VMware vSphere

Data Protection 5.5

Automatic Backup Verification (ABV)

TECHNICAL WHITE PAPER

Table of Contents

What is Automatic Backup Verification?

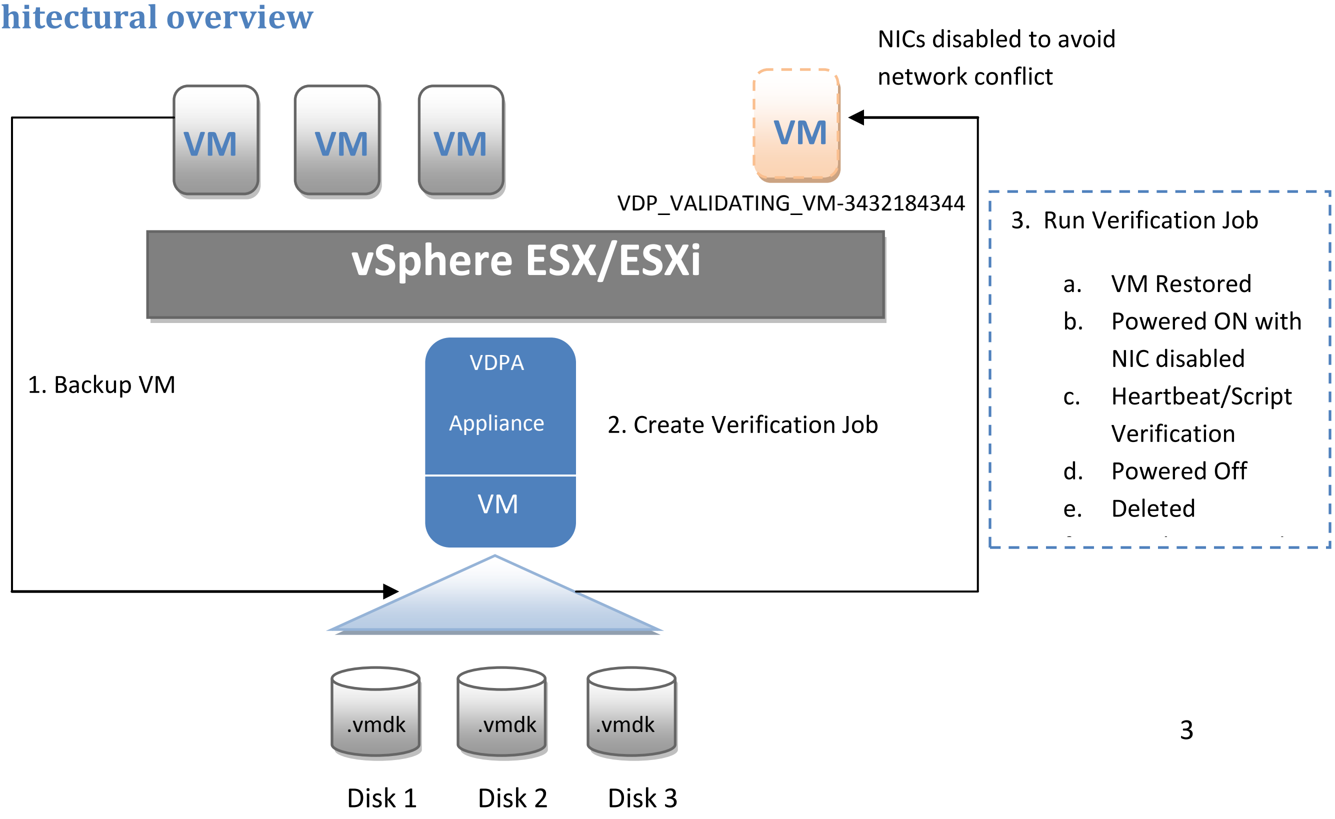
Automatic Backup Verification (ABV) is one of the most desirable features included in the vSphere Data Protection Advanced 5.5 (VDP Advanced) Appliance. ABV provides backup administrators the ability to verify the integrity of the restore points created using the appliance, to perform verification manually on existing backups, or to schedule verification for future backups in sync with the backup schedule.
NOTE: ABV is an advanced feature. You must apply the VDP Advanced license to the host to enable the ABV feature.

Some of the key characteristics and benefits of the ABV feature are as follows:

a. Provides a fast, efficient, and simple way to verify backups of vSphere virtual machines.
b. Verification of virtual machine image backups can be performed on full backups or incremental backups.
c. As a best practice users can create an isolated environment for verification process but that's NOT a prerequisite because the backups are always restored and verified with the virtual machine NIC(s) disabled to avoid any network conflict with production VMs.
d. Provides two levels of verification options:
   - ○ VMware Tools heartbeat, used for simple verification
   - ○ Verification script, used for advanced level of verification

   The verification options are described in later sections of this document.

Architectural overview



The architectural overview, shown above, illustrates the events that occur during a verification job. The following tasks occur during the verification process, regardless of whether the verification job is run manually or is triggered as a part of a schedule.

1. Once a virtual machine (VM) is backed up, a restore point exists that can be verified for its integrity.
2. The backup administrator creates a verification job for the VM on which the backup will be verified.
3. The backup administrator can trigger the verification job at a scheduled time, or can manually run the job at any point of time.
4. The verification job runs the following process:
   a. The backup to be verified will be restored as a temporary VM on a specified host and datastore. The VM in the vCenter inventory is named using the following convention: *" VDP_VALIDATING_<vm name> - <unique number> "*
   b. The restored VM is powered ON. If the VM cannot power ON for any reason, then the verification job will fail with the proper error message and the backup is not verified. The NICs on the restored VMs are disabled in order to avoid any network conflict with production VMs. If Backup files are corrupt then Restored VMs won't even startup.
   c. Once the VM is powered ON and boot up successfully, by default it is checked for a VMware tools heartbeat, which ensures that the VM guest OS booting is successful. Optionally, users can select script verification while creating a verification job to ensure their applications and services are in good health.
   d. The VM powers OFF once verification completes.
   e. The restored VM is deleted automatically from the vCenter inventory to free up all the resources it consumed during verification. If, due to unavoidable circumstances, the VM is NOT deleted, the user must manually delete it.
   f. Results are reported on Tasks/Events pane of vCenter server as Failed or Success, depending on whether or not the backup is verified. If verification job is passed, user should see the backup with timestamp that has been verified and if the result is "Failed" then user should get proper error messages.

Prerequisites

- VDP Advanced must be installed, configured, and properly licensed.
- A backup job or a restore point must exist before you create a verification job for a virtual machine. The backup job must be a full image backup type.
- VMware Tools must be installed on virtual machine(s) at the time of backup. If no VMware Tools are found on the validating VM, the heartbeat verification will fail.
- A user-defined script and Guest credentials are required on the guest OS if the user wishes to choose the Verification Script option.

- Depending upon VM file size and number of VMs those are verified simultaneously, users must have an ESXi host and a datastore with resources available to restore temporary VMs for purpose of verification.

Verifying a Backup

The vSphere Web Client is used to access VDP plug-in and the VDP plug-in is used to create and manage verification jobs, for reporting, and for configuration.

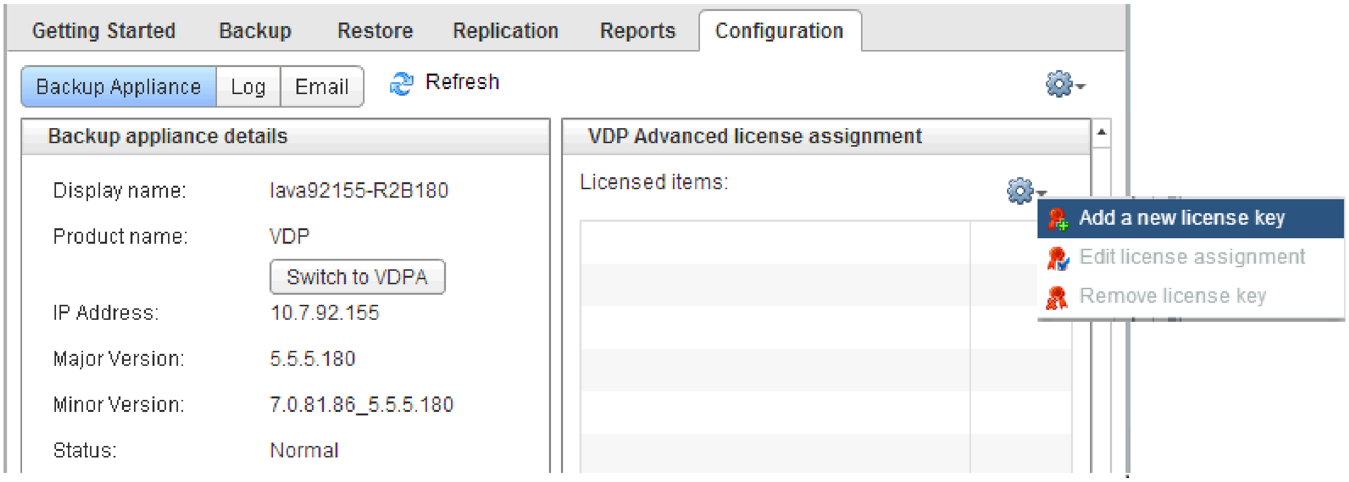
Applying the VDP Advanced license

1. Select the VDP Advanced plug-in from the left pane of the vCenter Web Client.
2. From the VDP user interface, select the Configuration tab (by default you are on the Backup Appliance Details view).
3. Click Add a new license key in the VDP Advanced License Assignment view.

Once the VDP Advanced license is decoded, it can be applied to different hosts depending upon CPU Sockets. For more details on adding VDP Advanced license key, refer to the *vSphere Data Protection 5.5 Administration Guide*.

Switching to VDP Advanced mode

Once the VDP Advanced licenses have been applied to the hosts, you can enable VDP Advanced mode. To enable VDP Advanced mode, go to the Configuration tab of the VDP Advanced plug-in and click the “Switch to VDPA” button under the Backup Appliance Details section.

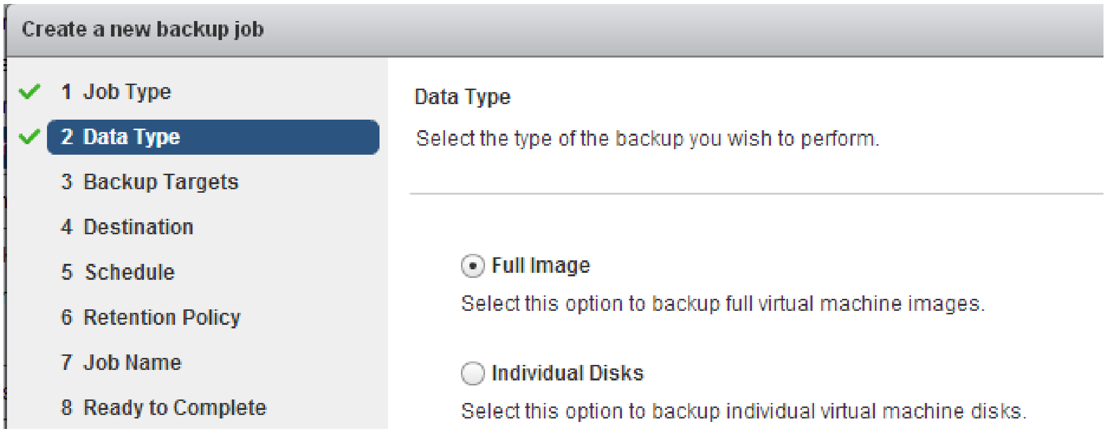


Display name: lava92155-R2B180
Product name: VDP
IP Address: 10.7.92.155
Major Version: 5.5.5.180
Minor Version: 7.0.81.86_5.5.5.180
Status: Normal

Creating a full image backup job

1. Click the Backup tab on the VDP Advanced plug-in.
2. From the Backup Job Actions menu, select **New** to launch the Create new backup job wizard.
3. On the Job Type page, select **Guest Images**.
4. Select **Full Image** as the data type.

For complete details on how to create a backup job, refer to *the vSphere Data Protection 5.5 Administration Guide*.



Create a new backup job

✓ 1 Job Type
✓ 2 Data Type
3 Backup Targets
4 Destination
5 Schedule
6 Retention Policy
7 Job Name
8 Ready to Complete

Data Type

Select the type of the backup you wish to perform.

● Full Image

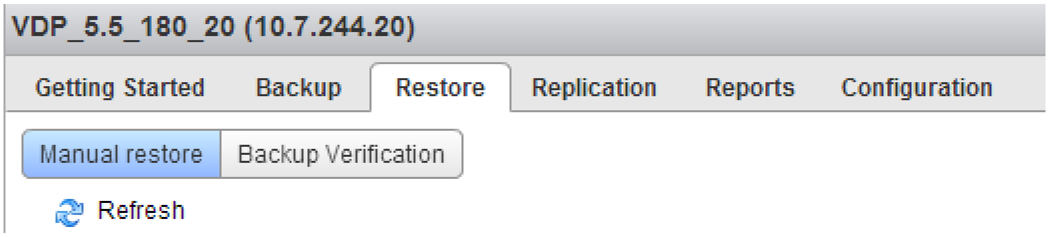
Select this option to backup full virtual machine images.

○ Individual Disks

Select this option to backup individual virtual machine disks.

Creating a backup verification job

Once you have switched to VDP Advanced mode, the Restore tab splits into two logical sections: Manual Restore and Backup Verification.



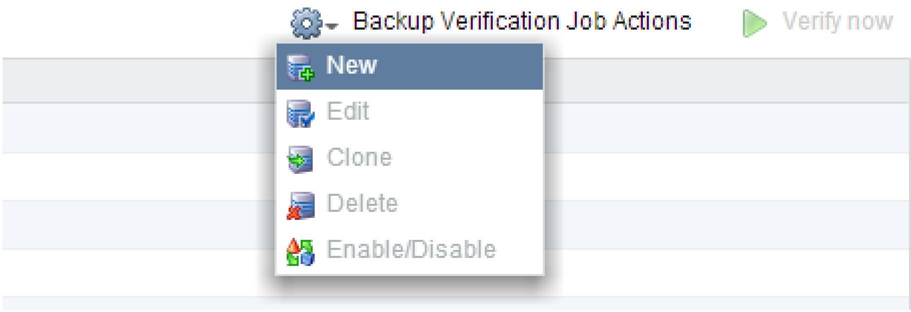
VDP_5.5_180_20 (10.7.244.20)

Getting Started | Backup | Restore | Replication | Reports | Configuration

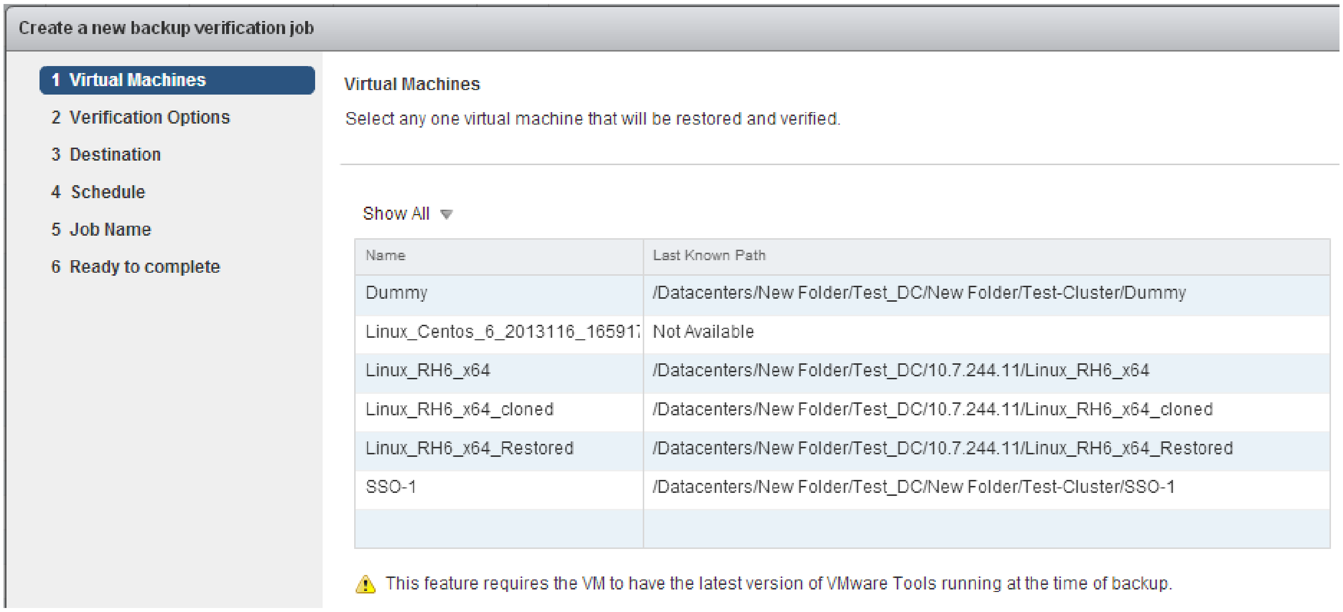
Manual restore | Backup Verification

Refresh

Select the Backup Verification tab and click **New** from the Backup Verification Job Actions menu.



The Create a new backup verification job wizard launches, as shown below.



Create a new backup verification job

1 Virtual Machines
2 Verification Options
3 Destination
4 Schedule
5 Job Name
6 Ready to complete

Virtual Machines

Select any one virtual machine that will be restored and verified.

Show All ▼

Name	Last Known Path
Dummy	/Datacenters/New Folder/Test_DC/New Folder/Test-Cluster/Dummy
Linux_Centos_6_2013116_16591	Not Available
Linux_RH6_x64	/Datacenters/New Folder/Test_DC/10.7.244.11/Linux_RH6_x64
Linux_RH6_x64_cloned	/Datacenters/New Folder/Test_DC/10.7.244.11/Linux_RH6_x64_cloned
Linux_RH6_x64_Restored	/Datacenters/New Folder/Test_DC/10.7.244.11/Linux_RH6_x64_Restored
SSO-1	/Datacenters/New Folder/Test_DC/New Folder/Test-Cluster/SSO-1

⚠ This feature requires the VM to have the latest version of VMware Tools running at the time of backup.

Follow the instructions on each step of the wizard as described below:

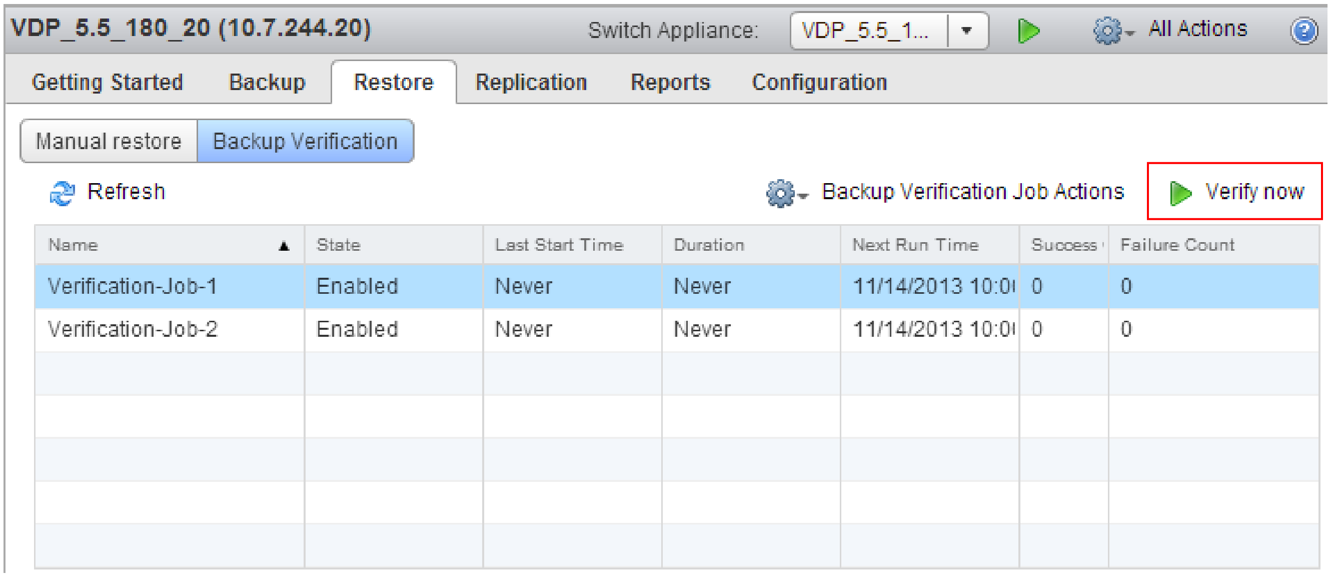
Step-1 (Virtual Machines)	▪ Select a virtual machine (VM) for which you want to create a verification job. ▪ You may select only one VM per verification job. ▪ The VM must be part of a full image backup job or it must have restore points. ▪ VMware Tools must be installed in the protected VM prior to backup. ▪ You have an option to filter VMs by name.
Step-2 (Verification Options)	Heartbeat Verification ▪ This is the default option for verification of a backup regardless of whether you select script verification or not. ▪ Heartbeat Verification checks whether VMware Tools heartbeat has been received within a specific time frame after the VM has powered on. ▪ If the VMware tools heartbeat is received, it is assumed that the guest OS has booted successfully and is in a good state.
Step-2 (Contd.)	Script Verification: ▪ This is the advanced option for verification. Check the Verification Script option if you would like the restored VM to pass custom-level verification. ▪ The script must be predefined and must pre-exist on the backup of a VM. ▪ You must provide the following information to execute the script on the Guest OS: ✓ Username to log in to Guest OS ✓ Password for Guest OS ✓ Confirm password field ✓ Full path and name of the script that pre-exist on Guest OS ▪ The script must exit with exitcode (0) or non-zero values. The test passes if 0 is returned and fails if a non-0 value is returned. ▪ For any script that cannot be run directly, enclose execution of the script inside supported script formats (for example: .bat, .cmd, and .sh).
Step-3 (Destination)	Destination: ▪ Destination Path: You must select a standalone host OR a host inside a cluster as the destination where backups will be restored temporarily for the purpose of verification.

	Note: Resource Pools and vApps are currently not supported as valid destinations. ▪ Datastore: Depending upon the host that is selected, a list of datastores is displayed. You must select one datastore to where the Validating VM will be restored. Make sure the selected datastore has sufficient space available
Step-4 (Schedule)	Verification Schedule: • The Schedule settings determine how often and at what time of the day your verification job will run. • Backup Verification Schedule: You can set up daily, weekly, or monthly schedules to run the verification job. • Start Time on Server: This value specifies the time that the verification job will run on the scheduled day.
Step-5 (Job Name)	Name: ▪ Enter a unique name to identify the verification job you are creating. ▪ All alphabet characters and numbers are allowed in the name. ▪ The only special characters allowed are spaces, underscores, hyphens and periods. ▪ Cannot use same name as already used to identify replication job.
Step-6 (Ready to Complete)	▪ Review the backup verification job summary for accuracy. You can click the Back button to correct any selections made on previous steps. ▪ Take note of any warning messages. ▪ If all the selections appear to be correct, click Finish to close the wizard. Note: You can review and execute the backup verification job from the Backup Verification section of the Restore tab.

Completed verification jobs appear on the table under the Backup Verification tab. From here, you can run, edit, clone, disable, and delete verification jobs.

Running a backup verification job

Once you have created a backup verification job, you can invoke verification using on demand verification or by waiting for the schedule to trigger the backup verification job. To run an on demand verification job, select the job from backup verification job and click Verify Now, as shown in the image below.



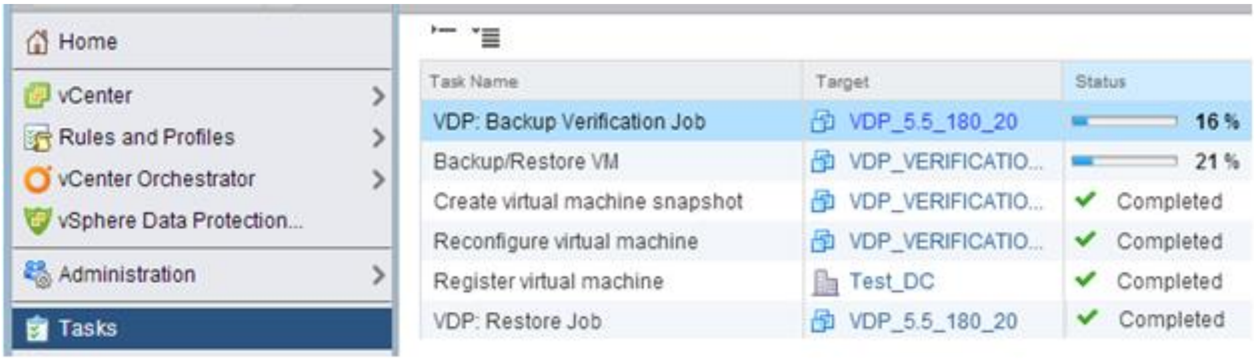
Name	State	Last Start Time	Duration	Next Run Time	Success	Failure Count
Verification-Job-1	Enabled	Never	Never	11/14/2013 10:0	0	0
Verification-Job-2	Enabled	Never	Never	11/14/2013 10:0	0	0

Regardless of whether or not a verification job is run on-demand, the job always triggers on a scheduled time.   Schedule the verification job in sync with backup jobs to ensure that the backups are created as part of a scheduled backup job.

ABV Reporting

You can use any of the methods below to monitor running or completed verification jobs:

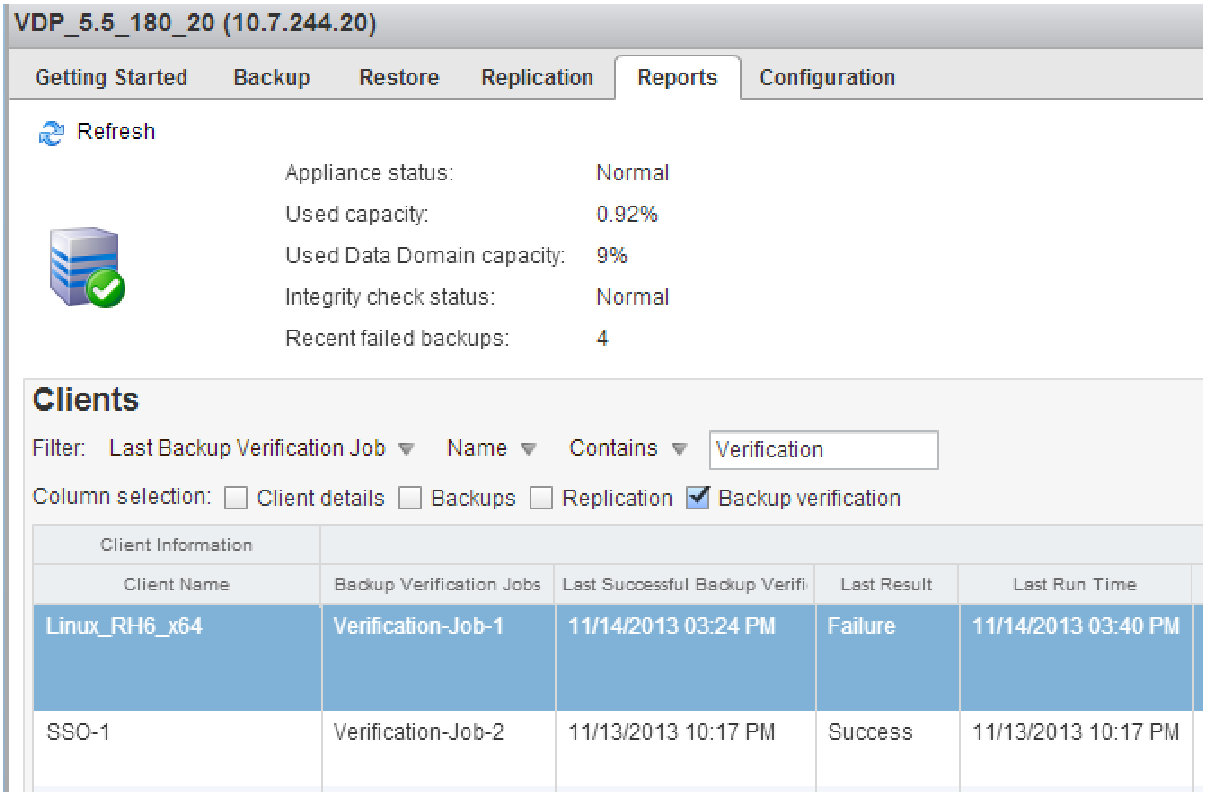
- vCenter Tasks and Events: You can track the progress of a running verification job and the status of recently completed jobs from vCenter Tasks and Events, as shown below:



Task Name	Target	Status
VDP: Backup Verification Job	VDP_5.5_180_20	16 %
Backup/Restore VM	VDP_VERIFICATIO...	21 %
Create virtual machine snapshot	VDP_VERIFICATIO...	✓ Completed
Reconfigure virtual machine	VDP_VERIFICATIO...	✓ Completed
Register virtual machine	Test_DC	✓ Completed
VDP: Restore Job	VDP_5.5_180_20	✓ Completed

Only the last, successful backup for any VM is verified. The verified backup is reported with a timestamp in the Job Completion summary.

- Reports Tab: You can select a virtual machine from the Reports tab of VDP plug-in, as shown below. For more information on the Reports tab, refer to the vSphere *Data Protection 5.5 Administration Guide*.



VDP_5.5_180_20 (10.7.244.20)

Appliance status: Normal
Used capacity: 0.92%
Used Data Domain capacity: 9%
Integrity check status: Normal
Recent failed backups: 4

Clients

Filter: Last Backup Verification Job ▾ Name ▾ Contains ▾ Verification

Column selection: □ Client details □ Backups □ Replication ☑ Backup verification

Client Information				
Client Name	Backup Verification Jobs	Last Successful Backup Verifi	Last Result	Last Run Time
Linux_RH6_x64	Verification-Job-1	11/14/2013 03:24 PM	Failure	11/14/2013 03:40 PM
SSO-1	Verification-Job-2	11/13/2013 10:17 PM	Success	11/13/2013 10:17 PM

- Email Reporting: Alternatively, you can configure for email reports and the appliance will send an email with the jobs summary at the scheduled time.
- Client logs. You can download client logs from https://<*IP address or hostname of VDP*>:8543/vdp-configure.

Best Practices and Recommendations

Timing and resource conflicts

You can take steps to avoid timing and resource conflicts when using the backup verification feature.

- When you first install VDP Advanced, run initial full backups.
- Determine how long it takes for the backups to run, and schedule backup verification jobs to run after the backups have completed. Ideal time difference between scheduling two jobs should be more than the average time it takes to backup the VM.

- As a best practice, schedule verification jobs in co-ordination with backup jobs. For example, if a backup job is scheduled to run daily at 8:00 pm, you can schedule the verification job to run anytime after 8:00 pm, depending on how much data is to be backed up. This ensures that every time a backup is taken; there's a verification job following a backup job that ensures its recoverability.
- Backup jobs go into a queue until a running verification job completes; therefore, you should schedule the verification job in coordination with other jobs. This will also ensure that VDP appliance resources are NOT overloaded with all the jobs running at the same time.

Selecting the destination

Consider the following recommendations while selecting the destination:

- Load balance if multiple verification jobs are to be run at the same time. It is recommended you limit the number of jobs to six if they are run simultaneously.
- Make sure there are sufficient resources available on the host and the datastore where the temporary VM will be restored. Users should load balance jobs among different hosts or it may impact the performance of production VM's during the verification process if host doesn't have sufficient resources.
- If possible, select a datastore that is also shared by the host where the VDPA appliance VM is registered. This will enable the use of hot-add transport mode to restore and verify a backup. Hot-Add transport mode is considered to be faster than network mode of data transfer.
- As a best practice, for Users who do NOT want validating_VMs to interfere with normal production environment, they can alternatively create an isolated environment where hosts and datastores may be reserved for Verification process.

General

- Verify VMware Tools are installed on the VM at the time the VM is backed up. If VMware Tools are not found on the backup after it has been restored, users should see proper error message as "*VDP: Failure heartbeat verification. Either there is no VMtools installed or backup is a non-bootable Virtual Machine*"
- Even if VMware Tools are installed and still user sees error message above, it could be because VM failed to boot properly and backup may NOT be considered in good state.
- Set the heartbeat timeout interval to its optimal value, depending on the environment. Note that some VMs may take longer to send and receive the VMware Tools heartbeat than others. In case appliance fails to detect heartbeat because it is taking long time to boot, it will still be reported as failure.
- Periodically verify the availability of the destination host and a datastore. Edit the job and reconfigure the destination if needed. If the destination host or datastore is unavailable, edit the job and choose a new destination. Most common error message that user will get in case of destination unavailability is "*Failed to create VM*"

- If you plan to create a backup user account, refer to the *vSphere Data Protection Advanced 5.5 Administration Guide* to go through all new permissions that have been added to the VDP role.
- If you plan to use a *verification script*, supported script formats are .bat, .cmd, .sh, and .exe. A valid script file is a file that runs simply by double-clicking it in the file manager or Explorer view. If the script is an unsupported format, you must enclose the execution of the script inside a supported format. For example, a Windows Power Shell (.ps1) script cannot be called and run directly using VDP Advanced, because the .ps format is not supported. You can, however, call the .ps script through a supported format (such as .bat), and then specify the full path to the location of the script on the guest OS. Make sure to set the execution policy to **Unrestricted** before you run the script. The script must exit with exitcode (0) or non-0 integer. If 0 is returned, the script verification succeeded. If a non-0 value is returned, the script verification failed.
- The Verification script should already exist on the backup and should not depend upon connecting to other VMs, because validating VMs are always restored with the NICs disabled.

Limitations

There are certain limitations to the ABV feature, as described below:

What cannot be verified?

- Backups that are not taken using the VDP Appliance.
- Replicated backups on a Target VDP Advanced appliance.
- Application or Application Database backups.
- Backups of individual disks cannot be verified.
- If VDP disks have been imported from an existing appliance, preexisting backups on the imported disks cannot be verified.
- Backups taken with RDM/independent disk attached to VMs cannot be verified.

General limitations

- If a selected destination host or datastore is changed, you must edit the job to select the destination again. VDP Advanced does not track migrated hosts or changed datastore names.
- There may be instances where the VDP Advanced Appliance fails to automatically delete the validating VM (for example, if a VDP Advanced Appliance loses connection to the vCenter or when relevant appliance services are stopped during verification). In these situations, you can manually delete the VM from the disk to clean up the environment.
- Resource pools and vApps cannot be selected as destinations to restore temporary validating VMs.
- ESX and ESXi hosts prior to version 5.0 are not supported as destination hosts to where temporary VMs will be restored.
- Perl Scripts are NOT supported for custom level verification.
- Verification Job cannot be created with the same name that has already been used to identify replication job on the same appliance.

For more information about limitations related to the ABV feature, refer to *the vSphere Data Protection 5.5.5 Release 1 Release Notes*.

Summary

Automatic Backup Verification (ABV) is a key feature introduced in vSphere Data Protection Advanced, version 5.5. ABV provides peace of mind to backup administrators by ensuring that backups taken are restorable. Once VDP is switched to advanced mode, you can access this simple-to-use feature from the Restore tab of the VDP plug-in. This paper discussed overview, basic administration, best practices, and limitations of the ABV feature.