

Backup and Recovery Best Practices With vSphere Data Protection Advanced

www.tintri.com

Contents

Intended Audience1
Introduction1
Consolidated list of practices
Backup
Deploying And Configuring VDP Appliance For VDP Advanced4
Creating And Configuring VDP Advanced Backup Jobs 6 Guest Images Job Type
Automatic Backup Verification
Restore 13 File Level Restore 14
Restoring Microsoft Application Servers 16 Restoring Microsoft SQL Server Databases 16 Restoring Microsoft Exchange Server Databases or Individual Mailboxes 17
Replication18VDP Replication18Tintri VMstore SnapVM™, CloneVM™ and ReplicateVM™19
Summary

Intended Audience

This document will discuss best practices of protecting your virtual machines in a VMware vSphere environment using vSphere Data Protection Advanced (VDP Advanced). This Tintri Best Practice Guide for backup and recovery will assist individuals who are responsible for the design and deployment of data protection and disaster recovery solutions for VMs deployed on Tintri VMstore[™] systems. This document will encompass vStorage APIs for Data Protection (VADP) for backups and the use of Tintri's SnapVM[™], CloneVM[™] and ReplicateVM[™] features to complement data protection of virtual machines and critical applications hosted on Tintri's VMstores with vSphere Data Protection 5.5 or later.

Introduction

Deploying storage into your virtual environment should be a straightforward process. What if you didn't have to do LUN masking on a storage array? What if didn't have to worry about raid levels or queue depth settings ever again? What if you could just connect a datastore to an ESXi host, discover the datastore and start deploying your virtual machines? Tintri VMstore[™] is designed so that IT administrators with a working knowledge of vSphere can successfully deploy Tintri's purpose-built VM storage with ease.

Tintri VMstore delivers extreme performance and VM density, and a wide variety of powerful features, which are seamlessly integrated with vSphere. Examples include snapshots, clones, replication, instant bottleneck visualization, and automatic virtual disk alignment. Tintri VMstore extends and simplifies the management of virtual machines (VMs) through an intrinsic VM-awareness that reaches from the top of the computing stack, all the way down into the storage system.

This best practice guide includes the following when using vSphere Data Protection Advanced (VDP Advanced):

- An overview of the VMware environment with VDP deployed on a Tintri VMstore.
- VDP Appliance configuration settings on a Tintri VMstore.
- Protecting virtual machines and applications such as Microsoft Exchange and Microsoft SQL servers.
- Performing recovery of virtual machines and using granular level recovery (GLR) to recover individual items.
- Performing recovery of Microsoft Exchange mailboxes and Microsoft SQL databases.
- Using VDP Advanced Replication to protect backups.
- Using Tintri CloneVM and ReplicateVM to protect virtual machines.

Consolidated list of practices

Tags	Recommendation
Deploying And Configuring VDP	DO: Ensure that the DNS entries exist and are correct before deploying a VDP
Deploying And Configuring VDP	DO: Use Thin provisioning for deploying VDP Appliances OVF templates.
Deploying And Configuring VDP	DO: Use Thin provisioning for Device Allocation for all VDP Appliances deployed on
Appliance For VDP Advanced Guest Images Job Type	DO: Use Applications for application consistent backups with VDP Advanced supported
Guest Images Job Type	Microsoft applications. DO: As a workaround, Tintri's recommendation is to deploy a new VDP Advanced
	appliance with NBD transport if using image-based backups for critical VMs that cannot handle the pauses during snapshot removal phase of a HotAdd backup.
Applications Job Type	DO: Install VMware VDP for Exchange Server plug-in on all Microsoft Exchange virtual servers.

Tags	Recommendation
Applications Job Type	DO: Install the Exchange GLR plug-in only on the server that will be used for granular level recovery. It is not necessary to install the Exchange GLR plug-in on all Exchange servers.
Applications Job Type	DO: Ensure that the VDP appliance is reachable, on the network, from the Microsoft application server. Attempt the re-install of the Microsoft application plug-in when the network issue is resolved.
Applications Job Type	DO: Select only one Microsoft Exchange Server per VDP Advanced Application backup job. This is a VDP Advanced best practice.
Applications Job Type	DO: Ensure that the new ESXi host is licensed for VDP Advanced.
Applications Job Type	DO: Ensure the ESXi host and the Tintri VMstore is accessible on the network for VDP Advanced.
Automatic Backup Verification	DO: Schedule ABV jobs to run after incremental backups to avoid resource contention. Run an initial incremental backup to determine the backup duration for scheduling ABV jobs.
Restore	DO: Remove any existing VMware snapshots on the VM before attempting a restore to the original VM. Restore to original location, if the VM has existing VMware snapshots, will fail with VDP Advanced 5.5 and higher.
Restore	DO: Power off the virtual machine before attempting a restore to original location. If the virtual machine is not powered off, the restore to original location will fail.
File Level Restore	DO: It is a requirement that the VM client has network access to the VDP Restore Client web interface for FLR.
File Level Restore	DO: The local host credential must have local administrator privileges on the VM for VDP Restore Client log on.
Restoring Microsoft SQL Server Databases	DO NOT: For redirected restores to a different Microsoft SQL Server instance, do not select tail-log backup.
Restoring Microsoft SQL Server Databases	DO: Ensure that the Authentication method is supported by the Microsoft SQL Server instance. If the authentication method is not configured on the Microsoft SQL Server instance, the restore operation will fail.
Restoring Microsoft Exchange Server Databases or Individual Mailboxes	DO: Enable VDP Advanced GLR log files before attempting GLR.
VDP Replication	DO: Ensure that the source replication server always has the updated root account User ID and password for the destination target server.
Tintri VMstore SnapVM [™] , CloneVM [™] and ReplicateVM [™]	DO: Rollback to the latest validated checkpoint.
Tintri VMstore SnapVM [™] , CloneVM [™] and ReplicateVM [™]	DO NOT: Allow VDP to continue running backups if the integrity check is out-of-date. Running backups if the integrity check is out of date increases your risk of losing potential backup data. An alarm will be generated in the vSphere Web Client Alarms pane if the integrity check is out-of-date.
Tintri VMstore SnapVM [™] , CloneVM [™] and ReplicateVM [™]	DO NOT: Backup jobs should not be running (scheduled/manual) during a VDP maintenance window. Although backup jobs will run, the resources VDP needs for maintenance tasks will be consumed by the backup jobs. It is a VMware recommendation to reserve a portion of each day for routine VDP maintenance activities.
Tintri VMstore SnapVM [™] , CloneVM [™] and ReplicateVM [™]	DO: Always run an integrity check before performing new backups with a cloned VDP appliance (VMware Clone/Tintri CloneVM).

Backup

Environment

VMware vSphere Data Protection (VDP) is a disk-based backup and recovery solution. It has two available tiers:

- Basic VDP
- VDP Advanced

Basic VDP does not require a license key whereas the VDP Advanced requires one. One of the main differences between basic and advanced version is the latter supports guest-level backups and restores of Microsoft Exchange Servers, SQL Servers, and SharePoint Servers. In addition, VDP Advanced also supports application-level replication and automatic backup verification (ABV). Underneath the hood of the data protection technology, EMC Avamar is the engine that powers VDP. Deduplication is automatically performed with every backup job and VDP also supports Changed Block Tracking (CBT). A VDP virtual appliance OVA file is used to deploy VDP to protect a VMware virtual environment. Similar to EMC Avamar, which is the basis of VDP, VDP is able to protect backups with checkpoints and rollbacks. In this document, the referenced architecture consists of a single VDP virtual appliance deployed with VDP Advanced to back up VMs and Microsoft applications in the VMware data center.



NOTE: In this document, VDP will be used to reference Basic VDP/VDP Advanced.

VDP relies on a set of components that run on different machines to provide data protection for virtual machines. These components are:

- vCenter Server
- VDP Appliance
- vSphere Web Client

vSphere Data Protection uses variable-length method to determine data segment size. This key factor allows VDP to efficiently determine logical boundary points to optimize data deduplication during backups. Each VDP Appliance can simultaneously support up to eight virtual machine backups. In a large-scale environment, multiple VDP Appliances can be deployed to support an expanding VMware environment. VDP 5.5 or later requires a minimum of the following:

- VMware vCenter Server version 5.1 or later.
- vCenter Server Linux or Windows.
- vSphere Web Client (see the VMware website for current vSphere 5.5 web browser support).
- Web browsers must support Adobe Flash Player 11.3 or higher to access vSphere Web Client and VDP functionality.
- VDP supported VMware ESX/ESXi version (review the <u>latest vSphere Data Protection Administration</u> <u>Guide</u> for details).

Other major difference between basic VDP and VDP Advanced are the following:

- The size of the VDP Appliance cannot be changed once Basic VDP is deployed
- The size of the VDP Appliance can be increased with VDP Advanced
- Basic VDP supports up to 100 VM's per VDP appliance
- VDP Advanced supports up to 400 VM's per VDP appliance

Deploying And Configuring VDP Appliance For VDP Advanced

Deploying and configuring a VDP Appliance is easy. There are a few do's that must be followed to ensure that the deployment and configuration of a VDP Appliance is successful:

- Ensure that a static IP address entry exist for the VDP Appliance on the DNS Server.
- Ensure that the FQDN entry for the VDP Appliance is correct on the DNS Server.
- Ensure that the forward and reverse lookup for the VDP Appliance entry is correct.
- Ensure that the VMware proxy node can communicate with the DNS Server using port 53 over TCP and UDP protocols.
- Ensure that the vCenter user account for VDP is explicitly added as administrator on the vCenter root node.

For additional details on configuration requirements, review the <u>vSphere Data Protection Administration</u> <u>Guide</u>. Use *nslookup* to validate forward and reverse DNS entry of the following before attempting to configure the VDP Appliance:

- The static IP address for the VDP Appliance
- The FQDN entry of the VDP Appliance

🗷 Windows PowerShell
PS C:\Users\dcheah> nslookup Dom-VDPA Server: ucsad <u>.ttucs.tm.tin</u> tri.com Address: 10
Name: Dom- <u>VDPA.ttucs.tm.</u> tintri.com Address: 10
PS C:\Users\dcheah> nslookup Dom-VDPA.ttucs.tm.tintri.com 🔶 2 Server: ucsad.ttucs.tm.tintri.com Address: 10
Name: Dom-VDPA.ttucs.tm.tintri.com Address: 10
PS C:\Users\dcheah> nslookup 10. Server: ucsad.ttucs.tm.tintri.com Address: 10
Name: dom- <u>vdpa.ttucs.tm</u> .tintri.com Address: 10

In addition, ensure that the user account assignment for VDP Advanced in the vCenter is valid and has the Administrator role assigned.

with the vc2.ttucs.tm.tintri.com ad to the right.	m folder
Role	Propagate
Administrator	Yes
	with the vc2.ttucs.tm.tintri.com ad to the right. Role Administrator

For example, the reference vCenter architecture in this document; uses TTUCS active directory domain for users and groups. If the vCenter credentials are invalid, a Test Connection attempt in the vCenter registration step could fail.

Network settings	Identify the hostname or IP add username and password for a r	ess of your vCenter server. Also provide a user that has rights to register objects with	
Time zone	the vCenter pervet.		The connection test did not complete
VDP credentials	vCenter userhame:	NanC	successfully. Modify your network settings or
vCenter registration	vCenter password		Contex and antiple and then slick Test
VDP license	vCenter FODN or IP.	vc2 Buce tm tintri com	voenter credentials and then click rest
Create Storage	vCenter port.	443	Connection to run the connection test again.
Device Allocation	Use vCenter for SSO aut	entration	
CPU and Memory	-		OK
Ready to complete	Test	Connection 🛖 1	
Complete			
		second distances in the local distances in th	

In the case where the vCenter credentials are invalid, the test connection will fail with the above connection error.

NOTE: The VDP backup user account referenced in this white paper belongs to an Active Directory domain. The backup user is entered in the following format: "System-Domain\user-account" in the vCenter username field.

You could also run into one of the following connection errors using the VDP Advanced configuration wizard if the nslookup fails to validate the static IP address or the FQDN assigned to the VDP Appliance.



DO: Ensure that the DNS entries exist and are correct **before** deploying a VDP Appliance. This is a VMware requirement.

When the DNS entries have been corrected, re-deploy the VDP Appliance. The test connection should complete successfully.



In the *Device Allocation* step of the configuration wizard, select *Provision: Thin* when configuring VDP storage disks on a Tintri VMstore.

2004	Store With Appl	Esnce	Protesion	Thin	
credentials	Datastores.	Capacity	Provinies.	free.	INS.
registration	Tines_T548_A	12.2718	253710	3.47/0	0
erise					
Storage					
Abocation					
nd Memory					
to compilete					
iete					
	ANO. 200 0.08.25	100 1 H 1019 23	e ven,		

DO: Use Thin provisioning for deploying VDP Appliances OVF templates.

DO: Use Thin provisioning for Device Allocation for all VDP Appliances deployed on Tintri VMstores.

When VDP Advanced is successfully configured, all VDP services should be running.

Sphere Data Protection Status	Log collector
Core centors & Running Stop Kanagement sentors & Running Stop Pile system sentors & Running Stop Pile level restors sentors & Running Stop Bartelio scheduler & Running Stop	The log collector aggregate log files from all VCP related a excess to sastal it movalestroniting. Circ. Voiet logs from van wite le prompted to download a all piles containing all system service logs. • Core VCP excise logs • File system service logs • File system service logs • File system service logs • Collect trailine logs • Collect as logs. • Collect as logs. • File system would like the diservice logs for all follows did: "Collect diservices" relevand og would like the diservice logs. • Collect strailine logs. • Collect strend logs.
Last updated 65/12(014 02:36 FM	

Creating And Configuring VDP Advanced Backup Jobs

Guest Images Job Type

Logon to the vSphere Web Client, the vSphere Data Protection 5.5 pane should appear. Connect to the VDP Appliance and from the *Getting Started* tab, use the *Create Backup Job* to configure new backups for protecting your virtual machines and applications in your VMware environment.

e agricere Divisi Pre	testion 8.5					_
VDP						
Getting Elarted	Backup	Restore	Replication	Reports	Configuration	
Sphere Data	rotection	Advance	bi		*	_
vSonere Data Pro Movisoft SGL, M SharePoint SGN, M machines, It data privitous state of machines, can be Uaero determine Advanced tasks a points are saved scheckale hackor resulting restore prestore weeks, months, o	rection Adv krosoft Exc es in addition loss serve restored, atten vSphored, For examp for examp to for early to points mght r years.	variated back thange, and in to virtual ruption occu- ins or virtual ere Data Pr how long n ple, users m incerning hos t be retained	ts up are, the obsolion rebre right rs and the d for	-		
Basic Tasks						
R Add a VDP	advanced	license				
O Download	Application	Backup C	lient			
Create Dac	kup Job	-	- (1)			
E. Restore Ba	ckup		0			

When creating a new backup job, VDP Advanced provides the following backup types:

- Guest images. Guest images uses VMware's VADP to protect virtual machines.
- Applications. Application protects application servers such as Microsoft Exchange Servers or Microsoft SQL servers using VDP's recommended guest level approach.

Loko Type Loko Type	sale a new backup job	
	Lobi Type 2 Data Type 2 Data Type 3 Backop Targata 4 Softenito Manaminin Positry 4 Job Name 7 Ready to Complete	Jub Type Exclup jobs an be one of several types. Select the type of Sacolup job you with to create

If Guest Images is selected, virtual machines will be protected using VADP. VADP is an image-based backup of a virtual machine using one of the following supported VMware's VADP transport modes with a

Tintri VMstore:

- HotAdd
- NBD
- NBDSSL

DO: Use *Applications* for application consistent backups with VDP Advanced supported Microsoft applications.

By default, VDP Advanced will attempt to use HotAdd transport for guest image backups. If a VM cannot be backed up using HotAdd, VDP Advanced will automatically attempt with Network Block Device (NBD) transport. With HotAdd transport, be aware that a VM can be paused for a long time during snapshot removal of a backup process (VMware KB Article). In some cases, application servers serving data will experience long pauses and this could interrupt application services. For applications that cannot handle the pauses, Tintri recommends using NBD transport for those application servers.

It is recommended to deploy a new VDP Advanced appliance that will use NBD transport for backups of critical VMs, which cannot handle the pause during snapshot removal, with image-based backups. For more information on VADP transports, review Tintri's <u>Backup and Recovery Best Practices</u>.

DO: As a workaround, Tintri's recommendation is to deploy a new VDP Advanced appliance with NBD transport if using image-based backups for critical VMs that cannot handle the pauses during snapshot removal phase of a HotAdd backup.

To change VDP Advanced preferred transport, review the following <u>Changing VMware VDP Transport</u> <u>Methods</u>. The new line should consist of the following: *--transport="nbd:nbdssl"* for the particular VDP Advanced appliance. When the preferred transport method is updated and the avagent has been restarted, backup jobs to the updated VDP Advanced appliance will use NBD transport.



VDP uses VMware's CBT. In addition, VDP also has a very efficient in-line deduplication and compression technology for backups. Subsequent VDP image-based backups using NBD transport will utilize incrementals with CBT after the first initial full. Tintri VMstore deduplication and compression is similar to VDP Advanced, both solutions for a virtualized data center uses in-line deduplication to dedupe data blocks on entire systems.

If *Guest Images* is selected, the *Data Type* step will have the option to protect a virtual machine by performing a full image backup or the option to protect the individual disks of the particular VMs. Select *Full Image* to protect entire VMs. In the *Backup Targets* step, select the virtual machines to be protected with image-based backup. Complete the *Create a new backup job* wizard process to create a new backup job. By default, the *retention policy* of a VDP Advanced backup job is 60 days.

Use the options in the Retention Policy step to configure a retention policy that will meet the local backup retention requirements in your data center.

		\sim
Create a new backup job		8
1 Job Type 2 Data Type 3 Backup Targets	Backup Targets Select the backup targets from the list below.	
4 Schedule 5 Retention Policy		K Clear All Selections
6 Job Name 7 Ready to Complete	Image: Second December 2004 President Apple Image: Second December 2004 President Apple <t< td=""><td></td></t<>	
		Back Next Finish Cancel

In the *Backup* tab of the vSphere Data Protection pane, an *Image* backup job is created following a successful creation using *Guest Images*. This particular backup job will protect 2 VMs with image-based backups.

setting Started	Backu	p Restore	Replication	Reports Confi	guration			
2 Refresh								
Name		State	Type	Lost Start Time	Duration	Next Run Time	Success	Falure Count
Backup 2VMs		Enabled	Image	Never	Never	05/13/2014 08:0:	0	0
			1)				

Applications Job Type

From the *Configuration* tab of the vSphere Data Protection pane, select the appropriate *Client downloads* to protect your Microsoft application servers. For example, from the Microsoft Exchange 2013 virtual machine server, log in to the vCenter UI and download the Microsoft Exchange Server 64 bit plug-in from the vSphere Data Protection 5.5 pane.

vSphere Data Protection 5.5		
vSphere Data Protection (10.	Switch Applance: vSphere Da * 🎍	🥘 - Al Actions 😧
Getting Started Backup Restore Replication Reports Configuration		
Backup Applance Log Email 🤤 Refresh		0-
Backup applance details	YDP Advanced license assignment	
Disaliay name: vdiptere Data Protection 5.5	Licensed Iems	a .
Product name: VDP Advanced		(200)
IP Address: 10		1
Major Version: 5.5.6.56		
Minor Version: 7.0.82.99_5.5.6.56		
Status: Normal		
Host: 192		
vCenter server: vc2 tlucs th (Intel.com		
VDP backup user: Buck/backup		
VOP appliance time: 09/132014 03:20 PM		
Time zone: GMT -7:00		
VDP Appliance storage summary		
Capacity: 536.3 GB		
Space free: 536.3 GB		
Deduplicated size: 0 bytes		
Non-Deduplicated size: 0 bytes		
Client downloads		
Moranot Exchange Server 54 bit 🔶 1 Microsoft 504, Server 32 bit	Monsect. BOX. Server. 64.16 🦛 (2)	
Monaolt, Shareford, Bener, 54,58	÷	
Backup window configuration		
(1)Berlup	Stewa	
ne de la companya de		
		11 12a 11 12a
ਹੋਸ਼ਨ 77 ਲੱਡੇ 10 ਜੋ 10p ਜੋ 2 3 4 8 8 1	7 8 8 10 11 12 1 2 3 4 8	6 7
		Edt

Run the Microsoft Exchange Server 64 bit plug-in installation on all the Microsoft Exchange 2013 servers. Be aware that the installation of the Exchange GLR plug-in requires a system reboot at the end of the installation.

DO: Install VMware VDP for Exchange Server plug-in on all Microsoft Exchange virtual servers.

DO: Install the Exchange GLR plug-in only on the server that will be used for granular level recovery. It is not necessary to install the Exchange GLR plug-in on all Exchange servers.

VMware VDP for Exchange Server Setup	VDP appliance server unreachable	×
where KP for Exchange Server Setze Belet the operation you wish to perform. Oct on the core in the the below to change the way features will be retailed. Image: Influence KPF for Exchange Server (SEA), which you will be retailed. Image: Influence KPF for Exchange Server (SEA), which you will be retailed. Image: Influence KPF for Exchange Server (SEA), which you will be retailed. Image: Influence KPF for Exchange Server (SEA), which you will be retailed. Image: Influence KPF for Exchange Server Serv	RegisterAgent: Cannot connect to VDP appliance. This might be because the VDP appliance server is down or the host-name/IP you have provided does not exit or is not a VDPA appliance. Make sure the host-name or IP address you have provided is valid and run the installer again.	
Sack Hent Cancel		

If the VDP appliance is not reachable from the Microsoft application server, your Microsoft application plugin installation will fail with the following error.

DO: Ensure that the VDP appliance is reachable, on the network, from the Microsoft application server. Attempt the re-install of the Microsoft application plug-in when the network issue is resolved.

After installing VMware VDP for Exchange Server plug-in, use the VMware VDP Exchange Backup User Configuration Tool wizard to configure the VMwareVDPBackupUser account. This user account must have domain and administrator-level permissions to perform a successful VDP application-consistent backup. Execute Check to validate the VMwareVDPBackupUser account has valid credentials and permissions.

	VMware VDP Exchange Backup User Configuration Tool
User configuration	
Username	VMwareVDPBadupUser
	New user O Existing user Contigure Services
Password	•••••
Confirm password	
Exchange server	DC-W2012-3 V
Storage group	· · · · · · · · · · · · · · · · · · ·
Mailbox store	MainD8 V
Checks done VM-ware/DPBackupU/ VM-ware/DPBackupU/ VM-ware/DPBackupU/ Creating malbox for VM-mare/DPBackupU/ DC-AP/VM-mare/DPBackupU/ Local service restart Creating and configure	Check Clear Display Open Log File 2 respires PASED ar setting passind, as the ropines PASED ar setting passind, as the ropines PASED ar created malbox PASED ar crea
<	III 5
_	

From the Exchange server, you can also validate that the VMwareVDPBackupUser account has been successfully created. Create a new backup job with Applications job type. Select either a Full Server or Selected Databases option in the Data Type step. To protect your Microsoft Exchange servers, select the available Microsoft Exchange Server in the Backup Targets step. Complete the Create a new backup job wizard to configure an Application backup job for Exchange.

/ 1 Job Type	Backup Tarpets	
2 Data Type	Detect the backup largets from the kid betow	
3 Dataup Targets		
4 Backup Options		Clear All Detections
5 Schedule		
6 Relation Policy	 Et Murraut Sci. Server(s) 	
7 Job Name	In the construction of the second secon	
8 Ready to Complete		-
	B Microsoft SharePoint Sever(s)	7
	C	
		Back Niert Fruit Cancel

DO: Select only one Microsoft Exchange Server per VDP Advanced Application backup job. This is a VDP Advanced best practice.

NOTE: Only Microsoft Exchange servers installed with *VMware VDP for Exchange Servers* plug-in are discovered.

You can also configure an *Application* backup job to protect any SQL servers in the VMware environment. Install the VMware VDP for SQL server plug-in on the SQL servers. In this document, Microsoft Exchange 2013 servers, a Microsoft SQL 2012 server and VMs are protected using VDP Advanced. Select a backup job and execute *Backup now* to protect your Microsoft application servers and virtual machines.

Review the latest <u>VDP Administration Guide 5.5</u> for supported Microsoft Exchange Servers and Microsoft SQL Servers.

Create a new backup job		8
Create a new backup job	Backwp Taryers Select the backup sargets from the list below.	Clear All Selections
		Back Net Finish Cancel

VDP Advanced utilizes EMC Avama's in-line deduplication and compression technology; only unique blocks are backed up regardless of the backup job type. In addition, VDP Advanced also uses VMware's CBT for image-based backup. The combination of using VMware's CBT and EMC Avamar's efficient in-line deduplication and compression technology makes VDP Advanced a powerful data protection solution for VMware. VDP Advanced 5.5 also supports backup to EMC Data Domain Systems for additional data protection. From the *Configuration* tab of the vSphere Data Protection pane, a VDP Advanced administrator can easily deduce the efficiency and storage savings with VDP Advanced deduplication and compression technology for data protection.

VDP Appliance storage s	ummary	
Capacity:	536.3 GIB	
Space free:	423.2 GiB	
Deduplicated size:	113.0 GiB	
Non-Deduplicated size:	1.2 TiB	

You can monitor a VDP Advanced job progress from vCenter's Recent Tasks pane. A VDP job can be identified from the *Details* column. For example, in the following screen capture, a unique job identifier is appended to the backup job named *Backup 2VMs*. Keeping track of the job identifier is useful when attempting to review VDP logs to debug VDP Advanced job issues. In this example, the VDP:Backup Job is protecting 2 VMs using *Job Type: Guest Images*.

Recent Tasks Name. Target or Status contains									
Name	Target	Status	Oetals	Initiated by					
Reconfigure virtual machine	Sphere Data Protection 5.5	Campleted		TTUCS/packup					
Reconfigure virtual machine	Sphere Data Protection 5.5	Completed		TTUC9/backup					
Reconfigure virtual machine	Sohere Data Protection 5.5	Completed		TTUCS/Backup					
Reconfigure virtual machine	Sohere Data Protection 5.3	Completed	Internet and the company of the	TTUC5/beckup					
Backup/Restore VM	B DOW2512_HOUNS	1%	Backing up Disk 1/1:(F) - 2	dom-vdpa.ttucs.tm.tintri.compro					
Backup/Restore VM	6 DC-W28128-5QL-1	1%	Backing up Disk 1/1:(F)	dom-vdpa.ttucs.tm.tintri.compro_					
VDP: Backup Job	Suttere DetaRistation 5.5	12%	Backup 2vHs-1400024316351	1) thics/badap					
Part and the second second	THE CONSTRUCTION OF A DOMESTIC								

In the following example, a *VDP:Backup Job* with job identifier *BackupSQL2-1400171792645* failed. A VDP Advanced administrator can utilize this information to review the VDP logs, debug, and resolve VDP Advanced backup issue.

The VDP Advanced administrator was able to conclude that the Microsoft SQL 2012 server backup failed due to NT Authentication error.

Recent Tasks				1 Name, Target o	r Status contains: •	Clasr
Name	Target	Status	Ortals	Instand by	VCenter Server	Requested Star
VDP: Bankup Jub	D vishare Data Protection-DG2	O Error	BeckupSQL2-1400171792648	ttucs/(tadop)	🦉 ve2.thuse.tm.hi.	5/15/2014 9:38
Avtar log:						
8014-05-15 09:37:14 avtar 8014-05-15 09:37:15 avtar 8014-05-15 09:37:15 avtar 8014-05-15 09:37:15 avtar 8014-05-15 09:37:15 avtar 8044-05-15 09:37:15 avtar 8014-05-15 09:37:15 avtar 8014-05-15 09:37:15 avtar 8014-05-15 09:37:15 avtar	Info (22022): Backup (ZAIKELED,) Info (21035): Reading 13 user p Warning (10052): Could not get Info (21036): Dome reading user Info (3157): BARTIAL Backup #2 Info (5559): Label "Duckup502_ Info (2683): Finished at 2014.0 Info (26455): Sending warpup mes Info (3314): Command failed (1	mapping-up sessi mofiles DNS domain name profiles timestamp 2014-0 1400121792645027 in 0.27 minutes: 5-15 00:37:15 Par usage to parent warming, exit co	on with Server for domain NT AUTHORITY; 5-15 09:37:13, 1 files, , none backup, backup ty 0 bytes/hour (221 files cific Daylight Time, fia de 10013: externally can	; error 1212 { 2 folders, 0 bytes pe: level0_full s/hour) upsed time: 0000h:00 ncelled)	• (2) (1 files, 0 bytes, 0.00 m:16s	15 new)

After resolving the NT Authentication error, a new VDP Advanced application backup of the Microsoft SQL 2012 server successfully makes progress and completes the Microsoft application backup.

lecent Tasks		Name, Target or Status contains: •		
Nation	Target	Status	Detais	Initiated by
F VDP: Backup Job	Sphere DataProtection 5.5	12%	Beckup SQL-1400088194643	thurs'badup

A VDP Advanced administrator can also use the VDP logs to review historical data. In the following example, a Microsoft Exchange 2013 server was successfully protected with VDP Advanced with 0 warnings, 0 errors, and 0 fatal errors on 2014-05-15.

2014-05-15 14:54:18 avexvss Info <7726>: LISTENING ON PORT 51148	
2014-05-15 14:54:18 averyss Into <77445: bindir: [C:\Program Files\avp\bin]	
2014-05-15 14:54:18 avexues Info <13044>: ctl spawn successful	
2014-05-15 14:54:18 avexyss Info <7729>: original key [3018-BackupExchangeServers-1400190242040]	. clone [3018-BackupExchangeServers-1400190242040]
2014-05-15 14:54:10 avexyss Info <13114>: ctl man successful	
2014-05-15 14:54:18 avexyss Info <13045>: after ctl man start successful	
2014-05-15 14:54:18 averuss Info c66865: Process 5784 (C:\Program Files\aup\hin\autar) for works	under BackupExchangeServers-1400190242040#0 started
2014-05-15 14:54:18 avexyss Info (7732): Waiting for avtar to finish	
2014-05-15 14:54:19 avexyss Info <10684>: Setting ctl message version to 3 (from 1)	
2014-05-15 14:54:19 avexyss Info <16136>; Setting ctl max message size to 268435456	
2014-05-15 14:54:20 avexyss Info <6688>: Process 5784 (C:\Program Files\avp\bln\avtar) finished	(code 0: success)
2014-05-15 14:54:20 avexyss Info <13115>: avexyss shapup assist::hire new manager sub-process sr	paun returned 0
2014-05-15 14:54:20 avexvcc Info <7734>: manager finished	
2014-05-15 14:54:20 avexyss Info <13069>: dc u2012-3 completed snapview creation.	
2014-05-15 14:54:21 avexvss Info <8782>: Writing V55 exclude files	
2014-05-15 14:54:21 avexyss Info (13073): Full backup successful, log file truncation requested	
2014-05-15 14:54:22 averyss Info <7753>: Exit main body	
2014-05-15 14:54:22 avexvss into (131805: Final summary	
2014-05-15 14:54:22 avexvss Info <13181>: snapview wid: BackupExchangeServers-1400190242840#0	
2014-05-15 14:54:22 avexyss Info <7271>: Final summary generated subwork 1911, cancelled/aborter	0, snepview 1, exitcode 0
2014-05-15 14:54:27 avexyss Info c12951>; Plug-in avexyss returning with exitcode 0	and a second
END avexvss log 2014-05-15 14:54:27 Pacific Daylight Time (0 warnings, 0 errors, 0 fatal	errors)
	0.004.0055

Additionally, the vSphere Data Protection *Reports* provide a granular approach in reporting data protection at the virtual machine level. In the VDP Advanced report, a VDP Administrator can determine when a VM was backed up, the Job Type of the backup, the success or failure of the last executed backup job.

	Chan the								
Sphere Data Pro	tectionD.	(10.1)				Switz	ch Appliance: vOphere Da	
Getting Started	Backup	Restore	Replication	Reports Configu	ration				
2 Refresh									
	Applia	ince status.	1	éormal					
	Used	capacity:	7	30%					
	Integr	ity check stat	an: A	lormal					
	Rece	nt tailed back	ups: 0						
Titler: Show All #									
Filter: Show All # Column selection: (Client de	italis 📝 Bac	XUDS 🗍 RED	ication 🗍 Backup vent	ication	3	Last Beaksy July		
Chents Filter: Show All # Column selection:) Chem Neme	Chert de	itans 📝 Bac	Rubs 🗔 Reb	Backup verit		3 Last Nexut	Let Body July Let Fun Time), Last J00 1	verne
Chents Filter: Show All + Column selection: Crem Neme dc-w20127-egi- 2.dcad.local	Client de	Mails 💕 Bac metron State Ictivated	NUDS 🗔 Rep Type 🏄 Application	Backup Wert	Lant Successful module 1. 05/15/2014 10:30 AM	3 Last Menut Success	Let Bisky Job Let Part Ime 05/15/2014 10:30 AM	Last Job 1	seme
Clients Filter: Show All & Column selection: 1 Client terms do-w20122-eq 2.dcad.local do-w2012-3.dcad.l	Client de Client Indur Client Indur Client Indur Client Indur	itaits 🗹 Bac metion bare Ictivated	Rups 🗔 Kep Type 🏒 Application Application	Icabon Description Backup90L2 Backup90L2 Descup5change0erv ert.BackupErchange	Cabon Law Successful Testing 1 DS/15/2014 10:30 AM 05/15/2014 04:15 PM	Last Heauth Success Buccess	Let Beaugrado Last Part Time 05/15/2014 10:30 AM 05/15/2014 04:15 PM	Eachup90L2 Bachup90L2 DachupEuchangs0erver1	serve
Column selection:) Column selection:) Column selection:) Count reems do-w20127.eqt- 2.dcad.local do-w2012-3.dcad.l DC-VM-Close-1	Client de Client Infor	Italis 🗹 Bac metion State Ictivated Ictivated Powered Off	Type Application Application Image	Icabon Backup vent	Cabon Last Successful Record 8 & DS/15/2014 10:30 AM 05/15/2014 04:15 PM 00/04/2014 09:44 AM	Last Result Success Duccess Success	Lett Binatop Julo Last Pun Time 05/15/2014 03.0 AM 05/15/2014 04.15 PM 00/04/2014 08:44 AM	Lait Job 1 BachupSQL2 BachupEichangsGener1 BachupCione 1	úame

Tintri VMstore's dashboard and VM view provides a rich feature to monitor resources. This is one of the advantages of Tintri VMstores. The hypervisor agnostic storage solution provides a virtualization administrator the tools to monitor and manage resources on a per VM basis. For example, during a backup using VDP Advanced, the VMware administrator can easily review IOPS, throughput, and latency of each virtual machine that is part of the VDP Advanced backup job.

A VMware VDP Advanced administrator can easily focus on the source of the latency for a particular VDP

Appliance. In this case, the ESXi host is the main contributor of the VDP Appliance latency. Troubleshooting a virtualized data center issue is simplified with a storage solution that was designed, from the ground-up, with virtualization in mind. A VMware administrator can easily fix this latency issue by adding more CPU and memory to the ESXi host or migrating the VDP Advanced appliance to another ESXi host that has additional CPU and memory resources.

Dashboard Dat	astore Virtual M	achines				
VMs Virtual disks	Snapshots Y		(1)		
VM	IOPS	MBps	Latency ms	Provisioned GiB	Used GiB	Change MB/day
vSphere Data Protec	b 183	29.0	130.9	874	39.7	80,77
MCSLoginVSI-010	0	0.0	0.0	40	0.1	
		ALCOUNT OF BUILDING	host 127	.8 network 0.2 storage 2.9	disk 0.0	
ravisioned	at vest, 1,018 30PS, 128 (Hr	conserves,	10,054 208 020 204 4			241611661 1 494, 183 KM/S

Migrating a VDP Appliance to another ESXi host will affect HotAdd transport availability.

DO: Ensure that the new ESXi host is licensed for VDP Advanced.

DO: Ensure the ESXi host and the Tintri VMstore is accessible on the network for VDP Advanced.

Automatic Backup Verification

The backup administrator, the Microsoft application administrators and the VMware data center administrator can take a breather knowing that their critical Microsoft applications and virtual machines are protected with VDP Advanced on Tintri VMstores. But how do a VMware data center administrator and the backup administrator address backup restores for tests or rely on the data integrity of a restore point to perform restores in a disaster recovery scenario? What other additional features and functionality are there with VDP Advanced?

To ensure the integrity of backup restore points, VDP Advanced has an additional feature. Automatic Backup Verification (ABV) is a backup verification feature that can be started manually or automatically scheduled. ABV provides the following verification options:

- Heartbeat verification. Default verification option. Check if VMware tools heartbeat has been received within a specific timeframe after the VM is powered on .
- Script verification. Allows VDP administrator to script and test health status of applications and services on the Guest OS. There must be no dependency, in the script, on other VMs in the network.

Editing beckap verification job fie	achag/Verification						
 Virtual Machines Verification Options J Destination 	Ready to complete Review the settings for this backup verification yits. Click Finish to accept these settings, or click Back to make changes						
 ✓ 4 Schedula ✓ 5 Arle Name 	Narre.	BackagVerthadon					
 It measy to compare 	Selected Bern:	DC-W29128-80K-12014.05.15.13.32.04					
	Ventication Option	s: Heartbeat Verification only 🗲 🔳					
	Destination Path:	Vetual Machines/vc2:thucs.tm.tetts.com/UCS/10.60.0.20					
	Datastore:	Tem_7540_4					
	Schedule:	The Rist Sunday of every month					
		Back Finan Ga	ricel				

Automatic Backup Verification VMs are always restored to a temporary virtual machine with **VDP_ VERIFICATION_**<vm-name><unique number> attached. NICs on the temporary VM are always disabled to avoid network conflict and the temporary virtual machines are deleted once a backup verification job completes.

Recent Tasks						
None	Target	Status	Details	-	Initiated by	
Backup/Restore VM	DP_VERIFICATION_DC-W20128-SQ_	42%	Restoring Disk 1/1:(P)		dc-vdpa2.ttucs.tm.tintri.com-prox.	
VDP: Backup Verification Job	Sphere Data Protection -DC2	40%	BackupVerification-1400275328833		ttucs\badup	

When running ABV on a Tintri VMstore, be aware that there will be temporary changes to latency and flash hit ratio on the Tintri VMstore as cold parts of VM data are read from HDD storage.

DO: Schedule ABV jobs to run after incremental backups to avoid resource contention. Run an initial incremental backup to determine the backup duration for scheduling ABV jobs.

Restore

In the previous sections, we've addressed configuring VDP Appliance in a VMware environment, configuring image-based backups with VADP, configuring Microsoft application backups, running backups with *Job Type: Guest Images* and *Job Type: Applications* with virtual machines hosted on a Tintri VMstore, and executing ABV jobs.

VDP Advanced has the following restores options:

- Image restore of an entire VM.
- Restore of individual disks.
- File level restore.
- Restore of supported Microsoft application server databases.
- Granular level recovery of supported Microsoft application servers.

Restore backup		
1 Select Backup 2 Set Restore Options 3 Ready to complete	Set Restore Options Set the restore options for each backup that you are restoring.	
	℃ Client: DC-VM-Clone-1 Backup: 06/04/2014 09.44 AM ☑ Restore to original location ▼ Advanced options Datastore: Tintri_T540_A(1.9 TiB free) ☑ Power On ☑ Reconnect NIC	
	Back Next Finish Cancel	

DO: Remove any existing VMware snapshots on the VM before attempting a restore to the original VM. Restore to original location, if the VM has existing VMware snapshots, will fail with VDP Advanced 5.5 and higher.

DO: Power off the virtual machine before attempting a restore to original location. If the virtual machine is not powered off, the restore to original location will fail.

As a data protection solution, VDP Advanced also uses CBT on restore to original location for *Guest Images* backup. This dramatically improves restore performance when the original VM is still available in the VMware data center. For example, CBT on restore to original location for a 70GB VM was completed within milliseconds.



VDP will automatically evaluate the workload to determine the best restore method to achieve the fastest VM image restore time. In a scenario where the change rate is high and CBT overhead would be less efficient for restore, CBT will not be the fastest restore method. VDP will intelligently choose the fastest recovery method for the image-based restore.

File Level Restore

To perform file level restore (FLR) from a guest image backup, log on to VDP Restore Client web interface from the VM client using either the local host credentials or the vCenter credentials. In the following example, file level restore will be executed from the virtual machine that was backed up using the local host vm credentials.

DO: It is a requirement that the VM client has network access to the VDP Restore Client web interface for FLR.

DO: The local host credential must have local administrator privileges on the VM for VDP Restore Client log on.



When VDP Advanced log on credentials have been validated and restore points are discovered, mount the required restore point for FLR. The mount and browsing of restore points may temporarily affect a Tintri VMstore latency and flash hit ratio as cold VM data is read from HDD storage.

Browse the restore point to find the file or folder for restore. Once the files or folders have been selected, click *Restore selected files...* to continue with the FLR process.

	≂ C	rogie	P 🛊 🗈 🖡 🕯	≡
vmware vSphere Data Protection	n Restore Client			
Restore Files @ Monitor Restores				
Mounted Backups	Name	 Size 	Date modified	
v 👼 Wed May 21 15:48:28 GMT-070 🔺	desitop.ini	524	2014-04-09 17:05:55	
v 🖾 [Disk#1]	Everywhere.search-ms	248	2014-04-09 17:05:55	
► 🛄 🔤 SRecycle.Bin	Indexed Locations.search-ma	248	2014-04-09 17:05:55	
► 🛄 🛄 PerfLogs				- 1
Program Files Program Files				- 1
ProgramData	\sim			- 1
System Volume Infor				- 1
v 🖂 📖 Users				- 1
¥ 🗋 💼 Administrator				_
AppData				- 1
P Contacts				_
Documents				- 1
🗆 💼 Downloads				
► 🛄 🖬 Favorites				- 1
Links		\frown		
Music	(2)		- 1
Pictures Saved Games		-		
► E Searches ▼			2	- 1
			Restore selected fil	15.
			Laferraneer	

Select a destination folder for restore. Create a new folder on the virtual machine if there is a need to restore to a new location. Click on *Refresh* to discover the new folder for restore. Select the destination for restore and click on *Restore* to initiate FLR.

Select Destination	Initiate Destare?
Please specify a destination folder on your login VM to restore to.	initiale Restore?
	Are you sure you want to initiate this restore job? If you have selected many files or a set of files of large size, the restore may take a long time to complete.

Be aware that FLR restore could take time to complete. An *Initiate Restore* pop-up window will appear to provide the administrator an option to continue with FLR or cancel FLR.

From the *Monitor Restores* tab, FLR job progress can be monitored for success or failure.

😗 Restore Files 🖪	D Monitor Restores]				
Status	Error Code	Client	OS	Start Time	Elapsed Time	End Time
SUCCESS		DC-W2012-8-VDPA	0	G Wed May 21 16:13:14 GMT-0700 2	00h:00m:15s	🕒 Wed May 21 15:13:29

On large VM image backups with lots of small files, be aware that the FLR browse could temporarily affect the latency and flash hit ratio on a Tintri VMstore as cold data is read from HDD storage. As another file recovery option, the restored file can be copied from the existing VM to any other VM in the VMware data center using the guest VM network.

Restoring Microsoft Application Servers

Restoring Microsoft SQL Server Databases

From the Manual restore tab, select the virtual machine backup with MS SQL backup type for restore.

2 Refresh		Restore 9	LocoUnitock 🏠 Delete 🕅	
ter: Show all V Selected Items V Name		Backup Types	Last Known Path	Location
	>	MS SOL	/dc-w20127-sql-2.dcad.local	
dc-w20127-sql-2 dcad local				
DC-W20127-sql-2 dcad local DC-W20128-SQL-1	>	Image	/Datacenters/UCS/10.60.0.20/Don	

Be aware that selecting Use SQL REPLACE option for a Microsoft SQL database restore to original location can result in potential data loss. This is because this option specifies that the database or related file will be created even though another database or file with the same name already exists in the Microsoft SQL instance. The Use SQL REPLACE option is an override of the Microsoft SQL Server safety check.

1 Select Backup 2 Set Restore Options 3 Ready to complete	Set Restore Options Set the restore options for each backup that you a	re ressonng	
	Client do-W20127-56/-2 ocad socal beau Backup: 05/15/2014 10:30 AM W Restore to original location ♥ Advanced options Use SQL REPLACE option: Tai-top backup: Restore system databases: Authendiadon method Login ID Login ID Login ID Advanced options (Stupport Only)	Z SQL authentication Administrator	Reset options

DO NOT: For redirected restores to a different Microsoft SQL Server instance, do not select tail-log backup.

DO: Ensure that the Authentication method is supported by the Microsoft SQL Server instance. If the authentication method is not configured on the Microsoft SQL Server instance, the restore operation will fail.

Fix all authentication issues and validate that the restore options are valid for the particular Microsoft SQL Server instance database restore. When the issues are resolved and a database restore is attempted, you can also view if the database is being restored from the Microsoft SQL Server instance.

SOLQuery1.sql File Edit View Project	DC-W20127-SQL-2.master (Admin Debug SQL Prompt Tools Window New Query 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
Object Explorer	• # :	×
Connect - 🛃 🛃 🗉 🍸	23	
Dock Values Social 2 Dock Values Social 2 Dock 2012 Soc	SQL Server 1103128 Addministrator) ases prhots lempDB (Restoring)	

Restoring Microsoft Exchange Server Databases or Individual Mailboxes

VDP Advanced Microsoft Exchange Server restore options allow restores to:

- Original location
- Alternate location
- Restore Storage Groups (RSG for Microsoft Exchange 2007)
- Recovery Databases (RDB for Microsoft Exchange 2010 and Microsoft Exchange 2013)

MENTORE DECKIED			
1 Select Backup 22Set Resson Options 3 Heady to complete	Set Restore Options Set the restore options for each flackup that you?	protection of the second se	
	 Advanced options Anne ditabase ouwerns Dn net replay transaction logs Move loga pade Restars into ROGROD Ontware spanding RGGROB RGGROB name REDERDE log pade Advanced options (Support Only) 	restore edb Theodow Z'rescover	₹2

Select the appropriate options for the Microsoft Exchange Server database restore. Complete the restore backup options in the *Restore backup* job Window to start a VDP Advanced restore. In the Events tab of the VMware vSphere Web Client, the VDP Advanced administrator can review if the Microsoft Exchange Server database completes successfully. All VDP Advanced jobs are logged, the avtar log will also provide detailed information on the Exchange restore job.

VDP: Restore Job	
tantes Compreted Initiator Burstdachup Target Briven Data Protection OC2 Server vs2 Burstin Ioki sem	
Related avents:	
Thursday, May 15, 2014 5 57 19 PM	VDP Restore completed
() Thursday, May 15, 3014 5.51 19 PM	VDP Restore dow0012-3 dataflocal started
(i) Thursday, May 15, 2014 5.51.19 PM	Taar VOP Nantov Jan
AVTAR log:	
2014-00.01 L7-00130 avtar 2010 (5120) - 800 2014-00.01 L7-00130 avtar 2010 (5200) - 800 2014-00.01 L7-00130 avtar 2010 (5200) - 2014-00.01 L7-00130 avtar 2010 (5200) - 2014-00.01 L7-00130 avtar 2010 (5200) - 800 2014-00.01 L7-000 2014-00.01 L7-000 2014-00.00 2014-00.00 2014-00.00 2014-00.00 2014-00.00 2014-00.00 2014-00.00 2014-00 2	In the Consequences prevent sectors are "tented in the number of the construction o

For GLR of individual mailboxes, VDP Advanced mounts a temporary virtual drive on the target server that has the VDP Advanced Plug-in for Exchange Granular Level Recovery installed. The backup must be a full application type backup.

Reflech Hen Ohow all +			to factory of	the state of the second	
CI Name	Backup Types	Last Known Path	Location	Expiration Date	
de (A) Personal Active - HealthNalbod28011	Abattons	20	YOP Applance	0502502014	1
📋 🍪 (A) Personal Archive - HeadMalboxd2x24	Malber		VDP Appliance	05/25/2014	
📋 🤹 (A) Personal Active - HealthMatboer28283	Malbox		VOP Appliance	05/25/2014	
01.001.00-W2012-4 73538CCD-L0U0006341	thatton		VDP Appliance	05/25/2014	
0 (D) DO-W2012-4 735300000-LGU808642+	Matter	(1)	VDP Appliance	95(25)2014	
(b) DC-W2012-4 73538CCD-LGU800848+	Malbox.	0	VDP Appliance	05/25/2014	
#6 (010C-W2012-4 72538CCD-LGA0005889+	Mailton		VDP Appliance	05/25/2014	
d) DC-W2012-473538CCD-LOUB00782+	Malbox		VOP Appliance	95/25/2014	
📋 🚳 (D) DO W2012 4 735300000-LGU300797 i	Mattern		VDP Appliance	05/25/2014	
🗋 🤞 (D) DC-W2012-4 73538C-CD-L CL8008868+	Malbox		VOP Appliance	05/25/2014	
6 (D) DC-W2012-4 73538CCD-LG00008021	Maites		VDP Appliance	05/25/2014	
3 1 (D) DG-W2012-4 7353BCCD-LOUG09806 -	Malicox		VDP Appliance	05(25)2014	
3 🚯 (0) 00 W2042 4 73538000D L60801945+	Malbox		VDP Appliance	05/25/2014	
the second is reasonable to the second	-				_

Select the individual mailbox to restore and complete the restore options. Click on *Finish* to start the GLR restore. The progress of the restore job can be monitored in the Recent Tasks pane in the vSphere Web Client interface.

Restore backup		
Set Restore Option Set Restore Option Ready to complete	Select Backup Verify that the list of backups to restore is correct and remove any that you wigh to exclose from the restore operation.	
	 ManCel (D) DC-W2012-4 735380CD-L0U000834 (MeV20-DCFirst ChuSev2Cup-Exchange Administrative Group) 	upi
	2	
	Tank Ned Point Car	cel)

DO: Enable VDP Advanced GLR log files before attempting GLR.

When GLR logging is enabled, debugging GLR restore failures such as the following is made a lot simpler.

15:37:37 evexchg2 15:37:57 evexchg1 15:38:04 evexchg2	waring (VIE): Soud annue section 'sroue' from estable' in verkonter, ipporing Info colobi: sourting the Awamar Virtual Disk Drive Error (2000): India Mauri Inter, mai likely cased by Aufs mourt failore: Aufs_volume:mourt error: The parameter is incorrect. 🖕 (1)
15:38:04 avenchgl: 15:38:04 avenchgl: 15:38:04 avenchgl: 15:38:04 avenchgl: 15:38:04 avenchgl: 15:38:04 avenchgl: 15:38:04 avenchgl: 15:38:04 avenchgl: 15:38:20 avenchgl: 15:38:20 avenchgl: 15:38:21 avenchgl: 15:38:21 avenchgl:	<pre>constitution instage is invite fulled to process 'unitage_fulles' event, backup at Sint_Port_Instals - Ipseing requires state transition for the 'unitage_fulles' maining ditto: fulles: Initializing at Neurotell interface 104 ditto: Initializing at Neurotelli interface 104 d</pre>
weachgle log 2014	45-35 15:30:35 Festils Deplayet Time (2 warrangs, 1 errors, 0 festi errors)

RSG/RDB is also another alternative for individual mailbox restores. RSG/RDB option allows a particular Microsoft Exchange database to be restored to a non-production database. The use of a RSG/RDG restore solution minimizes the risk of corrupting a production database. In the following example, the individual mailbox was restored from a RDB to a new mailbox for test purposes.



Replication

VDP Replication

Replication takes place between two independent VMware VDP products or EMC products deployed in remote locations. Replication is efficient, encrypted, and asynchronous. Replication with VDP ensures backups are protected across sites in a disaster recovery scenario. Review the latest <u>VDP Administration</u> <u>Guide 5.5</u> for replication compatibility between VMware VDP products and EMC products. It is recommended by VMware to schedule replication during periods of low backup activity to ensure the greatest number of client backups can be replicated during each scheduled replication job.

DO: Ensure that the source replication server always has the updated root account User ID and password for the destination target server.

1 Select Clients 2 Backup Selection	Destination Please specify a destination to replicate your backups to
S Destination Solvaste Solvaste Solvaste Solvaste Solvaste Solvaste T Ready to complete	Hostaanse or IP.
	Back, Need, Frank, Cancer

Tintri VMstore SnapVM[™], CloneVM[™] and ReplicateVM[™]

A VDP Appliance and backup restore points can be protected using VDP's rollback option. This option ensures that all backups before the checkpoints are valid in case of a disaster recovery scenario.

DO: Rollback to the latest validated checkpoint.

DO NOT: Allow VDP to continue running backups if the integrity check is out-of-date. Running backups if the integrity check is out of date increases your risk of losing potential backup data. An alarm will be generated in the vSphere Web Client Alarms pane if the integrity check is out-of-date.

Status	Configuration	Storage	Rollback	Upgrade	Emergency Restore				
The vSpher to a check p will no long	re Data Protection point ensures tha per be available in	system prov t all of the bac the system.	ides a mecha ckups on or b	anism to roll l efore the che	back the backup reposit ickpoint date are valid. H	ory on the app owever, any t	pliance to a known and valid state. Rol backups that occurred after the checkp	ling back oint date	
Checkpoir	nt tag		Da	te		Va	lid		
cp.201406	605160149		06	/05/2014 09:0	01:49 AM, PDT -0700	Va	lidate d		
cp.201408	cp.20140605161119		06	06/05/2014 09:11:19 AM, PDT -0700			Notvalidated		
A Unlock	to enable the roll	back operatio	n				Partners VDR collback to salected ch	ackmaint	
								o criptura .	
								1000	
								a anna anna anna anna anna anna anna a	

To execute an integrity check on a VDP Advanced appliance, select *Run integrity check* from the vSphere Data Protection Configuration tab.

and Antonia Line Lines . Contract		
lacitat garlerra delati	W9 Advanced Runnis annumment	and public the
inging name angenin (ani Presignation Velexie Lines	followerd forth:	0-
Podulinaria: IDP showed		

DO NOT: Backup jobs should not be running (scheduled/manual) during a VDP maintenance window. Although backup jobs will run, the resources VDP needs for maintenance tasks will be consumed by the backup jobs. It is a VMware recommendation to reserve a portion of each day for routine VDP maintenance activities.

VDP checkpoints and rollbacks are an advantage for protecting your VDP backups. But there is also a requirement to protect your VDP Advanced appliance to encompass all disaster recovery scenarios. Tintri's <u>SnapVM™</u>, CloneVM™, and ReplicateVM™ complements VDP Advanced data protection solution to provide protection for your VDP Appliance.

Tintri's SnapVM can be used to protect your VDP Appliance on the local Tintri VMstore and ReplicateVM can be used to protect your VDP Appliance at a remote site. SnapVM snapshot is on a per VM basis and it is efficient, as it consumes virtually zero disk space.

Sphere Data Prote	ctionDC	Powered On	 Normal 		
Win2012Goldimg Win81-MSDN-Befo Win81-TestCloneW Win81-TestCloneW Win81_Clone Win81_MSDN_Free Win81EntEval Win81EntEval Win81EntEval Win81EntEvalVS Win81Goldimage Win81LooinVSI	reOptin IthCust sh iato2 Sh Sh Sh Sh Sh Sh Sh Sh	Actions - vSphere Da Power On Shut Down Guest G Restart Guest OS Migrate Take Snapshot Revert to Current S Manage Snapshot Clone Edit Settings Move To	ta ProtectionDC2-VMw DS inapshot S	a	
Preview: vSphere Da	ta Prote	Assign tag Alarms	,		-
 Hard disk 1 	100 0	All vCenter Actions	2	3	La
 Hard disk 2 Hard disk 3 	256 C	Ali Tintri Actions	× 1	Take s	napshot
+ Hard disk 4	256 GB			Protect	
» Naturk adapter 1	du VM N	laturate (connector	0	-	1000

Tintri's replication feature is efficient as it sends only unique data blocks, after in-line deduplication and compression, across LAN/WAN to another Tintri VMstore to provide off-site protection for your VDP appliance.



To utilize Tintri's SnapVM and ReplicateVM features, select the Protect option in the All Tintri Actions. Select the appropriate snapshot schedule that meets your data center data protection requirements. In addition, configure the local and remote retention requirements for your VDP Appliance snapshot. The local and remote snapshot retention periods are independent of each other. This provides an added benefit to configure longer off-site retention periods to meet remote site data protection requirements for your VDP Appliance.

Protect vSphere Dat	a Protection -DC2	TintriClone				
Protect with	a snapshot	schedule			Use system de	fault 🖾
				istal Johnstei		
Hourly					2	
🖸 Daily	2:30am	on Sun-Sat	Keep 5	7	days Grash-consis	stent -
U weekty			1			
Disoritiy						
Costerly						
Protect by r	eplicating s	napshots 🛛				
Replicate to :		-				
Alert Threshol	a 50	nours				
					Protect	Cancel

Complete the configuration by selecting Protect. To recover a VDP Appliance on the local Tintri VMstore or on a remote Tintri VMstore, select Clone operation from *All Tintri Actions* in the vSphere Web Client interface to create a cloned VDP appliance.

Dashboard Virtual Ma	chines					
VMs Virtual disks Snapshots Y						
VM 🔺	IOPS					
vSphere Data ProtectionDC2	-\					
Win2012GoldImg	Show graphs					
Win2012R2	Brotoct					
Win2012R2_bc_kval	Take spanshot					
Win81-MSDN-BeforeOptim	View snapshot					
Win81-TestCloneWithCus	Clone					
Win81_Clone	Pin					
Datastore: 305 of 305 total VMs	FIII					
IOPS MBps Latency	Refresh					

NOTE: Tintri vSphere Web Client Plugin is required to utilize Tintri features from the vSphere Web Client.

When attempting to power on a cloned VDP appliance (VMware Clone/Tintri CloneVM), be aware that the network MAC address for the cloned VDP Appliance could be changed if the original VDP Appliance still exists.



If the VDP Appliance MAC address is changed, the console of the VDP Appliance will reflect that the network is unreachable. If this occurs, VMware's KB solution <u>VDP Appliance has no network connection</u> <u>after re-registering, cloning, or restoring from backup</u> can be applied to bring the VDP appliance back online.



When a cloned VDP Appliance (VMware Clone/Tintri CloneVM) has no network issues, the VDP appliance will perform a normal boot with no network errors.

.... Check the MCS status - Fri Jun 6 14:23:24 PDT 2014 Identity added: /homc/dpn/.ssh/dpnid (/homc/dpn/.ssh/dpnid) dpnctl: INFO: MCS status: down. dpnctl: INFO: Isee log file "/usr/local/avamar/var/log/dpnctl.log"] MCS is NOT ready - not starting agents Starting VDP Normal Boot Starting VDP appliance systems. Estimated time to complete: 10 minutes Run VDP integrity check on the cloned VDP Appliance to validate VDP checkpoints. Once the VDP integrity check is completed successfully, the VDP Administrator can continue with new backups to protect VMs and Microsoft Applications.

O VDP: Integrity Check cp.20140605160149 completed.	0	info	6/5/2014 9:15:43 AM
VDP: Integrity started.	0	info	6/5/2014 9:06:42 AM
Task: VDP: Integrity Check	0	info	6/5/2014 9:06:42 AM

DO: Always run an integrity check before performing new backups with a cloned VDP appliance (VMware Clone/Tintri CloneVM).

Tintri's SnapVM, CloneVM, and ReplicateVM can able be used to protect critical VMs deployed on a Tintri VMStore.

Summary

VDP Advanced is a really efficient and effective backup solution on a Tintri VMstore. The in-line deduplication and compression technology of VDP for backups provides additional storage savings. When backups are stored on a VDP Appliance, VDP Advanced has the built-in intelligence to choose the optimal restore technology (CBT restore/full VM restore) for restoring VMs.

Tintri SnapVM, CloneVM, and ReplicateVM technology can be used to provide additional protection to a VMware Data Center protected with VDP Advanced. Tintri's protect VM feature can be used to protect VDP appliances, Microsoft application servers, and VMs locally and remotely. It is recommended to use Tintri SnapVM and ReplicateVM to protect VDP appliances.

If a VDP appliance is protected with Tintri SnapVM and VMware snapshot locally, you can restore using any of the snapshot technology. It is, however, recommended to use Tintri SnapVM because it is fast and can be easily scheduled. When a VDP appliance is restored from a snapshot, an integrity check must be run prior to performing new backups. It is recommended to run the latest Tintri OS with the latest patches.

Combined, a Tintri VMstore and VDP Advanced is a powerful solution for deploying VMs and protecting a VMware data center.



201 Ravendale Dr., Mt. View CA 94043 650.810.8200 info@tintri.com | www.tintri.com

Tintri, Tintri VMstore, Zero Management Storage and FlashFirst are trademarks or registered trademarks of Tintri, Inc. All other trademarks or service marks are the property of their respective holders and are hereby acknowledged. ©2014 Tintri, Inc. All rights reserved.