PARAGON
VM BACKUP

User Manual

Paragon Software GmbH
Systemprogrammierung
Leo-Wohleb-Straße 8
79098 Freiburg, Germany

Tel. +49 (0) 761 59018201
Fax +49 (0) 761 59018130
Web www.paragon-software.com
E-Mail sales@paragon-software.com

Table of Contents

About this Guide

The purpose of this document is to provide information about key benefits, installation and main user scenarios of Paragon VM BACKUP. It targets anyone who wants to use this product, primarily backup administrators who deal with VMware virtual infrastructure and IT consultants.

Revision History

Revision	Date	Changes
0.2	2018/02/14	GUI changes, new functions

As we continuously update and improve the product, live product screens may not match the screenshots contained in this document, despite the best effort to keep the document consistent with the product outlook.

About the Product

Paragon VM BACKUP is an easy-to-use backup and replication solution for virtual environments hosted by VMware vSphere or standalone ESX(i) servers. Paragon VM BACKUP operates at the virtualization layer, directly employing the VMware snapshot mechanism, this way it does not need to inject a backup agent to each target virtual machine to create consistent point-in-time VM copies. This approach significantly enhances the backup performance, while minimizing the load on target machines and the hypervisor during the process.

Paragon VM BACKUP is optimized for regular backup routines: a flexible backup scheduler, redundant data exclusion filters, highly compressed backup containers, smart incremental imaging and Paragon Image Transfer Engine strengthened by data retention options allows keeping backup data precisely up to date with minimal effort and backup storage footprint.

Paragon VM BACKUP is complemented with the VM replication capabilities to efficiently protect high-availability environments. Since VM replicas or clones are stored uncompressed in their native format on ESX datastore, they are ready-to-go at any moment, providing the best RTO (Recovery Time Objective).

Paragon VM BACKUP allows you to back up MS Exchange and MS Active Directory virtual servers at application-level. Database consistency is achieved by taking special snapshots when transaction logs are truncated automatically either at the moment of creating a snapshot or after the backup process is over (recommended).

Paragon VM BACKUP includes several methods that let you test recoverability of backup data: backup integrity validation, launch backup, and replica test failover options. The last two allow “live” verification by non-disruptively simulating recovery procedure in an isolated network environment to check viability of a certain restore point or do field test for an existing recovery plan.

Several restore options are available for you to rule out an emergency situation as quickly as possible from retrieval of individual files, granular recovery of specific Exchange or Active directory items, complete VM restore, failover to a VM replica to running a VM directly from backup.

In this guide you will find the answers to many of the technical questions, which might arise while using Paragon VM BACKUP.

Getting Started

Before you install Paragon VM BACKUP, please make sure that the virtual infrastructure and machines you are going to use as backup targets and for installing product components meet product hardware and system requirements.

Platform Support

Paragon VM BACKUP supports the following VMware virtual configurations:

Hypervisors	• VMware® vSphere® 6.0, 6.5, 6.7, 7.0, 8.0 • VMware ESXi™ 6.x – 8.0 Note: VMware fault-tolerant configurations are not supported Note: Non-commercial VMware ESXi is not supported because snapshotting and some other VMware technologies utilized by Paragon VM BACKUP are disabled
Guest Machines	- All guest operating systems supported by VMware - All types and versions of virtual hardware are supported Note: VMware Tools and all latest OS patches are recommended
Privileges	To do backup, restore, and other tasks on guest machines, Paragon VM BACKUP may require up to 50 different privileges. You can granularly configure necessary permissions for one or several users, or simply use an administrative account of the datacenter you're going to manage + add it the 'Global.Licenses' privilege (see Appendix)

System Requirements

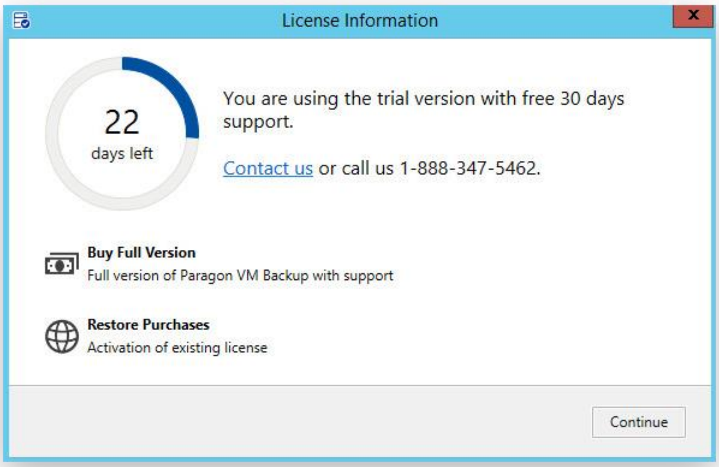
You need a Windows machine to install Paragon VM BACKUP:

Hardware	• CPU: x86 64 bit processor (minimum 2 cores / 4 cores and more recommended) • Memory: 2GB or higher • Disk Space: 1 GB for Paragon VM BACKUP and 4.5 GB for Microsoft .NET Framework 4.6.1 • Network: 1 Gbps or faster is recommended
Operating System	• Windows 7 SP1, 8, 8.1, 10 64 bit • Windows Server 2008 R2, 2012 R1/R2, 2016
Software	Microsoft .NET Framework 4.6.1. If you don't have it installed, you will be prompted to install it during setup
Environment	Active Directory domain or Workgroup
Credentials	Credentials of a domain administrator that joins the 'local admins' group or a local administrator

Licensing and Evaluation

Paragon VM BACKUP is distributed as a 30-day fully functional evaluation version, available for download from the corporate website. During this period, you're also entitled to unconditional technical support.

You can always buy the product online by following the corresponding link or activate a valid license in a dialog shown on program start. This dialog is also available in **Home > Licensing**.



You are using the trial version with free 30 days support.

Contact us or call us 1-888-347-5462.

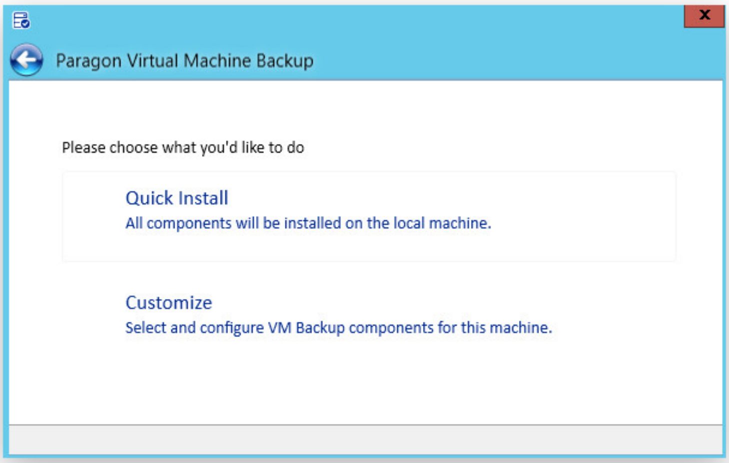
Buy Full Version
Full version of Paragon VM Backup with support

Restore Purchases
Activation of existing license

Installation

Before the installation, please make sure the systems requirements are met.

Paragon VM BACKUP includes two installation modes that correspond to simple and distributed deployment scenarios. The choice depends on your production environment and needs.



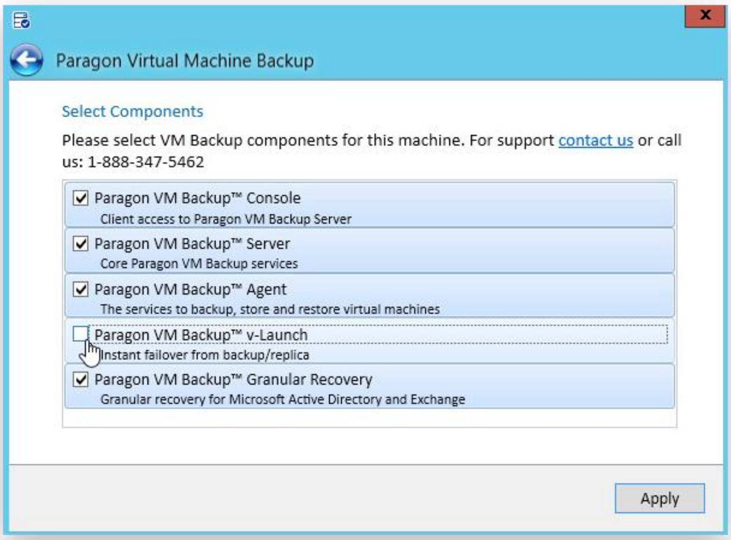
Paragon Virtual Machine Backup

Please choose what you'd like to do

Quick Install
All components will be installed on the local machine.

Customize
Select and configure VM Backup components for this machine.

The simple deployment scenario is recommended for simplified VMware configurations and for evaluation purposes, while distributed backup infrastructure allows better administration, more efficient utilization of resources, and higher performance.



Paragon Virtual Machine Backup

Select Components

Please select VM Backup components for this machine. For support contact us or call us: 1-888-347-5462

☑ Paragon VM Backup™ Console
Client access to Paragon VM Backup Server

☑ Paragon VM Backup™ Server
Core Paragon VM Backup services

☑ Paragon VM Backup™ Agent
The services to backup, store and restore virtual machines

□ Paragon VM Backup™ v-Launch
Instant failover from backup/replica

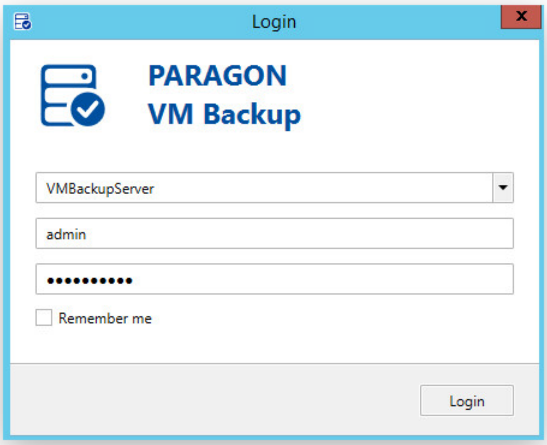
☑ Paragon VM Backup™ Granular Recovery
Granular recovery for Microsoft Active Directory and Exchange

Please note that:

- The maximum backup performance is achieved when VM BACKUP AGENT is located as close to datastores containing backup targets as possible. Obviously, when having to protect guest machines from several ESX hosts, this requirement cannot be complied with via one access point. This problem is addressed by allowing installation of as many backup agents as necessary. The system then automatically chooses one of the agents as primary to delegate it the management role.
- Having an auxiliary VM BACKUP SERVER on a machine from another ESX host allows storing replica machines directly on that host.
- Granular restore scenarios become available when VM BACKUP CONSOLE is installed on the machine to which the local backup storage is attached.
- An additional VM BACKUP CONSOLE on a laptop opens up the possibility to administer the backup infrastructure from any place.

Accessing Console

VM BACKUP CONSOLE connects to the localhost automatically on program start if the simple deployment scenario was the choice. For distributed scenarios, you may need to provide a DNS name (IP address) and credentials of a domain or local administrator of a machine that hosts VM BACKUP SERVER.



Login

VMBackupServer

admin

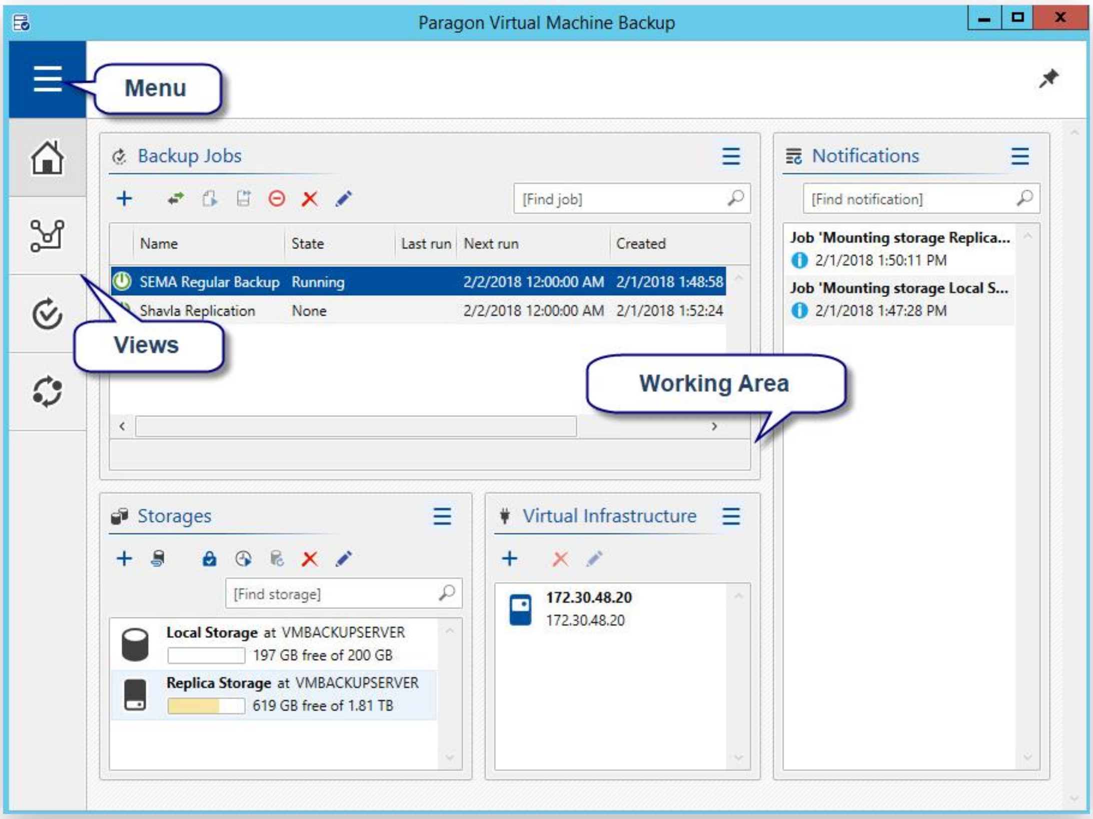
•••••••••••

□ Remember me

Product Interface

Paragon VM BACKUP is designed to let you quickly set up the backup infrastructure, configure backup tasks, monitor current activities, perform restore and other operations.

- **Menu**
- **Views**
- **Working Area**



Name	State	Last run	Next run	Created
SEMA Regular Backup	Running		2/2/2018 12:00:00 AM	2/1/2018 1:48:58
Shavla Replication	None		2/2/2018 12:00:00 AM	2/1/2018 1:52:24

Job 'Mounting storage Replica...
2/1/2018 1:50:11 PM

Job 'Mounting storage Local S...
2/1/2018 1:47:28 PM

Local Storage at VMBACKUPSERVER
197 GB free of 200 GB

Replica Storage at VMBACKUPSERVER
619 GB free of 1.81 TB

172.30.48.20
172.30.48.20

Menu

From the menu you can edit the general application settings, view and collect program logs, connect to another VM BACKUP SERVER, manage your product licenses, and open this manual.

Find more details in:

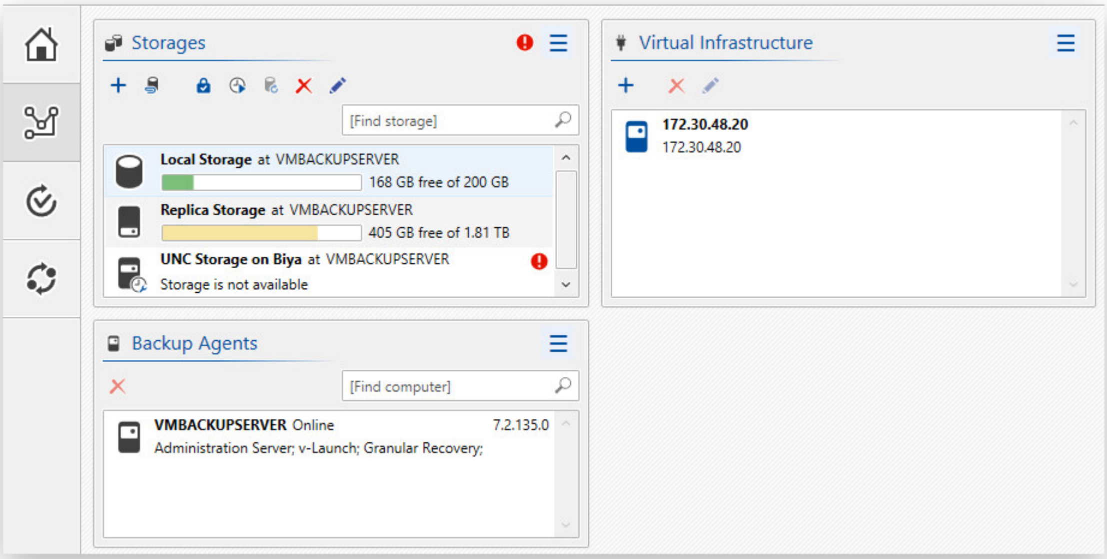
- **Licensing and Evaluation**
- **Configuring E-mail Notifications**
- **Troubleshooting**

Views

Paragon VM BACKUP shows items in several views. Contents of the currently active view is displayed in the working area. You can resize and move views to adjust your environment.

- The **Home** view is displayed on program start. It's good for managing backup and replication jobs, backup storages and virtual server connections, and provides statistics on recently performed tasks.
- The **Environment** view displays detailed information on backup infrastructure members: storages, virtual server connections, and all machines that have installed product components (relevant for distributed deployment scenarios). Use this view to configure new storages, attach already existing

storages from another VM BACKUP infrastructure, check backup data integrity, and free up storage space by getting rid of obsolete restore points.



Local Storage at VMBACKUPSERVER
168 GB free of 200 GB

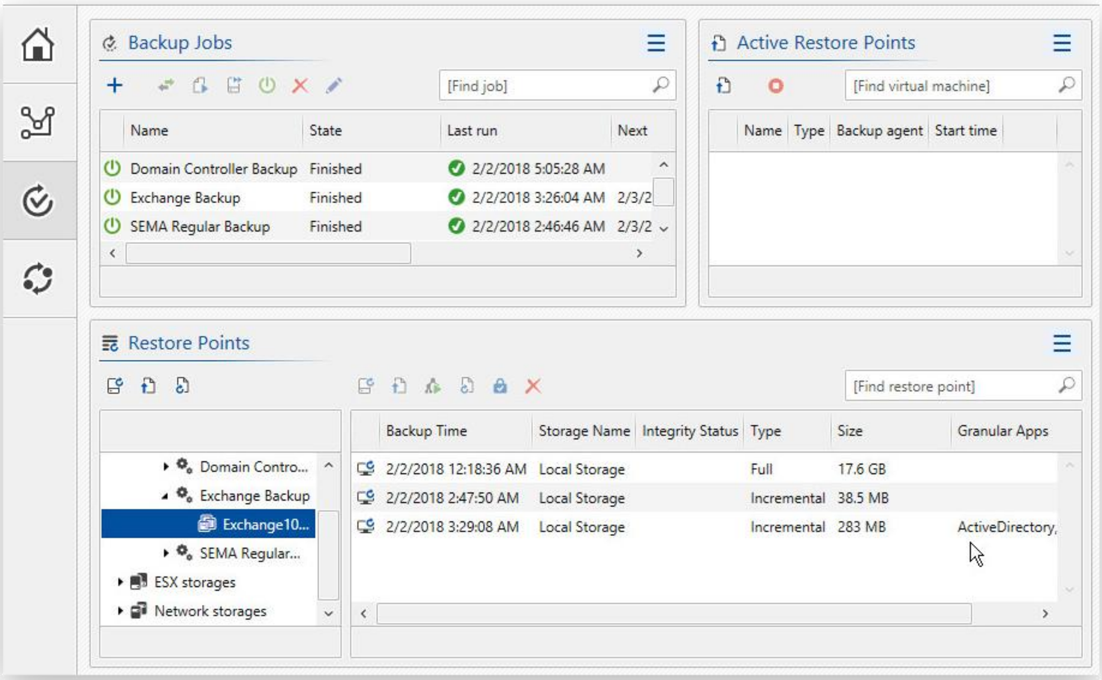
Replica Storage at VMBACKUPSERVER
405 GB free of 1.81 TB

UNC Storage on Biya at VMBACKUPSERVER
Storage is not available

172.30.48.20
172.30.48.20

VMBACKUPSERVER Online 7.2.135.0
Administration Server; v-Launch; Granular Recovery;

- The **Backups** view displays detailed information on backup data: storages where specific backup targets are resided, existing backups chains with restore point properties, and currently active restore points (being launched, failed over, etc.). Use this view for restoring virtual machines, retrieving individual files from backup, launching VM from backup, and running replica failover or test failover operations.



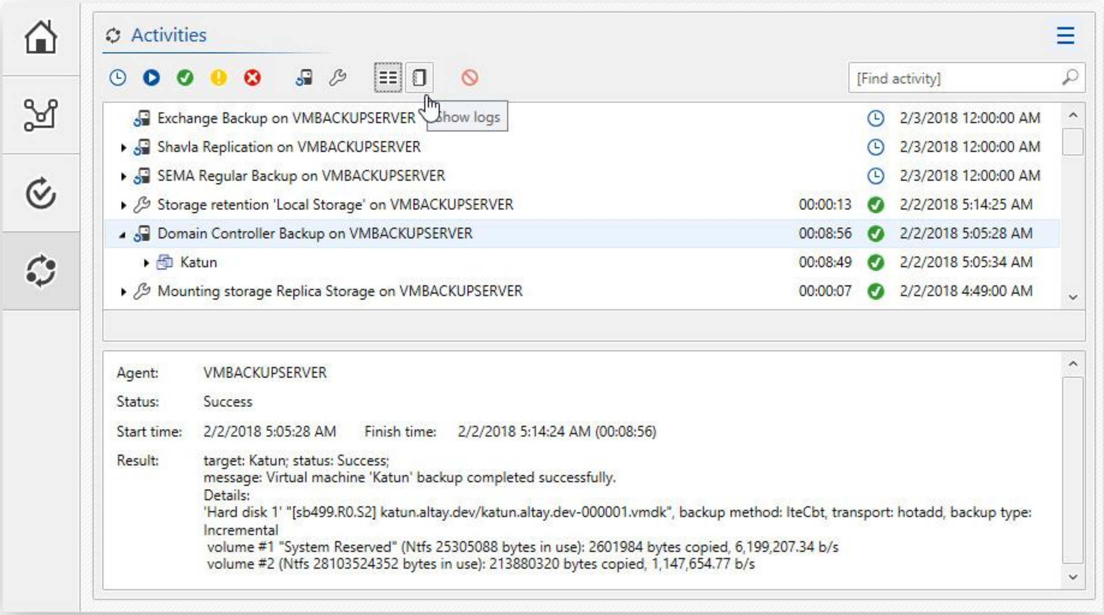
Name	State	Last run	Next
Domain Controller Backup	Finished	✓ 2/2/2018 5:05:28 AM	
Exchange Backup	Finished	✓ 2/2/2018 3:26:04 AM	2/3/2
SEMA Regular Backup	Finished	✓ 2/2/2018 2:46:46 AM	2/3/2

Name	Type	Backup agent	Start time

Domain Contro...
Exchange Backup
Exchange10...
SEMA Regular...
ESX storages
Network storages

Backup Time	Storage Name	Integrity Status	Type	Size	Granular Apps
2/2/2018 12:18:36 AM	Local Storage		Full	17.6 GB	
2/2/2018 2:47:50 AM	Local Storage		Incremental	38.5 MB	
2/2/2018 3:29:08 AM	Local Storage		Incremental	283 MB	ActiveDirectory,

- The **Activities** view displays detailed information on running, scheduled and already accomplished operations, including auxiliary service tasks created automatically by the main service, e.g. storage retention. You can filter activities by time, specific computers, selected jobs, and so on. Use the corresponding buttons to drill down to details, and check logs.



Exchange Backup on VMBACKUPSERVER		◷	2/3/2018 12:00:00 AM
Shavla Replication on VMBACKUPSERVER		◷	2/3/2018 12:00:00 AM
SEMA Regular Backup on VMBACKUPSERVER		◷	2/3/2018 12:00:00 AM
Storage retention 'Local Storage' on VMBACKUPSERVER	00:00:13	✓	2/2/2018 5:14:25 AM
Domain Controller Backup on VMBACKUPSERVER	00:08:56	✓	2/2/2018 5:05:28 AM
Katun	00:08:49	✓	2/2/2018 5:05:34 AM
Mounting storage Replica Storage on VMBACKUPSERVER	00:00:07	✓	2/2/2018 4:49:00 AM

```
Agent:       VMBACKUPSERVER
Status:      Success
Start time:  2/2/2018 5:05:28 AM    Finish time:    2/2/2018 5:14:24 AM (00:08:56)
Result:      target: Katun; status: Success;
             message: Virtual machine 'Katun' backup completed successfully.
             Details:
             'Hard disk 1' "[sb499.R0.S2] katun.altay.dev/katun.altay.dev-000001.vmdk", backup method: IteCbt, transport: hotadd, backup type:
             Incremental
              volume #1 "System Reserved" (Ntfs 25305088 bytes in use): 2601984 bytes copied, 6,199,207.34 b/s
              volume #2 (Ntfs 28103524352 bytes in use): 213880320 bytes copied, 1,147,654.77 b/s
```

Find more details in:

- Configuring Backup Job
- Verifying Backup Viability
- Restoring Complete Virtual Machine
- Retrieving Individual Files and Folders
- Restoring Application Objects Granularly
- Launching VM Backup
- Failing over to VM Replica

Working Area

The working area displays contents of the currently active view. For instance, if you click the Environment view, the working area will display configured backup infrastructure members, and all machines that have installed product components, while for the Backups view it will display storages where specific backup targets are resided, existing backups chains with restore point properties, and currently active restore points.

Typical Scenarios

Configuring Backup Job

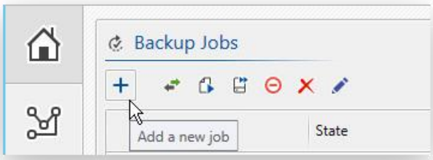
Paragon VM BACKUP does agentless disk-imaging backup of virtual machines resided on VMware vSphere or a standalone ESX(i) server. By default, for every machine our program creates a full backup during the first run, then incremental updates according to a set timetable. As backup destination a local folder, network share, and ESX datastore are allowed to use. Backup storage footprint is minimized by utilizing incremental imaging technologies, redundant data exclusion filters (OS page files, zero data blocks, etc.) and the patent-pending backup container. Backup data is retained according to set criteria that determine lifespan and the maximum occupied space. When time comes, all restore points beyond the set limit are merged with their full backup, thus creating a new full backup.

Generally, Paragon VM BACKUP backs up virtual machines completely. However, you can exclude specific VM disks from backup with the help of VM Storage Policies, but this option is available in vSphere 5.5+ virtual infrastructure.

Prerequisites

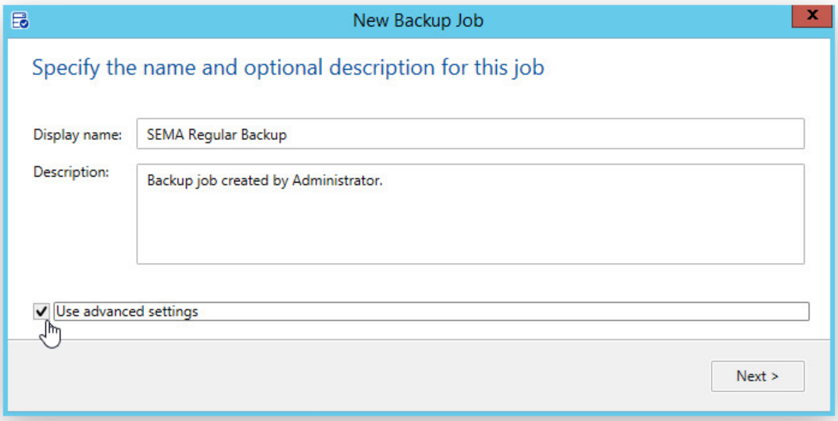
- Though you don't have to pre-configure all backup infrastructure components necessary for performing backup, as our wizard prompts you to do that in the process, you should be ready to provide address of an ESX(i) host where backup target machines are resided or vCenter Server to which this host is connected and access credentials.
- You need to specify e-mail notification settings in **Home > Settings**, if you want to be notified by e-mail about backup infrastructure events. Find more details in **Configuring E-mail Notifications**.
- If you plan to back up MS Exchange or Active Directory virtual servers at application-level and then granularly restore data from their backups, make sure the following requirements are met:
    - Exchange VM Backup Requirements are met.
    - Backup data is resided on a non-encrypted local backup storage.
    - The application-aware image processing is enabled (access credentials are set for the target machine). These credentials are also required for a correct operation of the snapshot mechanism (logs truncation), metadata processing, and for running pre-/post-snapshot scripts.

1. On the first program start, the New Backup Job wizard starts automatically. You can call it later by clicking the plus icon in the 'Backup Jobs' pane, located in the Home view (also the Backups view).



2. Give a name to your backup job and a detailed description (optional).

   If you'd like to exclude VM disks from backup, specify processing method, VMware transport mode or other advanced parameters, mark the corresponding checkbox and these options will get available later in the wizard.



New Backup Job

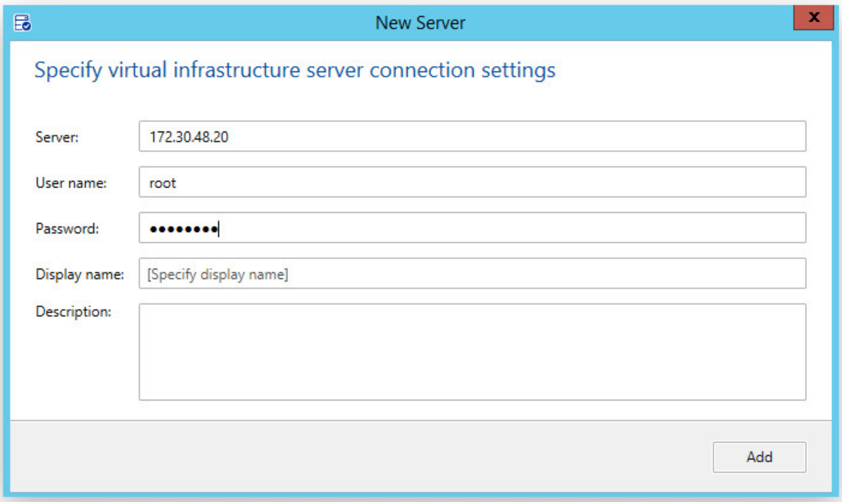
Specify the name and optional description for this job

Display name: SEMA Regular Backup

Description: Backup job created by Administrator.

☑ Use advanced settings

3. As no virtual server connection has been added yet, the wizard prompts you to do it at this step. Click the plus icon, then enter address of the required vCenter or ESX(i) host, administrator credentials, and additional info in the corresponding fields, then click **Add**. If a success, this connection will be added to the list, just select it to proceed further.



New Server

Specify virtual infrastructure server connection settings

Server: 172.30.48.20

User name: root

Password: ••••••••

Display name: [Specify display name]

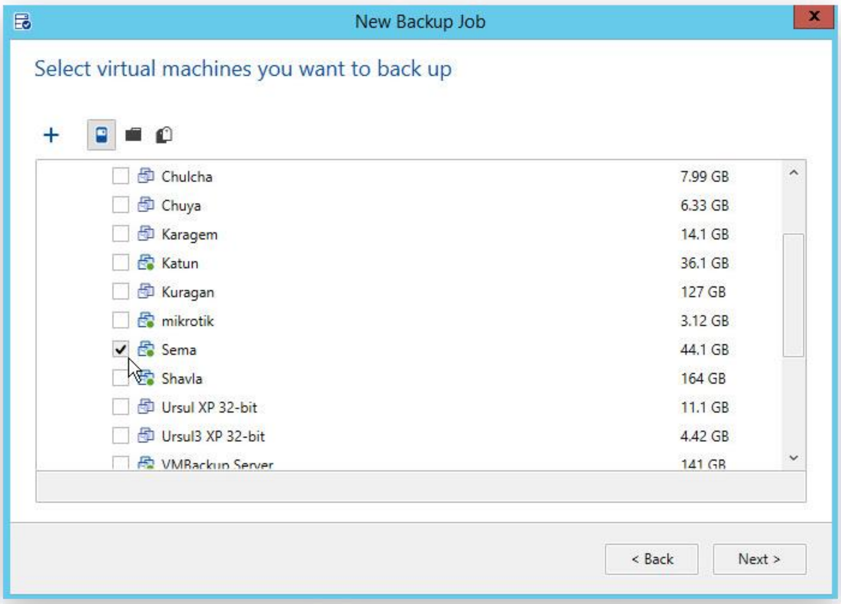
Description:

If a virtual server connection is not established, please check the following:

- A network adapter on the machine where VM BACKUP AGENT is installed can access outer resources;
- If the required ESX host is a member of a vCenter, make sure IP address and credentials of that vCenter is provided;
- The provided ESX access credentials are valid and allow enough privileges (see Appendix).

4. Browse the connected virtual infrastructure to mark machines you're going to protect.

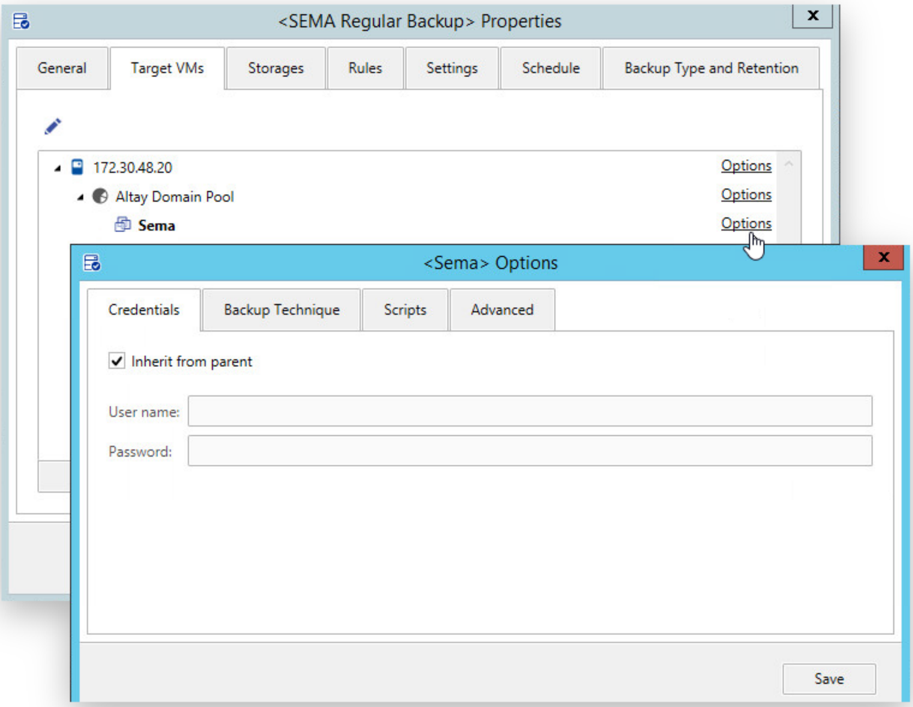
   If you use the tags feature (available from vSphere 5.1), then we recommend you to group virtual machines you'd like to back up by category, e.g. guest operating system type, and just select one tag as backup object instead of several machines. Please note that tags can only be created in vSphere Web Client. To see existing tags in our interface, just switch to the corresponding view in the upper left corner. For more information about tags, please consult VMware Documentation.



Select virtual machines you want to back up

□	Chulcha	7.99 GB
□	Chuya	6.33 GB
□	Karagem	14.1 GB
□	Katun	36.1 GB
□	Kuragan	127 GB
□	mikrotik	3.12 GB
☑	Sema	44.1 GB
□	Shavla	164 GB
□	Ursul XP 32-bit	11.1 GB
□	Ursul3 XP 32-bit	4.42 GB
□	VMBackup Server	141 GB

5. At this step you can modify general backup settings, either for all target machines resided on the connected host, those that join the selected resource pool, or a particular VM.



172.30.48.20 Options

Altay Domain Pool Options

Sema Options

☑ Inherit from parent

User name:

Password:

- **Credentials.** Providing guest OS credentials with enough privileges to allow our program log in to the machine, is a must if you need to run pre-/post-snapshot scripts or do application-aware image processing.
- **Backup Technique.** By default, for every machine Paragon VM BACKUP creates a full backup for the first run, and then only saves changes since the last performed operation in incremental images. The delta to write is either parsed through VMware CBT or Paragon ITE. So here you've got five options to choose from:
  - **Auto**. It's the default mode, when **Intelligent CBT** is used whenever possible, while **Paragon ITE** is in reserve. Please note that in situations when CBT is turned off on the target machine,

but this machine contains file systems unsupported by Paragon, the **Raw Copy** mode is automatically activated, which doesn't allow incremental imaging at all.

- **Intelligent CBT**. In this mode changes since the last backup are parsed through VMware CBT, and then this data is considerably reduced through Paragon's patent-pending algorithms, thus producing a much smaller backup image. If VMware CBT is turned off on the target machine, backup tasks will fail with a corresponding warning.
- **Paragon ITE only**. In this mode changes since the last backup are parsed through Paragon's ITE only. Resulted backup images will take a bit more time to create and be larger in size, but it's the only decent option when CBT cannot be used on the target machine. Another benefit comes from the fact that an active CBT significantly degrades the disk subsystem performance of target machines.
- **Pure CBT**. In this mode changes since the last backup are parsed through VMware CBT only and then saved in the resulted image without any optimization.
- **Raw Copy**. Use this mode if none of the other options can help you back up target machines. Only full images will be created.

▪ **Scripts.** If guest machines you're going to protect run applications that do not support Microsoft VSS (an old version of MS SQL Server, Linux-based PostgreSQL or Oracle Database, etc.), you need to run custom scripts to provide a coherent state of all open files and databases involved in backup. Pre-snapshot scripts can help to freeze (quiesce) applications before Paragon VM BACKUP initiates creation of a snapshot, while post-snapshot scripts bring these applications back to normal work.

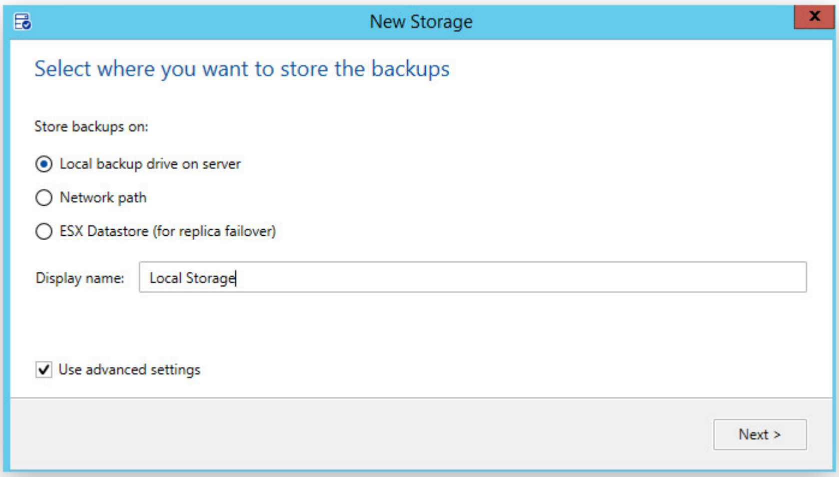
Currently supported script formats:

Windows VMs	Linux VMs
.cmd	.bash, .sh, .tcsh (Shell scripts)
.bat	.php (Perl scripts)
.js (Java scripts)	
.vbs (Visual Basic scripts)	

▪ **Advanced.**

- **Disable VM quiescing.** If you're protecting non-Windows VMs that are having third-party VMware tools that do not support quiescing, use this option to accelerate the backup. It can also help you to obtain crash-consistent snapshots without utilizing VSS inside Windows-based virtual machines.
- **Transaction logs processing**. If you're trying to protect a machine that hosts MS Exchange or any other enterprise-class application, please select either the **Delayed Truncation** (recommended) or **Truncate Immediately** mode to obtain consistent backup images.

6. As no backup storage has been configured yet, the wizard prompts you to do it right now. Click the plus icon, then specify the preferred storage type and give it a name. Please note that local and network storages can only store VM backups, while ESX datastore – VM replicas.


New Storage

Select where you want to store the backups

Store backups on:

● Local backup drive on server

○ Network path

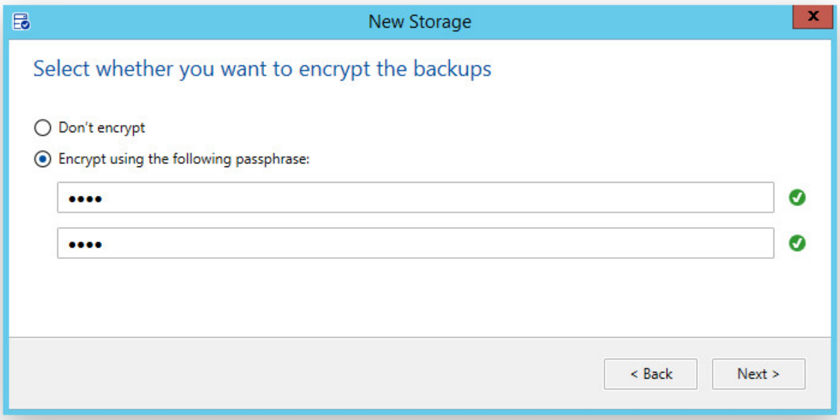
○ ESX Datastore (for replica failover)

Display name: Local Storage

☑ Use advanced settings

- **Local drive on server**. This type of storage is actually a local folder on a machine where Paragon VM BACKUP is installed.
- **Network path**. Please note that backup to a network share located on a machine under control of a non-server OS may fail due to certain limitation on simultaneous connections. Thus if you're planning to store many backup objects (backup catalogs with multiple incremental updates), we strongly recommend you to use a specially-dedicated network repository for that.
- **ESX datastore**. Please note that if the required ESX host is a member of a vCenter, always use address and credentials of that vCenter.

To protect backup data from unauthorized access, mark the 'Use advanced settings' checkbox to set a passphrase. Paragon VM BACKUP uses 256-bit Advanced Encryption Standard (AES) with a 256-bit key length, which ensures complete safety for sensitive VM data.


New Storage

Select whether you want to encrypt the backups

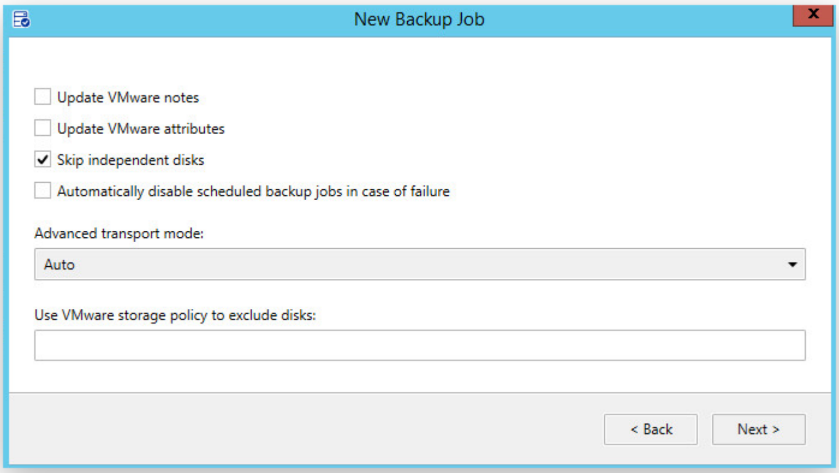
○ Don't encrypt

● Encrypt using the following passphrase:

•••• ✓

•••• ✓

7. At this step you can modify advanced backup settings, if the corresponding checkbox has been marked on the first page of the wizard.



□ Update VMware notes

□ Update VMware attributes

☑ Skip independent disks

□ Automatically disable scheduled backup jobs in case of failure

Advanced transport mode: Auto

Use VMware storage policy to exclude disks:

- **Update VMware notes/attributes during backup job**. If necessary, Paragon VM BACKUP can document the backup status within the virtual machine's annotations in the "Notes" field, thus you can monitor the backup status directly in the vSphere Client. Additionally, you can allow adding the same info to the "Attributes" field as well. Using a virtual machine attribute is better than using a note, because the notes field is general for all events and is updated entirely, while the attributes field contains a list of items, one for a specific type of event. However, this feature is not available for standalone ESX hosts.

- **Skip independent disks**. Use this option to ignore found independent disks (persistent / non-persistent) during backup. Independent disks can have different behavior when the VM snapshot is taken. A persistent disk continues to behave as if there is no snapshot being taken and all writes go directly to disk. When you configure a non-persistent disk, a special redo log is created to capture all subsequent writes to that disk. When the virtual machine is powered off or the snapshot is deleted, all these changes are discarded.

- **Advanced transport mode**. There are several modes VMware vStorage API can provide access to data inside disk containers of virtual machines to do backup or restore:

  - **Auto.** VMware picks the fastest and most efficient mode by trying each one on the fly (recommended);

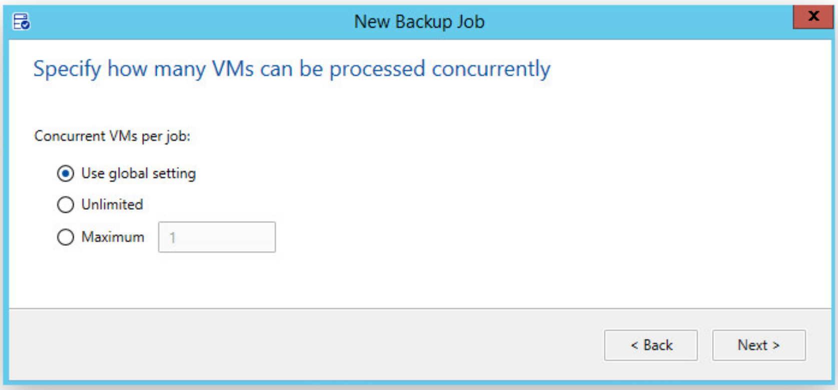
  - **Advanced**. It's also an auto mode, but here only two high-performance modes are considered to use (Virtual Appliance or SAN). **Virtual Appliance** will be selected if ESX Agent is deployed on a virtual machine hosted by ESX, which guests are being protected. **SAN** will be selected if ESX Agent is deployed on a physical machine running Windows Server 2008 / 2012 / 2016, which have access to LUNs (Logical Unit Number) with virtual machines. Both modes do not load CPU of ESX. If Virtual Appliance is configured to not use the production networking, then the production bandwidth is also not used. However, both these modes require special configuration of virtual machines.

  - **Network**. It's a universal mode that can be used no matter where ESX Agent is deployed. It supports all configurations of virtual machines and can process virtual disks that do not support the snapshot mechanism (Independent or Physical RDM disks). Please note that this mode uses the external network interface of ESX, thus it can heavily load its CPU and bandwidth. Besides, VMware limits for it the number of simultaneously processed disks by all parallel vStrorage API activities (32 disks for ESX 5.x, 27 for ESX 4.x, 23 for ESXi 4.x).

- **Encrypted Network**. It's the network mode additionally encrypted through SSL (Secure Sockets Layer). Obviously, it's the slowest mode of all and it requires special configuration of virtual machines. VMware doesn't limit the number of simultaneously processed virtual disks for it. We recommend this mode if ESX Agent connects ESX via public network with low level of confidence.

- **Use VMware storage policy to exclude disks**. Generally Paragon VM BACKUP completely backs up target virtual machines, but if you're having vSphere 5.5+ virtual infrastructure, then you can specify VM disks you'd like to exclude from backup by configuring so called VM Storage Policies. Please note that storage policies can only be created in vSphere Web Client. Once done, type in an existing storage policy name in the corresponding field to exclude unimportant disks from backup. For more information about storage policies, please consult VMware Documentation.

8. This step also becomes available when the advanced backup settings are enabled on the first page of the wizard. By default, four virtual machines are allowed to back up simultaneously by one backup job, which you can change to any value in **Home > Settings**. Please note that the value you set right here will be relevant for this backup job only.



New Backup Job

Specify how many VMs can be processed concurrently

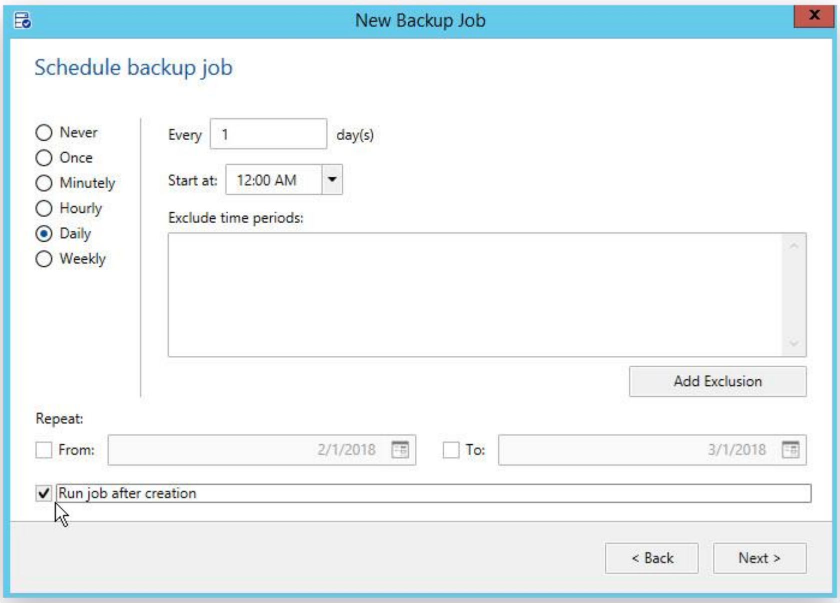
Concurrent VMs per job:

● Use global setting

○ Unlimited

○ Maximum 1

9. Schedule your backup job. We suggest protecting non-critical virtual machines daily, while for production environments like SQL Server or Exchange Server, where multiple transactions occur every second, the optimal interval between backups is 30-60 minutes. By reducing this interval even further, you risk to heavily overload the entire infrastructure. So consider actual business needs and possible compliance requirements.



New Backup Job

Schedule backup job

○ Never
○ Once
○ Minutely
○ Hourly
● Daily
○ Weekly

Every 1 day(s)

Start at: 12:00 AM

Exclude time periods:

Repeat:

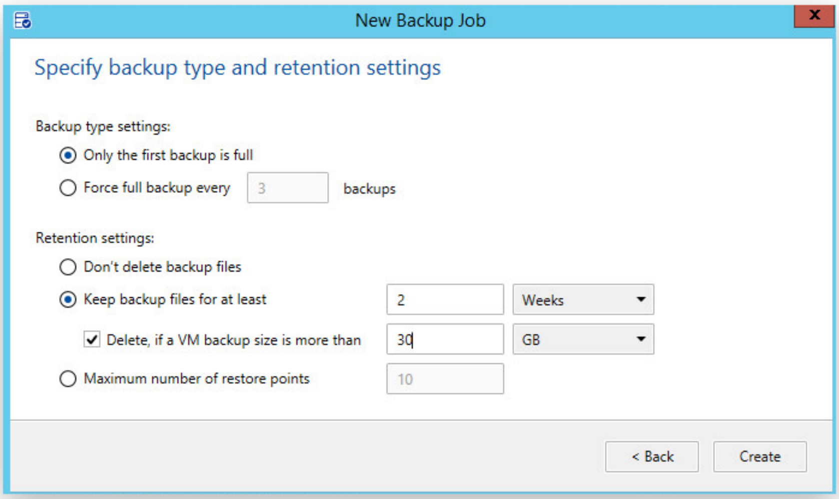
□ From: 2/1/2018 □ To: 3/1/2018

☑ Run job after creation

10. Further you may change the default incremental backup chain policy by specifying occurrence of full backups. Though the incremental imaging considerably saves your backup storage space, this backup method becomes ineffective with a growing number of chain members. The problem is that the entire chain needs to be processed when you restore the latest image. Obviously, it may take plenty of time for a long chain that includes tens of increments, in addition to the fact that having one corrupted image somewhere in the middle makes the restore operation impossible.

    As you know, a full backup always starts a new backup chain. Thus by specifying occurrence of full backups, you specify a backup cycle that suits your needs at best. For non-critical VMs we suggest a 7-day cycle of one full backup followed by six incremental updates. It is a reasonable compromise between backup storage consumption and restore performance. VMs with sensitive data require individual approach. If you need our help in working out optimal backup cycles for your production environments, please contact our Support Team.

    To avoid the situation when backup data eats up the entire storage space, we suggest configuring retention policy to get rid of obsolete restore points automatically. Your choice may depend on whether this applies to a regular machine for which you may want only a few restore points to roll back, or a production environment that contains sensitive data. You may need this data for the future forensic analysis and/or it can be subject to compliance requirements.



New Backup Job

Specify backup type and retention settings

Backup type settings:

● Only the first backup is full

○ Force full backup every 3 backups

Retention settings:

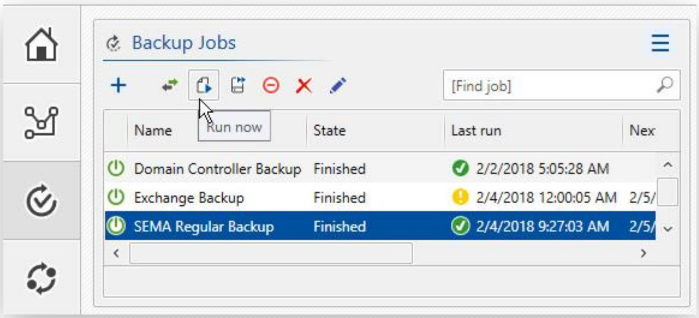
○ Don't delete backup files

● Keep backup files for at least 2 Weeks

☑ Delete, if a VM backup size is more than 30 GB

○ Maximum number of restore points 10

11. Complete the wizard to save changes. Now that your backup job is created, it will run automatically on schedule. To start it manually, select the job in the 'Backup Jobs' pane, then click the corresponding icon.



Name	State	Last run	Nex
Domain Controller Backup	Finished	2/2/2018 5:05:28 AM	
Exchange Backup	Finished	2/4/2018 12:00:05 AM	2/5/
SEMA Regular Backup	Finished	2/4/2018 9:27:03 AM	2/5/

If everything went smooth, the resulted status would be 'Success' (the green OK icon). You might also see 'SuccessWithInfo' (the yellow exclamatory icon). This means that the backup job run is valid and can be used for restore, but the embedded diagnostic tool has detected one or several issues with the target virtual machine(s), which is negatively affecting its performance, namely:

- One or several target VM disks needs consolidation. Sometimes a virtual machine continues to run on delta disk files (also called REDO logs) after backup. It's like running on a snapshot, but this snapshot is not available and can't be administered in the snapshot manager. As you know, running on a snapshot leads to gradual performance degradation. In most cases this issue occurs after a failed snapshot action, which is fundamental part of backup. Our diagnostic tool verifies target virtual machines for leftover delta disks before and after backup. For more information, please go at https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2045116.
- VM BACKUP AGENT keeps holding some target disks in HotAdd mode after backup. This usually happens when a virtual machine hosting VM BACKUP AGENT had been switched off or disconnected from target virtual disks during backup, which resulted in a failed backup job run. These disks need to be manually removed before attempting the next backup.
- File layout of a VMDK target disk was changed, e.g. there were appeared or disappeared some VMDK files during backup. This doesn't concern other file types (log, VMSN, VMSS, etc.).
- A post-snapshot script completed with an error.

Status and detailed information on every job run can be found in the 'Activities' pane.

Please administer backup data only in the VM BACKUP CONSOLE to avoid malfunctioning of the backup infrastructure.

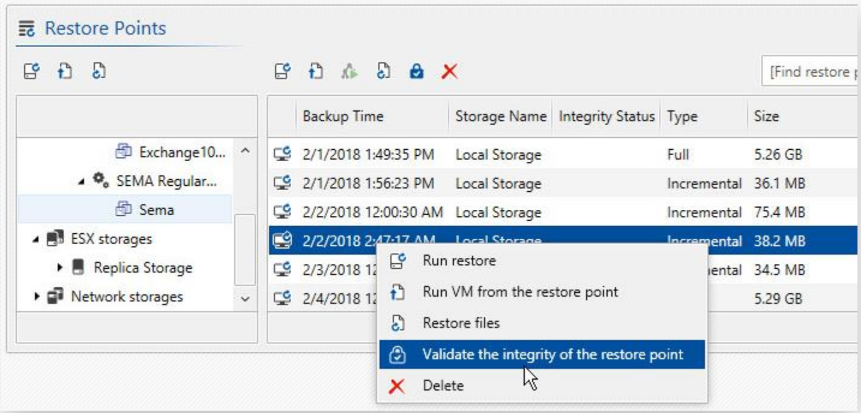
Verifying Backup Viability

Backup data must be tested for viability. If not done that periodically, you won't know until it's too late. We recommend you to check generated backup data at least once every few months. Paragon VM BACKUP includes several options to achieve this goal.

Checking Backup Integrity

In Paragon VM BACKUP you can check integrity either for a given restore point, all restore points of a given machine, or an entire backup storage.

1. Open the Backups view, right click a backup storage, virtual machine, or an individual restore point in the 'Restore Points' pane, then select **Validate the integrity**.



Restore Points

Backup Time	Storage Name	Integrity Status	Type	Size
2/1/2018 1:49:35 PM	Local Storage		Full	5.26 GB
2/1/2018 1:56:23 PM	Local Storage		Incremental	36.1 MB
2/2/2018 12:00:30 AM	Local Storage		Incremental	75.4 MB
2/2/2018 2:47:17 AM	Local Storage		Incremental	38.2 MB
2/3/2018 12			ental	34.5 MB
2/4/2018 12				5.29 GB

2. Depending on the amount of processed backup data, verification of the selected object for errors may take a while. If it turns out to be invalid, it will be marked by a special icon.

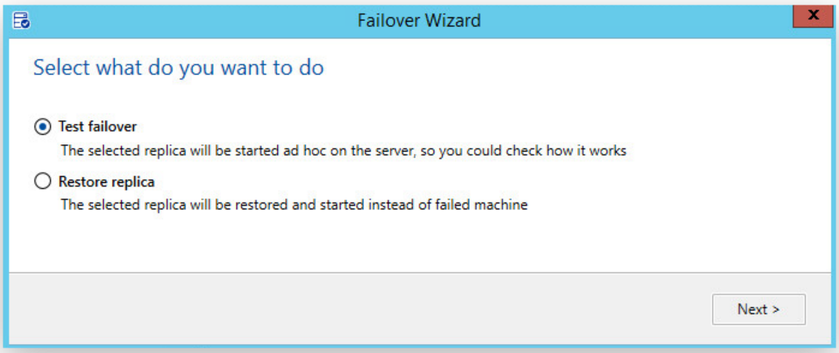
Running Replica Test Failover

Paragon VM BACKUP allows you to test the sanity of an existing replica machine by non-disruptively simulating recovery procedure in an isolated network environment. This can help to make sure a certain replication job produces valid replica machines, do field test for an existing recovery plan, or train IT personnel on what is to be done in case of emergency.

Paragon VM BACKUP triggers a VMware snapshot for the necessary restore point of the original VM replica, which protects it from changes, as they are written to a delta file. When the test failover process is over, our program removes this delta file and powers off the replica machine.

This operation may take plenty of system resources (CPU, RAM, disk IO), so please do not forget to stop test replicas.

1. Open the Backups view, browse an existing ESX storage for a replica machine in the 'Restore Points' pane, right click the required restore point, then select **Run VM from the restore point**.
2. In the opened wizard just proceed to the next page without changing the default option.



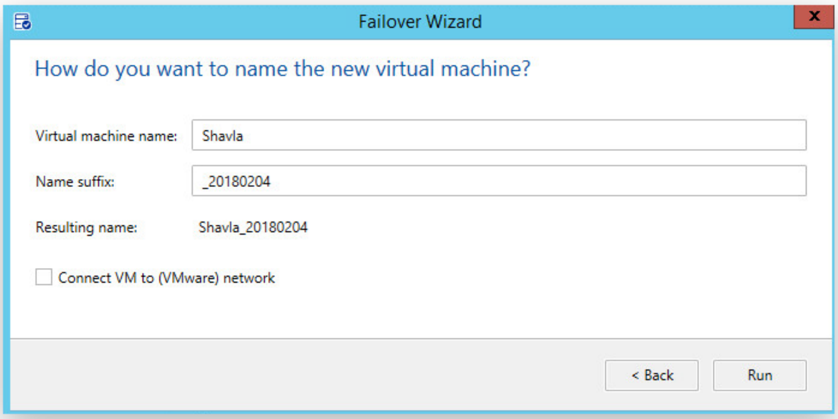
Failover Wizard

Select what do you want to do

● Test failover
The selected replica will be started ad hoc on the server, so you could check how it works

○ Restore replica
The selected replica will be restored and started instead of failed machine

3. By default, the network support on the target replica machine is disabled to avoid possible problems of having two identical machines in one network environment. At this stage you can also change the offered machine name. When done with the configuration, click **Run**, then complete the wizard.



Failover Wizard

How do you want to name the new virtual machine?

Virtual machine name: Shavla

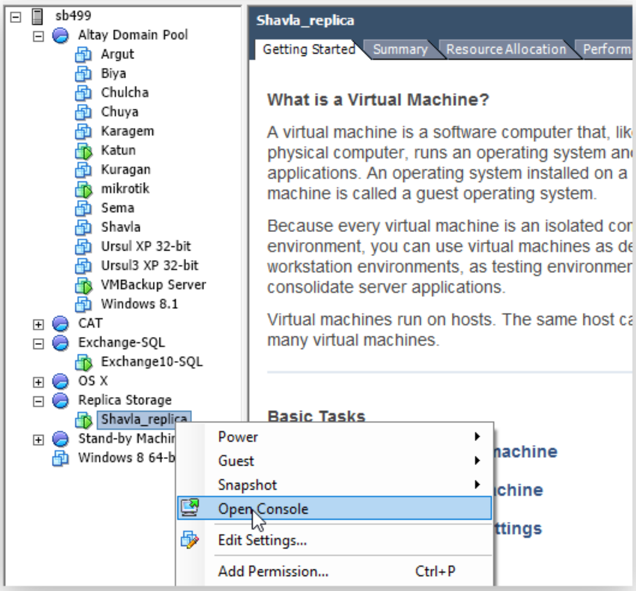
Name suffix: _20180204

Resulting name: Shavla_20180204

□ Connect VM to (VMware) network

4. When the operation is over you can find the resulted test replica machine in the online state located next to the original replica. A corresponding new item will also appear in the list of replica restore points in our interface. Check that it works as required.

   Please note that Paragon VM BACKUP forces the launch of the original replica machine if it’s resided on a standalone ESX(i), as VMware doesn’t support creation of linked VM clones for this type of configurations.



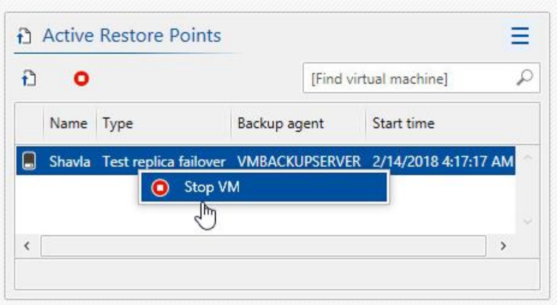
What is a Virtual Machine?

A virtual machine is a software computer that, lik physical computer, runs an operating system an applications. An operating system installed on a machine is called a guest operating system.

Because every virtual machine is an isolated cor environment, you can use virtual machines as de workstation environments, as testing environmer consolidate server applications.

Virtual machines run on hosts. The same host ca many virtual machines.

5. Right click the test replica machine in the ‘Active Restore Points’ pane, then select **Stop VM** to power it off and perform the other necessary actions, including removal of the test replica machine (for vCenter) or the delta file (for a standalone ESX(i)).



Name	Type	Backup agent	Start time
Shavla	Test replica failover	VMBACKUPSERVER	2/14/2018 4:17:17 AM

Paragon VM BACKUP also allows you to test the sanity of existing VM backup images by running a virtual machine directly from one of available restore points. Find more details in Launching VM Backup.

Restoring Complete Virtual Machine

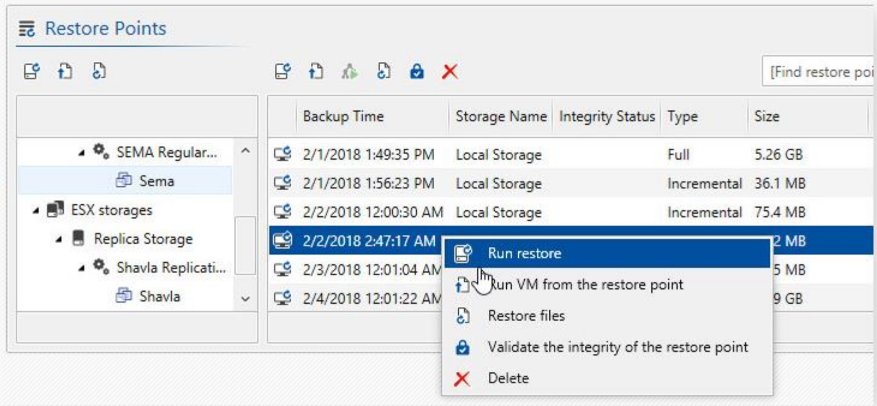
Paragon VM BACKUP can help to recover a virtual machine to any good-to-know point in time and place it to the original or a new location. When restored to a new location you will be prompted to provide a new name for the machine, and a host and datastore to reside. Paragon VM BACKUP will change the VM configuration file and store the target machine according to the defined location. When restored to the original location, the original machine will be deleted (it should be offline).

Prerequisites:

- Despite the fact that you’re allowed to restore data from invalid backup images, please do it at your own risk. We highly recommend you to validate the required restore point for viability before you start the restore. Find more details in Verifying Backup Viability.

- Restore to the original location can only be a success if the target virtual machine is offline. Please note that all changes appeared on the target VM after the specified restore point will be irreversibly lost.
- You need to specify e-mail notification settings in **Home > Settings**, if you want to be notified by e-mail about backup infrastructure events. Find more details in **Configuring E-mail Notifications**.

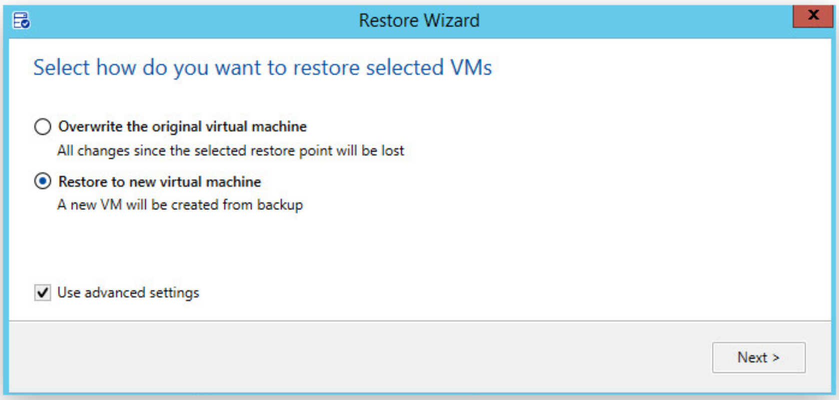
1. Open the Backups view, browse an existing backup storage for a virtual machine in the 'Restore Points' pane, right click the required restore point, then select **Run restore**. If launching the wizard some other way, you may need to choose a desired VM and restore point, if several.



Backup Time	Storage Name	Integrity Status	Type	Size
2/1/2018 1:49:35 PM	Local Storage		Full	5.26 GB
2/1/2018 1:56:23 PM	Local Storage		Incremental	36.1 MB
2/2/2018 12:00:30 AM	Local Storage		Incremental	75.4 MB
2/2/2018 2:47:17 AM				2 MB
2/3/2018 12:01:04 AM				5 MB
2/4/2018 12:01:22 AM				9 GB

2. Choose how VM should be restored. You can simply overwrite the original virtual machine, which will be replaced from the backup as of the specified restore point. Alternatively, you can spin up a new virtual machine in a different location. This can be handy if, for whatever reasons, you experience problems with the host running the troublesome machine.

   As with the Backup Job Wizard, mark the corresponding checkbox to configure additional options later in the wizard.



Restore Wizard

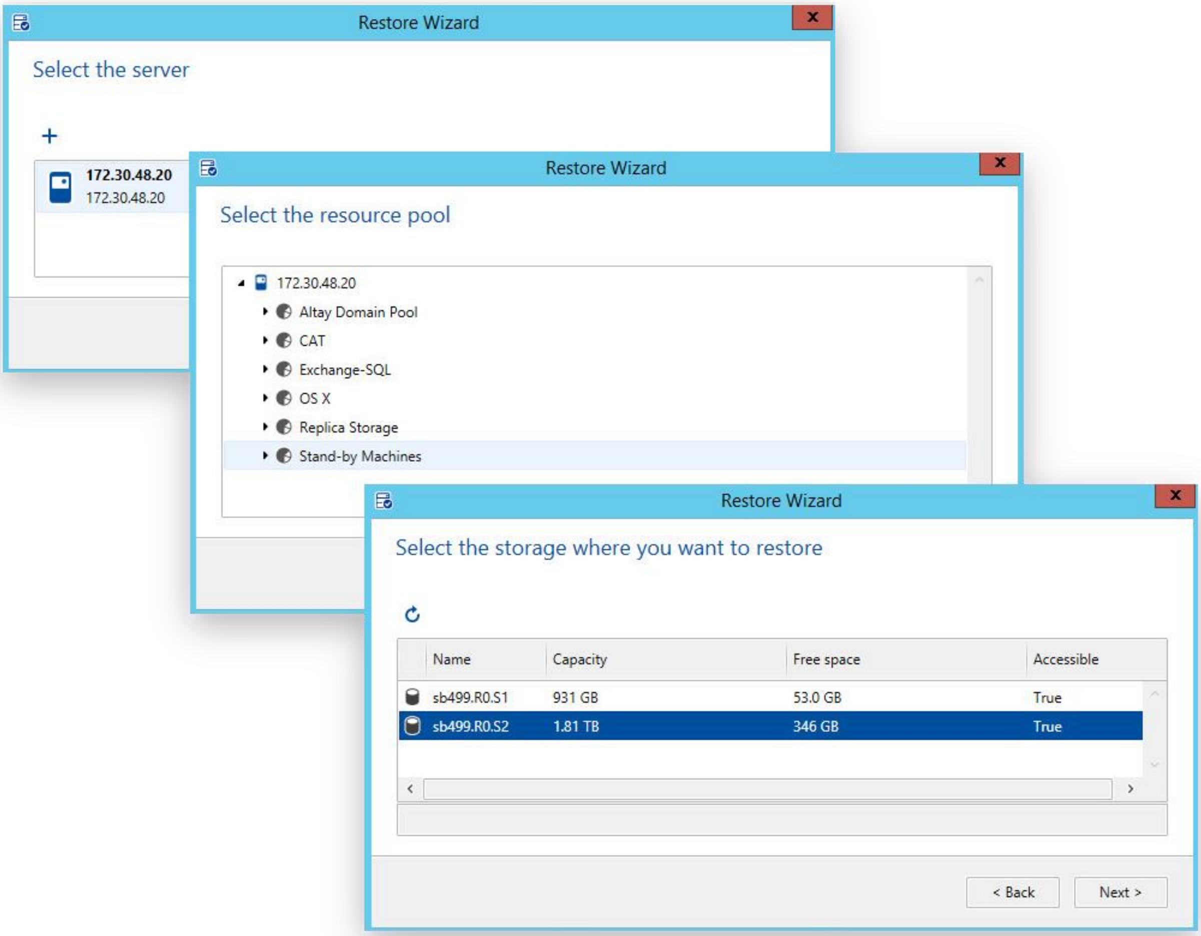
Select how do you want to restore selected VMs

○ Overwrite the original virtual machine
All changes since the selected restore point will be lost

● Restore to new virtual machine
A new VM will be created from backup

☑ Use advanced settings

3. When restored to a different location, you need to specify the target ESX host, resource pool and datastore to place the restored VM.



Restore Wizard

Select the server

172.30.48.20
172.30.48.20

Restore Wizard

Select the resource pool

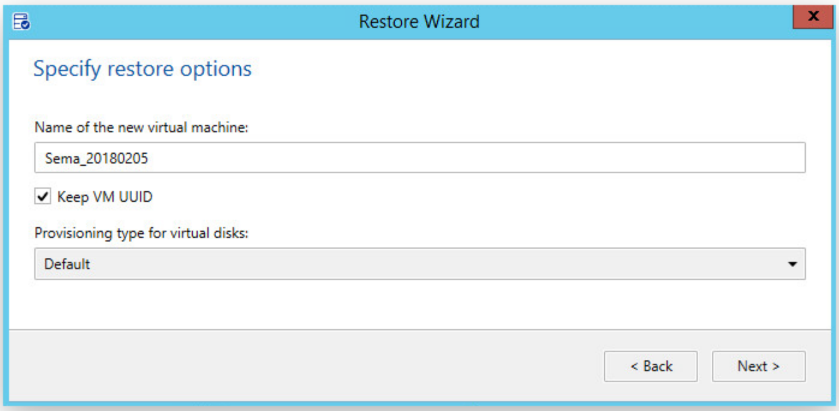
- 172.30.48.20
  - Altay Domain Pool
  - CAT
  - Exchange-SQL
  - OS X
  - Replica Storage
  - Stand-by Machines

Restore Wizard

Select the storage where you want to restore

Name	Capacity	Free space	Accessible
sb499.R0.S1	931 GB	53.0 GB	True
sb499.R0.S2	1.81 TB	346 GB	True

4. At this step you can modify advanced restore settings, if the corresponding checkbox has been marked on the first page of the wizard. Please note that the number of available options depends on the chosen restore scenario and your backup infrastructure.



Restore Wizard

Specify restore options

Name of the new virtual machine: Sema_20180205

☑ Keep VM UUID

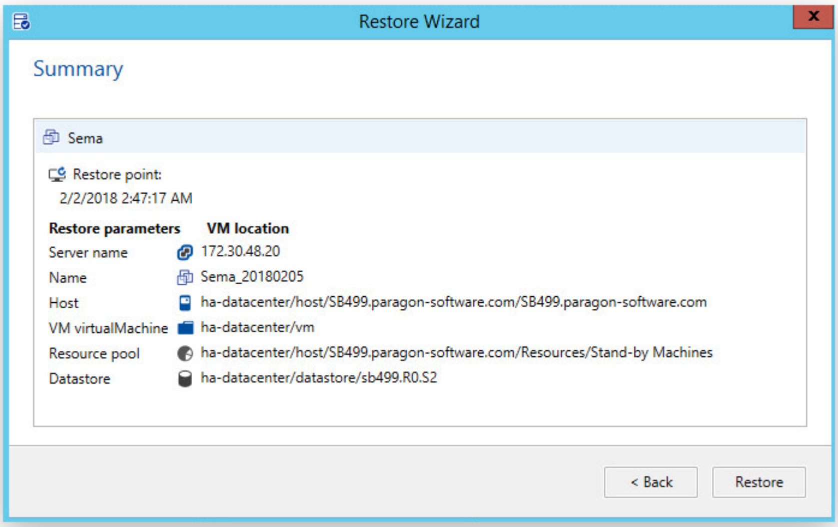
Provisioning type for virtual disks: Default

- Edit the default machine name.
- Choose a VM BACKUP AGENT to accomplish the restore operation (if several have been deployed).
- Choose whether to keep the original UUID (recommended) or generate a new one. The main rule here is that there should not exist several VMs with the identical UUID in one virtual infrastructure. If you decide to generate a new UUID, please be ready to face activation issues with Windows OS, applications, broken user account, etc. on the restored VM.

- If you decide to keep the original UUID, please make sure there's no the same VM in your virtual infrastructure, otherwise you will face
- Specify the required provisioning type for virtual disks. VMware ESX(i) hosts support two types of disk provisioning, namely "Thin" and "Thick". With the "thin provisioning" the size of a VDMK file on a datastore is exactly the amount of data it contains, so if you create a 300GB virtual disk, and place 50GB of data in it, the VMDK file will be 50GB in size. With the "thick provisioning" the size of a VMDK file on a datastore is always its maximum size, so no matter how much data the virtual disk contains, the VMDK file will be 300GB in size anyway. Obviously, conversion from the "thick provisioning" to the "thin" during the VM restore operation may help to fit in to a smaller target datastore.

5. Review all parameters of the operation and modify them if necessary by going back to any of the required steps. Click **Restore** to start.

   After the operation is over you can go to the ESX host where you chose to deploy the backed up machine and see a new virtual machine in the offline state. You can turn it on, if the original machine is off. Otherwise, there will be a conflict of DNS names or IP addresses (if static addresses are used).



Summary

Sema

Restore point:
2/2/2018 2:47:17 AM

Restore parameters	VM location
Server name	172.30.48.20
Name	Sema_20180205
Host	ha-datacenter/host/SB499.paragon-software.com/SB499.paragon-software.com
VM virtualMachine	ha-datacenter/vm
Resource pool	ha-datacenter/host/SB499.paragon-software.com/Resources/Stand-by Machines
Datastore	ha-datacenter/datastore/sb499.R0.S2

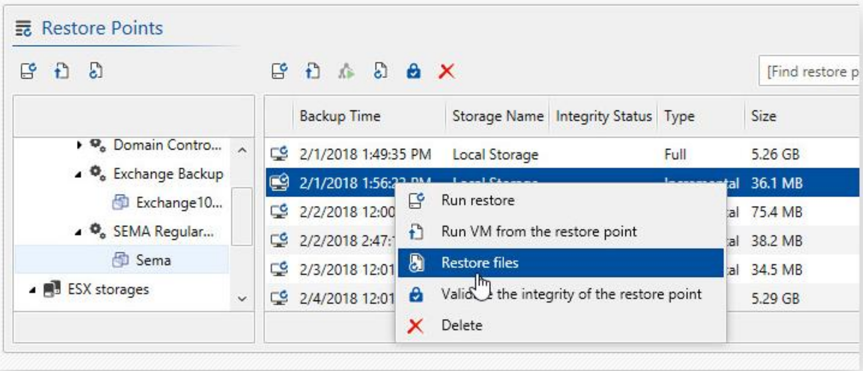
Retrieving Individual Files and Folders

Paragon VM BACKUP allows browsing contents of VM backups and replicas to extract individual files and/or folders. Backup data can be restored locally (on a machine where Paragon VM BACKUP is installed) or on a network share, provided the original directory structure is kept intact, if necessary.

Prerequisites:

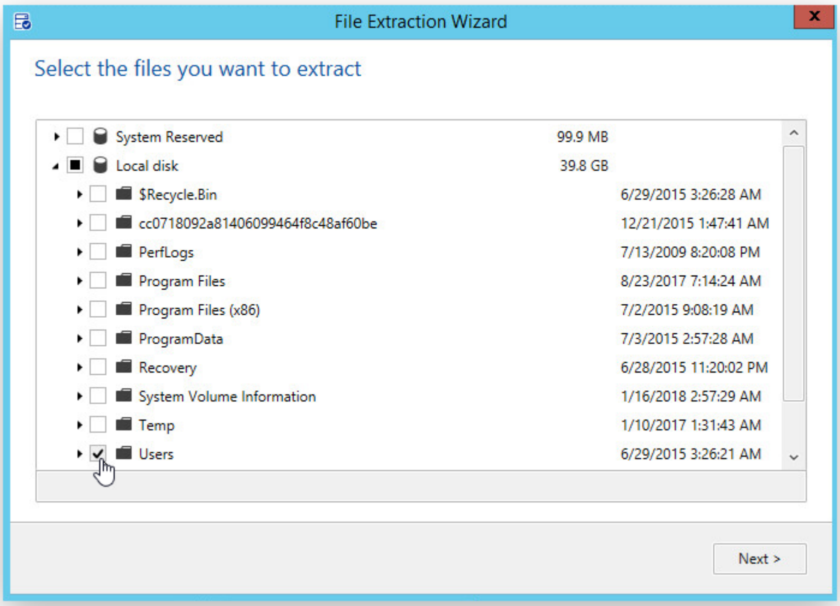
- Despite the fact that you're allowed to restore data from invalid backup images, please do it at your own risk. We highly recommend you to validate the required restore point for viability before you start the restore. Find more details in Verifying Backup Viability.

1. Open the Backups view, browse an existing backup storage for a virtual machine in the 'Restore Points' pane, right click the required restore point, then select **Restore files**. If launching the wizard some other way, you may need to choose a desired VM and restore point, if several.



Backup Time	Storage Name	Integrity Status	Type	Size
2/1/2018 1:49:35 PM	Local Storage		Full	5.26 GB
2/1/2018 1:56:			al	36.1 MB
2/2/2018 12:00			al	75.4 MB
2/2/2018 2:47:			al	38.2 MB
2/3/2018 12:01			al	34.5 MB
2/4/2018 12:01				5.29 GB

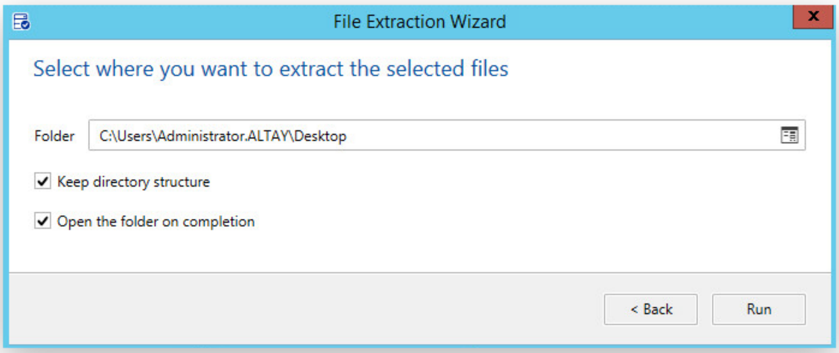
2. Browse the selected restore point and mark data items you'd like to extract.



Select the files you want to extract

□ System Reserved	99.9 MB	
■ Local disk	39.8 GB	
□ $Recycle.Bin		6/29/2015 3:26:28 AM
□ cc0718092a81406099464f8c48af60be		12/21/2015 1:47:41 AM
□ PerfLogs		7/13/2009 8:20:08 PM
□ Program Files		8/23/2017 7:14:24 AM
□ Program Files (x86)		7/2/2015 9:08:19 AM
□ ProgramData		7/3/2015 2:57:28 AM
□ Recovery		6/28/2015 11:20:02 PM
□ System Volume Information		1/16/2018 2:57:29 AM
□ Temp		1/10/2017 1:31:43 AM
☑ Users		6/29/2015 3:26:21 AM

3. Choose where the selected backup data should be extracted. By default, the original directory structure will be preserved and Windows Explorer will be opened in the specified folder once the operation is over, which you can change according to your needs. Click **Restore** when ready.



Select where you want to extract the selected files

Folder C:\Users\Administrator.ALTAY\Desktop

☑ Keep directory structure

☑ Open the folder on completion

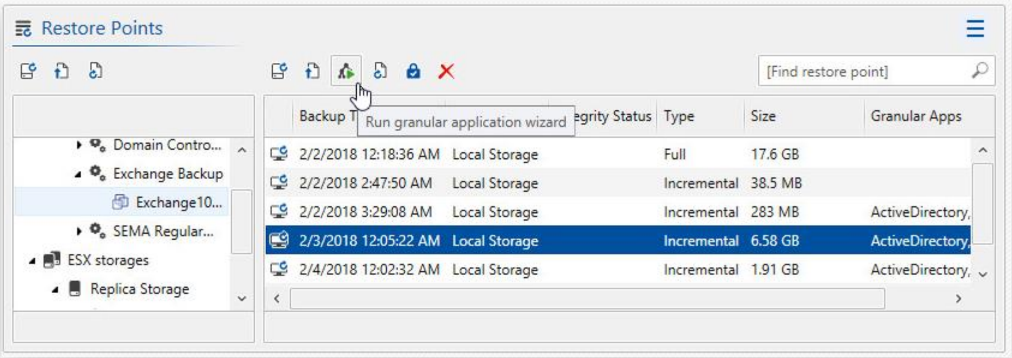
Restoring Application Objects Granularly

Paragon VM BACKUP GRANULAR RESTORE component lets you accomplish granular restore scenarios for VM backups containing enterprise-class applications. Currently our program supports MS Exchange and Active Directory.

Prerequisites:

- Despite the fact that you're allowed to restore data from invalid backup images, please do it at your own risk. We highly recommend you to validate the required restore point for viability before you start the restore. Find more details in Verifying Backup Viability.
- VM BACKUP GRANULAR RESTORE component also utilizes capabilities of the VM BACKUP V-LAUNCH component, so make sure the Launch Backup Requirements are met before you start.
- The granular restore option becomes available when:
    - A virtual machine running MS Exchange or Active Directory is backed up in the application-aware image processing mode (requires guest OS access credentials). Find more details in Configuring Backup Job.
    - VM BACKUP CONSOLE is launched on a machine that hosts backup storage with desired backup images. So if backups are stored on a network storage, simply install and run the console on that machine.

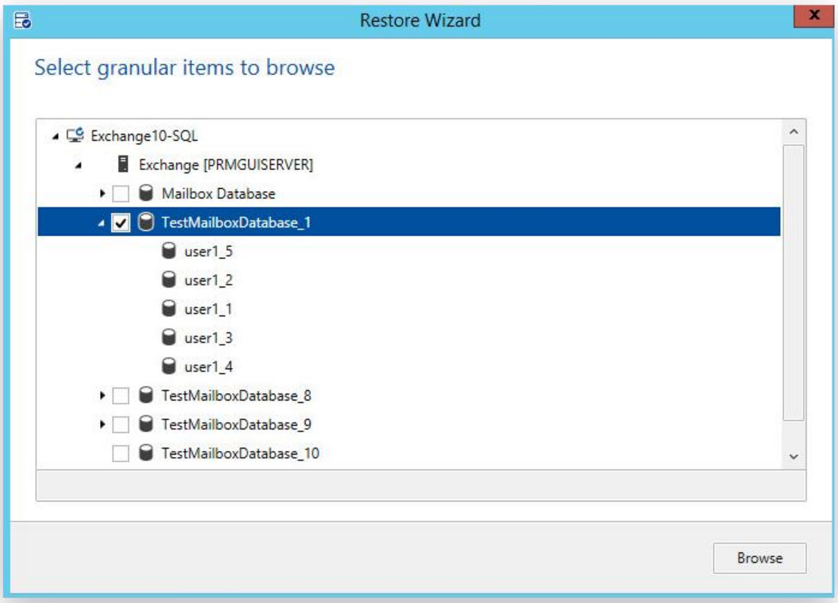
1. Open the Backups view, browse an existing backup storage for a previously backed up virtual Exchange Server or Active Directory Server in the 'Restore Points' pane, select the required restore point, then **Run granular application**... Please note that your restore point must contain data in the 'Granular Apps' field - it indicates the backup is application-aware.



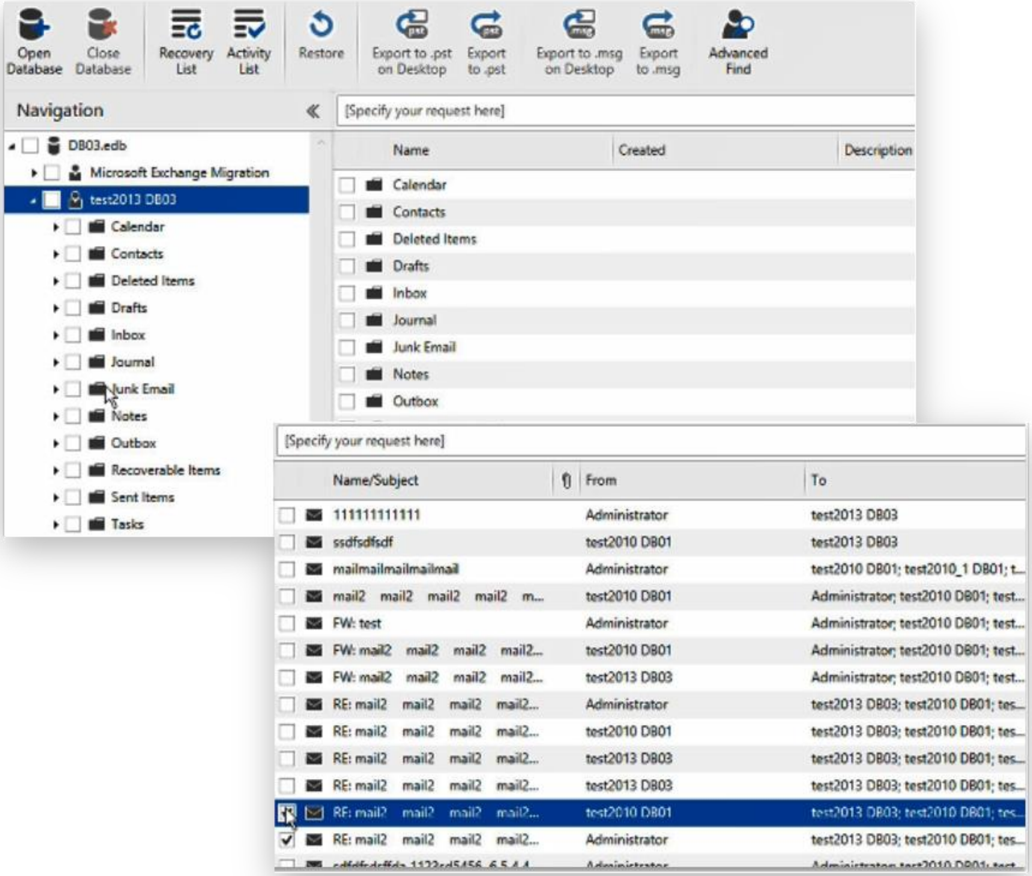
Backup T		egrity Status	Type	Size	Granular Apps
2/2/2018 12:18:36 AM	Local Storage		Full	17.6 GB	
2/2/2018 2:47:50 AM	Local Storage		Incremental	38.5 MB	
2/2/2018 3:29:08 AM	Local Storage		Incremental	283 MB	ActiveDirectory,
2/3/2018 12:05:22 AM	Local Storage		Incremental	6.58 GB	ActiveDirectory,
2/4/2018 12:02:32 AM	Local Storage		Incremental	1.91 GB	ActiveDirectory,

Restoring Exchange Objects

2. Select the database(s) from which you want to restore, then click **Browse**. Paragon VM Backup will utilize the failover functionality to mount dedicated partitions where you can explore the objects you want.

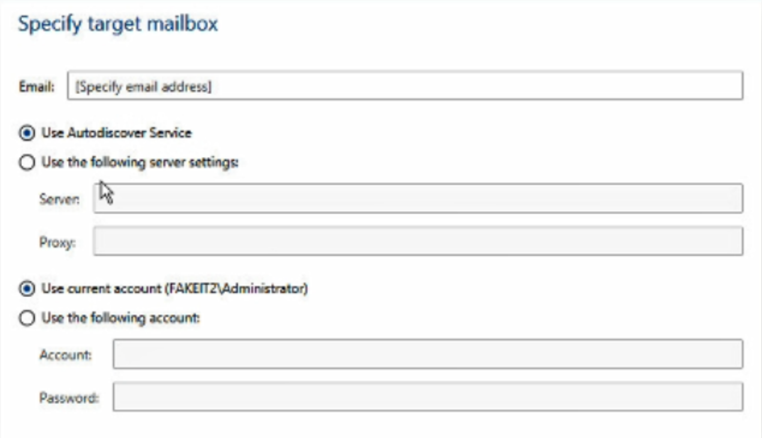


3. Browse for a mailbox(s) you want. You can select entire mailbox folders or individual emails. Use the filter panel to easily find required database objects (by start/end day, received date, subject text, from/to).



	Name/Subject		From	To
☐	111111111111		Administrator	test2013 DB03
☐	ssdfsdfsdf		test2010 DB01	test2013 DB03
☐	mailmailmailmailmail		Administrator	test2010 DB01; test2010_1 DB01; t...
☐	mail2 mail2 mail2 mail2 m...		test2010 DB01	Administrator; test2010 DB01; test...
☐	FW: test		Administrator	Administrator; test2010 DB01; test...
☐	FW: mail2 mail2 mail2 mail2...		test2010 DB01	Administrator; test2010 DB01; test...
☐	FW: mail2 mail2 mail2 mail2...		test2013 DB03	Administrator; test2010 DB01; test...
☐	RE: mail2 mail2 mail2 mail2...		Administrator	test2013 DB03; test2010 DB01; tes...
☐	RE: mail2 mail2 mail2 mail2...		test2010 DB01	test2013 DB03; test2010 DB01; tes...
☐	RE: mail2 mail2 mail2 mail2...		test2013 DB03	test2013 DB03; test2010 DB01; tes...
☐	RE: mail2 mail2 mail2 mail2...		test2013 DB03	test2013 DB03; test2010 DB01; tes...
☑	RE: mail2 mail2 mail2 mail2...		test2010 DB01	test2013 DB03; test2010 DB01; tes...
☑	RE: mail2 mail2 mail2 mail2...		Administrator	test2013 DB03; test2010 DB01; tes...

4. When ready, export the selected objects to .pst or .msg files, which you can later attach or import into the Microsoft Outlook. Alternatively, you can click **Restore** to restore the selected objects directly to the specified Microsoft Exchange account.



Specify target mailbox

Email: [Specify email address]

● Use Autodiscover Service

○ Use the following server settings:

Server:

Proxy:

● Use current account (FAKEIT2\Administrator)

○ Use the following account:

Account:

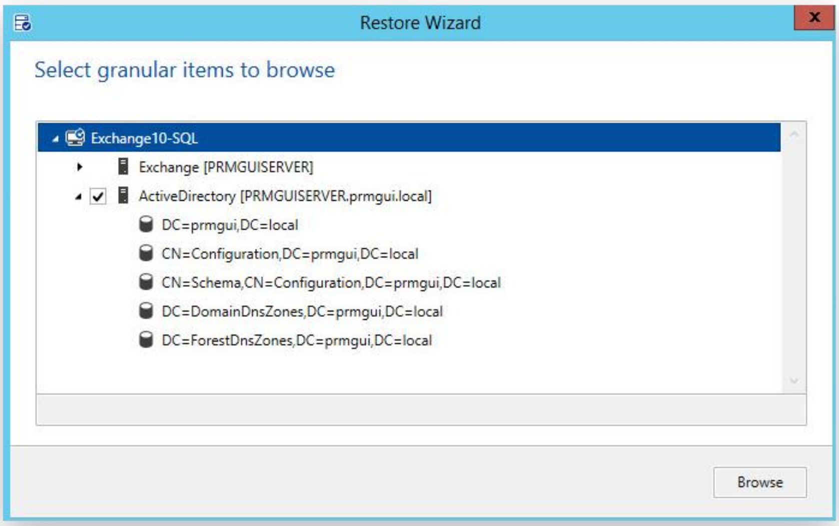
Password:

Please note that you can specify any valid Microsoft Exchange account as restore target. By this means, you can:

- Recover lost or damaged mailbox items for specific users.
- Transfer items to another account (suppose an employee quits and someone must take up correspondence for a specific project or client).
- Set up an ad hoc account and consolidate .pst files across multiple users to make forensic analysis.

Restoring Active Directory Objects

2. Select the Active Directory instance(s) from which you want to restore, then click **Browse**.

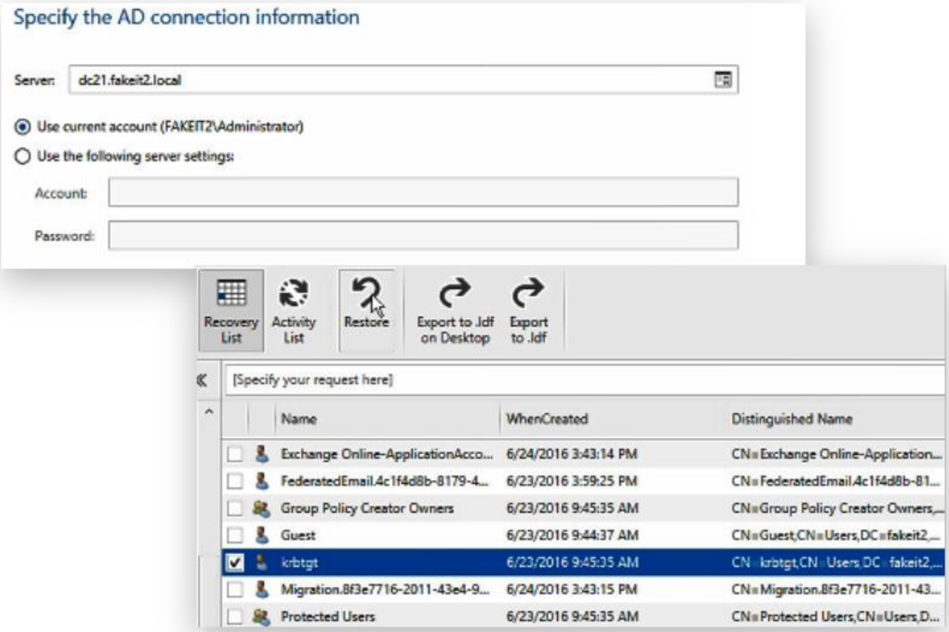


Restore Wizard

Select granular items to browse

- Exchange10-SQL
  - Exchange [PRMGUISERVER]
  - ☑ ActiveDirectory [PRMGUISERVER.prmgui.local]
    - DC=prmgui,DC=local
    - CN=Configuration,DC=prmgui,DC=local
    - CN=Schema,CN=Configuration,DC=prmgui,DC=local
    - DC=DomainDnsZones,DC=prmgui,DC=local
    - DC=ForestDnsZones,DC=prmgui,DC=local

3. Suppose, you want to restore a specific user, which has been accidentally deleted. Select this user, and export to .ldf file to later add it to your Active Directory Server. It would be much easier, however, to connect to this server and restore the selected objects directly there.



Specify the AD connection information

Server: dc21.fakeit2.local

● Use current account (FAKEIT2\Administrator)

○ Use the following server settings:

Account:

Password:

[Specify your request here]

	Name	WhenCreated	Distinguished Name
□	Exchange Online-ApplicationAcco...	6/24/2016 3:43:14 PM	CN=Exchange Online-Application...
□	FederatedEmail.4c1f4d8b-8179-4...	6/23/2016 3:59:25 PM	CN=FederatedEmail.4c1f4d8b-81...
□	Group Policy Creator Owners	6/23/2016 9:45:35 AM	CN=Group Policy Creator Owners,...
□	Guest	6/23/2016 9:44:37 AM	CN=Guest,CN=Users,DC=fakeit2,...
☑	krbtgt	6/23/2016 9:45:35 AM	CN=krbtgt,CN=Users,DC=fakeit2,...
□	Migration.8f3e7716-2011-43e4-9...	6/24/2016 3:43:15 PM	CN=Migration.8f3e7716-2011-43...
□	Protected Users	6/23/2016 9:45:35 AM	CN=Protected Users,CN=Users,D...

Launching VM Backup

Paragon VM BACKUP comes with V-LAUNCH component, which helps you minimize downtime of a failed production system by running a virtual machine directly from one of available restore points. This way users may continue their activities, while you've got enough time to pinpoint and fix the failed system.

When a backup failover operation is being performed, Paragon VM BACKUP creates an NFS (Network File System) datastore on the specified ESX host and a special temporary restore point to the selected backup image. Then it maps the restore point to the NFS datastore and configures a virtual machine that uses it as disk storage. Since there is no need to extract and copy the image contents to specific location, the whole operation takes a couple of minutes.

All changes are stored to the temporary restore point and discarded once the launch backup operation has stopped. It's ok if using this feature for testing purposes just to make sure the target OS and applications are functioning properly. But if you’re planning to use it in a real disaster recovery scenario, you obviously need to save the changes and complete the restore job. There are several options for you:

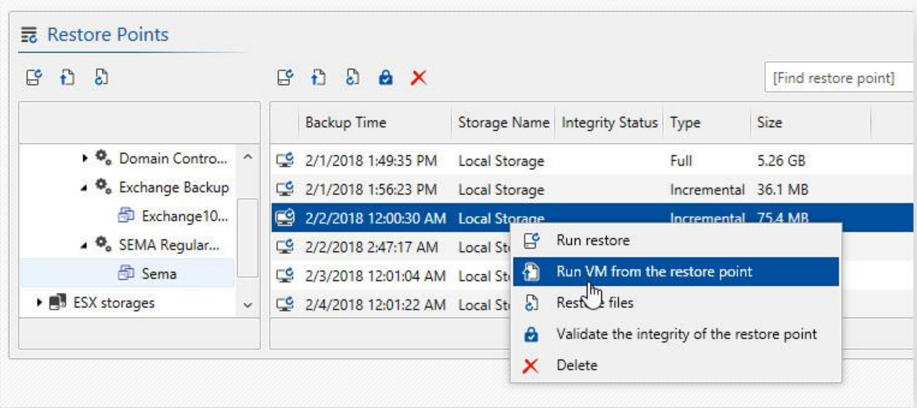
- Migrate the launched machine to production storage through the VMware vMotion technology (no downtime at all);
- Replicate the launched machine to fail over to it when most appropriate (some downtime is inevitable).

Machines launched out of backup may take plenty of system resources (CPU, RAM, disk IO), thus please do not forget to stop these machines.

Prerequisites:

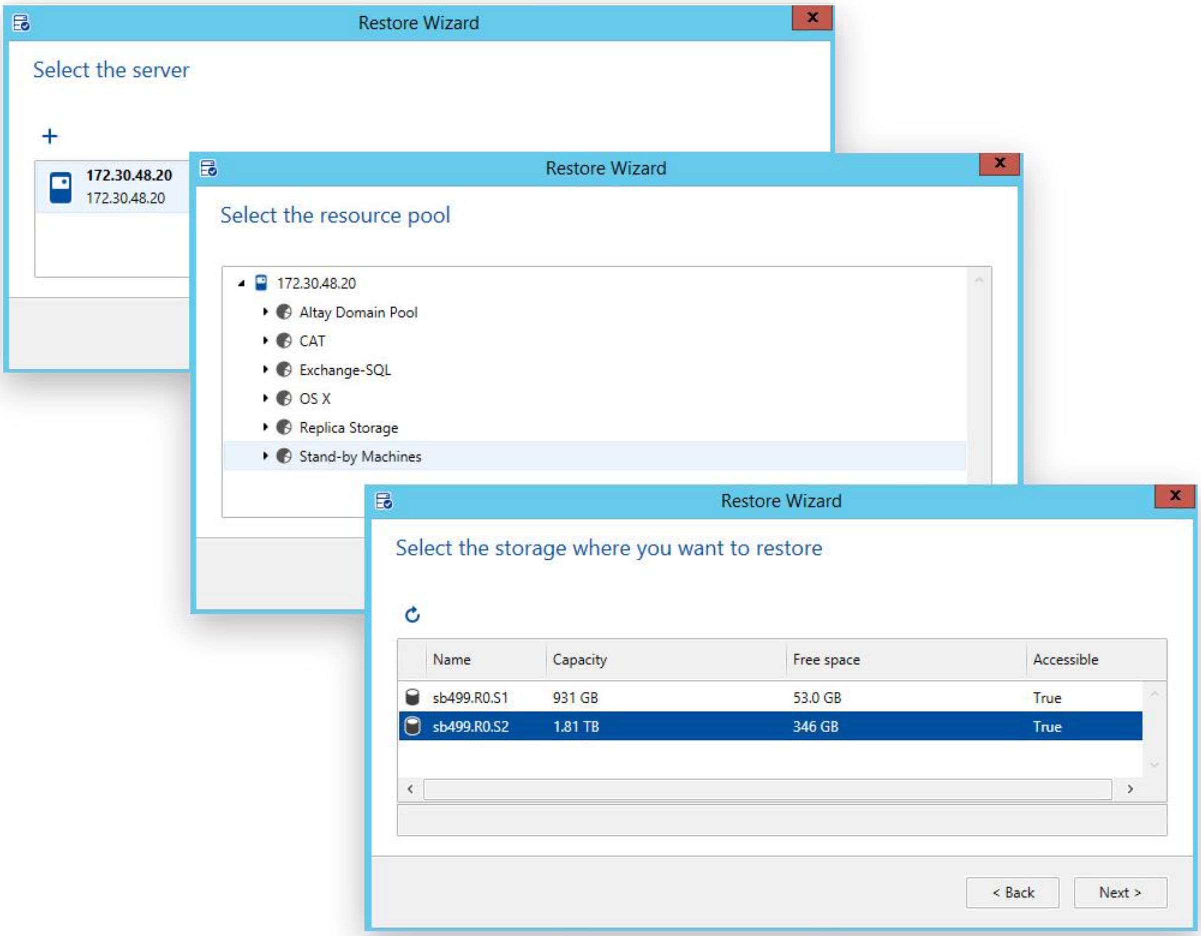
- Make sure the Launch Backup Requirements are met before you start.

1. Open the Backups view, browse an existing backup storage for a virtual machine in the 'Restore Points' pane, right click the required restore point, then select **Run VM from the restore point**. If launching the wizard some other way, you may need to choose a desired VM and restore point, if several.



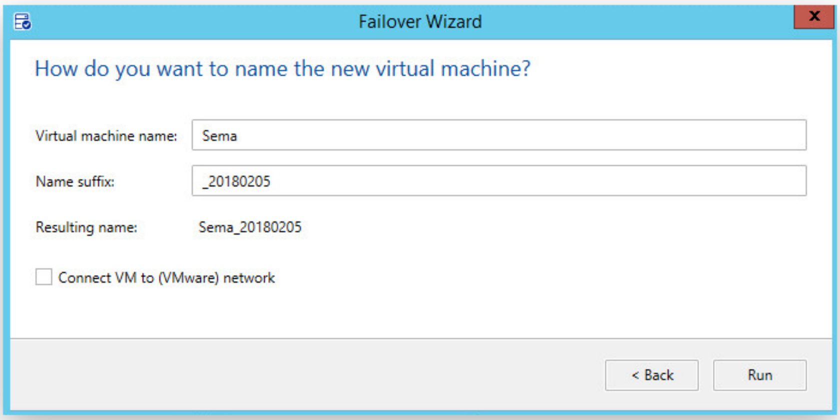
Backup Time	Storage Name	Integrity Status	Type	Size
2/1/2018 1:49:35 PM	Local Storage		Full	5.26 GB
2/1/2018 1:56:23 PM	Local Storage		Incremental	36.1 MB
2/2/2018 12:00:30 AM	Local Storage		Incremental	75.4 MB
2/2/2018 2:47:17 AM	Local St			
2/3/2018 12:01:04 AM	Local St			
2/4/2018 12:01:22 AM	Local St			

2. Specify the target ESX host, resource pool and datastore to host the launched VM.



Name	Capacity	Free space	Accessible
sb499.R0.S1	931 GB	53.0 GB	True
sb499.R0.S2	1.81 TB	346 GB	True

3. By default, the network support on the target machine is disabled to avoid possible problems of having two identical machines in one network environment. At this stage you can also change the default machine name. When done with the configuration, click **Run**, then complete the wizard.



Failover Wizard

How do you want to name the new virtual machine?

Virtual machine name: Sema

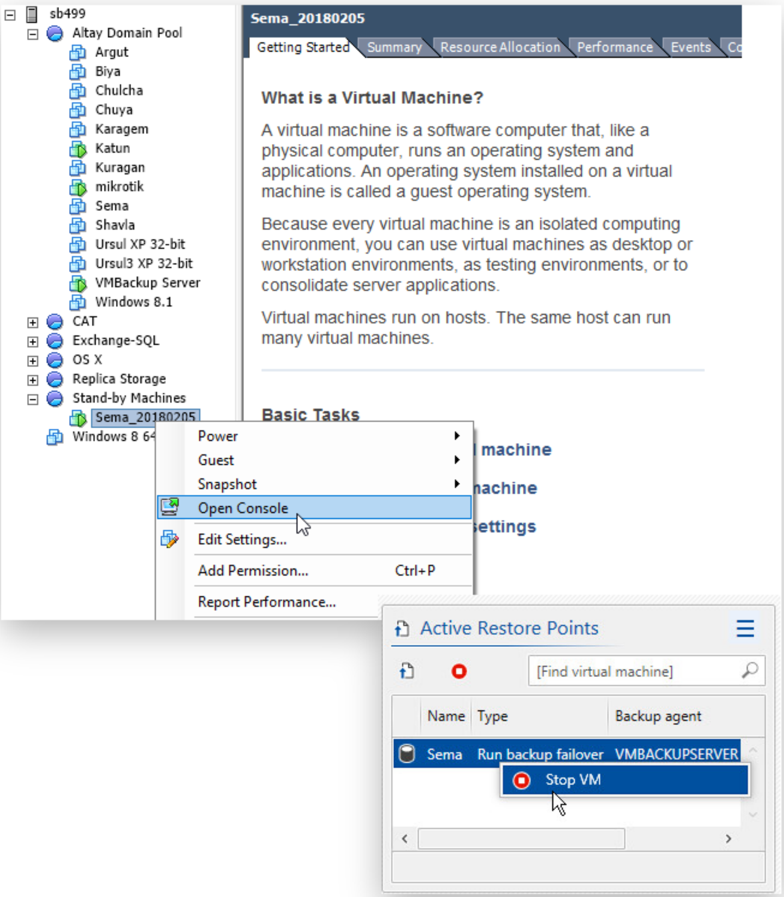
Name suffix: _20180205

Resulting name: Sema_20180205

☐ Connect VM to (VMware) network

4. When the operation is over you can find the resulted machine in the online state in the specified resource pool. Check that the VM works as required.

   A corresponding new item will also appear in the ‘Active Restore Points’ pane. When you’re done with the validation or disaster recovery procedures, right click the launched machine, then select **Stop VM** to power it off and delete from the datastore.



What is a Virtual Machine?

A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. An operating system installed on a virtual machine is called a guest operating system.

Because every virtual machine is an isolated computing environment, you can use virtual machines as desktop or workstation environments, as testing environments, or to consolidate server applications.

Virtual machines run on hosts. The same host can run many virtual machines.

Active Restore Points

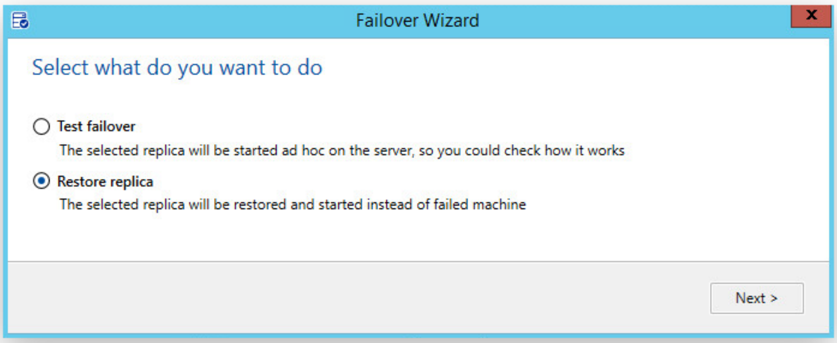
[Find virtual machine]

Name	Type	Backup agent
Sema	Run backup failover	VMBACKUPSERVER

Failing over to VM Replica

In case of emergency you can get a problem virtual machine back on track by failing over to one of its replicas, this way a replicated machine takes over the role of the original production machine. You’ve got the option to fail over to any available restore point. The whole operation may take a couple of seconds only.

This scenario is similar to Running Replica Test Failover, except for step 2, where you need to choose the **Restore Replica** scenario.



Failover Wizard

Select what do you want to do

○ Test failover
The selected replica will be started ad hoc on the server, so you could check how it works

● Restore replica
The selected replica will be restored and started instead of failed machine

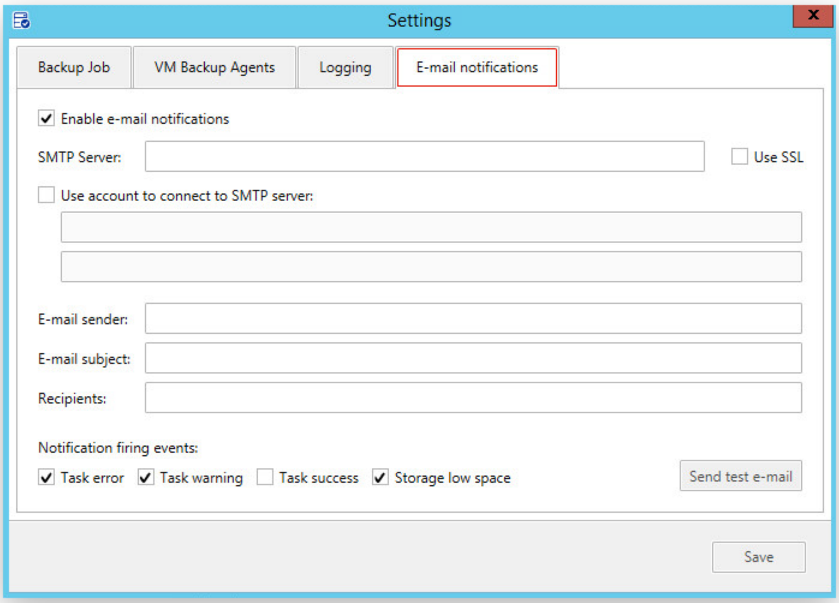
Please do not fail over to replicas in the vSphere interface, but use our program. Otherwise, all incremental updates created by Paragon VM BACKUP since the start of the launched this way replica will be corrupted.

Please do not delete replicas in the vSphere interface, but use our program. Otherwise, you won't be able to do replicas again to the specified ESX storage.

Configuring E-mail Notifications

Paragon VM BACKUP can be set up to notify you by e-mail about specific backup infrastructure events. You can create your notification policy and configure the e-mail transport in the general application settings.

1. Go to **Menu > Settings**, then click **E-mail notifications**.
2. Enable notifications and specify the e-mail transport parameters.



Settings

☑ Enable e-mail notifications

SMTP Server: □ Use SSL

□ Use account to connect to SMTP server:

E-mail sender:

E-mail subject:

Recipients:

Notification firing events:

☑ Task error ☑ Task warning □ Task success ☑ Storage low space

- **SMTP Server**. To send notifications, it is necessary to have access to a computer running an SMTP (Simple Mail Transfer Protocol) server. All outgoing messages are first sent to this server, which then delivers them to recipients. The address may be represented as a traditional Internet host name (e.g.: smtp.gmail.com) or as an IP numeric address (e.g. xxx.xxx.xxx.xx).

- **Use SSL** (Secure Socket Layer). If necessary, activate the option to establish a secure connection to the email server.
- **Use account to connect to SMTP Server**. If necessary, activate the option to allow the program to authenticate on the SMTP server before sending messages, then provide valid user credentials in the corresponding fields.
- **E-mail sender**. Enter an e-mail from which notifications should be sent.
- **E-mail subject**. Enter an e-mail subject to help in easy identification of received notifications.
- **Recipients**. Enter one or several e-mail recipients. Use a semicolon to separate multiple addresses.

3. Select task events you'd like to be notified about (errors, warnings, success, storage low space).
4. When you're done with the configuration, check notifications can reach destination mailbox(s) by clicking the corresponding button. You don't need to reply to the test email. Click **Save** to complete.

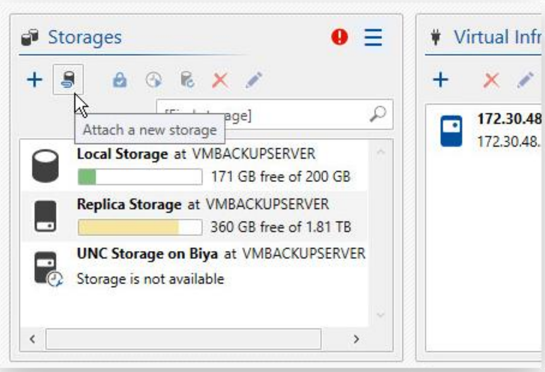
Attaching Storages

You can attach storages from another Paragon VM BACKUP infrastructure or those you have detached previously and use backup data they contain.

- Deploy an additional VM BACKUP SERVER or use an existing one on a machine that contains the required storage, then attach this storage as a local storage.
- Use an existing VM BACKUP SERVER to attach the required storage as a network storage.
- Deploy an additional VM BACKUP SERVER or use an existing one to attach ESX storage.

To avoid any conflicts, make sure the storage you're going to attach is not registered in some other backup infrastructure. If it is registered, then detach this storage before you continue.

1. Click the corresponding icon in the 'Storages' pane, located in the Home view (also the Environment view).



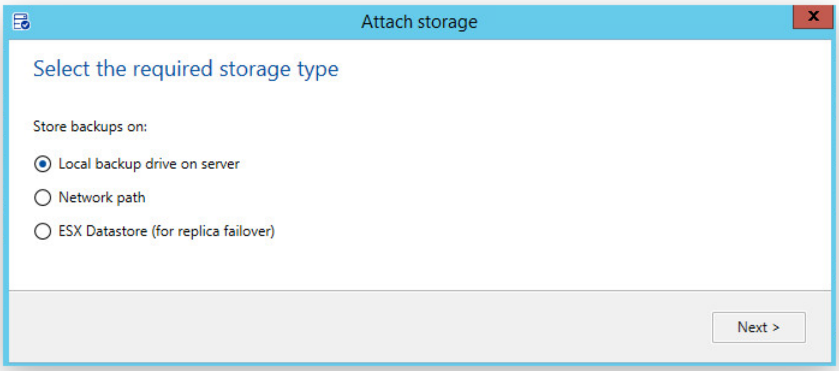
Local Storage at VMBACKUPSERVER
171 GB free of 200 GB

Replica Storage at VMBACKUPSERVER
360 GB free of 1.81 TB

UNC Storage on Biya at VMBACKUPSERVER
Storage is not available

172.30.48
172.30.48.

2. First you need to choose type of the storage you're going to attach (local, network, or ESX). Depending on your choice, the wizard will guide you through the necessary scenario.



Attach storage

Select the required storage type

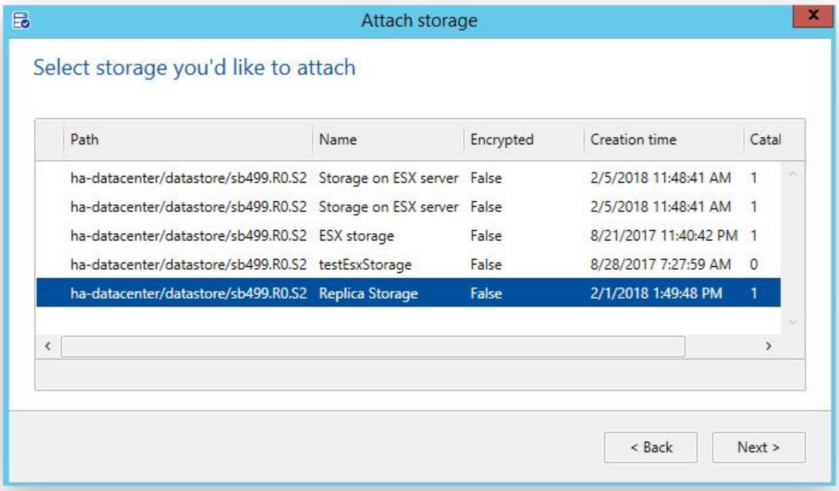
Store backups on:

● Local backup drive on server

○ Network path

○ ESX Datastore (for replica failover)

3. If there are several storages in the specified location, you will be prompted to choose the desired object. To help you make the right choice it also outputs a number of storage properties at this stage.

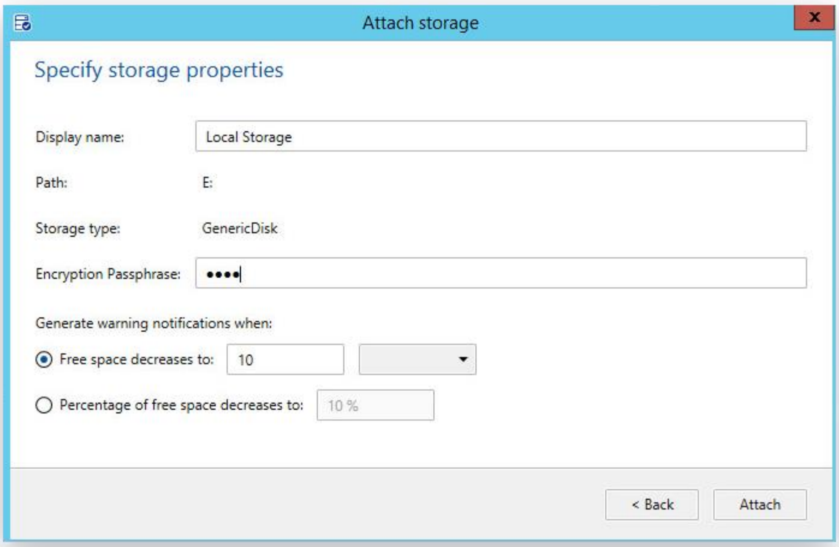


Attach storage

Select storage you'd like to attach

Path	Name	Encrypted	Creation time	Catal
ha-datacenter/datastore/sb499.R0.S2	Storage on ESX server	False	2/5/2018 11:48:41 AM	1
ha-datacenter/datastore/sb499.R0.S2	Storage on ESX server	False	2/5/2018 11:48:41 AM	1
ha-datacenter/datastore/sb499.R0.S2	ESX storage	False	8/21/2017 11:40:42 PM	1
ha-datacenter/datastore/sb499.R0.S2	testEsxStorage	False	8/28/2017 7:27:59 AM	0
ha-datacenter/datastore/sb499.R0.S2	Replica Storage	False	2/1/2018 1:49:48 PM	1

4. You will need to provide a password when attempting to attach an encrypted storage. You may also want to edit the old storage name and the storage space notification policy. Click **Attach** when ready.



Attach storage

Specify storage properties

Display name: Local Storage

Path: E:

Storage type: GenericDisk

Encryption Passphrase: ••••

Generate warning notifications when:

● Free space decreases to: 10

○ Percentage of free space decreases to: 10 %

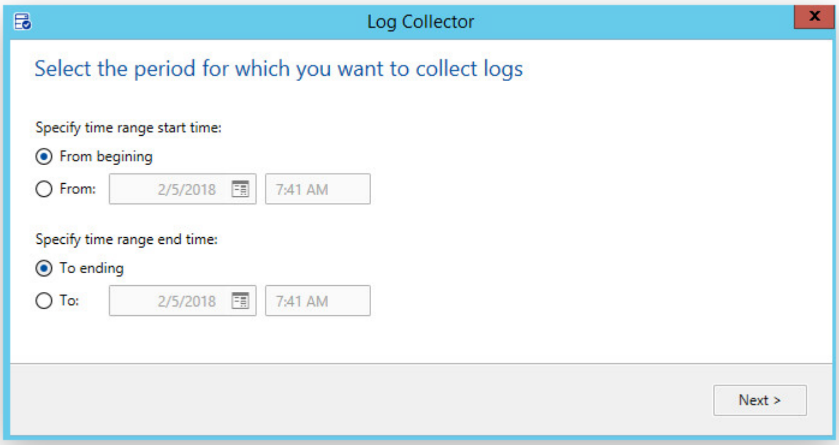
Troubleshooting

In case of having difficulties with handling Paragon VM BACKUP you can address our support engineers for assistance. To submit a support ticket, first you need to collect operation logs.

1. Reproduce your issue (make it happen again).

2. Go to **Menu > Collect logs**.

3. If you know when the encountered problem first started, please specify a time period to collect logs for. That will help you to minimize the created logs package. If you're not sure, leave the default option as is. Please note that the entire logs database may be several gigabytes in size.

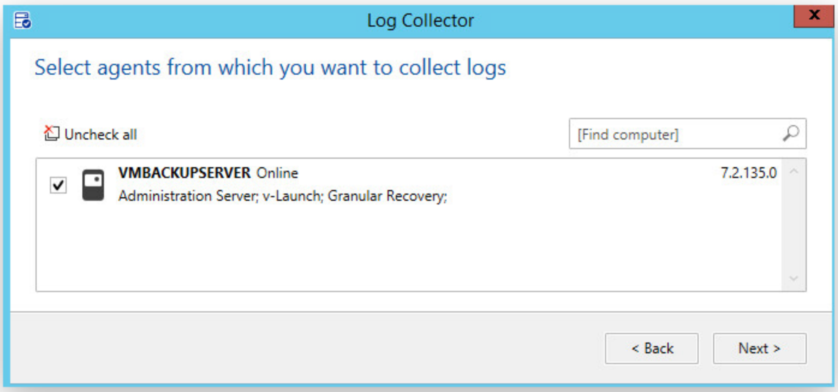


Select the period for which you want to collect logs

Specify time range start time:
● From begining
○ From: 2/5/2018 7:41 AM

Specify time range end time:
● To ending
○ To: 2/5/2018 7:41 AM

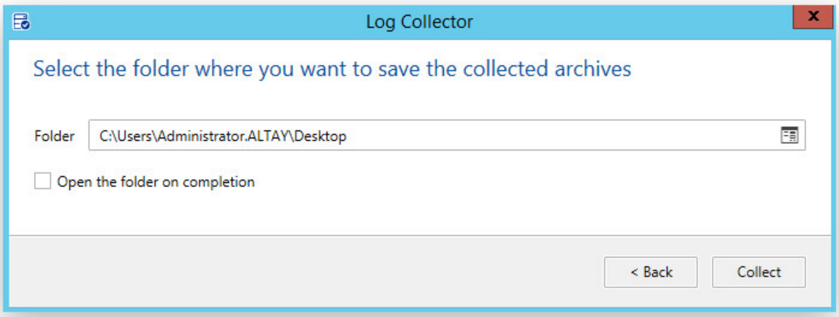
4. If you're having several machines with installed product components (the distributed deployment scenario), you can remove those, which logs you're not interested in. Please note logs from VM BACKUP SERVER can help to figure out and resolve 90% of issues.



Select agents from which you want to collect logs

☑ **VMBACKUPSERVER** Online 7.2.135.0
Administration Server; v-Launch; Granular Recovery;

5. Browse to a place where you'd like to save the logs to. If you'd like Windows Explorer to open in the specified folder once the operation is over, additionally mark the corresponding option. Click **Collect** to initiate the operation.



Select the folder where you want to save the collected archives

Folder C:\Users\Administrator.ALTAY\Desktop

□ Open the folder on completion

Log files do not contain any confidential information on the operating system settings or the user documents.

Appendix

vSphere VMs Management Privileges

The security model of VMware allows much flexibility in limiting access and management rights of any object of the virtual infrastructure. In vSphere 5.0 for instance, there are distinguished 255 privileges. To do backup, restore and other tasks on ESX guest machines, Paragon VM BACKUP may require up to 50 privileges.

Depending on tasks you're going to accomplish with Paragon VM BACKUP, you can create one or several users in vSphere or modify already existed users according to the information above. For instance, the standard user 'VMBackupUser2' can well be used to do backup of virtual machines. If you don't want to waste time on configuring users with specific privileges, you can use an administrative account of the datacenter you're going to manage + add it the 'Global.Licenses' privilege.

Only one account is allowed to use for one virtual server connection, thus if you need to back up and restore VMs for instance, you need to provide an account that cover privileges for both operations.

Let's see what privileges are needed for each type of operations:

Privilege	**Backup**	**Align**	**Store**	**Restore**
Category 'Global'				
Global.CancelTask	+	+	+	+
Global.Licenses	+	+	+	+
Category 'Folder'				
Folder.Create	-	-	+	+
Folder.Delete	-	-	+	+
Category 'Datastore'				
Datastore.Browse	+	+	+	+
Datastore.FileManagement	+	+	+	+
Datastore.AllocateSpace	+	+	+	+
Datastore.UpdateVirtualMachineFiles	-	+	+	+
Category 'Network'				
Network.Assign	-	-	-	+
Category 'Host > Configuration'				
Host.Config.Storage	+	+	+	+
Category 'Virtual machine > Inventory'				
VirtualMachine.Inventory.Create	-	-	+	+
VirtualMachine.Inventory.Delete	-	-	+	+

VirtualMachine.Inventory.Move	-	-	-	+
Category 'Virtual machine > Interaction'				
VirtualMachine.Interact.PowerOn	-	+	-	+
VirtualMachine.Interact.PowerOff	-	+	-	+
VirtualMachine.Interact.DeviceConnection	-	-	+	+
Category 'Virtual machine > Configuration'				
VirtualMachine.Config.Rename	-	-	+	+
VirtualMachine.Config.AddExistingDisk	-	-	+	+
VirtualMachine.Config.AddNewDisk	-	-	+	+
VirtualMachine.Config.RemoveDisk	-	-	+	+
VirtualMachine.Config.CPUCount	-	-	+	+
VirtualMachine.Config.Memory	-	-	+	+
VirtualMachine.Config.AddRemoveDevice	-	-	+	+
VirtualMachine.Config.Settings	+	+	+	+
VirtualMachine.Config.Resource	-	+	+	+
VirtualMachine.Config.DiskLease	+	+	+	+
VirtualMachine.Config.ChangeTracking	+	-	-	-
Category 'Virtual machine > State'				
VirtualMachine.State.CreateSnapshot	+	+	+	+
VirtualMachine.State.RevertToSnapshot	-	+	+	+
VirtualMachine.State.RemoveSnapshot	+	+	+	+
VirtualMachine.State.RenameSnapshot	+	+	+	+
Category 'Virtual machine > Provisioning'				
VirtualMachine.Provisioning.Clone	-	-	-	+
VirtualMachine.Provisioning.DiskRandomAccess	-	+	+	+
VirtualMachine.Provisioning.DiskRandomRead	+	+	+	+
Category 'Resource'				
Resource.AssignVMToPool	-	-	+	+
Resource.CreatePool	-	-	+	+
Resource.RenamePool	-	-	+	+
Resource.EditPool	+	+	+	+
Resource.DeletePool	-	-	+	-

Resource.HotMigrate	-	-	-	+
Resource.ColdMigrate	-	-	-	+

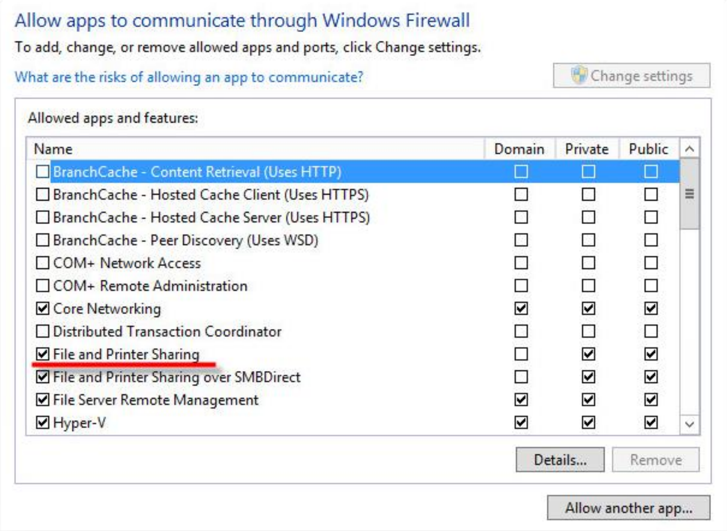
If you'd like to know how to create users with specific privileges in vSphere, please consult VMware Documentation.

Launch Backup Requirements

1. Access credentials used for creating a virtual server connection must have permissions to create an NFS datastore.
2. A machine running VM BACKUP AGENT that hosts backup storage should have enough free space on C: to store VM RAM cache (from 8 GB).
3. An NFS port on VM BACKUP SERVER should not be busy by some other third-party tool.
4. Access to NFS Server should be allowed in Firewall on VM BACKUP SERVER.

Exchange VM Backup Requirements

1. VM BACKUP AGENT is able to reach the Exchange Server VM by network.
2. The "File and Printing Sharing" service should be allowed in Firewall on the Exchange Server VM.



Allow apps to communicate through Windows Firewall

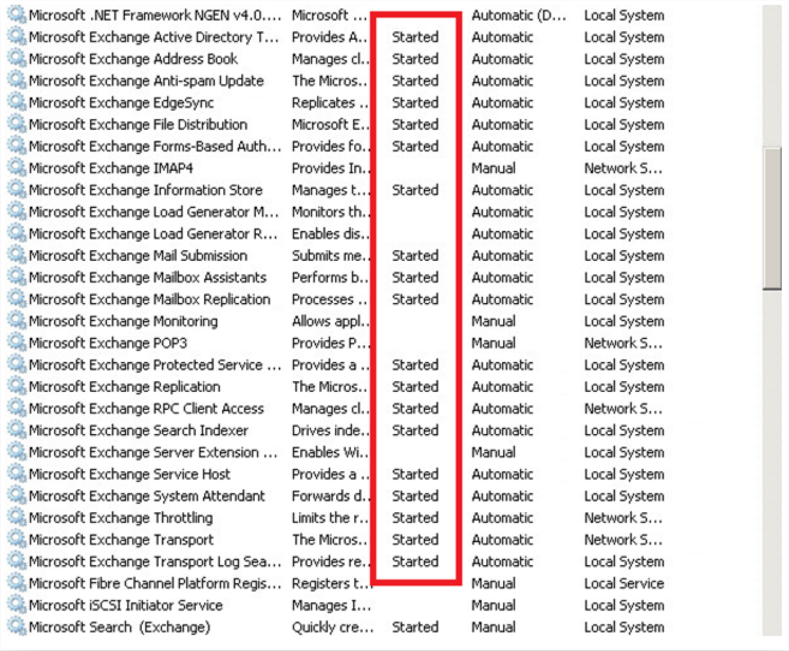
To add, change, or remove allowed apps and ports, click Change settings.

What are the risks of allowing an app to communicate?

Allowed apps and features:

Name	Domain	Private	Public
☐ BranchCache - Content Retrieval (Uses HTTP)	☐	☐	☐
☐ BranchCache - Hosted Cache Client (Uses HTTPS)	☐	☐	☐
☐ BranchCache - Hosted Cache Server (Uses HTTPS)	☐	☐	☐
☐ BranchCache - Peer Discovery (Uses WSD)	☐	☐	☐
☐ COM+ Network Access	☐	☐	☐
☐ COM+ Remote Administration	☐	☐	☐
☑ Core Networking	☑	☑	☑
☐ Distributed Transaction Coordinator	☐	☐	☐
☑ File and Printer Sharing	☐	☑	☑
☑ File and Printer Sharing over SMBDirect	☐	☑	☑
☑ File Server Remote Management	☑	☑	☑
☑ Hyper-V	☑	☑	☑

3. All Exchange services with the automatic start type should work properly.



Microsoft .NET Framework NGEN v4.0....	Microsoft ...		Automatic (D...	Local System
Microsoft Exchange Active Directory T...	Provides A..	Started	Automatic	Local System
Microsoft Exchange Address Book	Manages cl..	Started	Automatic	Local System
Microsoft Exchange Anti-spam Update	The Micros..	Started	Automatic	Local System
Microsoft Exchange EdgeSync	Replicates ..	Started	Automatic	Local System
Microsoft Exchange File Distribution	Microsoft E..	Started	Automatic	Local System
Microsoft Exchange Forms-Based Auth...	Provides fo..	Started	Automatic	Local System
Microsoft Exchange IMAP4	Provides In..		Manual	Network S...
Microsoft Exchange Information Store	Manages t...	Started	Automatic	Local System
Microsoft Exchange Load Generator M...	Monitors th..		Automatic	Local System
Microsoft Exchange Load Generator R...	Enables dis..		Automatic	Local System
Microsoft Exchange Mail Submission	Submits me..	Started	Automatic	Local System
Microsoft Exchange Mailbox Assistants	Performs b..	Started	Automatic	Local System
Microsoft Exchange Mailbox Replication	Processes ..	Started	Automatic	Local System
Microsoft Exchange Monitoring	Allows appl..		Manual	Local System
Microsoft Exchange POP3	Provides P...		Manual	Network S...
Microsoft Exchange Protected Service ...	Provides a ..	Started	Automatic	Local System
Microsoft Exchange Replication	The Micros..	Started	Automatic	Local System
Microsoft Exchange RPC Client Access	Manages cl..	Started	Automatic	Network S...
Microsoft Exchange Search Indexer	Drives inde..	Started	Automatic	Local System
Microsoft Exchange Server Extension ...	Enables Wi..		Manual	Local System
Microsoft Exchange Service Host	Provides a ..	Started	Automatic	Local System
Microsoft Exchange System Attendant	Forwards d..	Started	Automatic	Local System
Microsoft Exchange Throttling	Limits the r...	Started	Automatic	Network S...
Microsoft Exchange Transport	The Micros..	Started	Automatic	Network S...
Microsoft Exchange Transport Log Sea...	Provides re..	Started	Automatic	Local System
Microsoft Fibre Channel Platform Regis...	Registers t...		Manual	Local Service
Microsoft iSCSI Initiator Service	Manages I...		Manual	Local System
Microsoft Search (Exchange)	Quickly cre...	Started	Manual	Local System

4. The VSS Microsoft Exchange Writer should not have “retryable errors”. You can check it in Command Prompt:

```
vssadmin list writers

Writer name: 'Microsoft Exchange Writer'

  Writer Id: {76fe1ac4-15f7-4bcd-987e-8e1acb462fb7}

  Writer Instance Id: {e1d2d130-2123-46c9-a6d8-8b6af95158e8}

  State: [8] Failed

  Last error: Retryable error
```