastructure à faible coût avec tous les composants de base pour gérer un basculement. Un cluster pilote peut évoluer horizontalement et provisionner davantage d'hôtes AVS en cas de basculement. Par ailleurs, une fois le basculement terminé et les opérations normales restaurées, le cluster de pilotage peut revenir en mode d'opérations à faible coût.

# Objectifs du présent document

Cet article décrit l'utilisation du datastore Azure NetApp Files avec Veeam Backup et la réplication pour configurer la reprise d'activité pour les machines virtuelles VMware sur site vers (AVS) à l'aide des fonctionnalités du logiciel de réplication de VM Veeam.

Veeam Backup & Replication est une application de sauvegarde et de réplication destinée aux environnements virtuels. Lors de la réplication de machines virtuelles, Veeam Backup & Replication est répliqué à partir de sur AVS, le logiciel crée une copie exacte des machines virtuelles au format natif VMware vSphere sur le cluster SDDC AVS cible. Avec Veeam Backup & Replication, la copie reste synchronisée avec la machine virtuelle d'origine. La réplication offre le meilleur objectif de délai de restauration (RTO), car une copie montée d'une machine virtuelle sur le site de reprise est prête à démarrer.

Ce mécanisme de réplication permet de s'assurer que les workloads peuvent démarrer rapidement dans un SDDC AVS en cas d'incident. Le logiciel Veeam Backup & Replication optimise également la transmission du trafic pour la réplication sur WAN et les connexions lentes. Il filtre également les blocs de données dupliqués, les blocs de données nuls, les fichiers swap et les « fichiers exclus du système d'exploitation invité des machines virtuelles ». Le logiciel compresse également le trafic de réplica. Pour éviter que les tâches de réplication ne consomment la totalité de la bande passante réseau, les accélérateurs WAN et les règles de restriction réseau peuvent être utilisés.

Dans Veeam Backup & Replication, le processus de réplication est piloté par des tâches, ce qui signifie que la réplication est effectuée via la configuration des tâches de réplication. En cas d'incident, le basculement peut être déclenché pour restaurer les machines virtuelles en basculant sur la copie de réplica. Lors d'un basculement, une machine virtuelle répliquée prend le rôle de la machine virtuelle d'origine. Le basculement peut être effectué vers l'état le plus récent d'une réplique ou vers l'un de ses points de restauration connus. La restauration est ainsi possible en cas d'attaque par ransomware ou de tests isolés les cas échéant. Veeam Backup & Replication propose plusieurs options pour gérer différents scénarios de reprise d'activité.

[]

# Déploiement de la solution

#### Marches de haut niveau

- 1. Le logiciel Veeam Backup and Replication s'exécute dans un environnement sur site avec une connectivité réseau appropriée.
- 2. "Déploiement d'une solution Azure VMware (AVS)" cloud privé et "Reliez des datastores Azure NetApp Files" Aux hôtes de la solution Azure VMware.

Un environnement de pilote léger configuré avec une configuration minimale peut être utilisé à des fins de reprise sur incident. Les machines virtuelles basculeront vers ce cluster en cas d'incident et d'autres nœuds pourront être ajoutés.)

- 3. Configurez la tâche de réplication pour créer des répliques de machine virtuelle à l'aide de Veeam Backup and Replication.
- 4. Création d'un plan de basculement et basculement
- 5. Revenez aux machines virtuelles de production une fois l'incident terminé et le site principal en marche.

#### Conditions préalables pour la réplication de VM Veeam vers les datastores AVS et ANF

- 1. Assurez-vous que la machine virtuelle de sauvegarde Veeam Backup & Replication est connectée à la source ainsi qu'aux clusters SDDC AVS cibles.
- 2. Le serveur de sauvegarde doit pouvoir résoudre les noms abrégés et se connecter aux vCenters source et cible.
- 3. Le datastore Azure NetApp Files cible doit disposer d'un espace libre suffisant pour stocker des VMDK de VM répliquées.

Pour plus d'informations, reportez-vous à la section « considérations et limitations » "ici".

### Détails du déploiement

Veeam Backup & Replication exploite les fonctionnalités Snapshot de VMware vSphere/pendant la réplication, Veeam Backup & Replication demande à VMware vSphere de créer un Snapshot de machine virtuelle. Le snapshot de machine virtuelle est la copie instantanée d'une machine virtuelle, qui comprend des disques virtuels, l'état du système, la configuration et les métadonnées. Veeam Backup & Replication utilise le snapshot comme source de données pour la réplication.

Pour répliquer des machines virtuelles, procédez comme suit :

- 1. Ouvrez Veeam Backup & Replication Console.
- 2. Dans la vue d'accueil. Cliquez avec le bouton droit de la souris sur le nœud Jobs et sélectionnez Replication Job > Virtual machine.
- 3. Spécifiez un nom de travail et cochez la case de contrôle avancé appropriée. Cliquez sur Suivant.
  - Cochez la case amorçage du réplica si la connectivité entre le site et Azure a une bande passante limitée.

\*Cochez la case Remapping réseau (pour les sites SDDC AVS avec différents réseaux) si les segments du SDDC solution Azure VMware ne correspondent pas à ceux des réseaux de sites sur site.

 Si le schéma d'adressage IP du site de production sur site diffère du schéma du site AVS cible, cochez la case Replica re-IP (pour les sites DR avec un schéma d'adressage IP différent).

[]

4. Sélectionnez les machines virtuelles à répliquer sur le datastore Azure NetApp Files attaché à un SDDC de solution Azure VMware à l'étape Virtual machines\*. Les machines virtuelles peuvent être placées sur VSAN pour remplir la capacité de datastore VSAN disponible. Dans un cluster à voyants, la capacité utilisable d'un cluster à 3 nœuds sera limitée. Le reste des données peut être facilement placé dans les datastores Azure NetApp Files afin que les machines virtuelles puissent être restaurées, et le cluster peut être étendu pour répondre aux besoins en processeur/en Mo. Cliquez sur Ajouter, puis dans la fenêtre Ajouter un objet, sélectionnez les machines virtuelles ou les conteneurs VM nécessaires et cliquez sur Ajouter. Cliquez sur Suivant.

[]

 Ensuite, sélectionnez la destination en tant que cluster/hôte SDDC pour la solution Azure VMware et le pool de ressources, le dossier VM et le datastore FSX pour ONTAP pour les répliques de VM. Cliquez ensuite sur Suivant.

[]

6. Dans l'étape suivante, créez le mappage entre le réseau virtuel source et le réseau virtuel de destination, selon vos besoins.

[]

- 7. À l'étape **Job Settings**, spécifiez le référentiel de sauvegarde qui stocke les métadonnées pour les répliques de VM, la stratégie de rétention, etc.
- Mettez à jour les serveurs proxy Source et cible à l'étape transfert de données et laissez la sélection automatique (par défaut) et conservez l'option Direct sélectionnée, puis cliquez sur Suivant.
- 9. À l'étape Guest Processing, sélectionnez l'option Activer le traitement compatible avec les

applications selon les besoins. Cliquez sur Suivant.

[]

10. Choisissez la planification de réplication pour exécuter la procédure de réplication à exécuter régulièrement.

[]

11. À l'étape **Résumé** de l'assistant, passez en revue les détails de la procédure de réplication. Pour démarrer le travail juste après la fermeture de l'assistant, cochez la case **Exécuter le travail lorsque je clique sur Terminer**, sinon ne cochez pas la case. Cliquez ensuite sur **Terminer** pour fermer l'assistant.

[]

Une fois la procédure de réplication lancée, les machines virtuelles dont le suffixe est spécifié sont renseignées sur le cluster/hôte AVS SDDC de destination.

## []

Pour plus d'informations sur la réplication Veeam, reportez-vous à la section "Fonctionnement de la réplication"

#### Étape 2 : création d'un plan de basculement

Lorsque la réplication ou l'amorçage initial est terminé, créez le plan de basculement. Le plan de basculement permet d'effectuer automatiquement le basculement des machines virtuelles dépendantes une par une ou en tant que groupe. La planification de basculement est la référence pour l'ordre dans lequel les machines virtuelles sont traitées, y compris les retards de démarrage. Le plan de basculement permet également de s'assurer que les machines virtuelles dépendantes critiques sont déjà en cours d'exécution.

Pour créer le plan, accédez à la nouvelle sous-section intitulée **replicas** et sélectionnez **Plan de basculement**. Choisissez les machines virtuelles appropriées. Veeam Backup & Replication recherche les points de restauration les plus proches à ce point dans le temps et les utilise pour démarrer les répliques de machine virtuelle.



Le plan de basculement ne peut être ajouté qu'une fois la réplication initiale terminée et les répliques de machine virtuelle à l'état prêt.



Le nombre maximum de machines virtuelles pouvant être démarrées simultanément lors de l'exécution d'un plan de basculement est de 10



Pendant le processus de basculement, les machines virtuelles source ne sont pas hors tension

Pour créer le Plan de basculement, procédez comme suit :

1. Dans la vue d'accueil. Cliquez avec le bouton droit de la souris sur le nœud répliques et sélectionnez plans de basculement > Plan de basculement > VMware vSphere.

[]

 Indiquez ensuite un nom et une description du plan. Des scripts de pré-basculement et de postbasculement peuvent être ajoutés si nécessaire. Par exemple, exécutez un script pour arrêter les machines virtuelles avant de démarrer les machines virtuelles répliquées.

[]

3. Ajoutez les machines virtuelles au plan et modifiez l'ordre de démarrage de la machine virtuelle et les délais de démarrage afin de répondre aux dépendances des applications.

[]

Pour plus d'informations sur la création de tâches de réplication, reportez-vous à la section "Création de travaux de réplication".

Lors du basculement, la machine virtuelle source du site de production est basculée vers sa réplique sur le site de reprise après incident. Dans le cadre du processus de basculement, Veeam Backup & Replication restaure le réplica de la machine virtuelle vers le point de restauration requis et déplace toutes les activités d'E/S de la machine virtuelle source vers son réplica. Les répliques peuvent être utilisées non seulement en cas d'incident, mais aussi pour simuler des exercices de DR. Pendant la simulation de basculement, la machine virtuelle source reste en cours d'exécution. Une fois tous les tests nécessaires effectués, vous pouvez annuler le basculement et revenir aux opérations normales.



Assurez-vous que la segmentation réseau est en place pour éviter les conflits d'adresses IP lors du basculement.

Pour démarrer le plan de basculement, cliquez simplement sur l'onglet **plans de basculement** et cliquez avec le bouton droit de la souris sur votre plan de basculement. Sélectionnez **\*Démarrer**. Cette opération basculera en utilisant les derniers points de restauration des répliques de machine virtuelle. Pour basculer vers des points de restauration spécifiques de répliques de machines virtuelles, sélectionnez **Démarrer** à.

[]

[]

L'état des répliques de machine virtuelle passe de Ready à Failover et les machines virtuelles démarrent sur le cluster/hôte SDDC Azure VMware solution (AVS) de destination.

[]

Une fois le basculement terminé, l'état des machines virtuelles passe à « basculement ».

[]



Veeam Backup & Replication arrête toutes les activités de réplication de la machine virtuelle source jusqu'à ce que son réplica revienne à l'état prêt.

Pour plus d'informations sur les plans de basculement, reportez-vous à la section "Plans de basculement".

Lorsque le plan de basculement est en cours d'exécution, il est considéré comme une étape intermédiaire et doit être finalisé en fonction de l'exigence. Les options sont les suivantes :

• **Retour en production** - revenez à la machine virtuelle d'origine et transférez toutes les modifications qui ont eu lieu pendant que la réplique de la machine virtuelle était en cours d'exécution sur la machine virtuelle d'origine.



Lorsque vous effectuez un retour arrière, les modifications sont uniquement transférées, mais pas publiées. Choisissez **commit readback** (une fois que la machine virtuelle d'origine a été confirmée pour fonctionner comme prévu) ou Annuler le retour arrière pour revenir au réplica de la machine virtuelle si la machine virtuelle d'origine ne fonctionne pas comme prévu.

- Annuler le basculement revenez à la machine virtuelle d'origine et supprimez toutes les modifications apportées à la réplique de la machine virtuelle pendant son exécution.
- **Basculement permanent** basculez de manière permanente de la machine virtuelle d'origine vers une réplique de machine virtuelle et utilisez cette réplique comme machine virtuelle d'origine.

Dans cette démo, le retour arrière à la production a été choisi. Le basculement vers la machine virtuelle d'origine a été sélectionné lors de l'étape destination de l'assistant et la case à cocher « mettre la machine virtuelle sous tension après la restauration » a été activée.

[]			
[]			
[]			
[]			

La validation du retour arrière est l'une des méthodes permettant de finaliser l'opération de restauration. Lorsque le retour arrière est validé, il vérifie que les modifications envoyées à la machine virtuelle qui est en retour (la machine virtuelle de production) fonctionnent comme prévu. Après l'opération de validation, Veeam Backup & Replication reprend les activités de réplication pour la machine virtuelle de production.

Pour plus d'informations sur le processus de restauration, reportez-vous à la documentation Veeam pour "Basculement et retour arrière pour la réplication".

[]

Une fois la restauration en production réussie, les machines virtuelles sont toutes restaurées vers le site de production d'origine.

[]

# Conclusion

Grâce à la fonctionnalité de datastore Azure NetApp Files, Veeam ou tout outil tiers validé fournit une solution de reprise d'activité économique en exploitant les clusters Pilot light au lieu de créer un cluster volumineux uniquement pour prendre en charge les réplicas de VM. Cela constitue un moyen efficace de gérer un plan de reprise d'activité personnalisé et de réutiliser les produits de sauvegarde en interne pour la reprise d'activité,

permettant ainsi la reprise d'activité dans le cloud en fermant les data centers de reprise d'activité sur site. Il est possible de basculer en cliquant sur un bouton en cas d'incident ou de basculer automatiquement en cas d'incident.

Pour en savoir plus sur ce processus, n'hésitez pas à suivre la vidéo de présentation détaillée.

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

#### Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de nonresponsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

#### Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site http://www.netapp.com/TM sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.