



Tintri

TECHNICAL
WHITE PAPER

Backup and Recovery Best Practices With vSphere Data Protection Advanced

Contents

Intended Audience	1
Introduction	1
Consolidated list of practices	1
Backup	3
Environment	3
Deploying And Configuring VDP Appliance For VDP Advanced	4
Creating And Configuring VDP Advanced Backup Jobs	6
Guest Images Job Type	6
Applications Job Type	8
Automatic Backup Verification	12
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
Replication	18
VDP Replication	18
Tintri VMstore SnapVM™, CloneVM™ and ReplicateVM™	19
Summary	22

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 Appliance For VDP Advanced	DO: Ensure that the DNS entries exist and are correct before deploying a VDP Appliance. This is a VMware requirement.
Deploying And Configuring VDP Appliance For VDP Advanced	DO: Use Thin provisioning for deploying VDP Appliances OVF templates.
Deploying And Configuring VDP Appliance For VDP Advanced	DO: Use Thin provisioning for Device Allocation for all VDP Appliances deployed on Tintri VMstores.
Guest Images Job Type	DO: Use Applications for application consistent backups with VDP Advanced supported Microsoft applications.
Guest Images Job Type	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

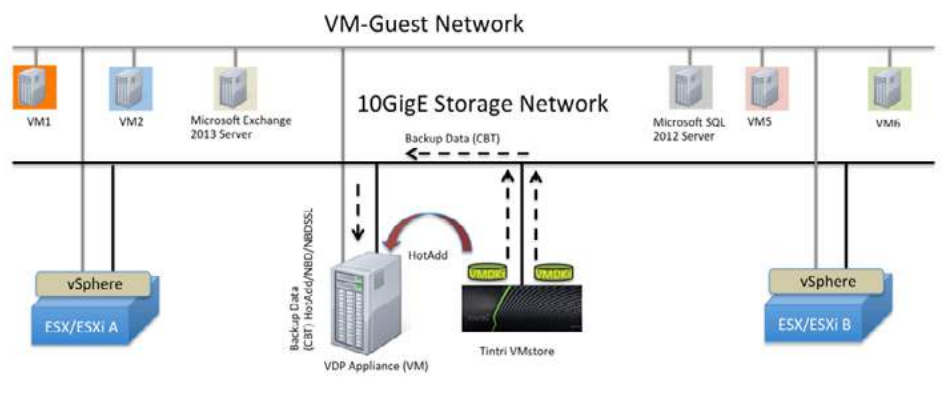
Environment

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 [latest vSphere Data Protection Administration Guide](#) 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 [vSphere Data Protection Administration Guide](#). 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.ttucs.tm.tintri.com
Address: 10.10.10.10
Name: Dom-VDPA.ttucs.tm.tintri.com
Address: 10.10.10.10

PS C:\Users\dcheah> nslookup Dom-VDPA.ttucs.tm.tintri.com
Server: ucsad.ttucs.tm.tintri.com
Address: 10.10.10.10
Name: Dom-VDPA.ttucs.tm.tintri.com
Address: 10.10.10.10

PS C:\Users\dcheah> nslookup 10.10.10.10
Server: ucsad.ttucs.tm.tintri.com
Address: 10.10.10.10
Name: dom-vdpa.ttucs.tm.tintri.com
Address: 10.10.10.10
```

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

Users and Groups		
These users or groups can interact with the vc2.ttucs.tm.tintri.com folder according the assigned role selected to the right.		
User/Group	Role	Propagate
 TTUCS\backup	Administrator	Yes

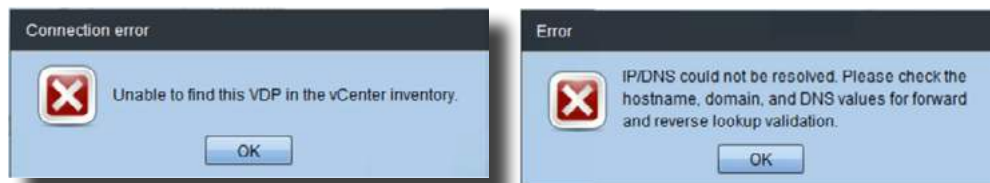
For example, the reference vCenter architecture in this document; uses TTUCS active directory domain for users and groups. If the vCenter credentials are invalid, a Test Connection attempt in the vCenter registration step could fail.



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

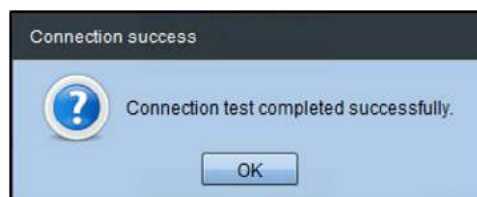
NOTE: The VDP backup user account referenced in this white paper belongs to an Active Directory domain. The backup user is entered in the following format: "System-Domain\user-account" in the vCenter username field.

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.



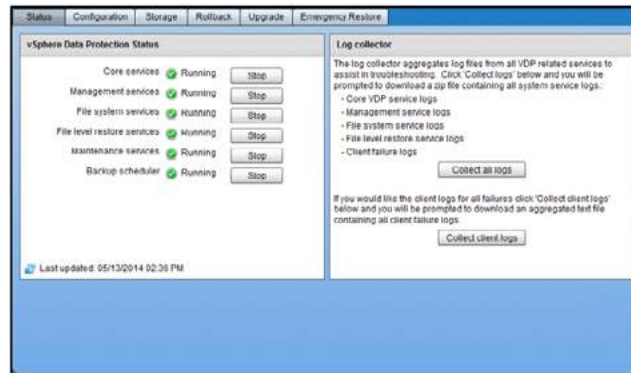
In the *Device Allocation* step of the configuration wizard, select *Provision: Thin* when configuring VDP storage disks on a Tintri VMstore.



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.

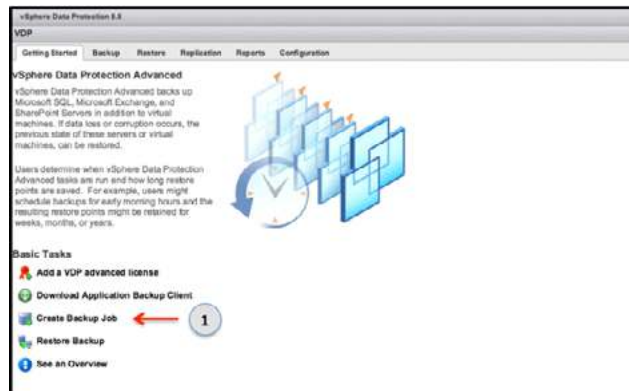
When VDP Advanced is successfully configured, all VDP services should be running.



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.



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.



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 [Backup and Recovery Best Practices](#).

```
2014-05-13T16:39:36.194-7:00 avvchimage Info <9478>: Connected with HotAdd transport to virtual disk [Tintri_T840_A] DCV0012_4CLMG/DOM_FPMSCRTCH.vmdk
2014-05-13T16:39:36.194-7:00 avvchimage Info <00000>: Connecting virtual disk [Tintri_T840_A] DCV0012_4CLMG/DOM_FPMSCRTCH.vmdk
2014-05-13T16:39:36.249-7:00 avvchimage Info <16041>: VDDK:VixDiskLib: VixDiskLib_GetInfo: Disk info.
2014-05-13T16:39:36.249-7:00 avvchimage Info <16041>: VDDK:VixDiskLib: VixDiskLib_FreeInfo: Clean up VixDiskLib.
```

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.

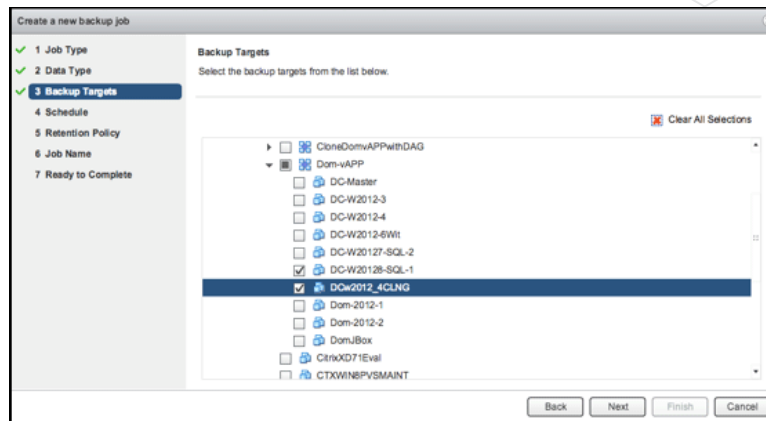
To change VDP Advanced preferred transport, review the following [Changing VMware VDP Transport Methods](#). The new line should consist of the following: `--transport="nbd:nbdssl"` for the particular VDP Advanced appliance. When the preferred transport method is updated and the avagent has been restarted,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

```
2014-04-03T19:32:10.926-7:00 avvchimage Info <9478>: Connected with Nbd transport to virtual disk [Tintri_T840_A] DC-VM-Clone1-1/DC-VM-Clone1-1-000002.vmdk
2014-04-03T19:32:10.926-7:00 avvchimage Info <00000>: Connecting virtual disk [Tintri_T840_A] DC-VM-Clone1-1/DC-VM-Clone1-1-000002.vmdk
2014-04-03T19:32:11.122-7:00 avvchimage Info <16041>: VDDK:VixDiskLib: VixDiskLib_GetInfo: Retrieve disk info.
```

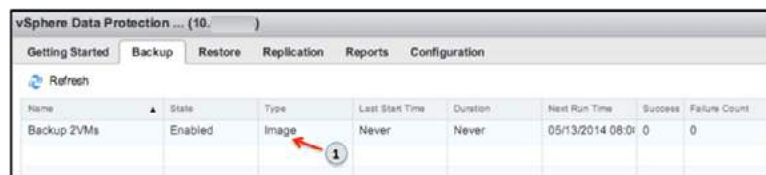
VDP uses VMware's CBT. In addition, VDP also has a very efficient in-line deduplication and compression technology for backups. Subsequent VDP image-based backups using NBD transport will utilize incrementals with CBT after the first initial full. Tintri VMstore deduplication and compression is similar 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.

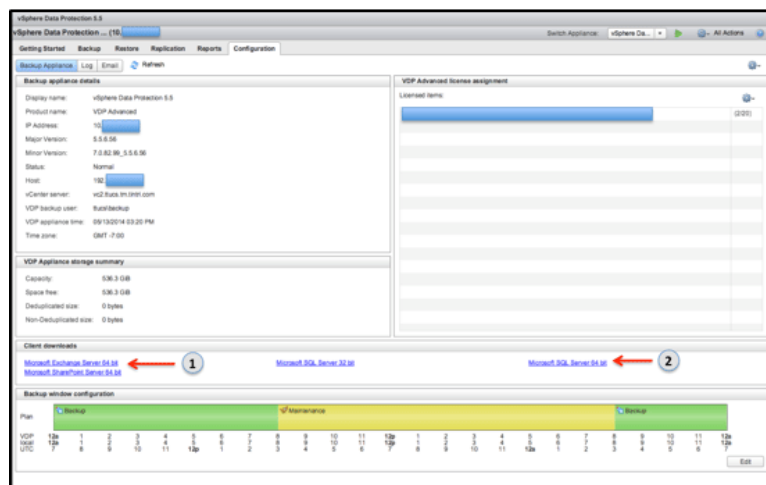


In the *Backup* tab of the vSphere Data Protection pane, an *Image* backup job is created following a successful creation using *Guest Images*. This particular backup job will protect 2 VMs with image-based backups.



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.



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.

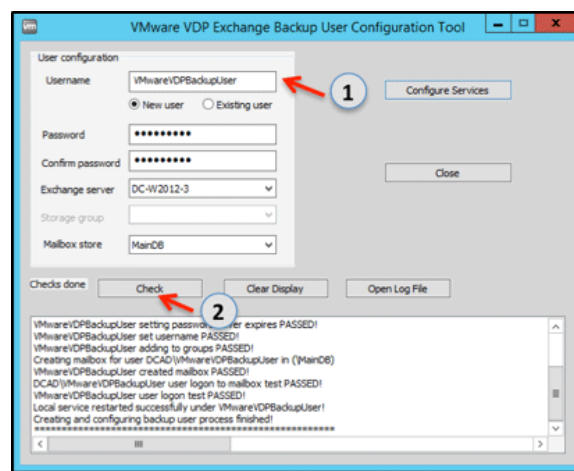
DO: Install the Exchange GLR plug-in only on the server that will be used for granular level recovery. It is not necessary to install the Exchange GLR plug-in on all Exchange servers.



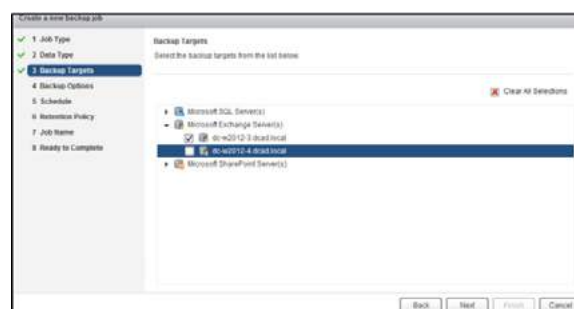
If the VDP appliance is not reachable from the Microsoft application server, your Microsoft application plug-in installation will fail with the following error.

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.



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.

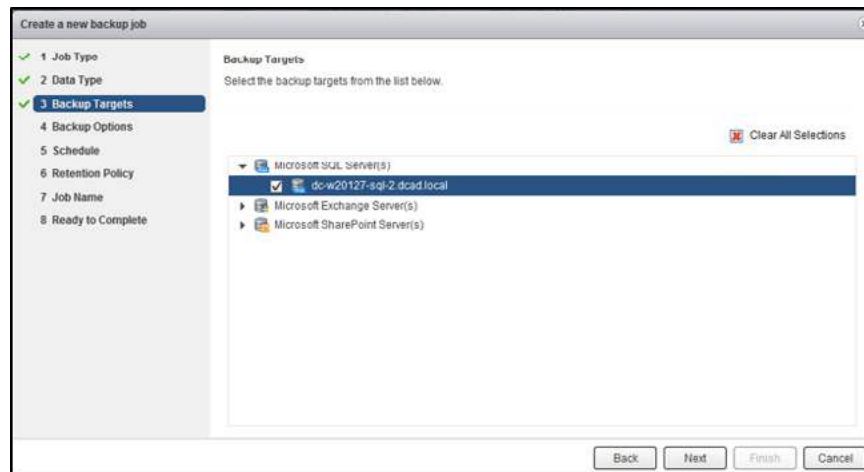


DO: Select only one Microsoft Exchange Server per VDP Advanced Application backup job. This is a VDP Advanced best practice.

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.

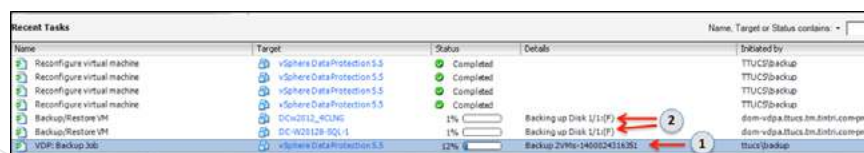
Review the latest [VDP Administration Guide 5.5](#) for supported Microsoft Exchange Servers and Microsoft SQL Servers.



VDP Advanced utilizes EMC Avamar'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.

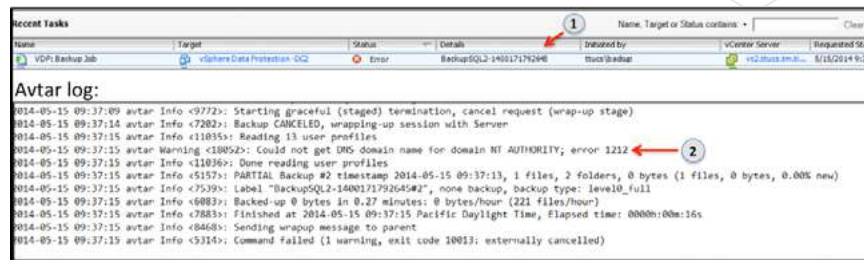
VDP Appliance storage summary	
Capacity:	536.3 GiB
Space free:	423.2 GiB
Deduplicated size:	113.0 GiB
Non-Deduplicated size:	1.2 TiB

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*.

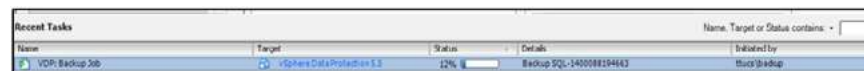


In the following example, a *VDP:Backup Job* with job identifier *BackupSQL2-1400171792645* failed. A VDP Advanced administrator can utilize this information to review the VDP logs, debug, and resolve VDP Advanced backup issue.

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



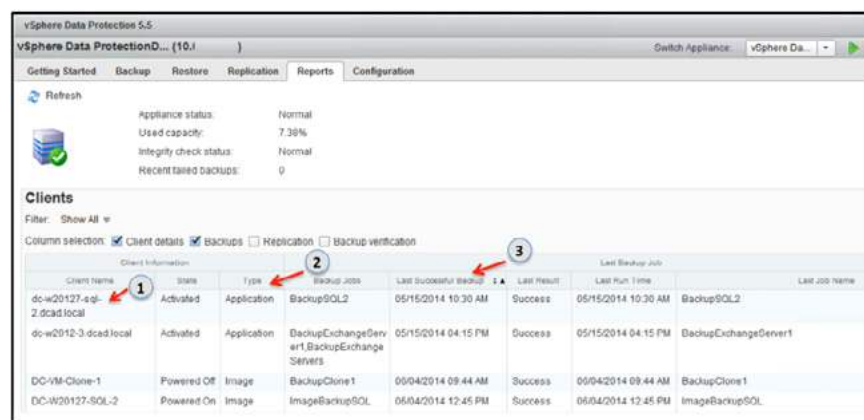
After resolving the NT Authentication error, a new VDP Advanced application backup of the Microsoft SQL 2012 server successfully makes progress and completes the Microsoft application backup.



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.



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.



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.

VM	IOPS	MBps	Latency ms	Provisioned GiB	Used GiB	Change MB/day
vSphere Data Protection	183	29.0	130.9	874	39.7	80,773
MCSLoginVSI-010	0	0.0	0.0	40	0.1	0

Host 127.8 | network 0.2 | storage 2.9 | disk 0.0

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.

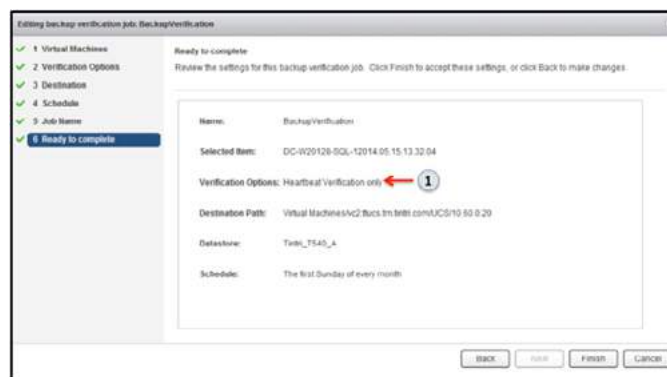
DO: Ensure the ESXi host and the Tintri VMstore is accessible on the network for VDP Advanced.

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.



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.

Name	Target	Status	Details	Initiated by
Backup/Restore VM	VDP_VERIFICATION_DC-W20128-SQ...	42%	Restoring Disk 1(10')	dc-vdp@2.ttucs.tn.tintri.com-prod...
VDP Backup Verification Job	vSphere Data Protection-DC	46%	BackupVerification-1400275328833	ttucs\backup

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.

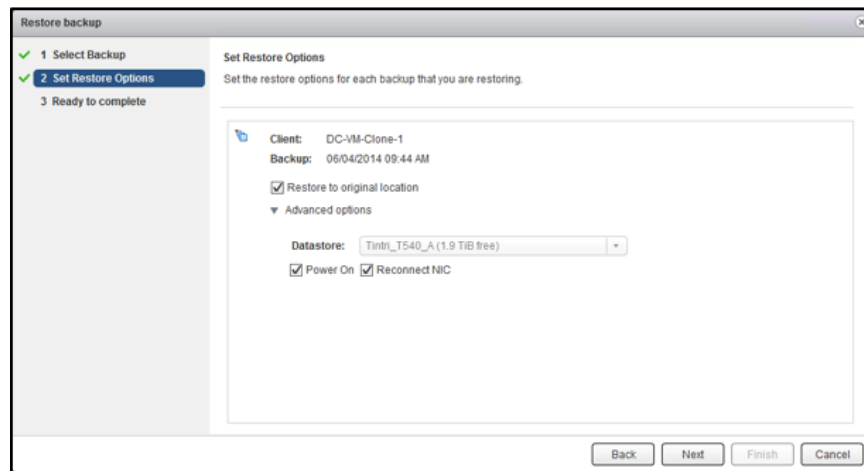
DO: Schedule ABV jobs to run after incremental backups to avoid resource contention. Run an initial incremental backup to determine the backup duration for scheduling ABV jobs.

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.



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.

```
</directives>
<catalog>
  <flag type="integer" pidnum="3016" value="5" name="run after_script_max_in_min" />
  <flag type="integer" pidnum="3016" value="5" name="run before_script_max_in_min" />
  <flag type="boolean" pidnum="3016" value="true" name="utilize_changed_block_list" />
</catalog>
<free-form />
<agent_directives>
  <flag type="string" value="/v02.ttuos.tn.tintri.com/VirtualMachines/DC-VM-Clone-1_UA0biVPrVtMgkhYfrag" name="account" />
  <flag type="string" value="restoreonly" name="id" />
  <flag type="string" value="DC-VDPAS.ttuos.tn.tintri.com" name="server" />
</agent_directives>

2014-04-04T10:14:54.553-7:00 avatar Info <5530> Backup from libar root /v02.ttuos.tn.tintri.com/VirtualMachines/DC-VM-Clone-1_UA0biVPrVtMgkhYfrag
2014-04-04T10:14:54.577-7:00 avatar Info <5530> Backup #1 label "BackupClone1-140189912844" timestamp 2014-04-04 09:14:50 PDT, 5 files, 70.00 GB
2014-04-04T10:14:54.633-7:00 avatar Info <5239> Restoring backup to directory "/usr/local/avamarclient/var-proxy-5/vmware/metadata"
2014-04-04T10:14:54.634-7:00 avatar Info <5240> Restore completed
2014-04-04T10:14:54.634-7:00 avatar Info <7925> Restored 7.337 KB from selection(s) with 7.337 KB in 3 files
2014-04-04T10:14:54.654-7:00 avatar Info <6090> Restored 7.337 KB in 0.01 minutes: 33.04 MB/hour (13,843 files/hour)
2014-04-04T10:14:54.654-7:00 avatar Info <7828> Finished at 2014-04-04 10:14:54 PDT, Elapsed time: 0000h:00m:00s
2014-04-04T10:14:54.694-7:00 avatar Info <8468> Sending wrapup message to parent
2014-04-04T10:14:54.697-7:00 avatar Info <5514> Command completed (exit code 0) success
```

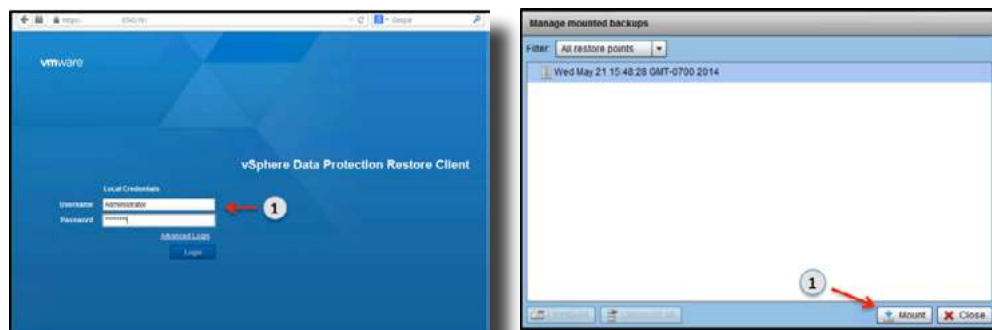
VDP will automatically evaluate the workload to determine the best restore method to achieve the fastest VM image restore time. In a scenario where the change rate is high and CBT overhead would be less efficient for restore, CBT will not be the fastest restore method. VDP will intelligently choose the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

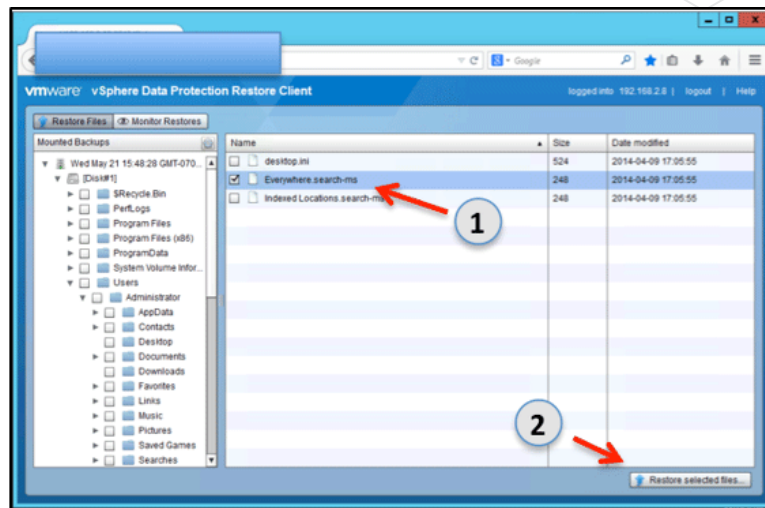
DO: It is a requirement that the VM client has network access to the VDP Restore Client web interface for FLR.

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

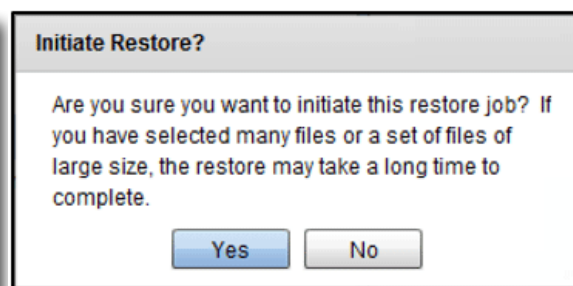
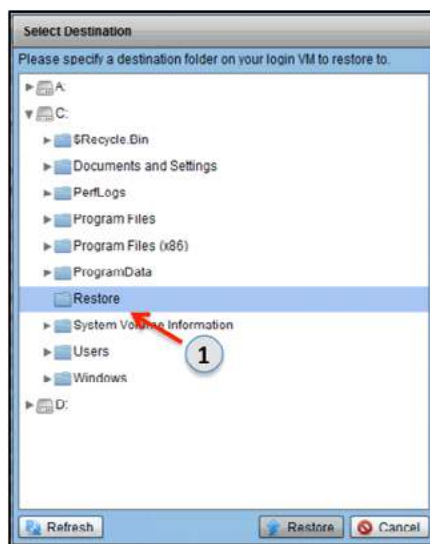


When VDP Advanced log on credentials have been validated and restore points are discovered, mount the required restore point for FLR. The mount and browsing of restore points may temporarily affect a Tintri VMstore latency and flash hit ratio as cold VM data is read from HDD storage.

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.



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.



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.

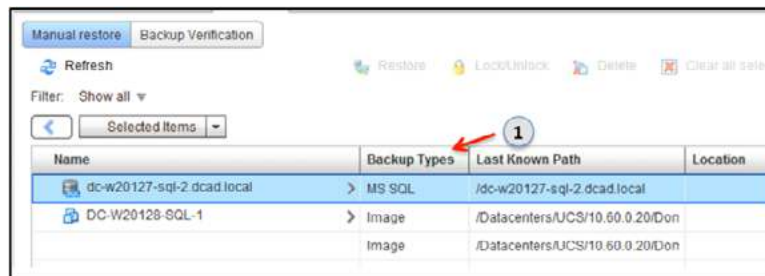
Restore Files Monitor Restores						
Status	Error Code	Client	OS	Start Time	Elapsed Time	End Time
✓ SUCCESS		DC-W2012-8-VDPA	Windows	Wed May 21 16:13:14 GMT-0700 2012	00h:00m:15s	Wed May 21 16:13:29

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.

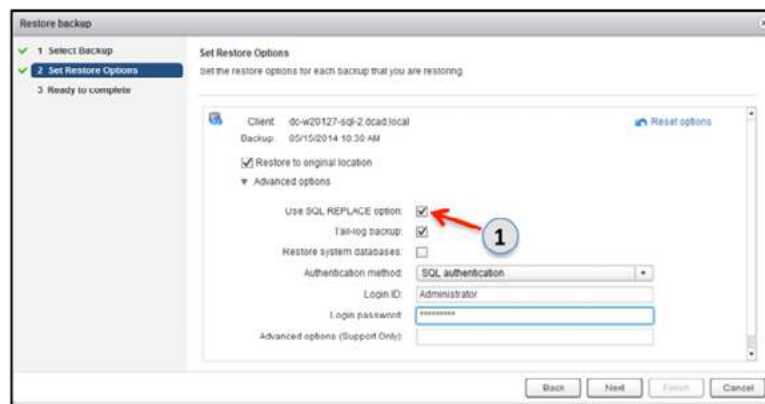
Restoring Microsoft Application Servers

Restoring Microsoft SQL Server Databases

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



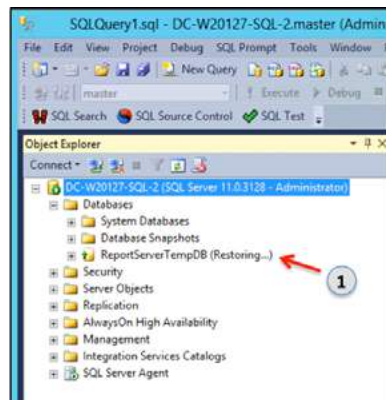
Be aware that selecting *Use SQL REPLACE* option for a Microsoft SQL database restore to original location can result in potential data loss. This is because this option specifies that the database or related file will be created even though another database or file with the same name already exists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



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.



Restoring Microsoft Exchange Server Databases or Individual Mailboxes

VDP Advanced Microsoft Exchange Server restore options allow restores to:

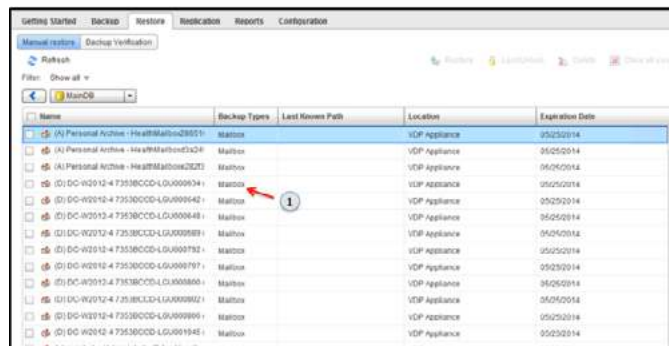
- Original location
- Alternate location
- Restore Storage Groups (RSG for Microsoft Exchange 2007)
- Recovery Databases (RDB for Microsoft Exchange 2010 and Microsoft Exchange 2013)



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 avatar log will also provide detailed information on the Exchange restore job.



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.



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.

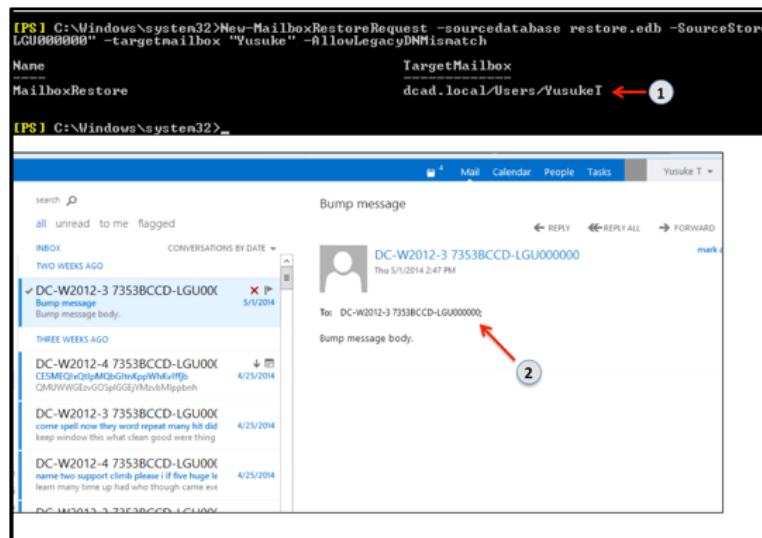


DO: Enable VDP Advanced GLR log files before attempting GLR.

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



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 [VDP Administration Guide 5.5](#) 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.

Create a new replication job

1 Select Clients
2 Backup Selection
3 Destination
4 Schedule
5 Retention
6 Job Name
7 Ready to complete

Destination
Please specify a destination to replicate your backups to:

Hostname or IP: This field is required. 1
Port: 29900
Username: This field is required. 2
Password: This field is required. 3

Verify authentication

Back Next Finish Cancel

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 vSphere Data Protection system provides a mechanism to roll back the backup repository on the appliance to a known and valid state. Rolling back to a checkpoint ensures that all of the backups on or before the checkpoint date are valid. However, any backups that occurred after the checkpoint date will no longer be available in the system.

Checkpoint tag	Date	Valid
cp.20140605160149	06/05/2014 09:01:49 AM, PDT -0700	Validated
cp.20140605161119	06/05/2014 09:11:19 AM, PDT -0700	Not validated

Unlock to enable the rollback operation

Perform VDP rollback to selected checkpoint

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

Getting Started Backup History Replication Reports Configuration

Backup appliance details

Appliance name: vSphere Data Protection VDP Advanced
Product name: VDP Advanced

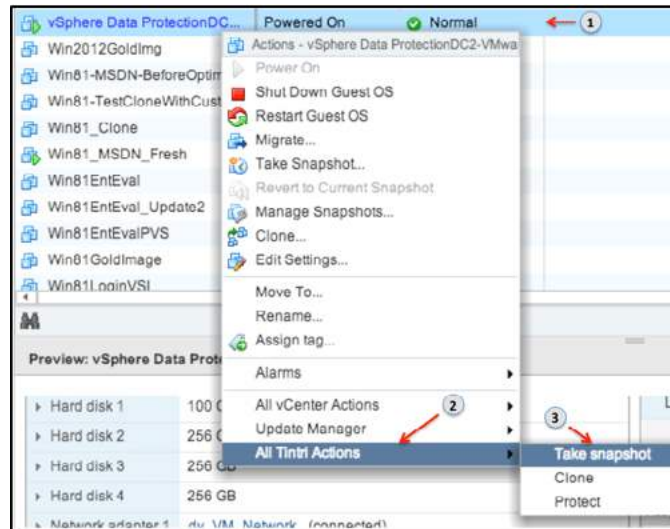
VDP Advanced backup management

Run integrity check

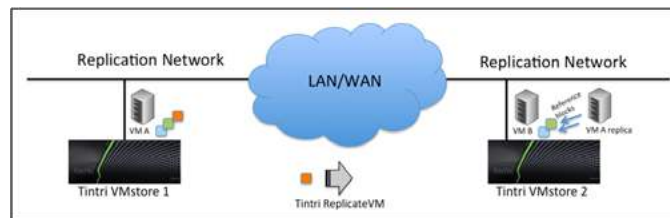
DO NOT: Backup jobs should not be running (scheduled/manual) during a VDP maintenance window. Although backup jobs will run, the resources VDP needs for maintenance tasks will be consumed by the backup jobs. It is a VMware recommendation to reserve a portion of each day for routine VDP maintenance activities.

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 [SnapVM™](#), [CloneVM™](#), and [ReplicateVM™](#) complements VDP Advanced data protection solution to provide protection for your VDP Appliance.

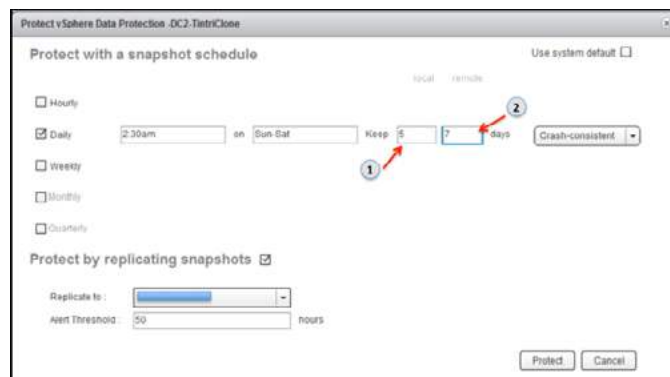
Tintri's SnapVM can be used to protect your VDP Appliance on the local Tintri VMstore and ReplicateVM can be used to protect your VDP Appliance at a remote site. SnapVM snapshot is on a per-VM basis and it is efficient, as it consumes virtually zero disk space.



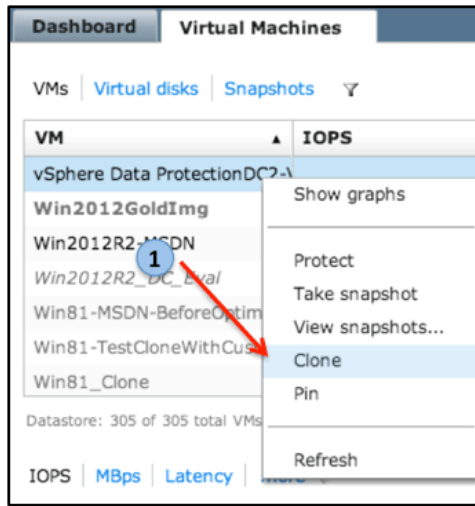
Tintri's replication feature is efficient as it sends only unique data blocks, after in-line deduplication and compression, across LAN/WAN to another Tintri VMstore to provide off-site protection for your VDP appliance.



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.



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.

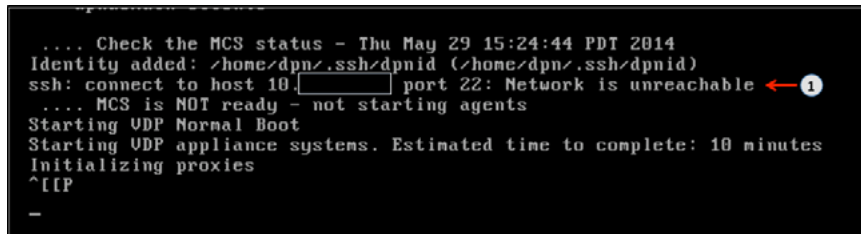


NOTE: Tintri vSphere Web Client Plugin is required to utilize Tintri features from the vSphere Web Client.

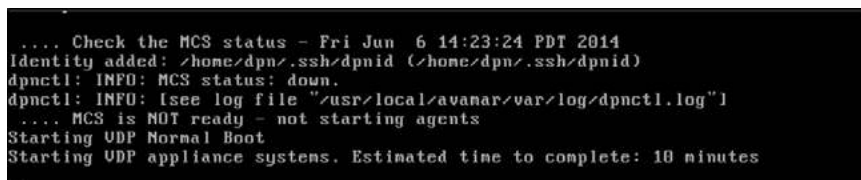
When attempting to power on a cloned VDP appliance (VMware Clone/Tintri CloneVM), be aware that the network MAC address for the cloned VDP Appliance could be changed if the original VDP Appliance still exists.



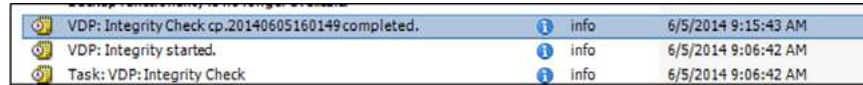
If the VDP Appliance MAC address is changed, the console of the VDP Appliance will reflect that the network is unreachable. If this occurs, VMware's KB solution [VDP Appliance has no network connection after re-registering, cloning, or restoring from backup](#) can be applied to bring the VDP appliance 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.



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.



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

