Backup Service

Version 7.9

USER'S GUIDE

Revision: 4/17/2019

Table of contents

1 About the backup service

This service enables backup and recovery of physical and virtual machines, files, and databases to local or cloud storage.

This service is available through a web interface called the backup console.

2 Software requirements

2.1 Supported web browsers

The web interface supports the following web browsers:

- Google Chrome 29 or later
- Mozilla Firefox 23 or later
- Opera 16 or later
- Windows Internet Explorer 10 or later
- Microsoft Edge 25 or later
- Safari 8 or later running in the macOS and iOS operating systems

In other web browsers (including Safari browsers running in other operating systems), the user interface might be displayed incorrectly or some functions may be unavailable.

2.2 Supported operating systems and environments

Agent for Windows

Windows XP Professional SP1 (x64), SP2 (x64), SP3 (x86)

Windows Server 2003 SP1/2003 R2 and later – Standard and Enterprise editions (x86, x64)

Windows Small Business Server 2003/2003 R2

Windows Vista – all editions

Windows Server 2008 – Standard, Enterprise, Datacenter, and Web editions (x86, x64)

Windows Small Business Server 2008

Windows 7 – all editions

Windows Server 2008 R2 – Standard, Enterprise, Datacenter, Foundation, and Web editions

Windows MultiPoint Server 2010/2011/2012

Windows Small Business Server 2011 – all editions

Windows 8/8.1 – all editions (x86, x64), except for the Windows RT editions

Windows Server 2012/2012 R2 – all editions

Windows Storage Server 2003/2008/2008 R2/2012/2012 R2/2016

Windows 10 – Home, Pro, Education, Enterprise, and IoT Enterprise editions

Windows Server 2016 – all installation options, except for Nano Server

Windows Server 2019 – all installation options, except for Nano Server

Agent for SQL, Agent for Exchange, and Agent for Active Directory

Each of these agents can be installed on a machine running any operating system listed above and a supported version of the respective application.

Agent for Office 365

Windows Server 2008 – Standard, Enterprise, Datacenter, and Web editions (x64 only)

Windows Small Business Server 2008

Windows Server 2008 R2 – Standard, Enterprise, Datacenter, Foundation, and Web editions

Windows Small Business Server 2011 – all editions

Windows 8/8.1 – all editions (x64 only), except for the Windows RT editions

Windows Server 2012/2012 R2 – all editions

Windows Storage Server 2008/2008 R2/2012/2012 R2/2016 (x64 only)

Windows 10 – Home, Pro, Education, and Enterprise editions (x64 only)

Windows Server 2016 – all installation options (x64 only), except for Nano Server

Agent for Linux

Linux with kernel from 2.6.9 to 4.19.8 and glibc 2.3.4 or later

Various x86 and x86_64 Linux distributions, including:

- Red Hat Enterprise Linux 4.x, 5.x, 6.x, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6
- Ubuntu 9.10, 10.04, 10.10, 11.04, 11.10, 12.04, 12.10, 13.04, 13.10, 14.04, 14.10, 15.04, 15.10, 16.04, 16.10, 17.04, 17.10, 18.04, 18.10
- Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29
- SUSE Linux Enterprise Server 10 and 11
- SUSE Linux Enterprise Server 12 – supported on file systems, except for Btrfs
- Debian 4, 5, 6, 7.0, 7.2, 7.4, 7.5, 7.6, 7.7, 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.11, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 9.8
- CentOS 5.x, 6.x, 7, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6
- Oracle Linux 5.x, 6.x, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6 – both Unbreakable Enterprise Kernel and Red Hat Compatible Kernel
- CloudLinux 5.x, 6.x, 7, 7.1, 7.2, 7.3, 7.4, 7.5
- ClearOS 5.x, 6.x, 7, 7.1, 7.4
- ALT Linux 7.0

Before installing the product on a system that does not use RPM Package Manager, such as an Ubuntu system, you need to install this manager manually; for example, by running the following command (as the root user): **`apt-get install rpm`**

Agent for Mac

OS X Mavericks 10.9

OS X Yosemite 10.10

OS X El Capitan 10.11

macOS Sierra 10.12

macOS High Sierra 10.13

macOS Mojave 10.14

Agent for VMware (Virtual Appliance)

This agent is delivered as a virtual appliance for running on an ESXi host.

VMware ESXi 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7

Agent for VMware (Windows)

This agent is delivered as a Windows application for running in any operating system listed above for Agent for Windows with the following exceptions:

- 32-bit operating systems are not supported.
- Windows XP, Windows Server 2003/2003 R2, and Windows Small Business Server 2003/2003 R2 are not supported.

VMware ESXi 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7

Agent for Hyper-V

Windows Server 2008 (x64 only) with Hyper-V

Windows Server 2008 R2 with Hyper-V

Microsoft Hyper-V Server 2008/2008 R2

Windows Server 2012/2012 R2 with Hyper-V

Microsoft Hyper-V Server 2012/2012 R2

Windows 8, 8.1 (x64 only) with Hyper-V

Windows 10 – Pro, Education, and Enterprise editions with Hyper-V

Windows Server 2016 with Hyper-V – all installation options, except for Nano Server

Microsoft Hyper-V Server 2016

Agent for Virtuozzo

Virtuozzo 6.0.10, 6.0.11, 6.0.12

2.3 Supported Microsoft SQL Server versions

- Microsoft SQL Server 2017
- Microsoft SQL Server 2016
- Microsoft SQL Server 2014
- Microsoft SQL Server 2012
- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2008
- Microsoft SQL Server 2005

2.4 Supported Microsoft Exchange Server versions

- **Microsoft Exchange Server 2016 –** all editions.
- **Microsoft Exchange Server 2013** – all editions, Cumulative Update 1 (CU1) and later.
- **Microsoft Exchange Server 2010** – all editions, all service packs. Recovery of mailboxes and mailbox items is supported starting with Service Pack 1 (SP1).
- **Microsoft Exchange Server 2007** – all editions, all service packs. Recovery of mailboxes and mailbox items is not supported.

2.5 Supported Microsoft SharePoint versions

Backup Service supports the following Microsoft SharePoint versions:

- Microsoft SharePoint 2013

- Microsoft SharePoint Server 2010 SP1
- Microsoft SharePoint Foundation 2010 SP1
- Microsoft Office SharePoint Server 2007 SP2*
- Microsoft Windows SharePoint Services 3.0 SP2*

*In order to use SharePoint Explorer with these versions, you need a SharePoint recovery farm to attach the databases to.

The backups or databases from which you extract data must originate from the same SharePoint version as the one where SharePoint Explorer is installed.

2.6 Supported virtualization platforms

The following table summarizes how various virtualization platforms are supported.

Platform	Backup at a hypervisor level (agentless backup)	Backup from inside a guest OS
VMware		
VMware vSphere versions: 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7 **VMware vSphere editions:** VMware vSphere Essentials* VMware vSphere Essentials Plus* VMware vSphere Standard* VMware vSphere Advanced VMware vSphere Enterprise VMware vSphere Enterprise Plus	+	+
VMware vSphere Hypervisor (Free ESXi)**		+
VMware Server (VMware Virtual server) VMware Workstation VMware ACE VMware Player		+
Microsoft		
Windows Server 2008 (x64) with Hyper-V Windows Server 2008 R2 with Hyper-V Microsoft Hyper-V Server 2008/2008 R2 Windows Server 2012/2012 R2 with Hyper-V Microsoft Hyper-V Server 2012/2012 R2 Windows 8, 8.1 (x64) with Hyper-V Windows 10 with Hyper-V Windows Server 2016 with Hyper-V – all installation options, except for Nano Server Microsoft Hyper-V Server 2016	+	+

Platform	Backup at a hypervisor level (agentless backup)	Backup from inside a guest OS
Microsoft Virtual PC 2004 and 2007 Windows Virtual PC		+
Microsoft Virtual Server 2005		+
Citrix		
Citrix XenServer 4.1.5, 5.5, 5.6, 6.0, 6.1, 6.2, 6.5, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5		Only fully virtualized (aka HVM) guests
Red Hat and Linux		
Red Hat Enterprise Virtualization (RHEV) 2.2, 3.0, 3.1, 3.2, 3.3, 3.4, 3.5, 3.6 Red Hat Virtualization (RHV) 4.0, 4.1		+
Kernel-based Virtual Machines (KVM)		+
Parallels		
Parallels Workstation		+
Parallels Server 4 Bare Metal		+
Oracle		
Oracle VM Server 3.0, 3.3, 3.4		Only fully virtualized (aka HVM) guests
Oracle VM VirtualBox 4.x		+
Nutanix		
Nutanix Acropolis Hypervisor (AHV) 20160925.x through 20180425.x		+
Virtuozzo		
Virtuozzo 6.0.10, 6.0.11, 6.0.12	+	(Virtual machines only. Containers are not supported)
Amazon		
Amazon EC2 instances		+
Microsoft Azure		
Azure virtual machines		+

* In these editions, the HotAdd transport for virtual disks is supported on vSphere 5.0 and later. On version 4.1, backups may run slower.

** Backup at a hypervisor level is not supported for vSphere Hypervisor because this product restricts access to Remote Command Line Interface (RCLI) to read-only mode. The agent works during the vSphere Hypervisor evaluation period while no serial key is entered. Once you enter a serial key, the agent stops functioning.

Limitations

- **Fault tolerant machines**

  Agent for VMware backs up a fault tolerant machine only if fault tolerance was enabled in VMware vSphere 6.0 and later. If you upgraded from an earlier vSphere version, it is enough to disable and enable fault tolerance for each machine. If you are using an earlier vSphere version, install an agent in the guest operating system.

- **Independent disks and RDM**

  Agent for VMware does not back up Raw Device Mapping (RDM) disks in physical compatibility mode or independent disks. The agent skips these disks and adds warnings to the log. You can avoid the warnings by excluding independent disks and RDMs in physical compatibility mode from the backup plan. If you want to back up these disks or data on these disks, install an agent in the guest operating system.

- **Pass-through disks**

  Agent for Hyper-V does not back up pass-through disks. During backup, the agent skips these disks and adds warnings to the log. You can avoid the warnings by excluding pass-through disks from the backup plan. If you want to back up these disks or data on these disks, install an agent in the guest operating system.

- **Hyper-V guest clustering**

  Agent for Hyper-V does not support backup of Hyper-V virtual machines that are nodes of a Windows Server Failover Cluster. A VSS snapshot at the host level can even temporarily disconnect the external quorum disk from the cluster. If you want to back up these machines, install agents in the guest operating systems.

- **In-guest iSCSI connection**

  Agent for VMware and Agent for Hyper-V do not back up LUN volumes connected by an iSCSI initiator that works within the guest operating system. Because the ESXi and Hyper-V hypervisors are not aware of such volumes, the volumes are not included in hypervisor-level snapshots and are omitted from a backup without a warning. If you want to back up these volumes or data on these volumes, install an agent in the guest operating system.

- **Linux machines containing logical volumes (LVM)**

  Agent for VMware and Agent for Hyper-V do not support the following operations for Linux machines with LVM:

  - P2V migration, V2P migration, and V2V migration from Virtuozzo. Use Agent for Linux to create the backup and bootable media to recover.
  - Running a virtual machine from a backup created by Agent for Linux.

- **Encrypted virtual machines** (introduced in VMware vSphere 6.5)

  - Encrypted virtual machines are backed up in an unencrypted state. If encryption is critical to you, enable encryption of backups when creating a backup plan (p. 52).
  - Recovered virtual machines are always unencrypted. You can manually enable encryption after the recovery is complete.
  - If you back up encrypted virtual machines, we recommend that you also encrypt the virtual machine where Agent for VMware is running. Otherwise, operations with encrypted machines may be slower than expected. Apply the **VM Encryption Policy** to the agent's machine by using vSphere Web Client.
  - Encrypted virtual machines will be backed up via LAN, even if you configure the SAN transport mode for the agent. The agent will fall back on the NBD transport because VMware does not support SAN transport for backing up encrypted virtual disks.

- **Secure Boot** (introduced in VMware vSphere 6.5)

  Secure Boot is disabled after a virtual machine is recovered as a new virtual machine. You can manually enable this option after the recovery is complete.

- **ESXi configuration backup** is not supported for VMware vSphere 6.7.

2.7 Compatibility with encryption software

There are no limitations on backing up and recovering data that is encrypted by *file-level* encryption software.

Disk-level encryption software encrypts data on the fly. This is why data contained in the backup is not encrypted. Disk-level encryption software often modifies system areas: boot records, or partition tables, or file system tables. These factors affect disk-level backup and recovery, the ability of the recovered system to boot and access to Secure Zone.

You can back up the data encrypted by the following disk-level encryption software:

- Microsoft BitLocker Drive Encryption
- McAfee Endpoint Encryption
- PGP Whole Disk Encryption.

To ensure reliable disk-level recovery, follow the common rules and software-specific recommendations.

Common installation rule

The strong recommendation is to install the encryption software before installing the backup agents.

The way of using Secure Zone

Secure Zone must not be encrypted with disk-level encryption. This is the only way to use Secure Zone:

1. Install the encryption software; then, install the agent.
2. Create Secure Zone.
3. Exclude Secure Zone when encrypting the disk or its volumes.

Common backup rule

You can do a disk-level backup in the operating system.

Software-specific recovery procedures

Microsoft BitLocker Drive Encryption

To recover a system that was encrypted by BitLocker:

1. Boot from the bootable media.
2. Recover the system. The recovered data will be unencrypted.
3. Reboot the recovered system.
4. Turn on BitLocker.

If you only need to recover one partition of a multi-partitioned disk, do so under the operating system. Recovery under bootable media may make the recovered partition undetectable for Windows.

McAfee Endpoint Encryption and PGP Whole Disk Encryption

You can recover an encrypted system partition by using bootable media only.

If the recovered system fails to boot, rebuild Master Boot Record as described in the following Microsoft knowledge base article: https://support.microsoft.com/kb/2622803

3 Supported file systems

A backup agent can back up any file system that is accessible from the operating system where the agent is installed. For example, Agent for Windows can back up and recover an ext4 file system if the corresponding driver is installed in Windows.

The following table summarizes the file systems that can be backed up and recovered (bootable media supports only recovery). The limitations apply to both the agents and bootable media.

File system	Supported by			Limitations
	Agents	Bootable media for Windows and Linux	Bootable media for Mac	
FAT16/32	All agents	+	+	No limitations
NTFS		+	+	
ext2/ext3/ext4		+	-	
HFS+	Agent for Mac	-	+	
APFS		-	+	▪ Supported starting with macOS High Sierra 10.13 ▪ Disk configuration should be re-created manually when recovering to a non-original machine or bare metal.
JFS	Agent for Linux	+	-	Files cannot be excluded from a disk backup
ReiserFS3		+	-	
ReiserFS4		+	-	▪ Files cannot be excluded from a disk backup ▪ Volumes cannot be resized during a recovery
ReFS	All agents	+	+	
XFS		+	+	
Linux swap	Agent for Linux	+	-	No limitations

File system	Supported by			Limitations
	Agents	**Bootable media for Windows and Linux**	**Bootable media for Mac**	
exFAT	All agents	+ Bootable media cannot be used for recovery if the backup *is stored on* exFAT	+	- Only disk/volume backup is supported - Files cannot be excluded from a backup - Individual files cannot be recovered from a backup

The software automatically switches to the sector-by-sector mode when backing up drives with unrecognized or unsupported file systems. A sector-by-sector backup is possible for any file system that:

- is block-based
- spans a single disk
- has a standard MBR/GPT partitioning scheme

If the file system does not meet these requirements, the backup fails.

4 Activating the account

When an administrator creates an account for you, an email message is sent to your email address. The message contains the following information:

- **An account activation link.** Click the link and set the password for the account. Remember your login that is shown on the account activation page.
- **A link to the backup console login page.** Use this link to access the console in the future. The login and password are the same as in the previous step.

5 Accessing the backup service

You can log in to the backup service if you activated your account.

To log in to the backup service

1. Go to the backup service login page. The login page address was included in the activation email message.
2. Type the login, and then click **Continue**.
3. Type the password, and then click **Sign in**.
4. If you have the administrator role in the backup service, click **Backup & Disaster Recovery**.

   Users who do not have the administrator role log in directly to the backup console.

You can change the language of the web interface by clicking the account icon in the top-right corner.

If **Backup & Disaster Recovery** is not the only service you are subscribed to, you can switch between the services by using the ⊞ icon in the top-right corner. Administrators can also use this icon for switching to the management portal.

6 Installing the software

6.1 Preparation

Step 1

Choose an agent, depending on what you are going to back up. The following table summarizes the information, to help you decide.

Note that Agent for Windows is installed along with Agent for Exchange, Agent for SQL, Agent for VMware, Agent for Hyper-V, and Agent for Active Directory. If you install, for example, Agent for SQL, you also will be able to back up the entire machine where the agent is installed.

What are you going to back up?	Which agent to install?	Where to install it?
Physical machines		
Physical machines running Windows	Agent for Windows	On the machine that will be backed up.
Physical machines running Linux	Agent for Linux	
Physical machines running macOS	Agent for Mac	
Applications		
SQL databases	Agent for SQL	On the machine running Microsoft SQL Server.
Exchange databases	Agent for Exchange	On the machine running the Mailbox role of Microsoft Exchange Server.
Microsoft Office 365 mailboxes	Agent for Office 365	On a Windows machine that is connected to the Internet. Depending on the desired functionality, you may or may not need to install Agent for Office 365. For more information, refer to "Protecting Office 365 data" (p. 130).
Microsoft Office 365 OneDrive files and SharePoint Online sites	—	This data can be backed up only by an agent that is installed in the cloud. For more information, refer to "Protecting Office 365 data" (p. 130).
G Suite Gmail mailboxes, Google Drive files, and Team Drive files	—	This data can be backed up only by an agent that is installed in the cloud. For more information, refer to "Protecting G Suite" (p. 144).
Machines running Active Directory Domain Services	Agent for Active Directory	On the domain controller.
Virtual machines		

What are you going to back up?	Which agent to install?	Where to install it?
VMware ESXi virtual machines	Agent for VMware (Windows)	On a Windows machine that has network access to vCenter Server and to the virtual machine storage.*
	Agent for VMware (Virtual Appliance)	On the ESXi host.
Hyper-V virtual machines	Agent for Hyper-V	On the Hyper-V host.
Virtuozzo virtual machines and containers	Agent for Virtuozzo	On the Virtuozzo host.
Virtual machines hosted on Amazon EC2	The same as for physical machines**	On the machine that will be backed up.
Virtual machines hosted on Windows Azure		
Citrix XenServer virtual machines		
Red Hat Virtualization (RHV/RHEV)		
Kernel-based Virtual Machines (KVM)		
Oracle virtual machines		
Nutanix AHV virtual machines		
Mobile devices		
Mobile devices running Android	Mobile app for Android	On the mobile device that will be backed up.
Mobile devices running iOS	Mobile app for iOS	

*If your ESXi uses a SAN attached storage, install the agent on a machine connected to the same SAN. The agent will back up the virtual machines directly from the storage rather than via the ESXi host and LAN. For detailed instructions, refer to "Agent for VMware - LAN-free backup" (p. 170).

**A virtual machine is considered virtual if it is backed up by an external agent. If an agent is installed in the guest system, the backup and recovery operations are the same as with a physical machine. Nevertheless, the machine is counted as virtual when you set quotas for the number of machines.

Step 2

Review the system requirements for the agents.

Agent	Disk space occupied by the agent(s)
Agent for Windows	550 MB
Agent for Linux	500 MB
Agent for Mac	450 MB
Agent for SQL	600 MB (50 MB + 550 MB Agent for Windows)
Agent for Exchange	750 MB (200 MB + 550 MB Agent for Windows)
Agent for Office 365	550 MB

Agent for Active Directory	600 MB (50 MB + 550 MB Agent for Windows)
Agent for VMware	700 MB (150 MB + 550 MB Agent for Windows)
Agent for Hyper-V	600 MB (50 MB + 550 MB Agent for Windows)
Agent for Virtuozzo	500 MB

The typical memory consumption is 300 MB above the operating system and running applications. The peak consumption may reach 2 GB, depending on the amount and type of data being processed by the agents.

Bootable media or a disk recovery with a reboot requires at least 1 GB of memory.

Step 3

Download the setup program. To find the download links, click **All devices** > **Add**.

The **Add devices** page provides web installers for each agent that is installed in Windows. A web installer is a small executable file that downloads the main setup program from the Internet and saves it as a temporary file. This file is deleted immediately after the installation.

If you want to store the setup programs locally, download a package containing all agents for installation in Windows by using the link at the bottom of the **Add devices** page. Both 32-bit and 64-bit packages are available. These packages enable you to customize the list of components to install. These packages also enable unattended installation, for example, via Group Policy. This advanced scenario is described in Deploying agents through Group Policy.

To download Agent for Office 365 setup program, click the account icon in the top-right corner, and then click **Downloads** > **Agent for Office 365**.

Installation in Linux and macOS is performed from ordinary setup programs.

All setup programs require an Internet connection to register the machine in the backup service. If there is no Internet connection, the installation will fail.

Step 4

Before the installation, ensure that your firewalls and other components of your network security system (such as a proxy sever) allow both inbound and outbound connections through the following TCP ports:

- **443** and **8443** These ports are used for accessing the backup console, registering the agents, downloading the certificates, user authorization, and downloading files from the cloud storage.
- **7770...7800** The agents use these ports to communicate with the backup management server.
- **44445** The agents use this port for data transfer during backup and recovery.

If a proxy server is enabled in your network, refer to the "Proxy server settings" (p. 18) section to understand whether you need to configure these settings on each machine that runs a backup agent.

The minimum Internet connection speed required for managing an agent from the cloud is 1 Mbit/s (not to be confused with the data transfer rate acceptable for backing up to the cloud). Consider this if you use a low-bandwidth connection technology such as ADSL.

6.2 Proxy server settings

The backup agents can transfer data through an HTTP/HTTPS proxy server. The server must work through an HTTP tunnel without scanning or interfering with the HTTP traffic. Man-in-the-middle proxies are not supported.

Because the agent registers itself in the cloud during the installation, the proxy server settings must be provided during the installation or in advance.

In Windows

If a proxy server is configured in Windows (**Control panel** > **Internet Options** > **Connections**), the setup program reads the proxy server settings from the registry and uses them automatically. Also, you can enter the proxy settings during the installation, or specify them in advance by using the procedure described below. To change the proxy settings after the installation, use the same procedure.

To specify the proxy settings in Windows

1. Create a new text document and open it in a text editor, such as Notepad.
2. Copy and paste the following lines into the file:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\Global\HttpProxy]
"Enabled"=dword:00000001
"Host"="proxy.company.com"
"Port"=dword:000001bb
"Login"="proxy_login"
"Password"="proxy_password"
```

3. Replace `proxy.company.com` with your proxy server host name/IP address, and `000001bb` with the hexadecimal value of the port number. For example, `000001bb` is port 443.
4. If your proxy server requires authentication, replace `proxy_login` and `proxy_password` with the proxy server credentials. Otherwise, delete these lines from the file.
5. Save the document as **proxy.reg**.
6. Run the file as an administrator.
7. Confirm that you want to edit the Windows registry.
8. If the backup agent is not installed yet, you can now install it. Otherwise, do the following to restart the agent:
   a. In the **Start** menu, click **Run**, and then type: **cmd**
   b. Click **OK**.
   c. Run the following commands:

```
net stop mms
net start mms
```

In Linux

Run the installation file with the parameters **`--http-proxy-host=`**`ADDRESS` **`--http-proxy-port=`**`PORT` **`--http-proxy-login=`**`LOGIN` **`--http-proxy-password=`**`PASSWORD`. To change the proxy settings after the installation, use the procedure described below.

To change the proxy settings in Linux

1. Open the file **/etc/Acronis/Global.config** in a text editor.
2. Do one of the following:
   - If the proxy settings were specified during the agent installation, find the following section:

```
<key name="HttpProxy">
    <value name="Enabled" type="Tdword">"1"</value>
    <value name="Host" type="TString">"ADDRESS"</value>
    <value name="Port" type="Tdword">"PORT"</value>
    <value name="Login" type="TString">"LOGIN"</value>
    <value name="Password" type="TString">"PASSWORD"</value>
</key>
```

- Otherwise, copy the above lines and paste them into the file between the **`<registry name="Global">...</registry>`** tags.

3. Replace ADDRESS with the new proxy server host name/IP address, and PORT with the decimal value of the port number.
4. If your proxy server requires authentication, replace `LOGIN` and `PASSWORD` with the proxy server credentials. Otherwise, delete these lines from the file.
5. Save the file.
6. Restart the agent by executing the following command in any directory:

```
sudo service acronis_mms restart
```

In macOS

You can enter the proxy settings during the installation, or specify them in advance by using the procedure described below. To change the proxy settings after the installation, use the same procedure.

To specify the proxy settings in macOS

1. Create the file **/Library/Application Support/Acronis/Registry/Global.config** and open it in a text editor, such as Text Edit.
2. Copy and paste the following lines into the file:

```
<?xml version="1.0" ?>
<registry name="Global">
    <key name="HttpProxy">
        <value name="Enabled" type="Tdword">"1"</value>
        <value name="Host" type="TString">"proxy.company.com"</value>
        <value name="Port" type="Tdword">"443"</value>
        <value name="Login" type="TString">"proxy_login"</value>
        <value name="Password" type="TString">"proxy_password"</value>
    </key>
</registry>
```

3. Replace `proxy.company.com` with your proxy server host name/IP address, and 443 with the decimal value of the port number.
4. If your proxy server requires authentication, replace `proxy_login` and `proxy_password` with the proxy server credentials. Otherwise, delete these lines from the file.
5. Save the file.
6. If the backup agent is not installed yet, you can now install it. Otherwise, do the following to restart the agent:
   a. Go to **Applications** > **Utilities** > **Terminal**
   b. Run the following commands:

```
sudo launchctl stop acronis_mms
sudo launchctl start acronis_mms
```

6.3 Linux packages

To add the necessary modules to the Linux kernel, the setup program needs the following Linux packages:

- The package with kernel headers or sources. The package version must match the kernel version.
- The GNU Compiler Collection (GCC) compiler system. The GCC version must be the one with which the kernel was compiled.
- The Make tool.
- The Perl interpreter.
- The **`libelf-dev`**, **`libelf-devel`**, or **`elfutils-libelf-devel`** libraries for building kernels starting with 4.15 and configured with CONFIG_UNWINDER_ORC=y. For some distributions, such as Fedora 28, they need to be installed separately from kernel headers.

The names of these packages vary depending on your Linux distribution.

In Red Hat Enterprise Linux, CentOS, and Fedora, the packages normally will be installed by the setup program. In other distributions, you need to install the packages if they are not installed or do not have the required versions.

Are the required packages already installed?

To check whether the packages are already installed, perform these steps:

1. Run the following command to find out the kernel version and the required GCC version:

   ```
   cat /proc/version
   ```

   This command returns lines similar to the following: **`Linux version 2.6.35.6`** and **`gcc version 4.5.1`**
2. Run the following command to check whether the Make tool and the GCC compiler are installed:

   ```
   make -v
   gcc -v
   ```

   For **gcc**, ensure that the version returned by the command is the same as in the **`gcc version`** in step 1. For **make**, just ensure that the command runs.
3. Check whether the appropriate version of the packages for building kernel modules is installed:

   - In Red Hat Enterprise Linux, CentOS, and Fedora, run the following command:

     ```
     yum list installed | grep kernel-devel
     ```

   - In Ubuntu, run the following commands:

     ```
     dpkg --get-selections | grep linux-headers
     dpkg --get-selections | grep linux-image
     ```

   In either case, ensure that the package versions are the same as in **`Linux version`** in step 1.
4. Run the following command to check whether the Perl interpreter is installed:

   ```
   perl --version
   ```

   If you see the information about the Perl version, the interpreter is installed.
5. In Red Hat Enterprise Linux, CentOS, and Fedora, run the following command to check whether **`elfutils-libelf-devel`** is installed:

   ```
   yum list installed | grep elfutils-libelf-devel
   ```

   If you see the information about the library version, the library is installed.

Installing the packages from the repository

The following table lists how to install the required packages in various Linux distributions.

Linux distribution	Package names	How to install
Red Hat Enterprise Linux	**kernel-devel** **gcc** **make** **elfutils-libelf-devel**	The setup program will download and install the packages automatically by using your Red Hat subscription.
	perl	Run the following command: `yum install perl`
CentOS Fedora	**kernel-devel** **gcc** **make** **elfutils-libelf-devel**	The setup program will download and install the packages automatically.
	perl	Run the following command: `yum install perl`

Ubuntu
Debian
	linux-headers
	linux-image
	gcc
	make
	perl
		Run the following commands:
		`sudo apt-get update`
		`` sudo apt-get install linux-headers-`uname -r` ``
		`` sudo apt-get install linux-image-`uname -r` ``
		`sudo apt-get install gcc-<package version>`
		`sudo apt-get install make`
		`sudo apt-get install perl`

SUSE Linux
OpenSUSE
	kernel-source
	gcc
	make
	perl
		`sudo zypper install kernel-source`
		`sudo zypper install gcc`
		`sudo zypper install make`
		`sudo zypper install perl`

The packages will be downloaded from the distribution's repository and installed.

For other Linux distributions, please refer to the distribution's documentation regarding the exact names of the required packages and the ways to install them.

Installing the packages manually

You may need to install the packages **manually** if:

- The machine does not have an active Red Hat subscription or Internet connection.
- The setup program cannot find the **kernel-devel** or **gcc** version corresponding to the kernel version. If the available **kernel-devel** is more recent than your kernel, you need to either update the kernel or install the matching **kernel-devel** version manually.
- You have the required packages on the local network and do not want to spend time for automatic search and downloading.

Obtain the packages from your local network or a trusted third-party website, and install them as follows:

- In Red Hat Enterprise Linux, CentOS, or Fedora, run the following command as the root user:

  ```
  rpm -ivh PACKAGE_FILE1 PACKAGE_FILE2 PACKAGE_FILE3
  ```

- In Ubuntu, run the following command:

```
sudo dpkg -i PACKAGE_FILE1 PACKAGE_FILE2 PACKAGE_FILE3
```

Example: Installing the packages manually in Fedora 14

Follow these steps to install the required packages in Fedora 14 on a 32-bit machine:

1. Run the following command to determine the kernel version and the required GCC version:

   ```
   cat /proc/version
   ```

   The output of this command includes the following:

   ```
   Linux version 2.6.35.6-45.fc14.i686
   gcc version 4.5.1
   ```

2. Obtain the **kernel-devel** and **gcc** packages that correspond to this kernel version:

   ```
   kernel-devel-2.6.35.6-45.fc14.i686.rpm
   gcc-4.5.1-4.fc14.i686.rpm
   ```

3. Obtain the **make** package for Fedora 14:

   ```
   make-3.82-3.fc14.i686
   ```

4. Install the packages by running the following commands as the root user:

   ```
   rpm -ivh kernel-devel-2.6.35.6-45.fc14.i686.rpm
   rpm -ivh gcc-4.5.1.fc14.i686.rpm
   rpm -ivh make-3.82-3.fc14.i686
   ```

   You can specify all these packages in a single **rpm** command. Installing any of these packages may require installing additional packages to resolve dependencies.

6.4 Installing agents

In Windows

1. Ensure that the machine is connected to the Internet.
2. Log on as an administrator and start the setup program.
3. [Optional] Click **Customize installation settings** and make the appropriate changes if you want:
   - To verify or change the proxy server host name/IP address, port, and credentials. If a proxy server is enabled in Windows, it is detected and used automatically.
   - To change the installation path.
   - To change the account for the agent service.
4. Click **Install**.
5. [Only when installing Agent for VMware] Specify the address and access credentials for the vCenter Server or stand-alone ESXi host whose virtual machines the agent will back up, and then click **Done**. We recommend using an account that has the **Administrator** role assigned. Otherwise, provide an account with the necessary privileges (p. 173) on the vCenter Server or ESXi.
6. [Only when installing on a domain controller] Specify the user account under which the agent service will run, and then click **Done**. For security reasons, the setup program does not automatically create new accounts on a domain controller.
7. Wait until the registration screen appears.
8. Do one of the following:
   - Click **Register the machine**. In the opened browser window, sign in to the backup console, review the registration details, and then click **Confirm registration**.
   - Click **Show registration info**. The setup program shows the registration link and the registration code. You can copy them and perform the registration steps on a different

machine. In this case, you will need to enter the registration code in the registration form. The registration code is valid for one hour.

Alternatively, you can access the registration form by clicking **All devices** > **Add**, scrolling down to **Registration via code**, and then clicking **Register**.

Tip *Do not quit the setup program until you confirm the registration. To initiate the registration again, you will have to restart the setup program, and then click* ***Register the machine****.*

As a result, the machine will be assigned to the account that was used to log in to the backup console.

In Linux

1. Ensure that the machine is connected to the Internet.
2. As the root user, run the installation file.

   If a proxy server is enabled in your network, when running the file, specify the server host name/IP address and port in the following format: `--http-proxy-host=ADDRESS --http-proxy-port=PORT --http-proxy-login=LOGIN --http-proxy-password=PASSWORD`.
3. Select the check boxes for the agents that you want to install. The following agents are available:
   - **Agent for Linux**
   - **Agent for Virtuozzo**

   Agent for Virtuozzo cannot be installed without Agent for Linux.
4. Wait until the registration screen appears.
5. Do one of the following:
   - Click **Register the machine**. In the opened browser window, sign in to the backup console, review the registration details, and then click **Confirm registration**.
   - Click **Show registration info**. The setup program shows the registration link and the registration code. You can copy them and perform the registration steps on a different machine. In this case, you will need to enter the registration code in the registration form. The registration code is valid for one hour.

   Alternatively, you can access the registration form by clicking **All devices** > **Add**, scrolling down to **Registration via code**, and then clicking **Register**.

Tip *Do not quit the setup program until you confirm the registration. To initiate the registration again, you will have to restart the setup program and repeat the installation procedure.*

As a result, the machine will be assigned to the account that was used to log in to the backup console.

Troubleshooting information is provided in the file:
/usr/lib/Acronis/BackupAndRecovery/HOWTO.INSTALL

In macOS

1. Ensure that the machine is connected to the Internet.
2. Double-click the installation file (.dmg).
3. Wait while the operating system mounts the installation disk image.
4. Double-click **Install**.
5. If a proxy server is enabled in your network, click **Backup Agent** in the menu bar, click **Proxy server settings**, and then specify the proxy server host name/IP address, port, and credentials.
6. If prompted, provide administrator credentials.

7. Click **Continue**.
8. Wait until the registration screen appears.
9. Do one of the following:
   - Click **Register the machine**. In the opened browser window, sign in to the backup console, review the registration details, and then click **Confirm registration**.
   - Click **Show registration info**. The setup program shows the registration link and the registration code. You can copy them and perform the registration steps on a different machine. In this case, you will need to enter the registration code in the registration form. The registration code is valid for one hour.

   Alternatively, you can access the registration form by clicking **All devices** > **Add**, scrolling down to **Registration via code**, and then clicking **Register**.

   Tip *Do not quit the setup program until you confirm the registration. To initiate the registration again, you will have to restart the setup program and repeat the installation procedure.*

As a result, the machine will be assigned to the account that was used to log in to the backup console.

6.5 Deploying Agent for VMware (Virtual Appliance) from an OVF template

6.5.1 Before you start

System requirements for the agent

By default, the virtual appliance is assigned 4 GB of RAM and 2 vCPUs, which is optimal and sufficient for most operations. We recommend increasing these resources to 8 GB of RAM and 4 vCPUs if the backup traffic bandwidth is expected to exceed 100 MB per second (for example, in 10-GBit networks), in order to improve backup performance.

The appliance's own virtual disks occupy no more than 6 GB. Thick or thin disk format does not matter, it does not affect the appliance performance.

How many agents do I need?

Even though one virtual appliance is able to protect an entire vSphere environment, the best practice is deploying one virtual appliance per vSphere cluster (or per host, if there are no clusters). This makes for faster backups because the appliance can attach the backed-up disks by using the HotAdd transport, and therefore the backup traffic is directed from one local disk to another.

It is normal to use both the virtual appliance and Agent for VMware (Windows) at the same time, as long as they are connected to the same vCenter Server *or* they are connected to different ESXi hosts. Avoid cases when one agent is connected to an ESXi directly and another agent is connected to the vCenter Server which manages this ESXi.

We do not recommend using locally attached storage (i.e. storing backups on virtual disks added to the virtual appliance) if you have more than one agent. For more considerations, see "Using a locally attached storage" (p. 27).

Disable automatic DRS for the agent

If the virtual appliance is deployed to a vSphere cluster, be sure to disable automatic vMotion for it. In the cluster DRS settings, enable individual virtual machine automation levels, and then set **Automation level** for the virtual appliance to **Disabled**.

6.5.2 Deploying the OVF template

1. Click **All devices** > **Add** > **VMware ESXi** > **Virtual Appliance (OVF)**.

   The .zip archive is downloaded to your machine.
2. Unpack the .zip archive. The folder contains one .ovf file and two .vmdk files.
3. Ensure that these files can be accessed from the machine running the vSphere Client.
4. Start the vSphere Client and log on to the vCenter Server.
5. Deploy the OVF template.
   - When configuring storage, select the shared datastore, if it exists. Thick or thin disk format does not matter, as it does not affect the appliance performance.
   - When configuring network connections, be sure to select a network that allows an Internet connection, so that the agent can properly register itself in the cloud.

6.5.3 Configuring the virtual appliance

1. **Starting the virtual appliance**

   In the vSphere Client, display the **Inventory**, right-click the virtual appliance's name, and then select **Power** > **Power On**. Select the **Console** tab.
2. **Proxy server**

   If a proxy server is enabled in your network:

   a. To start the command shell, press CTRL+ALT+F2 while in the virtual appliance UI.

   b. Open the file **/etc/Acronis/Global.config** in a text editor.

   c. Find the following section:

   ```
   <key name="HttpProxy">
       <value name="Enabled" type="Tdword">"0"</value>
       <value name="Host" type="TString">"ADDRESS"</value>
       <value name="Port" type="Tdword">"PORT"</value>
       <value name="Login" type="TString">"LOGIN"</value>
       <value name="Password" type="TString">"PASSWORD"</value>
   </key>
   ```

   d. Replace **0** with **1**.

   e. Replace ADDRESS with the new proxy server host name/IP address, and PORT with the decimal value of the port number.

   f. If your proxy server requires authentication, replace LOGIN and PASSWORD with the proxy server credentials. Otherwise, delete these lines from the file.

   g. Save the file.

   h. Execute the **reboot** command.

   Otherwise, skip this step.
3. **Network settings**

   The agent's network connection is configured automatically by using Dynamic Host Configuration Protocol (DHCP). To change the default configuration, under **Agent options**, in **eth0**, click **Change** and specify the desired network settings.

4. **vCenter/ESX(i)**

   Under **Agent options**, in **vCenter/ESX(i)**, click **Change** and specify the vCenter Server name or IP address. The agent will be able to back up and recover any virtual machine managed by the vCenter Server.

   If you do not use a vCenter Server, specify the name or IP address of the ESXi host whose virtual machines you want to back up and recover. Normally, backups run faster when the agent backs up virtual machines hosted on its own host.

   Specify the credentials that the agent will use to connect to the vCenter Server or ESXi. We recommend using an account that has the **Administrator** role assigned. Otherwise, provide an account with the necessary privileges (p. 173) on the vCenter Server or ESXi.

   You can click **Check connection** to ensure the access credentials are correct.

5. **Management server**
   1. Under **Agent options**, in **Management Server**, click **Change**.
   2. In **Server name/IP**, select **Cloud**. The software displays the backup service address. Do not change this address unless instructed otherwise.
   3. In **User name** and **Password**, specify the user name and password for the backup service. The agent and the virtual machines managed by the agent will be registered under this account.

6. **Time zone**

   Under **Virtual machine**, in **Time zone**, click **Change**. Select the time zone of your location to ensure that the scheduled operations run at the appropriate time.

7. **[Optional] Local storages**

   You can attach an additional disk to the virtual appliance so the Agent for VMware can back up to this locally attached storage.

   Add the disk by editing the settings of the virtual machine and click **Refresh**. The **Create storage** link becomes available. Click this link, select the disk, and then specify a label for it.

6.5.4 Using a locally attached storage

You can attach an additional disk to Agent for VMware (Virtual Appliance) so the agent can back up to this locally attached storage. This approach eliminates the network traffic between the agent and the backup location.

A virtual appliance that is running on the same host or cluster with the backed-up virtual machines has direct access to the datastore(s) where the machines reside. This means the appliance can attach the backed-up disks by using the HotAdd transport, and therefore the backup traffic is directed from one local disk to another. If the datastore is connected as **Disk/LUN**, rather than **NFS**, the backup will be completely LAN-free. In the case of NFS datastore, there will be network traffic between the datastore and the host.

Using a locally attached storage presumes that the agent always backs up the same machines. Otherwise, if the machines are redistributed among the agents by the management server, a machine's backups may be dispersed over multiple storages. We do not recommend using a locally attached storage if you have more than one agent.

You can add the storage to an already working agent or when deploying the agent from an OVF template (p. 26).

To attach a storage to an already working agent

1. In VMware vSphere inventory, right click the Agent for VMware (Virtual Appliance).
2. Add the disk by editing the settings of the virtual machine. The disk size must be at least 10 GB.

Warning *Be careful when adding an already existing disk. Once the storage is created, all data previously contained on this disk will be lost.*

3. Go to the virtual appliance console. The **Create storage** link is available at the bottom of the screen. If it is not, click **Refresh**.
4. Click the **Create storage** link, select the disk and specify a label for it. The label length is limited to 16 characters, due to file system restrictions.

To select a locally attached storage as a backup destination

When creating a backup plan (p. 33), in **Where to back up**, select **Local folders**, and then type the letter corresponding to the locally attached storage, for example, **D:\**.

6.6 Deploying agents through Group Policy

You can centrally install (or deploy) Agent for Windows onto machines that are members of an Active Directory domain, by using Group Policy.

In this section, you will find out how to set up a Group Policy object to deploy agents onto machines in an entire domain or in its organizational unit.

Every time a machine logs on to the domain, the resulting Group Policy object will ensure that the agent is installed and registered.

Prerequisites

Before proceeding with agent deployment, ensure that:

- You have an Active Directory domain with a domain controller running Microsoft Windows Server 2003 or later.
- You are a member of the **Domain Admins** group in the domain.
- You have downloaded the **All agents for installation in Windows** setup program. The download link is available on the **Add devices** page in the backup console.

Step 1: Generating a registration token

A registration token passes your identity to the setup program without storing your login and password for the backup console. This enables you to register any number of machines under your account. For more security, a token has limited lifetime.

To generate a registration token

1. Sign in to the backup console by using the credentials of the account to which the machines should be assigned.
2. Click **All devices** > **Add**.
3. Scroll down to **Registration token**, and then click **Generate**.
4. Specify the token lifetime, and then click **Generate token**.
5. Copy the token or write it down.

   You can click **Manage active tokens** to view and manage the already generated tokens.

Step 2: Creating the .mst transform and extracting the installation package

1. Log on as an administrator on any machine in the domain.
2. Create a shared folder that will contain the installation packages. Ensure that domain users can access the shared folder—for example, by leaving the default sharing settings for **Everyone**.
3. Start the setup program.

4. Click **Create .mst and .msi files for unattended installation**.
5. Click **Specify** next to **Registration token**, and then enter the token you generated.
6. Review or modify the installation settings that will be added to the .mst file, and then click **Proceed**.
7. In **Save the files to**, specify the path to the folder you created.
8. Click **Generate**.

As a result, the .mst transform is generated and the .msi and .cab installation packages are extracted to the folder you created.

Step 3: Setting up the Group Policy objects

1. Log on to the domain controller as a domain administrator; if the domain has more than one domain controller, log on to any of them as a domain administrator.
2. If you are planning to deploy the agent in an organizational unit, ensure that the organizational unit exists in the domain. Otherwise, skip this step.
3. In the **Start** menu, point to **Administrative Tools**, and then click **Active Directory Users and Computers** (in Windows Server 2003) or **Group Policy Management** (in Windows Server 2008 or later).
4. In Windows Server 2003:
   - Right-click the name of the domain or organizational unit, and then click **Properties**. In the dialog box, click the **Group Policy** tab, and then click **New**.

   In Windows Server 2008 or later:
   - Right-click the name of the domain or organizational unit, and then click **Create a GPO in this domain, and Link it here**.
5. Name the new Group Policy object **Agent for Windows.**
6. Open the **Agent for Windows** Group Policy object for editing, as follows:
   - In Windows Server 2003, click the Group Policy object, and then click **Edit**.
   - In Windows Server 2008 or later, under **Group Policy Objects**, right-click the Group Policy object, and then click **Edit**.
7. In the Group Policy object editor snap-in, expand **Computer Configuration**.
8. In Windows Server 2003 and Windows Server 2008:
   - Expand **Software Settings**.

   In Windows Server 2012 or later:
   - Expand **Policies** > **Software Settings**.
9. Right-click **Software installation**, then point to **New**, and then click **Package**.
10. Select the agent's .msi installation package in the shared folder that you previously created, and then click **Open**.
11. In the **Deploy Software** dialog box, click **Advanced**, and then click **OK**.
12. On the **Modifications** tab, click **Add**, and then select the .mst transform that you previously created.
13. Click **OK** to close the **Deploy Software** dialog box.

6.7 Updating agents

Agents starting with the following versions can be updated by using the web interface:

- Agent for Windows, Agent for VMware (Windows), Agent for Hyper-V: version 11.9.191 and later

- Agent for Linux: version 11.9.179 and later
- Other agents: any version can be updated

To find the agent version, select the machine, and then click **Overview**.

To update from earlier agent versions, download and install the newest agent manually. To find the download links, click **All devices** > **Add**.

To update an agent by using the web interface

1. Click **Settings** > **Agents**.

   The software displays the list of machines. The machines with outdated agent versions are marked with an orange exclamation mark.
2. Select the machines that you want to update the agents on. The machines must be online.
3. Click **Update agent**.

To update Agent for VMware (Virtual Appliance)

1. Remove Agent for VMware (Virtual Appliance), as described in "Uninstalling agents (p. 30)". In step 5, delete the agent from **Settings** > **Agents**, even though you are planning to install the agent again.
2. Deploy Agent for VMware (Virtual Appliance), as described in "Deploying the OVF template" (p. 26).
3. Configure Agent for VMware (Virtual Appliance), as described in "Configuring the virtual appliance" (p. 26).

   If you want to reconstruct the locally attached storage, in step 7 do the following:

   a. Add the disk containing the local storage to the virtual appliance.
   b. Click **Refresh** > **Create storage** > **Mount**.
   c. The software displays the original **Letter** and **Label** of the disk. Do not change them.
   d. Click **OK**.

   As a result, the backup plans that were applied to the old agent are re-applied automatically to the new agent.
4. The plans with application-aware backup enabled require the guest OS credentials to be re-entered. Edit these plans and re-enter the credentials.
5. The plans that back up ESXi configuration require the "root" password to be re-entered. Edit these plans and re-enter the password.

6.8 Uninstalling agents

In Windows

If you want to remove individual product components (for example, one of the agents or Backup Monitor), run the **All agents for installation in Windows** setup program, choose to modify the product, and clear the selection of the components that you want to remove. The link to the setup program is present on the **Downloads** page (click the account icon in the top-right corner > **Downloads**).

If you want to remove all of the product components from a machine, follow the steps described below.

1. Log on as an administrator.
2. Go to **Control panel**, and then select **Programs and Features** (**Add or Remove Programs** in Windows XP) > **Acronis Backup Agent** > **Uninstall**.

3. [Optional] Select the **Remove the logs and configuration settings** check box.

   If you are planning to install the agent again, keep this check box cleared. If you select the check box, the machine may be duplicated in the backup console and the backups of the old machine may not be associated with the new machine.
4. Confirm your decision.
5. If you are planning to install the agent again, skip this step. Otherwise, in the backup console, click **Settings** > **Agents**, select the machine where the agent was installed, and then click **Delete**.

In Linux

1. As the root user, run **/usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall**.
2. [Optional] Select the **Clean up all product traces (Remove the product's logs, tasks, vaults, and configuration settings)** check box.

   If you are planning to install the agent again, keep this check box cleared. If you select the check box, the machine may be duplicated in the backup console and the backups of the old machine may not be associated with the new machine.
3. Confirm your decision.
4. If you are planning to install the agent again, skip this step. Otherwise, in the backup console, click **Settings** > **Agents**, select the machine where the agent was installed, and then click **Delete**.

In macOS

1. Double-click the installation file (.dmg).
2. Wait while the operating system mounts the installation disk image.
3. Inside the image, double-click **Uninstall**.
4. If prompted, provide administrator credentials.
5. Confirm your decision.
6. If you are planning to install the agent again, skip this step. Otherwise, in the backup console, click **Settings** > **Agents**, select the machine where the agent was installed, and then click **Delete**.

Removing Agent for VMware (Virtual Appliance)

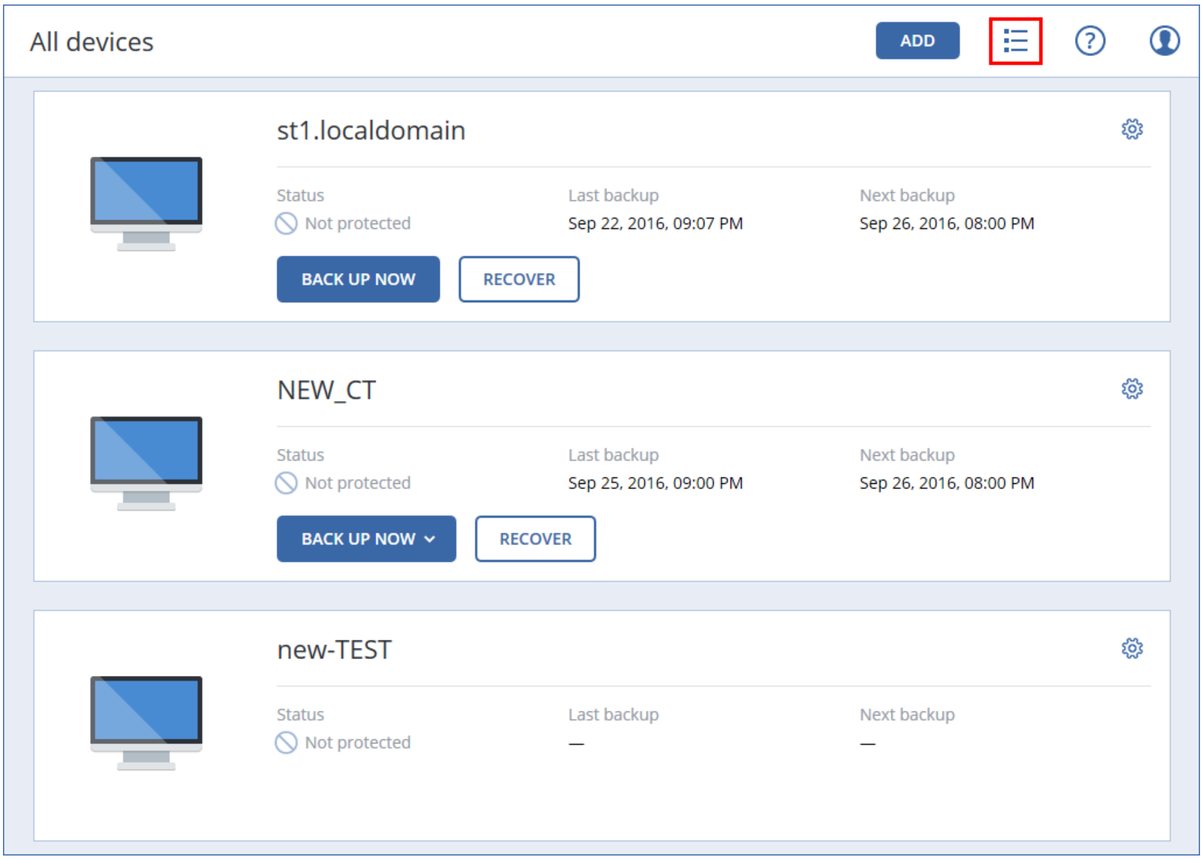
1. Start the vSphere Client and log on to the vCenter Server.
2. If the virtual appliance (VA) is powered on, right-click it, and then click **Power** > **Power Off**. Confirm your decision.
3. If the VA uses a locally attached storage on a virtual disk and you want to preserve data on that disk, do the following:
   a. Right-click the VA, and then click **Edit Settings**.
   b. Select the disk with the storage, and then click **Remove**. Under **Removal Options**, click **Remove from virtual machine**.
   c. Click **OK**.

   As a result, the disk remains in the datastore. You can attach the disk to another VA.
4. Right-click the VA, and then click **Delete from Disk**. Confirm your decision.
5. If you are planning to install the agent again, skip this step. Otherwise, in the backup console, do the following:
   a. Click **Settings** > **Agents**, select the virtual appliance, and then click **Delete**.
   b. Click **Backups** > **Locations**, and then delete the location corresponding to the locally attached storage.

7 Backup console views

The backup console has two views: a simple view and a table view. To switch between the views, click the corresponding icon in the top right corner.

The simple view supports a small number of machines.



st1.localdomain

Status: Not protected
Last backup: Sep 22, 2016, 09:07 PM
Next backup: Sep 26, 2016, 08:00 PM

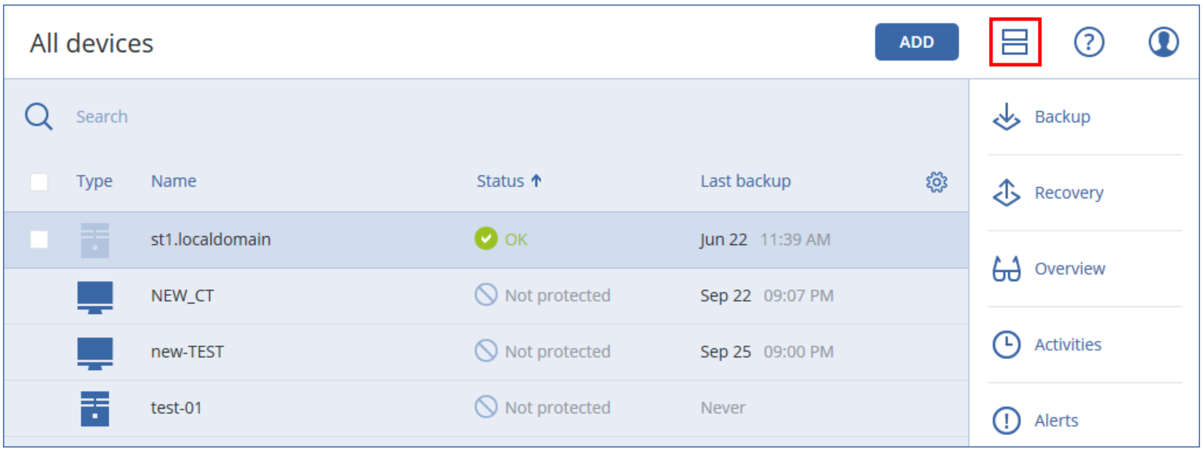
NEW_CT

Status: Not protected
Last backup: Sep 25, 2016, 09:00 PM
Next backup: Sep 26, 2016, 08:00 PM

new-TEST

Status: Not protected
Last backup: —
Next backup: —

The table view is enabled automatically when the number of machines becomes large.



Type	Name	Status ↑	Last backup
	st1.localdomain	✓ OK	Jun 22 11:39 AM
	NEW_CT	Not protected	Sep 22 09:07 PM
	new-TEST	Not protected	Sep 25 09:00 PM
	test-01	Not protected	Never

Both views provide access to the same features and operations. This document describes access to operations from the table view.

8 Backup

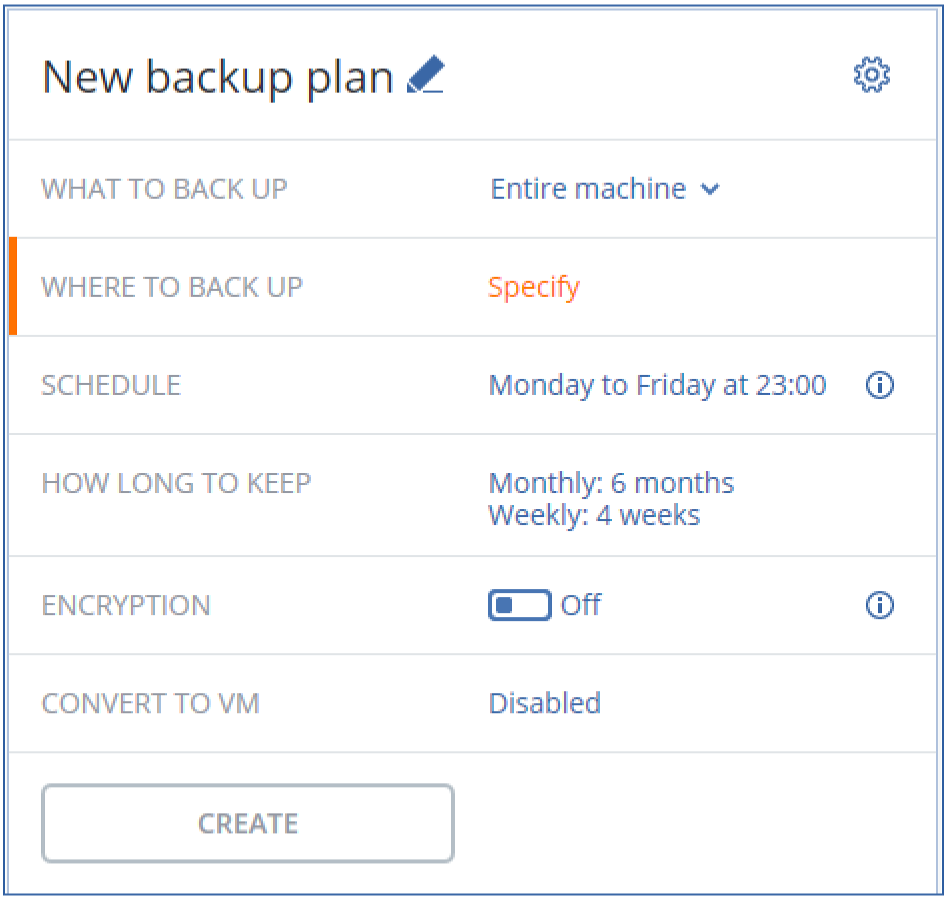
A backup plan is a set of rules that specify how the given data will be protected on a given machine.

A backup plan can be applied to multiple machines at the time of its creation, or later.

To create the first backup plan

1. Select the machines that you want to back up.
2. Click **Backup**.

   The software displays a new backup plan template.



New backup plan

WHAT TO BACK UP: Entire machine

WHERE TO BACK UP: Specify

SCHEDULE: Monday to Friday at 23:00

HOW LONG TO KEEP: Monthly: 6 months
Weekly: 4 weeks

ENCRYPTION: Off

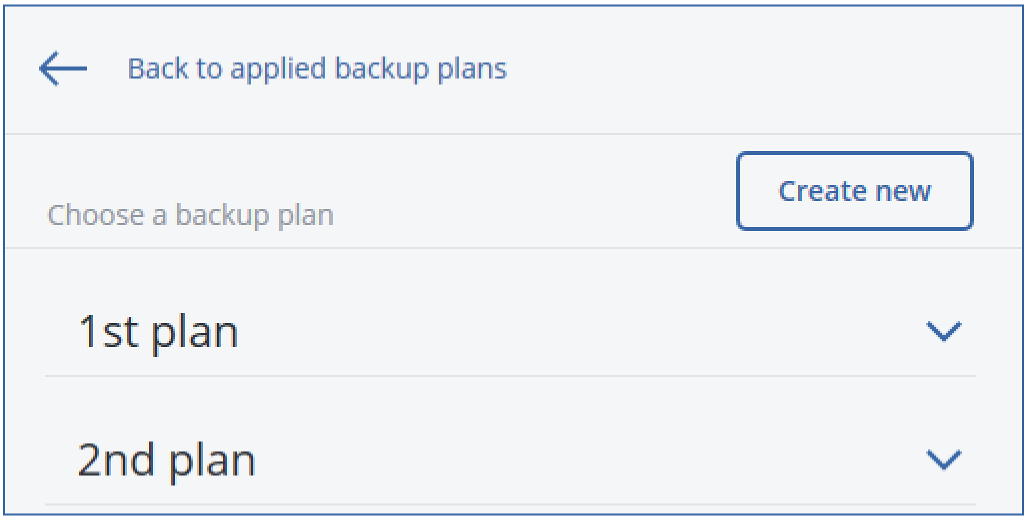
CONVERT TO VM: Disabled

3. [Optional] To modify the backup plan name, click the default name.
4. [Optional] To modify the plan parameters, click the corresponding section of the backup plan panel.
5. [Optional] To modify the backup options, click the gear icon.
6. Click **Create**.

To apply an existing backup plan

1. Select the machines that you want to back up.
2. Click **Backup**. If a common backup plan is already applied to the selected machines, click **Add backup plan**.

The software displays previously created backup plans.



3. Select a backup plan to apply.
4. Click **Apply**.

8.1 Backup plan cheat sheet

The following table summarizes the available backup plan parameters. Use the table to create a backup plan that best fits your needs.

WHAT TO BACK UP	ITEMS TO BACK UP Selection methods	WHERE TO BACK UP	SCHEDULE Backup schemes (not for Cloud)	HOW LONG TO KEEP
Disks/volumes (physical machines)	Direct selection (p. 36) Policy rules (p. 36) File filters (p. 62)	Cloud (p. 40) Local folder (p. 40) Network folder (p. 40) NFS (p. 40)* Secure Zone (p. 40)**	Always incremental (Single-file) (p. 43) Always full (p. 43) Weekly full, Daily incremental (p. 43) Custom (F-D-I) (p. 43)	By backup age (single rule/per backup set) (p. 51) By number of backups (p. 51) Keep indefinitely (p. 51)
Disks/volumes (virtual machines)	Policy rules (p. 36) File filters (p. 62)	Cloud (p. 40) Local folder (p. 40) Network folder (p. 40) NFS (p. 40)*		
Files (physical machines only)	Direct selection (p. 38) Policy rules (p. 38) File filters (p. 62)	Cloud (p. 40) Local folder (p. 40) Network folder (p. 40) NFS (p. 40)* Secure Zone (p. 40)**	Always full (p. 43) Weekly full, Daily incremental (p. 43) Custom (F-D-I) (p. 43)	

WHAT TO BACK UP		ITEMS TO BACK UP Selection methods	WHERE TO BACK UP	SCHEDULE Backup schemes (not for Cloud)	HOW LONG TO KEEP
ESXi configuration		Direct selection (p. 40)	Local folder (p. 40) Network folder (p. 40) NFS (p. 40)*		
Websites (files and MySQL databases)		Direct selection (p. 158)	Cloud (p. 40)	—	
System state		Direct selection (p. 39)	Cloud (p. 40) Local folder (p. 40) Network folder (p. 40)	Always full (p. 43) Weekly full, daily incremental (p. 43) Custom (F-I) (p. 43)	
SQL databases		Direct selection (p. 121)			
Exchange databases		Direct selection (p. 121)			
Microsoft Office 365	Mailboxes (local Agent for Office 365)	Direct selection (p. 133)	Cloud (p. 40) Local folder (p. 40) Network folder (p. 40)	Always incremental (Single-file) (p. 43)	
	Mailboxes (cloud Agent for Office 365)	Direct selection (p. 135)	Cloud (p. 40)	—	
	OneDrive files	Direct selection (p. 138) Policy rules (p. 138)			
	SharePoint Online data	Direct selection (p. 141) Policy rules (p. 141)			
G Suite	Gmail mailboxes	Direct selection (p. 146)	Cloud (p. 40)	—	
	Google Drive files	Direct selection (p. 150) Policy rules (p. 150)			
	Team Drive files	Direct selection (p. 153) Policy rules (p. 153)			

* Backup to NFS shares is not available in Windows.

** Secure Zone cannot be created on a Mac.

8.2 Selecting data to back up

8.2.1 Selecting disks/volumes

A disk-level backup contains a copy of a disk or a volume in a packaged form. You can recover individual disks, volumes, or files from a disk-level backup. A backup of an entire machine is a backup of all its disks.

There are two ways of selecting disks/volumes: directly on each machine or by using policy rules. You can exclude files from a disk backup by setting the file filters (p. 62).

Direct selection

Direct selection is available only for physical machines.

1. In **What to back up**, select **Disks/volumes**.
2. Click **Items to back up**.
3. In **Select items for backup**, select **Directly**.
4. For each of the machines included in the backup plan, select the check boxes next to the disks or volumes to back up.
5. Click **Done**.

Using policy rules

1. In **What to back up**, select **Disks/volumes**.
2. Click **Items to back up**.
3. In **Select items for backup**, select **Using policy rules**.
4. Select any of the predefined rules, type your own rules, or combine both.

   The policy rules will be applied to all of the machines included in the backup plan. If no data meeting at least one of the rules is found on a machine when the backup starts, the backup will fail on that machine.
5. Click **Done**.

Rules for Windows, Linux, and macOS

- **`[All volumes]`** selects all volumes on machines running Windows and all mounted volumes on machines running Linux or macOS.

Rules for Windows

- Drive letter (for example **C:\**) selects the volume with the specified drive letter.
- **`[Fixed Volumes (Physical machines)]`** selects all volumes of physical machines, other than removable media. Fixed volumes include volumes on SCSI, ATAPI, ATA, SSA, SAS, and SATA devices, and on RAID arrays.
- **`[BOOT+SYSTEM]`** selects the system and boot volumes. This combination is the minimal set of data that ensures recovery of the operating system from the backup.
- **`[Disk 1]`** selects the first disk of the machine, including all volumes on that disk. To select another disk, type the corresponding number.

Rules for Linux

- **`/dev/hda1`** selects the first volume on the first IDE hard disk.
- **`/dev/sda1`** selects the first volume on the first SCSI hard disk.
- **`/dev/md1`** selects the first software RAID hard disk.

To select other basic volumes, specify **`/dev/xdyN`**, where:

- "x" corresponds to the disk type
- "y" corresponds to the disk number (a for the first disk, b for the second disk, and so on)
- "N" is the volume number.

To select a logical volume, specify its name along with the volume group name. For example, to back up two logical volumes, **lv_root** and **lv_bin**, both of which belong to the volume group **vg_mymachine**, specify:

```
/dev/vg_mymachine/lv_root
/dev/vg_mymachine/lv_bin
```

Rules for macOS

- **`[Disk 1]`** Selects the first disk of the machine, including all volumes on that disk. To select another disk, type the corresponding number.

8.2.1.1 What does a disk or volume backup store?

A disk or volume backup stores a disk or a volume **file system** as a whole and includes all of the information necessary for the operating system to boot. It is possible to recover disks or volumes as a whole from such backups as well as individual folders or files.

With the **sector-by-sector (raw mode)** backup option (p. 71) enabled, a disk backup stores all the disk sectors. The sector-by-sector backup can be used for backing up disks with unrecognized or unsupported file systems and other proprietary data formats.

Windows

A volume backup stores all files and folders of the selected volume independent of their attributes (including hidden and system files), the boot record, the file allocation table (FAT) if it exists, the root and the zero track of the hard disk with the master boot record (MBR).

A disk backup stores all volumes of the selected disk (including hidden volumes such as the vendor's maintenance partitions) and the zero track with the master boot record.

The following items are *not* included in a disk or volume backup (as well as in a file-level backup):

- The swap file (pagefile.sys) and the file that keeps the RAM content when the machine goes into hibernation (hiberfil.sys). After recovery, the files will be re-created in the appropriate place with the zero size.
- If the backup is performed under the operating system (as opposed to bootable media or backing up virtual machines at a hypervisor level):
    - Windows shadow storage. The path to it is determined in the registry value **VSS Default Provider** which can be found in the registry key **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup**. This means that in operating systems starting with Windows Vista, Windows Restore Points are not backed up.
    - If the **Volume Shadow Copy Service (VSS)** backup option (p. 72) is enabled, files and folders that are specified in the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot** registry key.

Linux

A volume backup stores all files and directories of the selected volume independent of their attributes, a boot record, and the file system super block.

A disk backup stores all disk volumes as well as the zero track with the master boot record.

Mac

A disk or volume backup stores all files and directories of the selected disk or volume, plus a description of the volume layout.

The following items are excluded:

- System metadata, such as the file system journal and Spotlight index
- The Trash
- Time machine backups

Physically, disks and volumes on a Mac are backed up at a file level. Bare metal recovery from disk and volume backups is possible, but the sector-by-sector backup mode is not available.

8.2.2 Selecting files/folders

File-level backup is available only for physical machines.

A file-level backup is not sufficient for recovery of the operating system. Choose file backup if you plan to protect only certain data (the current project, for example). This will reduce the backup size, thus saving storage space.

There are two ways of selecting files: directly on each machine or by using policy rules. Either method allows you to further refine the selection by setting the file filters (p. 62).

Direct selection

1. In **What to back up**, select **Files/folders**.
2. Click **Items to back up**.
3. In **Select items for backup**, select **Directly**.
4. For each of the machines included in the backup plan:
   a. Click **Select files and folders**.
   b. Click **Local folder** or **Network folder**.

      The share must be accessible from the selected machine.
   c. Browse to the required files/folders or enter the path and click the arrow button. If prompted, specify the user name and password for the shared folder.

      Backing up a folder with anonymous access is not supported.
   d. Select the required files/folders.
   e. Click **Done**.

Using policy rules

1. In **What to back up**, select **Files/folders**.
2. Click **Items to back up**.
3. In **Select items for backup**, select **Using policy rules**.
4. Select any of the predefined rules, type your own rules, or combine both.

The policy rules will be applied to all of the machines included in the backup plan. If no data meeting at least one of the rules is found on a machine when the backup starts, the backup will fail on that machine.

5. Click **Done**.

Selection rules for Windows

- Full path to a file or folder, for example **D:\Work\Text.doc** or **C:\Windows**.
- Templates:
  - `[All Files]` selects all files on all volumes of the machine.
  - `[All Profiles Folder]` selects the folder where all user profiles are located (typically, **C:\Users** or **C:\Documents and Settings**).
- Environment variables:
  - `%ALLUSERSPROFILE%` selects the folder where the common data of all user profiles is located (typically, **C:\ProgramData** or **C:\Documents and Settings\All Users**).
  - `%PROGRAMFILES%` selects the Program Files folder (for example, **C:\Program Files**).
  - `%WINDIR%` selects the folder where Windows is located (for example, **C:\Windows**).

  You can use other environment variables or a combination of environment variables and text. For example, to select the Java folder in the Program Files folder, type: **%PROGRAMFILES%\Java**.

Selection rules for Linux

- Full path to a file or directory. For example, to back up **file.txt** on the volume **/dev/hda3** mounted on **/home/usr/docs**, specify **/dev/hda3/file.txt** or **/home/usr/docs/file.txt**.
  - `/home` selects the home directory of the common users.
  - `/root` selects the root user's home directory.
  - `/usr` selects the directory for all user-related programs.
  - `/etc` selects the directory for system configuration files.
- Templates:
  - `[All Profiles Folder]` selects **/home**. This is the folder where all user profiles are located by default.

Selection rules for macOS

- Full path to a file or directory.
- Templates:
  - `[All Profiles Folder]` selects **/Users**. This is the folder where all user profiles are located by default.

Examples:

- To back up **file.txt** on your desktop, specify **/Users/<username>/Desktop/file.txt**, where <username> is your user name.
- To back up all users' home directories, specify **/Users**.
- To back up the directory where the applications are installed, specify **/Applications**.

8.2.3 Selecting system state

System state backup is available for machines running Windows Vista and later.

To back up system state, in **What to back up**, select **System state**.

A system state backup is comprised of the following files:

- Task scheduler configuration
- VSS Metadata Store
- Performance counter configuration information
- MSSearch Service
- Background Intelligent Transfer Service (BITS)
- The registry
- Windows Management Instrumentation (WMI)
- Component Services Class registration database

8.2.4 Selecting ESXi configuration

A backup of an ESXi host configuration enables you to recover an ESXi host to bare metal. The recovery is performed under bootable media.

The virtual machines running on the host are not included in the backup. They can be backed up and recovered separately.

A backup of an ESXi host configuration includes:

- The bootloader and boot bank partitions of the host.
- The host state (configuration of virtual networking and storage, SSL keys, server network settings, and local user information).
- Extensions and patches installed or staged on the host.
- Log files.

Prerequisites

- SSH must be enabled in the **Security Profile** of the ESXi host configuration.
- You must know the password for the 'root' account on the ESXi host.

Limitations

- ESXi configuration backup is not supported for VMware vSphere 6.7.
- An ESXi configuration cannot be backed up to the cloud storage.

To select an ESXi configuration

1. Go to **VMware** > **Host and clusters**.
2. Browse to the ESXi hosts that you want to back up.
3. Select the ESXi hosts and click **Backup**.
4. In **What to back up**, select **ESXi configuration**.
5. In **ESXi 'root' password**, specify a password for the 'root' account on each of the selected hosts or apply the same password to all of the hosts.

8.3 Selecting a destination

Click **Where to back up**, and then select one of the following:

- **Cloud storage**

  Backups will be stored in the cloud data center.
- **Local folders**

If a single machine is selected, browse to a folder on the selected machine or type the folder path.

If multiple machines are selected, type the folder path. Backups will be stored in this folder on each of the selected physical machines or on the machine where the agent for virtual machines is installed. If the folder does not exist, it will be created.

- **Network folder**

  This is a folder shared via SMB/CIFS/DFS.

  Browse to the required shared folder or enter the path in the following format:

  - For SMB/CIFS shares: `\\<host name>\<path>\` or `smb://<host name>/<path>/`
  - For DFS shares: `\\<full DNS domain name>\<DFS root>\<path>`

    For example, `\\example.company.com\shared\files`

  Then, click the arrow button. If prompted, specify the user name and password for the shared folder.

  Backing up to a folder with anonymous access is not supported.

- **NFS folder** (available for machines running Linux or macOS)

  Browse to the required NFS folder or enter the path in the following format:

  `nfs://<host name>/<exported folder>:/<subfolder>`

  Then, click the arrow button.

  It is not possible to back up to an NFS folder protected with a password.

- **Secure Zone** (available if it is present on each of the selected machines)

  Secure Zone is a secure partition on a disk of the backed-up machine. This partition has to be created manually prior to configuring a backup. For information about how to create Secure Zone, its advantages and limitations, refer to "About Secure Zone" (p. 41).

8.3.1 About Secure Zone

Secure Zone is a secure partition on a disk of the backed-up machine. It can store backups of disks or files of this machine.

Should the disk experience a physical failure, the backups located in the Secure Zone may be lost. That's why Secure Zone should not be the only location where a backup is stored. In enterprise environments, Secure Zone can be thought of as an intermediate location used for backup when an ordinary location is temporarily unavailable or connected through a slow or busy channel.

Why use Secure Zone?

Secure Zone:

- Enables recovery of a disk to the same disk where the disk's backup resides.
- Offers a cost-effective and handy method for protecting data from software malfunction, virus attack, human error.
- Eliminates the need for a separate media or network connection to back up or recover the data. This is especially useful for roaming users.
- Can serve as a primary destination when using replication of backups.

Limitations

- Secure Zone cannot be organized on a Mac.
- Secure Zone is a partition on a basic disk. It cannot be organized on a dynamic disk or created as a logical volume (managed by LVM).

- Secure Zone is formatted with the FAT32 file system. Because FAT32 has a 4-GB file size limit, larger backups are split when saved to Secure Zone. This does not affect the recovery procedure and speed.
- Secure Zone does not support the single-file backup format (p. 181). When you change the destination to Secure Zone in a backup plan that has the **Always incremental (Single-file)** backup scheme, the scheme is changed to **Weekly full, daily incremental**.

How to create Secure Zone

1. Decide which disk you want to create Secure Zone on.
2. Start the command-line interface and type **`acrocmd list disks`** to see the disk's number.
3. Use the **`create asz`** command of the **`acrocmd`** utility. The command first uses the unallocated space on that disk and then, if the unallocated space is insufficient, takes free space from the specified volumes. For details, refer to "How creating Secure Zone transforms the disk" below.

   Examples:

   - Creating Secure Zone on disk 1 of the local machine. Secure Zone will be created with a default size that is the average between the maximum (all the unallocated space) and minimum (about 50 MB) values.

     ```
     acrocmd create asz --disk=1
     ```

   - Creating a password-protected Secure Zone of size 100 GB on disk 2 of the local machine. If the unallocated space is not enough, the space will be taken from the second volume of that disk.

     ```
     acrocmd create asz --disk=2 --volume=2-2 --asz_size=100gb --password=abc12345
     ```

   - Creating Secure Zone of size 20 GB on disk 1 of a remote machine.

     ```
     acrocmd create asz --host=192.168.1.2 --credentials=john,pass1 --disk=1
     --asz_size=20gb
     ```

   For the detailed description of the **`create asz`** command, see the command-line reference.

How creating Secure Zone transforms the disk

- Secure Zone is always created at the end of the hard disk. When calculating the final layout of the volumes, the program will first use unallocated space at the end.
- If there is no or not enough unallocated space at the end of the disk, but there is unallocated space between volumes, the volumes will be moved to add more unallocated space to the end.
- When all unallocated space is collected but it is still not enough, the program will take free space from the volumes you select, proportionally reducing the volumes' size. Resizing locked volumes requires a reboot.
- However, there should be free space on a volume, so that the operating system and applications can operate; for example, create temporary files. The software will not decrease a volume where free space is or becomes less than 25 percent of the total volume size. Only when all volumes on the disk have 25 percent or less free space, will the software continue decreasing the volumes proportionally.

As is apparent from the above, specifying the maximum possible Secure Zone size is not advisable. You will end up with no free space on any volume, which might cause the operating system or applications to work unstably and even fail to start.

8.4 Schedule

The schedule employs the time settings (including the time zone) of the operating system where the agent installed. The time zone of Agent for VMware (Virtual Appliance) can be configured in the agent's interface (p. 26).

For example, if a backup plan is scheduled to run at 21:00 and applied to several machines located in different time zones, the backup will start on each machine at 21:00 local time.

The scheduling parameters depend on the backup destination.

When backing up to cloud storage

By default, backups are performed on a daily basis, Monday to Friday. You can select the time to run the backup.

If you want to change the backup frequency, move the slider, and then specify the backup schedule.

You can schedule the backup to run by events, instead of by time. To do this, select the event type in the schedule selector. For more information, refer to "Schedule by events" (p. 44).

Important *The first backup is full, which means that it is the most time-consuming. All subsequent backups are incremental and take significantly less time.*

When backing up to other locations

You can choose one of the predefined backup schemes or create a custom scheme. A backup scheme is a part of the backup plan that includes the backup schedule and the backup methods.

In **Backup scheme**, select one of the following:

- [Only for disk-level backups] **Always incremental (single-file)**

  By default, backups are performed on a daily basis, Monday to Friday. You can select the time to run the backup.

  If you want to change the backup frequency, move the slider, and then specify the backup schedule.

  The backups use the new single-file backup format (p. 181).

  This scheme is not available when backing up to Secure Zone.

- **Always full**

  By default, backups are performed on a daily basis, Monday to Friday. You can select the time to run the backup.

  If you want to change the backup frequency, move the slider, and then specify the backup schedule.

  All backups are full.

- **Weekly full, Daily incremental**

  By default, backups are performed on a daily basis, Monday to Friday. You can modify the days of the week and the time to run the backup.

  A full backup is created once a week. All other backups are incremental. The day on which the full backup is created depends on the **Weekly backup** option (click the gear icon, then **Backup options** > **Weekly backup**).

- **Custom**

  Specify schedules for full, differential, and incremental backups.

Differential backup is not available when backing up SQL data, Exchange data, or system state.

With any backup scheme, you can schedule the backup to run by events, instead of by time. To do this, select the event type in the schedule selector. For more information, refer to "Schedule by events" (p. 44).

Additional scheduling options

With any destination, you can do the following:

- Specify the backup start conditions, so that a scheduled backup is performed only if the conditions are met. For more information, refer to "Start conditions" (p. 46).
- Set a date range for when the schedule is effective. Select the **Run the plan within a date range** check box, and then specify the date range.
- Disable the schedule. While the schedule is disabled, the retention rules are not applied unless a backup is started manually.
- Introduce a delay from the scheduled time. The delay value for each machine is selected randomly and ranges from zero to the maximum value you specify. You may want to use this setting when backing up multiple machines to a network location, to avoid excessive network load.

  Click the gear icon, then **Backup options** > **Scheduling**. Select **Distribute backup start times within a time window**, and then specify the maximum delay. The delay value for each machine is determined when the backup plan is applied to the machine and remains the same until you edit the backup plan and change the maximum delay value.

  Note *This option is enabled by default, with the maximum delay set to 30 minutes.*

- Click **Show more** to access the following options:
  - **If the machine is turned off, run missed tasks at the machine startup** (disabled by default)
  - **Prevent the sleep or hibernate mode during backup** (enabled by default)

    This option is effective only for machines running Windows.
  - **Wake up from the sleep or hibernate mode to start a scheduled backup** (disabled by default)

    This option is effective only for machines running Windows. This option is not effective when the machine is powered off, i.e. the option does not employ the Wake-on-LAN functionality.

8.4.1 Schedule by events

When setting up a schedule for a backup plan, you can select the event type in the schedule selector. The backup will be launched as soon as the event occurs.

You can choose one of the following events:

- **Upon time since last backup**

  This is the time since the completion of the last successful backup within the same backup plan. You can specify the length of time.
- **When a user logs on to the system**

  By default, logging on of any user will initiate a backup. You can change any user to a specific user account.
- **When a user logs off the system**

  By default, logging off of any user will initiate a backup. You can change any user to a specific user account.

***Note** The backup will not run at a system shutdown because shutting down is not the same as logging off.*

- **On the system startup**
- **On the system shutdown**
- **On Windows Event Log event**

  You must specify the event properties (p. 45).

The table below lists the events available for various data under Windows, Linux, and macOS.

WHAT TO BACK UP	Upon time since last backup	When a user logs on to the system	When a user logs off the system	On the system startup	On the system shutdown	On Windows Event Log event
Disks/volumes or files (physical machines)	Windows, Linux, macOS	Windows	Windows	Windows, Linux, macOS	Windows	Windows
Disks/volumes (virtual machines)	Windows, Linux	–	–	–	–	–
ESXi configuration	Windows, Linux	–	–	–	–	–
Office 365 mailboxes	Windows	–	–	–	–	Windows
Exchange databases and mailboxes	Windows	–	–	–	–	Windows
SQL databases	Windows	–	–	–	–	Windows

8.4.1.1 On Windows Event Log event

You can schedule a backup to start when a certain Windows event has been recorded in one of the event logs, such as the **Application**, **Security**, or **System** log.

For example, you may want to set up a backup plan that will automatically perform an emergency full backup of your data as soon as Windows discovers that your hard disk drive is about to fail.

To browse the events and view the event properties, use the **Event Viewer** snap-in available in the **Computer Management** console. To be able to open the **Security** log, you must be a member of the **Administrators** group.

Event properties

Log name

Specifies the name of the log. Select the name of a standard log (**Application**, **Security**, or **System**) from the list, or type a log name—for example: **Microsoft Office Sessions**

Event source

Specifies the event source, which typically indicates the program or the system component that caused the event—for example: **disk**

Event type

Specifies the event type: **Error**, **Warning**, **Information**, **Audit success**, or **Audit failure**.

Event ID

Specifies the event number, which typically identifies the particular kind of events among events from the same source.

For example, an **Error** event with Event source **disk** and Event ID **7** occurs when Windows discovers a bad block on a disk, whereas an **Error** event with Event source **disk** and Event ID **15** occurs when a disk is not ready for access yet.

Example: "Bad block" emergency backup

One or more bad blocks that have suddenly appeared on a hard disk usually indicate that the hard disk drive will soon fail. Suppose that you want to create a backup plan that will back up hard disk data as soon as such a situation occurs.

When Windows detects a bad block on a hard disk, it records an event with the event source **disk** and the event number **7** into the **System** log; the type of this event is **Error**.

When creating the plan, type or select the following in the **Schedule** section:

- **Log name**: **System**
- **Event source**: **disk**
- **Event type**: **Error**
- **Event ID**: **7**

Important *To ensure that such a backup will complete despite the presence of bad blocks, you must make the backup ignore bad blocks. To do this, in **Backup options**, go to **Error handling**, and then select the **Ignore bad sectors** check box.*

8.4.2 Start conditions

These settings add more flexibility to the scheduler, enabling it to execute a backup with respect to certain conditions. With multiple conditions, all of them must be met simultaneously to enable a backup to start. Start conditions are not effective when a backup is started manually.

To access these settings, click **Show more** when setting up a schedule for a backup plan.

The scheduler behavior, in case the condition (or any of multiple conditions) is not met, is defined by the Backup start conditions (p. 60) backup option. To handle the situation when the conditions are not met for too long and further delaying the backup is becoming risky, you can set the time interval after which the backup will run irrespective of the condition.

The table below lists the start conditions available for various data under Windows, Linux, and macOS.

WHAT TO BACK UP	**Disks/volumes or files (physical machines)**	**Disks/volumes (virtual machines)**	**ESXi configuration**	**Office 365 mailboxes**	**Exchange databases and mailboxes**	**SQL databases**
User is idle (p. 47)	Windows	–	–	–	–	–
The backup location's host is available (p. 47)	Windows, Linux, macOS	Windows, Linux	Windows, Linux	Windows	Windows	Windows
Users logged off (p. 48)	Windows	–	–	–	–	–
Fits the time interval (p. 48)	Windows, Linux, macOS	Windows, Linux	–	–	–	–

Save battery power (p. 49)	Windows	–	–	–	–	–
Do not start when on metered connection (p. 49)	Windows	–	–	–	–	–
Do not start when connected to the following Wi-Fi networks (p. 50)	Windows	–	–	–	–	–
Check device IP address (p. 51)	Windows	–	–	–	–	–

8.4.2.1 User is idle

"User is idle" means that a screen saver is running on the machine or the machine is locked.

Example

Run the backup on the machine every day at 21:00, preferably when the user is idle. If the user is still active by 23:00, run the backup anyway.

- Schedule: Daily, Run every day. Start at: **21:00**.
- Condition: **User is idle**.
- Backup start conditions: **Wait until the conditions are met, Start the backup anyway after 2** hour(s).

As a result,

(1) If the user becomes idle before 21:00, the backup will start at 21:00.

(2) If the user becomes idle between 21:00 and 23:00, the backup will start immediately after the user becomes idle.

(3) If the user is still active at 23:00, the backup will start at 23:00.

8.4.2.2 The backup location's host is available

"The backup location's host is available" means that the machine hosting the destination for storing backups is available over the network.

This condition is effective for network folders, the cloud storage, and locations managed by a storage node.

This condition does not cover the availability of the location itself — only the host availability. For example, if the host is available, but the network folder on this host is not shared or the credentials for the folder are no longer valid, the condition is still considered met.

Example

Data is backed up to a network folder every workday at 21:00. If the machine that hosts the folder is not available at that moment (for instance, due to maintenance work), you want to skip the backup and wait for the scheduled start on the next workday.

- Schedule: Daily, Run Monday to Friday. Start at: **21:00**.
- Condition: **The backup location's host is available**.
- Backup start conditions: **Skip the scheduled backup**.

As a result:

(1) If 21:00 comes and the host is available, the backup will start immediately.

(2) If 21:00 comes but the host is unavailable, the backup will start on the next workday if the host is available.

(3) If the host is never available on workdays at 21:00, the backup will never start.

8.4.2.3 Users logged off

Enables you to put a backup on hold until all users log off from Windows.

Example

Run the backup at 20:00 every Friday, preferably when all users are logged off. If one of the users is still logged on at 23:00, run the backup anyway.

- Schedule: Weekly, on Fridays. Start at: **20:00**.
- Condition: **Users logged off**.
- Backup start conditions: **Wait until the conditions are met**, **Start the backup anyway after 3** hour(s).

As a result:

(1) If all users are logged off at 20:00, the backup will start at 20:00.

(2) If the last user logs off between 20:00 and 23:00, the backup will start immediately after the user logs off.

(3) If any user is still logged on at 23:00, the backup will start at 23:00.

8.4.2.4 Fits the time interval

Restricts a backup start time to a specified interval.

Example

A company uses different locations on the same network-attached storage for backing up users' data and servers. The workday starts at 08:00 and ends at 17:00. Users' data should be backed up as soon as the users log off, but not earlier than 16:30. Every day at 23:00 the company's servers are backed up. So, all the users' data should preferably be backed up before this time, in order to free network bandwidth. It is assumed that backing up user's data takes no more than one hour, so the latest backup start time is 22:00. If a user is still logged on within the specified time interval, or logs off at any other time – do not back up the users' data, i.e., skip backup execution.

- Event: **When a user logs off the system**. Specify the user account: **Any user**.
- Condition: **Fits the time interval** from **16:30** to **22:00**.
- Backup start conditions: **Skip the scheduled backup**.

As a result:

(1) if the user logs off between 16:30 and 22:00, the backup will start immediately following the logging off.

(2) if the user logs off at any other time, the backup will be skipped.

8.4.2.5 Save battery power

Prevents a backup if the device (a laptop or a tablet) is not connected to a power source. Depending on the value of the Backup start conditions (p. 60) backup option, the skipped backup will or will not be started after the device is connected to a power source. The following options are available:

- **Do not start when on battery**

  A backup will start only if the device is connected to a power source.
- **Start when on battery if the battery level is higher than**

  A backup will start if the device is connected to a power source or if the battery level is higher than the specified value.

Example

Data is backed up every workday at 21:00. If the device is not connected to a power source (for instance, the user is attending a late meeting), you want to skip the backup to save the battery power and wait until the user connects the device to a power source.

- Schedule: Daily, Run Monday to Friday. Start at: 21:00.
- Condition: **Save battery power**, **Do not start when on battery**.
- Backup start conditions: **Wait until the conditions are met**.

As a result:

(1) If 21:00 comes and the device is connected to a power source, the backup will start immediately.

(2) If 21:00 comes and the device is running on battery power, the backup will start as soon as the device is connected to a power source.

8.4.2.6 Do not start when on metered connection

Prevents a backup (including a backup to a local disk) if the device is connected to the Internet by using a connection that is set as metered in Windows. For more information about metered connections in Windows, refer to https://support.microsoft.com/en-us/help/17452/windows-metered-internet-connections-faq.

As an additional measure to prevent backups over mobile hotspots, when you enable the **Do not start when on metered connection** condition, the condition **Do not start when connected to the following Wi-Fi networks** is enabled automatically. The following network names are specified by default: "android", "phone", "mobile", and "modem". You can delete these names from the list by clicking on the X sign.

Example

Data is backed up every workday at 21:00. If the device is connected to the Internet by using a metered connection (for instance, the user is on a business trip), you want to skip the backup to save the network traffic and wait for the scheduled start on the next workday.

- Schedule: Daily, Run Monday to Friday. Start at: 21:00.
- Condition: **Do not start when on metered connection**.

- Backup start conditions: **Skip the scheduled backup**.

As a result:

(1) If 21:00 comes and the device is not connected to the Internet by using a metered connection, the backup will start immediately.

(2) If 21:00 comes and the device is connected to the Internet by using a metered connection, the backup will start on the next workday.

(3) If the device is always connected to the Internet by using a metered connection on workdays at 21:00, the backup will never start.

8.4.2.7 Do not start when connected to the following Wi-Fi networks

Prevents a backup (including a backup to a local disk) if the device is connected to any of the specified wireless networks. You can specify the Wi-Fi network names, also known as service set identifiers (SSID).

The restriction applies to all networks that contain the specified name as a substring in their name, case-insensitive. For example, if you specify "phone" as the network name, the backup will not start when the device is connected to any of the following networks: "John's iPhone", "phone_wifi", or "my_PHONE_wifi".

This condition is useful to prevent backups when the device is connected to the Internet by using a mobile phone hotspot.

As an additional measure to prevent backups over mobile hotspots, the **Do not start when connected to the following Wi-Fi** condition is enabled automatically when you enable the **Do not start when on metered connection** condition. The following network names are specified by default: "android", "phone", "mobile", and "modem". You can delete these names from the list by clicking on the X sign.

Example

Data is backed up every workday at 21:00. If the device is connected to the Internet by using a mobile hotspot (for example, a laptop is connected in the tethering mode), you want to skip the backup and wait for the scheduled start on the next workday.

- Schedule: Daily, Run Monday to Friday. Start at: 21:00.
- Condition: **Do not start when connected to the following networks**, **Network name**: `<SSID of the hotspot network>`.
- Backup start conditions: **Skip the scheduled backup**.

As a result:

(1) If 21:00 comes and the machine is not connected to the specified network, the backup will start immediately.

(2) If 21:00 comes and the machine is connected to the specified network, the backup will start on the next workday.

(3) If the machine is always connected to the specified network on workdays at 21:00, the backup will never start.

8.4.2.8 Check device IP address

Prevents a backup (including a backup to a local disk) if any of the device IP addresses are within or outside of the specified IP address range. The following options are available:

- **Start if outside IP range**
- **Start if within IP range**

With either option, you can specify several ranges. Only IPv4 addresses are supported.

This condition is useful in the event of a user being overseas, to avoid large data transit charges. Also, it helps to prevent backups over a Virtual Private Network (VPN) connection.

Example

Data is backed up every workday at 21:00. If the device is connected to the corporate network by using a VPN tunnel (for instance, the user is working from home), you want to skip the backup and wait until the user brings the device to the office.

- Schedule: Daily, Run Monday to Friday. Start at: 21:00.
- Condition: **Check device IP address**, **Start if outside IP range**, **From**: `<beginning of the VPN IP address range>`, **To**: `<end of the VPN IP address range>`.
- Backup start conditions: **Wait until the conditions are met**.

As a result:

(1) If 21:00 comes and the machine IP address is not in the specified range, the backup will start immediately.

(2) If 21:00 comes and the machine IP address is in the specified range, the backup will start as soon as the device obtains a non-VPN IP address.

(3) If the machine IP address is always in the specified range on workdays at 21:00, the backup will never start.

8.5 Retention rules

1. Click **How long to keep**.
2. In **Cleanup**, choose one of the following:
   - **By backup age** (default)

     Specify how long to keep backups created by the backup plan. By default, the retention rules are specified for each backup set (p. 181) separately. If you want to use a single rule for all backups, click **Switch to single rule for all backup sets**.
   - **By number of backups**

     Specify the maximum number of backups to keep.
   - **Keep backups indefinitely**

What else you need to know

- If, according to the backup scheme and backup format, each backup is stored as a separate file, this file cannot be deleted until the lifetime of all its dependent (incremental and differential) backups expires. This requires extra space for storing backups whose deletion is postponed. Also, the backup age, number, or size of backups may exceed the values you specify.

  This behavior can be changed by using the "Backup consolidation" (p. 57) backup option.

- Retention rules are a part of a backup plan. They stop working for a machine's backups as soon as the backup plan is revoked from the machine, or deleted, or the machine itself is deleted from the backup service. If you no longer need the backups created by the plan, delete them as described in "Deleting backups" (p. 113).

8.6 Replication

If you enable backup replication, each backup will be copied to a second location immediately after creation. If earlier backups were not replicated (for example, the network connection was lost), the software also replicates all of the backups that appeared after the last successful replication.

Replicated backups do not depend on the backups remaining in the original location and vice versa. You can recover data from any backup, without access to other locations.

Usage examples

- **Reliable disaster recovery**

  Store your backups both on-site (for immediate recovery) and off-site (to secure the backups from local storage failure or a natural disaster).
- **Using the cloud storage to protect data from a natural disaster**

  Replicate the backups to the cloud storage by transferring only the data changes.
- **Keeping only the latest recovery points**

  Delete older backups from a fast storage according to retention rules, in order to not overuse expensive storage space.

Supported locations

You can replicate a backup *from* any of these locations:

- A local folder
- A network folder
- Secure Zone

You can replicate a backup *to* any of these locations:

- A local folder
- A network folder
- The cloud storage

To enable backup replication

1. On the backup plan panel, enable the **Replicate backups** switch.

   This switch is shown only if replication is supported from the location selected in **Where to back up**.
2. In **Where to replicate**, specify the replication destination, as described in "Selecting a destination" (p. 40).
3. In **How long to keep**, specify the retention rules, as described in "Retention rules" (p. 51).

8.7 Encryption

We recommend that you encrypt all backups that are stored in the cloud storage, especially if your company is subject to regulatory compliance.

Important *There is no way to recover encrypted backups if you lose or forget the password.*

Encryption in a backup plan

To enable encryption, specify the encryption settings when creating a backup plan. After a backup plan is applied, the encryption settings cannot be modified. To use different encryption settings, create a new backup plan.

To specify the encryption settings in a backup plan

1. On the backup plan panel, enable the **Encryption** switch.
2. Specify and confirm the encryption password.
3. Select one of the following encryption algorithms:
   - **AES 128** – the backups will be encrypted by using the Advanced Encryption Standard (AES) algorithm with a 128-bit key.
   - **AES 192** – the backups will be encrypted by using the AES algorithm with a 192-bit key.
   - **AES 256** – the backups will be encrypted by using the AES algorithm with a 256-bit key.
4. Click **OK**.

Encryption as a machine property

This option is intended for administrators who handle backups of multiple machines. If you need a unique encryption password for each machine or if you need to enforce encryption of backups regardless of the backup plan encryption settings, save the encryption settings on each machine individually. The backups will be encrypted using the AES algorithm with a 256-bit key.

Saving the encryption settings on a machine affects the backup plans in the following way:

- **Backup plans that are already applied to the machine.** If the encryption settings in a backup plan are different, the backups will fail.
- **Backup plans that will be applied to the machine later.** The encryption settings saved on a machine will override the encryption settings in a backup plan. Any backup will be encrypted, even if encryption is disabled in the backup plan settings.

This option can be used on a machine running Agent for VMware. However, be careful if you have more than one Agent for VMware connected to the same vCenter Server. It is mandatory to use the same encryption settings for all of the agents, because there is a type of load balancing among them.

After the encryption settings are saved, they can be changed or reset as described below.

Important *If a backup plan that runs on this machine has already created backups, changing the encryption settings will cause this plan to fail. To continue backing up, create a new plan.*

To save the encryption settings on a machine

1. Log on as an administrator (in Windows) or the root user (in Linux).
2. Run the following script:
   - In Windows: `<installation_path>`**\PyShell\bin\acropsh.exe -m manage_creds --set-password** `<encryption_password>`

     Here, `<installation_path>` is the backup agent installation path. By default, it is **%ProgramFiles%\BackupClient**.
   - In Linux: **/usr/sbin/acropsh -m manage_creds --set-password** `<encryption_password>`

To reset the encryption settings on a machine

1. Log on as an administrator (in Windows) or root user (in Linux).
2. Run the following script:
   - In Windows: `<installation_path>`**\PyShell\bin\acropsh.exe -m manage_creds --reset**

Here, `<installation_path>` is the backup agent installation path. By default, it is **%ProgramFiles%\BackupClient**.

- In Linux: **/usr/sbin/acropsh -m manage_creds --reset**

To change the encryption settings by using Backup Monitor

1. Log on as an administrator in Windows or macOS.
2. Click the **Backup Monitor** icon in the notification area (in Windows) or the menu bar (in macOS).
3. Click the gear icon.
4. Click **Encryption**.
5. Do one of the following:
   - Select **Set a specific password for this machine**. Specify and confirm the encryption password.
   - Select **Use encryption settings specified in the backup plan**.
6. Click **OK**.

How the encryption works

The AES cryptographic algorithm operates in the Cipher-block chaining (CBC) mode and uses a randomly generated key with a user-defined size of 128, 192 or 256 bits. The larger the key size, the longer it will take for the program to encrypt the backups and the more secure your data will be.

The encryption key is then encrypted with AES-256 using an SHA-256 hash of the password as a key. The password itself is not stored anywhere on the disk or in the backups; the password hash is used for verification purposes. With this two-level security, the backup data is protected from any unauthorized access, but recovering a lost password is not possible.

8.8 Starting a backup manually

1. Select a machine that has at least one applied backup plan.
2. Click **Backup**.
3. If more than one backup plans are applied, select the backup plan.
4. Click **Run now** on the backup plan panel.

The backup progress is shown in the **Status** column for the machine.

8.9 Backup options

To modify the backup options, click the gear icon next to the backup plan name, and then click **Backup options**.

Availability of the backup options

The set of available backup options depends on:

- The environment the agent operates in (Windows, Linux, macOS).
- The type of the data being backed up (disks, files, virtual machines, application data).
- The backup destination (the cloud storage, local or network folder).

The following table summarizes the availability of the backup options.

	Disk-level backup			File-level backup			Virtual machines			SQL and Exchange
	Windows	Linux	macOS	Windows	Linux	macOS	ESXi	Hyper-V	Virtuozzo	Windows
Alerts (p. 57)	+	+	+	+	+	+	+	+	+	+
Backup consolidation (p. 57)	+	+	+	+	+	+	+	+	+	-
Backup format (p. 58)	+	+	+	+	+	+	+	+	+	+
Backup validation (p. 59)	+	+	+	+	+	+	+	+	+	+
Backup start conditions (p. 60)	+	+	-	+	+	-	+	+	+	+
Changed block tracking (CBT) (p. 60)	+	-	-	-	-	-	+	+	-	-
Compression level (p. 60)	+	+	+	+	+	+	+	+	+	+
Error handling (p. 61)										
Re-attempt, if an error occurs	+	+	+	+	+	+	+	+	+	+
Do not show messages and dialogs while processing (silent mode)	+	+	+	+	+	+	+	+	+	+
Ignore bad sectors	+	+	+	+	+	+	+	+	+	-
Re-attempt, if an error occurs during VM snapshot creation	-	-	-	-	-	-	+	+	+	-
Fast incremental/differential backup (p. 62)	+	+	+	-	-	-	-	-	-	-

	Disk-level backup			File-level backup			Virtual machines			SQL and Exchange
	Windows	Linux	macOS	Windows	Linux	macOS	ESXi	Hyper-V	Virtuozzo	Windows
File-level backup snapshot (p. 63)	-	-	-	+	+	+	-	-	-	-
File filters (p. 62)	+	+	+	+	+	+	+	+	+	-
Log truncation (p. 64)	-	-	-	-	-	-	+	+	-	SQL only
LVM snapshotting (p. 64)	-	+	-	-	-	-	-	-	-	-
Mount points (p. 64)	-	-	-	+	-	-	-	-	-	-
Multi-volume snapshot (p. 65)	+	+	-	+	+	-	-	-	-	-
Performance (p. 65)	+	+	+	+	+	+	+	+	+	+
Physical Data Shipping (p. 66)	+	+	+	+	+	+	+	+	+	-
Pre/Post commands (p. 67)	+	+	+	+	+	+	+	+	+	+
Pre/Post data capture commands (p. 68)	+	+	+	+	+	+	-	-	-	+
Scheduling (p. 70)										
Distribute start times within a time window	+	+	+	+	+	+	+	+	+	+
Limit the number of simultaneously running backups	-	-	-	-	-	-	+	+	+	-
Sector-by-sector backup (p. 71)	+	+	-	-	-	-	+	+	+	-
Splitting (p. 71)	+	+	+	+	+	+	+	+	+	+
Task failure handling (p. 71)	+	+	+	+	+	+	+	+	+	+

	Disk-level backup			File-level backup			Virtual machines			SQL and Exchange
	Windows	Linux	macOS	Windows	Linux	macOS	ESXi	Hyper-V	Virtuozzo	Windows
Volume Shadow Copy Service (VSS) (p. 72)	+	-	-	+	-	-	-	+	-	+
Volume Shadow Copy Service (VSS) for virtual machines (p. 73)	-	-	-	-	-	-	+	+	-	-
Weekly backup (p. 73)	+	+	+	+	+	+	+	+	+	+
Windows event log (p. 73)	+	-	-	+	-	-	+	+	-	+

8.9.1 Alerts

No successful backups for a specified number of consecutive days

The preset is: **Disabled**.

This option determines whether to generate an alert if no successful backups were performed by the backup plan for a specified period of time. In addition to failed backups, the software counts backups that did not run on schedule (missed backups).

The alerts are generated on a per-machine basis and are displayed on the **Alerts** tab.

You can specify the number of consecutive days without backups after which the alert is generated.

8.9.2 Backup consolidation

This option defines whether to consolidate backups during cleanup or to delete entire backup chains.

The preset is: **Disabled**.

Consolidation is the process of combining two or more subsequent backups into a single backup.

If this option is enabled, a backup that should be deleted during cleanup is consolidated with the next dependent backup (incremental or differential).

Otherwise, the backup is retained until all dependent backups become subject to deletion. This helps avoid the potentially time-consuming consolidation, but requires extra space for storing backups whose deletion is postponed. The backups' age or number can exceed the values specified in the retention rules.

Important *Please be aware that consolidation is just a method of deletion, but not an alternative to deletion. The resulting backup will not contain data that was present in the deleted backup and was absent from the retained incremental or differential backup.*

This option is *not* effective if any of the following is true:

- The backup destination is the cloud storage.
- The backup scheme is set to **Always incremental (single-file)**.
- The backup format (p. 58) is set to **Version 12**.

Backups stored in the cloud storage, as well as single-file backups (both version 11 and 12 formats), are always consolidated because their inner structure makes for fast and easy consolidation.

However, if version 12 format is used, and multiple backup chains are present (every chain being stored in a separate .tibx file), consolidation works only within the last chain. Any other chain is deleted as a whole, except for the first one, which is shrunk to the minimum size to keep the meta information (~12 KB). This meta information is required to ensure the data consistency during simultaneous read and write operations. The backups included in these chains disappear from the GUI as soon as the retention rule is applied, although they physically exist until the entire chain is deleted.

In all other cases, backups whose deletion is postponed are marked with the trash can icon (🗑) in the GUI. If you delete such a backup by clicking the X sign, consolidation will be performed.

8.9.3 Backup format

This option defines the format of the backups created by the backup plan. You can choose between the new format (**Version 12**) designed for faster backup and recovery, and the legacy format (**Version 11**) preserved for backward compatibility and special cases.

This option is *not* available for backups of websites, Office 365 data, and G Suite data. These backups always have the new format.

The preset is: **Automatic selection**.

You can select one of the following:

- **Automatic selection**

  Version 12 will be used unless the backup plan appends backups to the ones created by earlier product versions.
- **Version 12**

  A new format recommended in most cases for fast backup and recovery. Each backup chain (a full or differential backup, and all incremental backups that depend on it) is saved to a single .tibx file.
- **Version 11**

  A legacy format to be used in a new backup plan that appends backups to the ones created by earlier product versions.

  Also, use this format (with any backup scheme except for **Always incremental (single-file)**) if you want full, incremental, and differential backups to be separate files.

Backup format and backup files

For backup locations that can be browsed with a file manager (such as local or network folders), the backup format determines the number of files and their extension. The following table lists the files that can be created per machine or mailbox.

	Always incremental (single-file)	Other backup schemes
Version 11 backup format	One .tib file and one .xml metadata file	Multiple .tib files and one .xml metadata file (traditional format)
Version 12 backup format	One .tibx file per backup chain (a full or differential backup, and all incremental backups that depend on it)	

Changing the backup format

For disk-level backups, after the backup plan is applied, the backup format cannot be modified.

For file-level backups and database backups, after the backup plan is applied, it is possible to change the backup format from **Version 11** to **Version 12**. The reverse operation is not possible.

If you change the backup format:

- The next backup will be full.
- In backup locations that can be browsed with a file manager (such as local or network folders), a new .tibx file will be created. The new file will have the name of the original file, appended with the **_v12A** suffix.
- Retention rules and replication will be applied only to the new backups.
- The old backups will not be deleted and will remain available on the **Backups** tab. You can delete them manually.
- The old cloud backups will not consume the **Cloud storage** quota.
- The old local backups will consume the **Local backup** quota until you delete them manually.

8.9.4 Backup validation

Validation is an operation that checks the possibility of data recovery from a backup. When this option is enabled, each backup created by the backup plan is validated immediately after creation.

The preset is: **Disabled**.

Validation calculates a checksum for every data block that can be recovered from the backup. The only exception is validation of file-level backups that are located in the cloud storage. These backups are validated by checking consistency of the metadata saved in the backup.

Validation is a time-consuming process, even for an incremental or differential backup, which are small in size. This is because the operation validates not only the data physically contained in the backup, but all of the data recoverable by selecting the backup. This requires access to previously created backups.

While the successful validation means a high probability of successful recovery, it does not check all factors that influence the recovery process. If you back up the operating system, we recommend performing a test recovery under the bootable media to a spare hard drive or running a virtual machine from the backup (p. 161) in the ESXi or Hyper-V environment.

8.9.5 Backup start conditions

This option is effective in Windows and Linux operating systems.

This option determines the program behavior in case a backup is about to start (the scheduled time comes or the event specified in the schedule occurs), but the condition (or any of multiple conditions) is not met. For more information about conditions refer to "Start conditions" (p. 46).

The preset is: **Wait until the conditions are met.**

Wait until the conditions are met

With this setting, the scheduler starts monitoring the conditions and launches the backup as soon as the conditions are met. If the conditions are never met, the backup will never start.

To handle the situation when the conditions are not met for too long and further delaying the backup is becoming risky, you can set the time interval after which the backup will run irrespective of the condition. Select the **Start the backup anyway after** check box and specify the time interval. The backup will start as soon as the conditions are met OR the maximum time delay lapses, depending on which comes first.

Skip the scheduled backup

Delaying a backup might be unacceptable, for example, when you need to back up data strictly at the specified time. Then it makes sense to skip the backup rather than wait for the conditions, especially if the backups occur relatively often.

8.9.6 Changed block tracking (CBT)

This option is effective for disk-level backups of virtual machines and of physical machines running Windows. It is also effective for backups of Microsoft SQL Server databases and Microsoft Exchange Server databases.

The preset is: **Enabled**.

This option determines whether to use Changed Block Tracking (CBT) when performing an incremental or differential backup.

The CBT technology accelerates the backup process. Changes to the disk or database content are continuously tracked at the block level. When a backup starts, the changes can be immediately saved to the backup.

8.9.7 Compression level

The option defines the level of compression applied to the data being backed up. The available levels are: **None**, **Normal**, **High**.

The preset is: **Normal**.

A higher compression level means that the backup process takes longer, but the resulting backup occupies less space.

The optimal data compression level depends on the type of data being backed up. For example, even maximum compression will not significantly reduce the backup size if the backup contains essentially compressed files, such as .jpg, .pdf or .mp3. However, formats such as .doc or .xls will be compressed well.

8.9.8 Error handling

These options enable you to specify how to handle errors that might occur during backup.

Re-attempt, if an error occurs

The preset is: **Enabled. Number of attempts: 30. Interval between attempts: 30 seconds.**

When a recoverable error occurs, the program re-attempts to perform the unsuccessful operation. You can set the time interval and the number of attempts. The attempts will be stopped as soon as the operation succeeds OR the specified number of attempts are performed, depending on which comes first.

For example, if the backup destination on the network becomes unavailable or not reachable, the program will attempt to reach the destination every 30 seconds, but no more than 30 times. The attempts will be stopped as soon as the connection is resumed OR the specified number of attempts is performed, depending on which comes first.

Cloud storage

If the cloud storage is selected as a backup destination, the option value is automatically set to **Enabled**. **Number of attempts: 300**. **Interval between attempts: 30 seconds.**

In this case, the actual number of attempts is unlimited, but the timeout before the backup failure is calculated as follows: (300 seconds + **Interval between attempts**) * (**Number of attempts** + 1).

Examples:

- With the default values, the backup will fail after (300 seconds + 30 seconds) * (300 + 1) = 99330 seconds, or ~27.6 hours.
- If you set **Number of attempts** to 1 and **Interval between attempts** to 1 second, the backup will fail after (300 seconds + 1 second) * (1 + 1) = 602 seconds, or ~10 minutes.

If the calculated timeout exceeds 30 minutes, and the data transfer has not started yet, the actual timeout is set to 30 minutes.

Do not show messages and dialogs while processing (silent mode)

The preset is: **Enabled**.

With the silent mode enabled, the program will automatically handle situations requiring user interaction (except for handling bad sectors, which is defined as a separate option). If an operation cannot continue without user interaction, it will fail. Details of the operation, including errors, if any, can be found in the operation log.

Ignore bad sectors

The preset is: **Disabled**.

When this option is disabled, each time the program comes across a bad sector, the backup activity will be assigned the **Interaction required** status. In order to back up the valid information on a rapidly dying disk, enable ignoring bad sectors. The rest of the data will be backed up and you will be able to mount the resulting disk backup and extract valid files to another disk.

Re-attempt, if an error occurs during VM snapshot creation

The preset is: **Enabled. Number of attempts: 3. Interval between attempts: 5 minutes.**

When taking a virtual machine snapshot fails, the program re-attempts to perform the unsuccessful operation. You can set the time interval and the number of attempts. The attempts will be stopped as soon as the operation succeeds OR the specified number of attempts are performed, depending on which comes first.

8.9.9 Fast incremental/differential backup

This option is effective for incremental and differential disk-level backup.

The preset is: **Enabled**.

Incremental or differential backup captures only data changes. To speed up the backup process, the program determines whether a file has changed or not by the file size and the date/time when the file was last modified. Disabling this feature will make the program compare the entire file contents to those stored in the backup.

8.9.10 File filters

File filters define which files and folders to skip during the backup process.

File filters are available for both disk-level and file-level backup, unless stated otherwise.

To enable file filters

1. Select the data to back up.
2. Click the gear icon next to the backup plan name, and then click **Backup options**.
3. Select **File filters**.
4. Use any of the options described below.

Exclude files matching specific criteria

There are two options that function in an inverse manner.

- **Back up only files matching the following criteria**

  Example: If you select to back up the entire machine and specify **C:\File.exe** in the filter criteria, only this file will be backed up.

  Note *This filter is not effective for file-level backup if **Version 11** is selected in **Backup format** (p. 58) and the backup destination is NOT cloud storage.*

- **Do not back up files matching the following criteria**

  Example: If you select to back up the entire machine and specify **C:\File.exe** in the filter criteria, only this file will be skipped.

It is possible to use both options simultaneously. The latter option overrides the former, i.e. if you specify **C:\File.exe** in both fields, this file will be skipped during a backup.

Criteria

- **Full path**

  Specify the full path to the file or folder, starting with the drive letter (when backing up Windows) or the root directory (when backing up Linux or macOS).

  Both in Windows and Linux/macOS, you can use a forward slash in the file or folder path (as in **C:/Temp/File.tmp**). In Windows, you can also use the traditional backslash (as in **C:\Temp\File.tmp**).

- **Name**

Specify the name of the file or folder, such as **Document.txt**. All files and folders with that name will be selected.

The criteria are *not* case-sensitive. For example, by specifying **C:\Temp**, you will also select **C:\TEMP**, **C:\temp**, and so on.

You can use one or more wildcard characters (*, **, and ?) in the criterion. These characters can be used both within the full path and in the file or folder name.

The asterisk (*) substitutes for zero or more characters in a file name. For example, the criterion **Doc*.txt** matches files such as **Doc.txt** and **Document.txt**

The double asterisk (**) substitutes for zero or more characters in a file name and path, including the slash character. For example, the criterion ****/Docs/**.txt** matches all txt files in all subfolders of all folders **Docs**.

The question mark (?) substitutes for exactly one character in a file name. For example, the criterion **Doc?.txt** matches files such as **Doc1.txt** and **Docs.txt**, but not the files **Doc.txt** or **Doc11.txt**

Exclude hidden files and folders

Select this check box to skip files and folders that have the **Hidden** attribute (for file systems that are supported by Windows) or that start with a period (.) (for file systems in Linux, such as Ext2 and Ext3). If a folder is hidden, all of its contents (including files that are not hidden) will be excluded.

Exclude system files and folders

This option is effective only for file systems that are supported by Windows. Select this check box to skip files and folders with the **System** attribute. If a folder has the **System** attribute, all of its contents (including files that do not have the **System** attribute) will be excluded.

Tip *You can view file or folder attributes in the file/folder properties or by using the attrib command. For more information, refer to the Help and Support Center in Windows.*

8.9.11 File-level backup snapshot

This option is effective only for file-level backup.

This option defines whether to back up files one by one or by taking an instant data snapshot.

Note *Files that are stored on network shares are always backed up one by one.*

The preset is:

- If only machines running Linux are selected for backup: **Do not create a snapshot.**
- Otherwise: **Create snapshot if it is possible.**

You can select one of the following:

- **Create a snapshot if it is possible**

  Back up files directly if taking a snapshot is not possible.
- **Always create a snapshot**

  The snapshot enables backing up of all files including files opened for exclusive access. The files will be backed up at the same point in time. Choose this setting only if these factors are critical, that is, backing up files without a snapshot does not make sense. If a snapshot cannot be taken, the backup will fail.

- **Do not create a snapshot**

  Always back up files directly. Trying to back up files that are opened for exclusive access will result in a read error. Files in the backup may be not time-consistent.

8.9.12 Log truncation

This option is effective for backup of Microsoft SQL Server databases and for disk-level backup with enabled Microsoft SQL Server application backup.

This option defines whether the SQL Server transaction logs are truncated after a successful backup.

The preset is: **Enabled**.

When this option is enabled, a database can be recovered only to a point in time of a backup created by this software. Disable this option if you back up transaction logs by using the native backup engine of Microsoft SQL Server. You will be able to apply the transaction logs after a recovery and thus recover a database to any point in time.

8.9.13 LVM snapshotting

This option is effective only for physical machines.

This option is effective for disk-level backup of volumes managed by Linux Logical Volume Manager (LVM). Such volumes are also called logical volumes.

This option defines how a snapshot of a logical volume is taken. The backup software can do this on its own or rely on Linux Logical Volume Manager (LVM).

The preset is: **By the backup software**.

- **By the backup software**. The snapshot data is kept mostly in RAM. The backup is faster and unallocated space on the volume group is not required. Therefore, we recommend changing the preset only if you are experiencing problems with backing up logical volumes.
- **By LVM**. The snapshot is stored on unallocated space of the volume group. If the unallocated space is missing, the snapshot will be taken by the backup software.

8.9.14 Mount points

This option is effective only in Windows for a file-level backup of a data source that includes mounted volumes or cluster shared volumes.

This option is effective only when you select for backup a folder that is higher in the folder hierarchy than the mount point. (A mount point is a folder on which an additional volume is logically attached.)

- If such folder (a parent folder) is selected for backup, and the **Mount points** option is enabled, all files located on the mounted volume will be included in the backup. If the **Mount points** option is disabled, the mount point in the backup will be empty.

  During recovery of a parent folder, the mount point content will or will not be recovered, depending on whether the **Mount points** option for recovery (p. 90) is enabled or disabled.
- If you select the mount point directly, or select any folder within the mounted volume, the selected folders will be considered as ordinary folders. They will be backed up regardless of the state of the **Mount points** option and recovered regardless of the state of the **Mount points** option for recovery (p. 90).

The preset is: **Disabled**.

Tip. *You can back up Hyper-V virtual machines residing on a cluster shared volume by backing up the required files or the entire volume with file-level backup. Just power off the virtual machines to be sure that they are backed up in a consistent state.*

Example

Let's assume that the **C:\Data1\** folder is a mount point for the mounted volume. The volume contains folders **Folder1** and **Folder2**. You create a backup plan for file-level backup of your data.

If you select the check box for volume C and enable the **Mount points** option, the **C:\Data1\** folder in your backup will contain **Folder1** and **Folder2**. When recovering the backed-up data, be aware of proper using the **Mount points** option for recovery (p. 90).

If you select the check box for volume C, and disable the **Mount points** option, the **C:\Data1\** folder in your backup will be empty.

If you select the check box for the **Data1**, **Folder1** or **Folder2** folder, the checked folders will be included in the backup as ordinary folders, regardless of the state of the **Mount points** option.

8.9.15 Multi-volume snapshot

This option is effective for backups of physical machines running Windows or Linux.

This option applies to disk-level backup. This option also applies to file-level backup when the file-level backup is performed by taking a snapshot. (The "File-level backup snapshot" (p. 63) option determines whether a snapshot is taken during file-level backup).

This option determines whether to take snapshots of multiple volumes at the same time or one by one.

The preset is:

- If at least one machine running Windows is selected for backup: **Enabled**.
- Otherwise: **Disabled**.

When this option is enabled, snapshots of all volumes being backed up are created simultaneously. Use this option to create a time-consistent backup of data spanning multiple volumes; for instance, for an Oracle database.

When this option is disabled, the volumes' snapshots are taken one after the other. As a result, if the data spans several volumes, the resulting backup may be not consistent.

8.9.16 Performance

Process priority

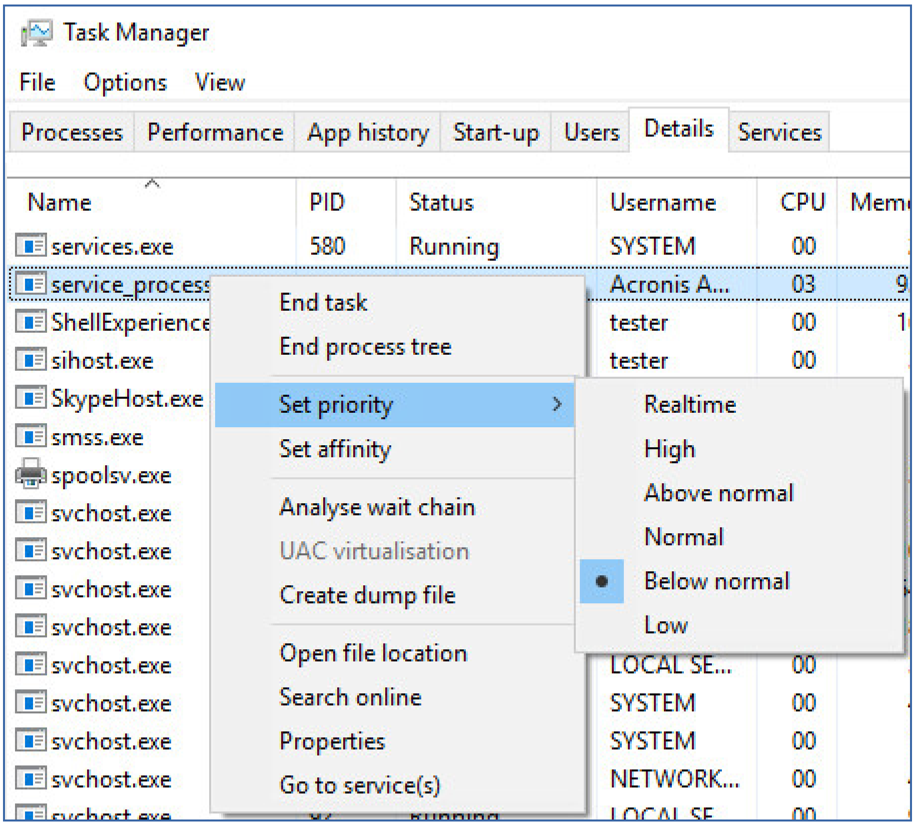
This option defines the priority of the backup process in the operating system.

The available settings are: **Low**, **Normal**, **High**.

The preset is: **Low** (in Windows, corresponds to **Below normal**).

The priority of a process running in a system determines the amount of CPU and system resources allocated to that process. Decreasing the backup priority will free more resources for other applications. Increasing the backup priority might speed up the backup process by requesting the operating system to allocate more resources like the CPU to the backup application. However, the resulting effect will depend on the overall CPU usage and other factors like disk in/out speed or network traffic.

This option sets the priority of the backup process (**service_process.exe)** in Windows and the niceness of the backup process (**service_process)** in Linux and macOS.



Name	PID	Status	Username	CPU	Mem
services.exe	580	Running	SYSTEM	00	
service_process			Acronis A...	03	9
ShellExperience			tester	00	1
sihost.exe			tester	00	
SkypeHost.exe					
smss.exe					
spoolsv.exe					
svchost.exe					
svchost.exe					
svchost.exe					
svchost.exe					
svchost.exe			LOCAL SE...	00	
svchost.exe			SYSTEM	00	
svchost.exe			SYSTEM	00	
svchost.exe			NETWORK...	00	

Output speed during backup

This option enables you to limit the hard drive writing speed (when backing up to a local folder) or the speed of transferring the backup data through the network (when backing up to a network share or to cloud storage).

The preset is: **Disabled**.

When this option is enabled, you can specify the maximum allowed output speed in KB/second.

8.9.17 Physical Data Shipping

This option is effective if the backup destination is the cloud storage and the backup format (p. 58) is set to **Version 12**.

This option is effective for disk-level backups and file backups created by Agent for Windows, Agent for Linux, Agent for Mac, Agent for VMware, Agent for Hyper-V, and Agent for Virtuozzo.

This option determines whether the first full backup created by the backup plan will be sent to the cloud storage on a hard disk drive by using the Physical Data Shipping service. The subsequent incremental backups can be performed over the network.

The preset is: **Disabled.**

About the Physical Data Shipping service

The Physical Data Shipping service web interface is available only to administrators.

For detailed instructions about using the Physical Data Shipping service and the order creation tool, refer to the Physical Data Shipping Administrator's Guide. To access this document in the Physical Data Shipping service web interface, click the question mark icon.

Overview of the physical data shipping process

1. Create a new backup plan. In this plan, enable the **Physical Data Shipping** backup option.

   You can back up directly to the drive or back up to a local or a network folder, and then copy/move the backup(s) to the drive.

   Important *Once the initial full backup is done, the subsequent backups must be performed by the same backup plan. Another backup plan, even with the same parameters and for the same machine, will require another Physical Data Shipping cycle.*

2. After the first backup is complete, use the Physical Data Shipping service web interface to download the order creation tool and create the order.

   To access this web interface, log in to the management portal, click **Overview** > **Usage**, and then click **Manage service** under **Physical Data Shipping**.
3. Package the drives and ship them to the data center.

   Important *Ensure that you follow the packaging instructions provided in the Physical Data Shipping Administrator's Guide.*

4. Track the order status by using the Physical Data Shipping service web interface. Note that the subsequent backups will fail until the initial backup is uploaded to the cloud storage.

8.9.18 Pre/Post commands

The option enables you to define the commands to be automatically executed before and after the backup procedure.

The following scheme illustrates when pre/post commands are executed.

Pre-backup command	Backup	Post-backup command

Examples of how you can use the pre/post commands:

- Delete some temporary files from the disk before starting backup.
- Configure a third-party antivirus product to be started each time before the backup starts.
- Selectively copy backups to another location. This option may be useful because the replication configured in a backup plan copies *every* backup to subsequent locations.

The agent performs the replication *after* executing the post-backup command.

The program does not support interactive commands, i.e. commands that require user input (for example, "pause").

8.9.18.1 Pre-backup command

To specify a command/batch file to be executed before the backup process starts

1. Enable the **Execute a command before the backup** switch.
2. In the **Command...** field, type a command or browse to a batch file. The program does not support interactive commands, i.e. commands that require user input (for example, "pause".)

3. In the **Working directory** field, specify a path to a directory where the command/batch file will be executed.
4. In the **Arguments** field specify the command's execution arguments, if required.
5. Depending on the result you want to obtain, select the appropriate options as described in the table below.
6. Click **Done**.

Check box	**Selection**			
Fail the backup if the command execution fails*	Selected	Cleared	Selected	Cleared
Do not back up until the command execution is complete	Selected	Selected	Cleared	Cleared
Result				
	Preset Perform the backup only after the command is successfully executed. Fail the backup if the command execution fails.	Perform the backup after the command is executed despite execution failure or success.	N/A	Perform the backup concurrently with the command execution and irrespective of the command execution result.

* A command is considered failed if its exit code is not equal to zero.

8.9.18.2 Post-backup command

To specify a command/executable file to be executed after the backup is completed

1. Enable the **Execute a command after the backup** switch.
2. In the **Command...** field, type a command or browse to a batch file.
3. In the **Working directory** field, specify a path to a directory where the command/batch file will be executed.
4. In the **Arguments** field, specify the command execution arguments, if required.
5. Select the **Fail the backup if the command execution fails** check box if successful execution of the command is critical for you. The command is considered failed if its exit code is not equal to zero. If the command execution fails, the backup status will be set to **Error**.

   When the check box is not selected, the command execution result does not affect the backup failure or success. You can track the command execution result by exploring the **Activities** tab.
6. Click **Done**.

8.9.19 Pre/Post data capture commands

The option enables you to define the commands to be automatically executed before and after data capture (that is, taking the data snapshot). Data capture is performed at the beginning of the backup procedure.

The following scheme illustrates when the pre/post data capture commands are executed.

	<----------------------------	Backup	---------------------------->		
Pre-backup command	Pre-data capture command	Data capture	Post-data capture command		Post-backup command

If the Volume Shadow Copy Service option (p. 72) is enabled, the commands' execution and the Microsoft VSS actions will be sequenced as follows:

"Before data capture” commands -> VSS Suspend -> Data capture -> VSS Resume -> "After data capture" commands.

By using the pre/post data capture commands, you can suspend and resume a database or application that is not compatible with VSS. Because the data capture takes seconds, the database or application idle time will be minimal.

8.9.19.1 Pre-data capture command

To specify a command/batch file to be executed before data capture

1. Enable the **Execute a command before the data capture** switch.
2. In the **Command...** field, type a command or browse to a batch file. The program does not support interactive commands, i.e. commands that require user input (for example, "pause".)
3. In the **Working directory** field, specify a path to a directory where the command/batch file will be executed.
4. In the **Arguments** field specify the command’s execution arguments, if required.
5. Depending on the result you want to obtain, select the appropriate options as described in the table below.
6. Click **Done**.

Check box	**Selection**			
Fail the backup if the command execution fails*	Selected	Cleared	Selected	Cleared
Do not perform the data capture until the command execution is complete	Selected	Selected	Cleared	Cleared
Result				
	Preset Perform the data capture only after the command is successfully executed. Fail the backup if the command execution fails.	Perform the data capture after the command is executed despite execution failure or success.	N/A	Perform the data capture concurrently with the command and irrespective of the command execution result.

* A command is considered failed if its exit code is not equal to zero.

8.9.19.2 Post-data capture command

To specify a command/batch file to be executed after data capture

1. Enable the **Execute a command after the data capture** switch.

2. In the **Command...** field, type a command or browse to a batch file. The program does not support interactive commands, i.e. commands that require user input (for example, "pause".)
3. In the **Working directory** field, specify a path to a directory where the command/batch file will be executed.
4. In the **Arguments** field specify the command's execution arguments, if required.
5. Depending on the result you want to obtain, select the appropriate options as described in the table below.
6. Click **Done**.

Check box	**Selection**			
Fail the backup if the command execution fails*	Selected	Cleared	Selected	Cleared
Do not back up until the command execution is complete	Selected	Selected	Cleared	Cleared
Result				
	Preset Continue the backup only after the command is successfully executed.	Continue the backup after the command is executed despite command execution failure or success.	N/A	Continue the backup concurrently with the command execution and irrespective of the command execution result.

* A command is considered failed if its exit code is not equal to zero.

8.9.20 Scheduling

This option defines whether backups start as scheduled or with a delay, and how many virtual machines are backed up simultaneously.

The preset is: **Distribute backup start times within a time window. Maximum delay: 30 minutes.**

You can select one of the following:

- **Start all backups exactly as scheduled**

  Backups of physical machines will start exactly as scheduled. Virtual machines will be backed up one by one.

- **Distribute start times within a time window**

  Backups of physical machines will start with a delay from the scheduled time. The delay value for each machine is selected randomly and ranges from zero to the maximum value you specify. You may want to use this setting when backing up multiple machines to a network location, to avoid excessive network load. The delay value for each machine is determined when the backup plan is applied to the machine and remains the same until you edit the backup plan and change the maximum delay value.

  Virtual machines will be backed up one by one.

- **Limit the number of simultaneously running backups by**

  This option is available only when a backup plan is applied to multiple virtual machines. This option defines how many virtual machines an agent can back up simultaneously when executing the given backup plan.

If, according to the backup plan, an agent has to start backing up multiple machines at once, it will choose two machines. (To optimize the backup performance, the agent tries to match machines stored on different storages.) Once any of the two backups is completed, the agent chooses the third machine and so on.

You can change the number of virtual machines for an agent to simultaneously back up. The maximum value is 10. However, if the agent executes multiple backup plans that overlap in time, the numbers specified in their options are added up. You can limit the total number of virtual machines (p. 176) that an agent can back up simultaneously, no matter how many backup plans are running.

Backups of physical machines will start exactly as scheduled.

8.9.21 Sector-by-sector backup

The option is effective only for disk-level backup.

This option defines whether an exact copy of a disk or volume on a physical level is created.

The preset is: **Disabled**.

If this option is enabled, all disk or volume's sectors will be backed up, including unallocated space and those sectors that are free of data. The resulting backup will be equal in size to the disk being backed up (if the "Compression level" (p. 60) option is set to **None**). The software automatically switches to the sector-by-sector mode when backing up drives with unrecognized or unsupported file systems.

8.9.22 Splitting

This option is effective for the **Always full**; **Weekly full, Daily incremental**; and **Custom** backup schemes.

This option enables you to select the method of splitting of large backups into smaller files.

The preset is: **Automatic**.

The following settings are available:

- **Automatic**

  A backup will be split if it exceeds the maximum file size supported by the file system.

- **Fixed size**

  Enter the desired file size or select it from the drop-down list.

8.9.23 Task failure handling

This option determines the program behavior when a scheduled execution of a backup plan fails. This option is not effective when a backup plan is started manually.

If this option is enabled, the program will try to execute the backup plan again. You can specify the number of attempts and the time interval between the attempts. The program stops trying as soon as an attempt completes successfully OR the specified number of attempts is performed, depending on which comes first.

The preset is: **Disabled**.

8.9.24 Volume Shadow Copy Service (VSS)

This option is effective only for Windows operating systems.

The option defines whether a Volume Shadow Copy Service (VSS) provider has to notify VSS-aware applications that the backup is about to start. This ensures the consistent state of all data used by the applications; in particular, completion of all database transactions at the moment of taking the data snapshot by the backup software. Data consistency, in turn, ensures that the application will be recovered in the correct state and become operational immediately after recovery.

The preset is: **Enabled**. **Automatically select snapshot provider**.

You can select one of the following:

- **Automatically select snapshot provider**

  Automatically select among the hardware snapshot provider, software snapshot providers, and Microsoft Software Shadow Copy provider.

- **Use Microsoft Software Shadow Copy provider**

  We recommend choosing this option when backing up application servers (Microsoft Exchange Server, Microsoft SQL Server, Microsoft SharePoint, or Active Directory).

Disable this option if your database is incompatible with VSS. Snapshots are taken faster, but data consistency of the applications whose transactions are not completed at the time of taking a snapshot cannot be guaranteed. You may use Pre/Post data capture commands (p. 68) to ensure that the data is backed up in a consistent state. For instance, specify pre-data capture commands that will suspend the database and flush all caches to ensure that all transactions are completed; and specify post-data capture commands that will resume the database operations after the snapshot is taken.

***Note** If this option is enabled, files and folders that are specified in the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot** registry key are not backed up. In particular, offline Outlook Data Files (.ost) are not backed up because they are specified in the **OutlookOST** value of this key.*

Enable VSS full backup

If this option is enabled, logs of Microsoft Exchange Server and of other VSS-aware applications (except for Microsoft SQL Server) will be truncated after each successful full, incremental or differential disk-level backup.

The preset is: **Disabled**.

Leave this option disabled in the following cases:

- If you use Agent for Exchange or third-party software for backing up the Exchange Server data. This is because the log truncation will interfere with the consecutive transaction log backups.
- If you use third-party software for backing up the SQL Server data. The reason for this is that the third-party software will take the resulting disk-level backup for its "own" full backup. As a result, the next differential backup of the SQL Server data will fail. The backups will continue failing until the third-party software creates the next "own" full backup.
- If other VSS-aware applications are running on the machine and you need to keep their logs for any reason.

Enabling this option does not result in the truncation of Microsoft SQL Server logs. To truncate the SQL Server log after a backup, enable the Log truncation (p. 64) backup option.

8.9.25 Volume Shadow Copy Service (VSS) for virtual machines

This option defines whether quiesced snapshots of virtual machines are taken. To take a quiesced snapshot, the backup software applies VSS inside a virtual machine by using VMware Tools or Hyper-V Integration Services.

The preset is: **Enabled**.

If this option is enabled, transactions of all VSS-aware applications running in a virtual machine are completed before taking snapshot. If a quiesced snapshot fails after the number of re-attempts specified in the "Error handling" (p. 61) option, and application backup is disabled, a non-quiesced snapshot is taken. If application backup is enabled, the backup fails.

If this option is disabled, a non-quiesced snapshot is taken. The virtual machine will be backed up in a crash-consistent state.

8.9.26 Weekly backup

This option determines which backups are considered "weekly" in retention rules and backup schemes. A "weekly" backup is the first backup created after a week starts.

The preset is: **Monday**.

8.9.27 Windows event log

This option is effective only in Windows operating systems.

This option defines whether the agents have to log events of the backup operations in the Application Event Log of Windows (to see this log, run eventvwr.exe or select **Control Panel** > **Administrative tools** > **Event Viewer**). You can filter the events to be logged.

The preset is: **Disabled**.

9 Recovery

9.1 Recovery cheat sheet

The following table summarizes the available recovery methods. Use the table to choose a recovery method that best fits your need.

What to recover	Recovery method
Physical machine (Windows or Linux)	Using the web interface (p. 75) Using bootable media (p. 79)
Physical machine (Mac)	Using bootable media (p. 79)
Virtual machine (VMware or Hyper-V)	Using the web interface (p. 77) Using bootable media (p. 79)
Virtual machine or container (Virtuozzo)	Using the web interface (p. 77)
ESXi configuration	Using bootable media (p. 87)
Files/Folders	Using the web interface (p. 82) Downloading files from the cloud storage (p. 83) Using bootable media (p. 85) Extracting files from local backups (p. 86)

What to recover		Recovery method
System state		Using the web interface (p. 86)
SQL databases		Using the web interface (p. 123)
Exchange databases		Using the web interface (p. 126)
Exchange mailboxes		Using the web interface (p. 127)
Websites		Using the web interface (p. 160)
Microsoft Office 365	Mailboxes (local Agent for Office 365)	Using the web interface (p. 133)
	Mailboxes (cloud Agent for Office 365)	Using the web interface (p. 136)
	OneDrive files	Using the web interface (p. 139)
	SharePoint Online data	Using the web interface (p. 142)
G Suite	Mailboxes	Using the web interface (p. 147)
	Google Drive files	Using the web interface (p. 150)
	Team Drive files	Using the web interface (p. 153)

Note for Mac users

- Starting with 10.11 El Capitan, certain system files, folders, and processes are flagged for protection with an extended file attribute com.apple.rootless. This feature is called System Integrity Protection (SIP). The protected files include preinstalled applications and most of the folders in /system, /bin, /sbin, /usr.

  The protected files and folders cannot be overwritten during a recovery under the operating system. If you need to overwrite the protected files, perform the recovery under bootable media.
- Starting with macOS Sierra 10.12, rarely used files can be moved to iCloud by the Store in Cloud feature. Small footprints of these files are kept on the file system. These footprints are backed up instead of the original files.

  When you recover a footprint to the original location, it is synchronized with iCloud and the original file becomes available. When you recover a footprint to a different location, it cannot be synchronized and the original file will be unavailable.

9.2 Creating bootable media

Bootable media is a CD, DVD, USB flash drive, or other removable media that enables you to run the agent without the help of an operating system. The main purpose of bootable media is to recover an operating system that cannot start.

We highly recommend that you create and test a bootable media as soon as you start using disk-level backup. Also, it is a good practice to re-create the media after each major update of the backup agent.

You can recover either Windows or Linux by using the same media. To recover macOS, create a separate media on a machine running macOS.

To create bootable media in Windows or Linux

1. Download the bootable media ISO file. To download the file, select a machine, and then click **Recover** > **More ways to recover...** > **Download ISO image**.
2. [Optional] Copy and print, or write down the registration token displayed by the backup console.

This token allows access to the cloud storage from bootable media without entering a login and password. It is necessary if you do not have a direct login to the cloud, but use third-party authentication instead.

3. Do any of the following:
   - Burn a CD/DVD using the ISO file.
   - Create a bootable USB flash drive by using the ISO file and one of the free tools available online.

     Use `ISO to USB` or RUFUS if you need to boot an UEFI machine, `Win32DiskImager` for a BIOS machine. In Linux, using the dd utility makes sense.
   - Connect the ISO file as a CD/DVD drive to the virtual machine that you want to recover.

To create bootable media in macOS

1. On a machine where Agent for Mac is installed, click **Applications** > **Rescue Media Builder**.
2. The software displays the connected removable media. Select the one that you want to make bootable.

   Warning *All data on the disk will be erased.*
3. Click **Create**.
4. Wait while the software creates the bootable media.

9.3 Recovering a machine

9.3.1 Physical machine

This section describes recovery of physical machines by using the web interface.

Use bootable media instead of the web interface if you need to recover:

- macOS
- Any operating system to bare metal or to an offline machine

Recovery of an operating system requires a reboot. You can choose whether to restart the machine automatically or assign it the **Interaction required** status. The recovered operating system goes online automatically.

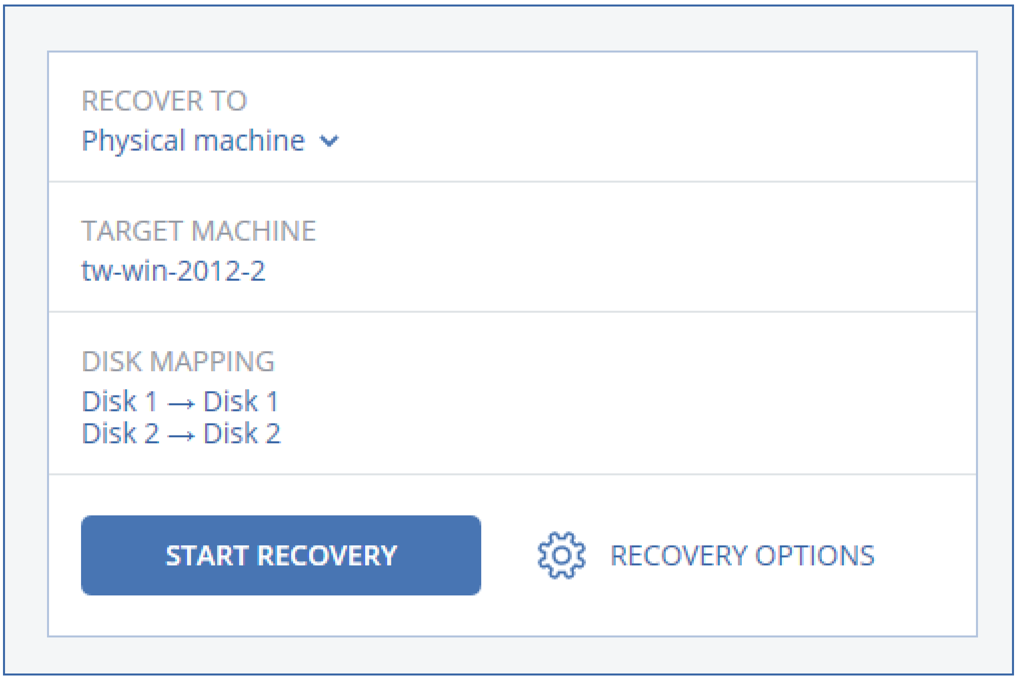
To recover a physical machine

1. Select the backed-up machine.
2. Click **Recovery**.
3. Select a recovery point. Note that recovery points are filtered by location.

   If the machine is offline, the recovery points are not displayed. Do any of the following:
   - If the backup location is cloud or shared storage (i.e. other agents can access it), click **Select machine**, select a target machine that is online, and then select a recovery point.
   - Select a recovery point on the Backups tab (p. 111).
   - Recover the machine as described in "Recovering disks by using bootable media" (p. 79).
4. Click **Recover** > **Entire machine**.

   The software automatically maps the disks from the backup to the disks of the target machine.
   - To recover to another physical machine, click **Target machine**, and then select a target machine that is online.

- If the disk mapping fails, recover the machine as described in "Recovering disks by using bootable media" (p. 79). The media enables you to choose disks for recovery and to map the disks manually.



RECOVER TO

Physical machine

TARGET MACHINE

tw-win-2012-2

DISK MAPPING

Disk 1 → Disk 1

Disk 2 → Disk 2

5. Click **Start recovery**.
6. Confirm that you want to overwrite the disks with their backed-up versions. Choose whether to restart the machine automatically.

The recovery progress is shown on the **Activities** tab.

9.3.2 Physical machine to virtual

This section describes recovery of a physical machine as a virtual machine by using the web interface. This operation can be performed if at least one Agent for VMware or Agent for Hyper-V is installed and registered.

For more information about P2V migration, refer to "Machine migration" (p. 169).

To recover a physical machine as a virtual machine

1. Select the backed-up machine.
2. Click **Recovery**.
3. Select a recovery point. Note that recovery points are filtered by location.

   If the machine is offline, the recovery points are not displayed. Do any of the following:

   - If the backup location is cloud or shared storage (i.e. other agents can access it), click **Select machine**, select a machine that is online, and then select a recovery point.
   - Select a recovery point on the Backups tab (p. 111).
   - Recover the machine as described in "Recovering disks by using bootable media" (p. 79).
4. Click **Recover** > **Entire machine**.
5. In **Recover to**, select **Virtual machine**.
6. Click **Target machine**.

   a. Select the hypervisor (**VMware ESXi** or **Hyper-V**).

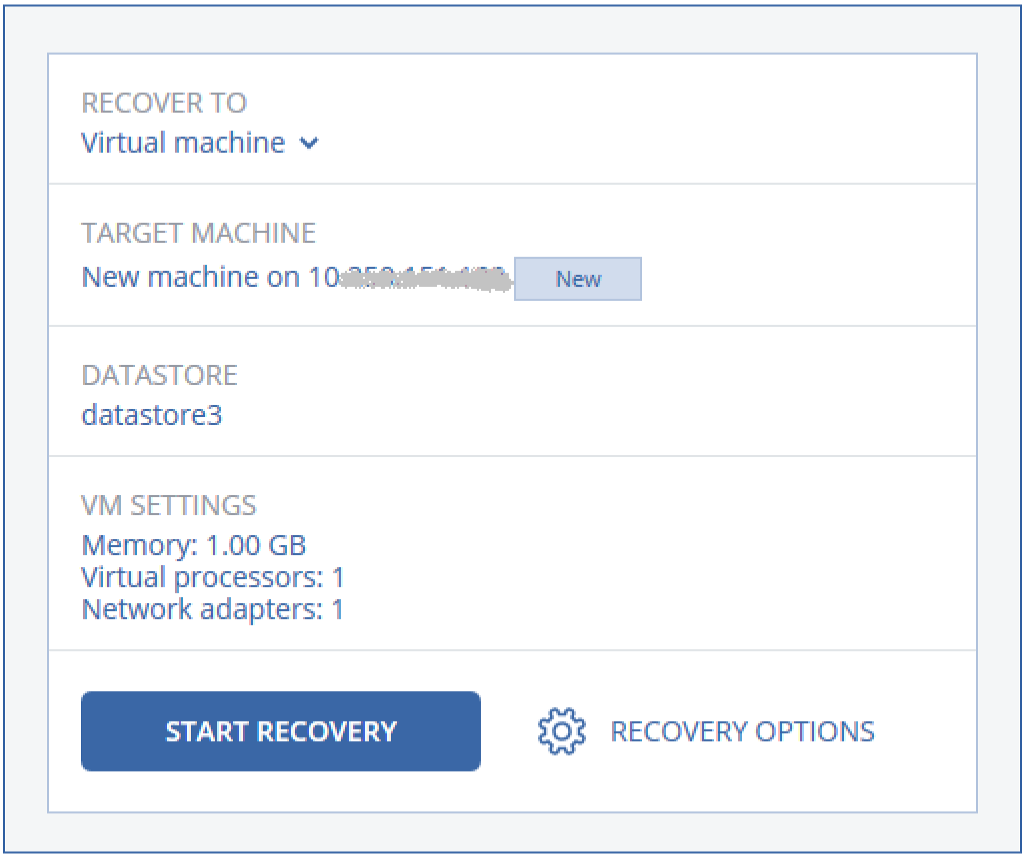
   At least one Agent for VMware or Agent for Hyper-V must be installed.

b. Select whether to recover to a new or existing machine. The new machine option is preferable as it does not require the disk configuration of the target machine to exactly match the disk configuration in the backup.

c. Select the host and specify the new machine name, or select an existing target machine.

d. Click **OK**.

7. [Optional] When recovering to a new machine, you can also do the following:
   - Click **Datastore** for ESXi or **Path** for Hyper-V, and then select the datastore (storage) for the virtual machine.
   - Click **VM settings** to change the memory size, the number of processors, and the network connections of the virtual machine.



RECOVER TO
Virtual machine

TARGET MACHINE
New machine on 10[redacted]

DATASTORE
datastore3

VM SETTINGS
Memory: 1.00 GB
Virtual processors: 1
Network adapters: 1

8. Click **Start recovery**.
9. When recovering to an existing virtual machine, confirm that you want to overwrite the disks.

The recovery progress is shown on the **Activities** tab.

9.3.3 Virtual machine

A virtual machine must be stopped during the recovery to this machine. The software stops the machine without a prompt. When the recovery is completed, you have to start the machine manually.

This behavior can be changed by using the VM power management recovery option (click **Recovery options** > **VM power management**).

To recover a virtual machine

1. Do one of the following:
   - Select a backed-up machine, click **Recovery**, and then select a recovery point.

- Select a recovery point on the Backups tab (p. 111).

2. Click **Recover** > **Entire machine**.
3. If you want to recover to a physical machine, select **Physical machine** in **Recover to**. Otherwise, skip this step.

   Recovery to a physical machine is possible only if the disk configuration of the target machine exactly matches the disk configuration in the backup.

   If this is the case, continue to step 4 in "Physical machine" (p. 75). Otherwise, we recommend that you perform the V2P migration by using bootable media (p. 79).
4. The software automatically selects the original machine as the target machine.

   To recover to another virtual machine, click **Target machine**, and then do the following:

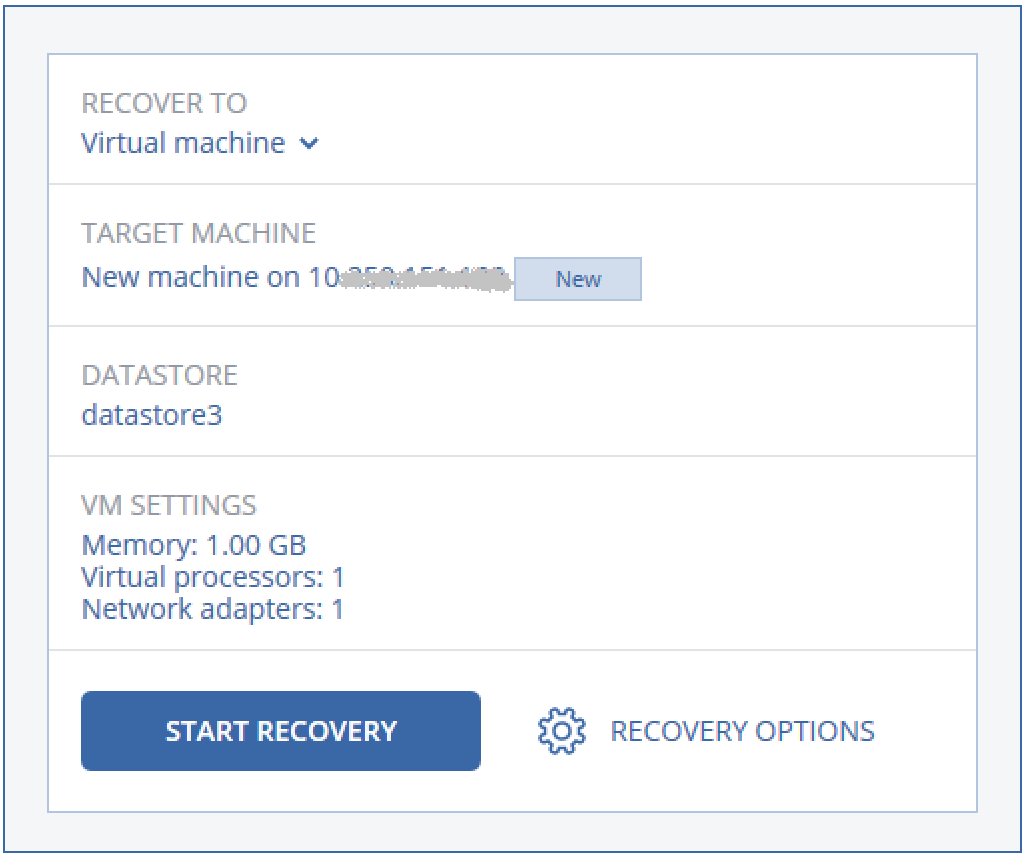
   a. Select the hypervisor (**VMware ESXi**, **Hyper-V**, or **Virtuozzo**).

      Only Virtuozzo virtual machines can be recovered to Virtuozzo. For more information about V2V migration, refer to "Machine migration" (p. 169).

   b. Select whether to recover to a new or existing machine.

   c. Select the host and specify the new machine name, or select an existing target machine.

   d. Click **OK**.
5. [Optional] When recovering to a new machine, you can also do the following:
   - Click **Datastore** for ESXi or **Path** for Hyper-V and Virtuozzo, and then select the datastore (storage) for the virtual machine.
   - Click **VM settings** to change the memory size, the number of processors, and the network connections of the virtual machine.



RECOVER TO
Virtual machine

TARGET MACHINE
New machine on 10[redacted]

DATASTORE
datastore3

VM SETTINGS
Memory: 1.00 GB
Virtual processors: 1
Network adapters: 1

6. Click **Start recovery**.
7. When recovering to an existing virtual machine, confirm that you want to overwrite the disks.

The recovery progress is shown on the **Activities** tab.

9.3.4 Recovering disks by using bootable media

For information about how to create bootable media, refer to "Creating bootable media" (p. 74).

To recover disks by using bootable media

1. Boot the target machine by using bootable media.
2. [Only when recovering a Mac] If you are recovering APFS-formatted disks/volumes to a non-original machine or to bare metal, re-create the original disk configuration manually:
   a. Click **Disk Utility**.
   b. Re-create the original disk configuration. For instructions, refer to https://support.apple.com/guide/disk-utility/welcome.
   c. Click **Disk Utility** > **Quit Disk Utility**.
3. Click **Manage this machine locally** or click **Rescue Bootable Media** twice, depending on the media type you are using.
4. If a proxy server is enabled in your network, click **Tools** > **Proxy server**, and then specify the proxy server host name/IP address, port, and credentials. Otherwise, skip this step.
5. [Optional] When recovering Windows or Linux, click **Tools** > **Register media in the backup service**, and then specify the registration token that you obtained when downloading the media. If you do this, you will not need to enter credentials or a registration code to access the cloud storage, as described in step 8.
6. On the welcome screen, click **Recover**.
7. Click **Select data**, and then click **Browse**.
8. Specify the backup location:
   - To recover from cloud storage, select **Cloud storage**. Enter the credentials of the account to which the backed up machine is assigned.

     When recovering Windows or Linux, you have the option to request a registration code and use it instead of the credentials. Click **Use registration code** > **Request the code**. The software shows the registration link and the registration code. You can copy them and perform the registration steps on a different machine. The registration code is valid for one hour.
   - To recover from a local or a network folder, browse to the folder under **Local folders** or **Network folders**.

   Click **OK** to confirm your selection.
9. Select the backup from which you want to recover the data. If prompted, type the password for the backup.
10. In **Backup contents**, select the disks that you want to recover. Click **OK** to confirm your selection.
11. Under **Where to recover**, the software automatically maps the selected disks to the target disks.

    If the mapping is not successful or if you are unsatisfied with the mapping result, you can re-map disks manually.

    Changing disk layout may affect the operating system bootability. Please use the original machine's disk layout unless you feel fully confident of success.
12. [When recovering Linux] If the backed-up machine had logical volumes (LVM) and you want to reproduce the original LVM structure:
    a. Ensure that the number of the target machine disks and each disk capacity are equal to or exceed those of the original machine, and then click **Apply RAID/LVM**.

   b. Review the volume structure, and then click **Apply RAID/LVM** to create it.

13. [Optional] Click **Recovery options** to specify additional settings.
14. Click **OK** to start the recovery.

9.3.5 Using Universal Restore

The most recent operating systems remain bootable when recovered to dissimilar hardware, including the VMware or Hyper-V platforms. If a recovered operating system does not boot, use the Universal Restore tool to update the drivers and modules that are critical for the operating system startup.

Universal Restore is applicable to Windows and Linux.

To apply Universal Restore

1. Boot the machine from the bootable media.
2. Click **Apply Universal Restore**.
3. If there are multiple operating systems on the machine, choose the one to apply Universal Restore to.
4. [For Windows only] Configure the additional settings (p. 80).
5. Click **OK**.

9.3.5.1 Universal Restore in Windows

Preparation

Prepare drivers

Before applying Universal Restore to a Windows operating system, make sure that you have the drivers for the new HDD controller and the chipset. These drivers are critical to start the operating system. Use the CD or DVD supplied by the hardware vendor or download the drivers from the vendor’s website. The driver files should have the *.inf extension. If you download the drivers in the *.exe, *.cab or *.zip format, extract them using a third-party application.

The best practice is to store drivers for all the hardware used in your organization in a single repository sorted by device type or by the hardware configurations. You can keep a copy of the repository on a DVD or a flash drive; pick some drivers and add them to the bootable media; create the custom bootable media with the necessary drivers (and the necessary network configuration) for each of your servers. Or, you can simply specify the path to the repository every time Universal Restore is used.

Check access to the drivers in bootable environment

Make sure you have access to the device with drivers when working under bootable media. Use WinPE-based media if the device is available in Windows but Linux-based media does not detect it.

Universal Restore settings

Automatic driver search

Specify where the program will search for the Hardware Abstraction Layer (HAL), HDD controller driver and network adapter driver(s):

- If the drivers are on a vendor's disc or other removable media, turn on the **Search removable media**.

- If the drivers are located in a networked folder or on the bootable media, specify the path to the folder by clicking **Add folder**.

In addition, Universal Restore will search the Windows default driver storage folder. Its location is determined in the registry value **DevicePath**, which can be found in the registry key **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion**. This storage folder is usually WINDOWS/inf.

Universal Restore will perform the recursive search in all the sub-folders of the specified folder, find the most suitable HAL and HDD controller drivers of all those available, and install them into the system. Universal Restore also searches for the network adapter driver; the path to the found driver is then transmitted by Universal Restore to the operating system. If the hardware has multiple network interface cards, Universal Restore will try to configure all the cards' drivers.

Mass storage drivers to install anyway

You need this setting if:

- The hardware has a specific mass storage controller such as RAID (especially NVIDIA RAID) or a fibre channel adapter.
- You migrated a system to a virtual machine that uses a SCSI hard drive controller. Use SCSI drivers bundled with your virtualization software or download the latest drivers versions from the software manufacturer website.
- If the automatic drivers search does not help to boot the system.

Specify the appropriate drivers by clicking **Add driver**. The drivers defined here will be installed, with appropriate warnings, even if the program finds a better driver.

Universal Restore process

After you have specified the required settings, click **OK**.

If Universal Restore cannot find a compatible driver in the specified locations, it will display a prompt about the problem device. Do one of the following:

- Add the driver to any of the previously specified locations and click **Retry**.
- If you do not remember the location, click **Ignore** to continue the process. If the result is not satisfactory, reapply Universal Restore. When configuring the operation, specify the necessary driver.

Once Windows boots, it will initialize the standard procedure for installing new hardware. The network adapter driver will be installed silently if the driver has the Microsoft Windows signature. Otherwise, Windows will ask for confirmation on whether to install the unsigned driver.

After that, you will be able to configure the network connection and specify drivers for the video adapter, USB and other devices.

9.3.5.2 Universal Restore in Linux

Universal Restore can be applied to Linux operating systems with a kernel version of 2.6.8 or later.

When Universal Restore is applied to a Linux operating system, it updates a temporary file system known as the initial RAM disk (initrd). This ensures that the operating system can boot on the new hardware.

Universal Restore adds modules for the new hardware (including device drivers) to the initial RAM disk. As a rule, it finds the necessary modules in the **/lib/modules** directory. If Universal Restore cannot find a module it needs, it records the module's file name into the log.

Universal Restore may modify the configuration of the GRUB boot loader. This may be required, for example, to ensure the system bootability when the new machine has a different volume layout than the original machine.

Universal Restore never modifies the Linux kernel.

Reverting to the original initial RAM disk

You can revert to the original initial RAM disk if necessary.

The initial RAM disk is stored on the machine in a file. Before updating the initial RAM disk for the first time, Universal Restore saves a copy of it to the same directory. The name of the copy is the name of the file, followed by the **_acronis_backup.img** suffix. This copy will not be overwritten if you run Universal Restore more than once (for example, after you have added missing drivers).

To revert to the original initial RAM disk, do any of the following:

- Rename the copy accordingly. For example, run a command similar to the following:

  ```
  mv initrd-2.6.16.60-0.21-default_acronis_backup.img
  initrd-2.6.16.60-0.21-default
  ```

- Specify the copy in the **initrd** line of the GRUB boot loader configuration.

9.4 Recovering files

9.4.1 Recovering files by using the web interface

1. Select the machine that originally contained the data that you want to recover.
2. Click **Recovery**.
3. Select the recovery point. Note that recovery points are filtered by location.

   If the selected machine is physical and it is offline, recovery points are not displayed. Do any of the following:

   - [Recommended] If the backup location is cloud or shared storage (i.e. other agents can access it), click **Select machine**, select a target machine that is online, and then select a recovery point.
   - Select a recovery point on the Backups tab (p. 111).
   - Download the files from the cloud storage (p. 83).
   - Use bootable media (p. 85).
4. Click **Recover** > **Files/folders**.
5. Browse to the required folder or use search to obtain the list of the required files and folders.

   You can use one or more wildcard characters (* and ?). For more details about using wildcards, refer to "File filters" (p. 62).

   Note *Search is not available for disk-level backups that are stored in the cloud storage.*
6. Select the files that you want to recover.
7. If you want to save the files as a .zip file, click **Download**, select the location to save the data to, and click **Save**. Otherwise, skip this step.

Downloading is not available if your selection contains folders or the total size of the selected files exceeds 100 MB.

8. Click **Recover**.

   In **Recover to**, you see one of the following:

   - The machine that originally contained the files that you want to recover (if an agent is installed on this machine).
   - The machine where Agent for VMware, Agent for Hyper-V, or Agent for Virtuozzo is installed (if the files originate from an ESXi, Hyper-V, or Virtuozzo virtual machine).

   This is the target machine for the recovery. You can select another machine, if necessary.

9. In **Path**, select the recovery destination. You can select one of the following:

   - The original location (when recovering to the original machine)
   - A local folder on the target machine
   - A network folder that is accessible from the target machine.

10. Click **Start recovery**.
11. Select one of the file overwriting options:

    - **Overwrite existing files**
    - **Overwrite an existing file if it is older**
    - **Do not overwrite existing files**

The recovery progress is shown on the **Activities** tab.

9.4.2 Downloading files from the cloud storage

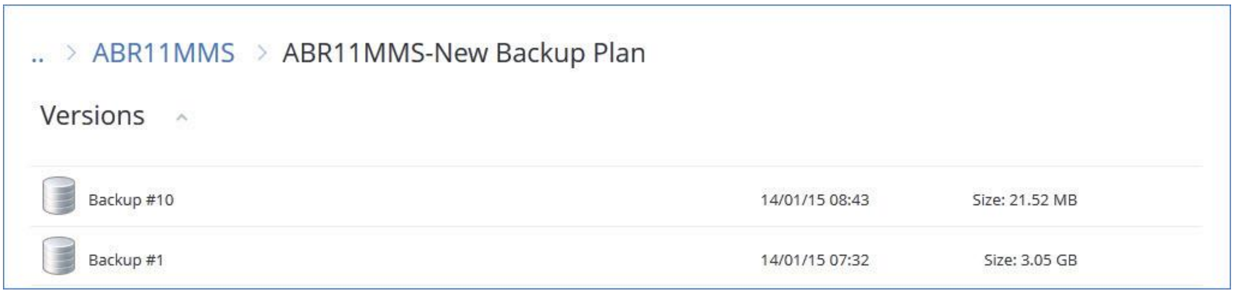
You can browse the cloud storage, view the contents of the backups, and download files that you need.

Limitations

- Backups of system state, SQL databases, and Exchange databases cannot be browsed.
- For a better downloading experience, download no more than 100 MB at a time. To quickly retrieve larger amounts of data from the cloud, use the file recovery procedure (p. 82).

To download files from the cloud storage

1. Select a machine that was backed up.
2. Click **Recover** > **More ways to recover...** > **Download files**.
3. Enter the credentials of the account to which the backed up machine is assigned.
4. [When browsing disk-level backups] Under **Versions**, click the backup from which you want to recover the files.



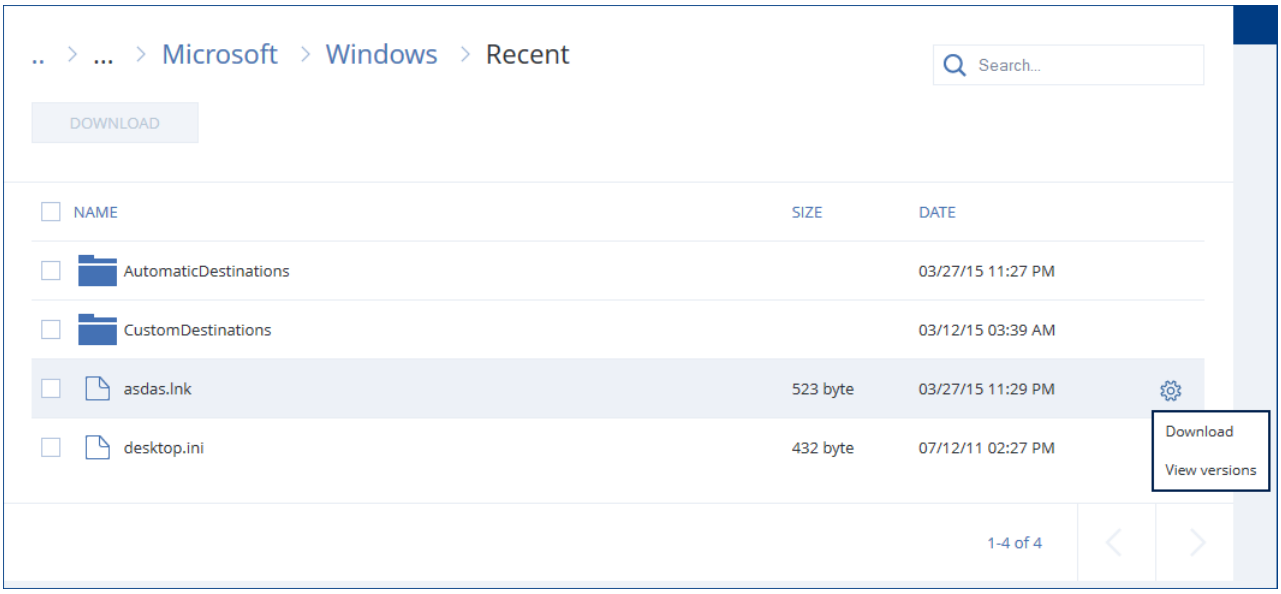
.. > ABR11MMS > ABR11MMS-New Backup Plan

Versions

Backup #10	14/01/15 08:43	Size: 21.52 MB
Backup #1	14/01/15 07:32	Size: 3.05 GB

[When browsing file-level backups] You can select the backup date and time in the next step, under the gear icon located to the right of the selected file. By default, files are recovered from the latest backup.

5. Browse to the required folder or use search to obtain the list of the required files.



NAME	SIZE	DATE
□ AutomaticDestinations		03/27/15 11:27 PM
□ CustomDestinations		03/12/15 03:39 AM
□ asdas.lnk	523 byte	03/27/15 11:29 PM
□ desktop.ini	432 byte	07/12/11 02:27 PM

6. Select the check boxes for the items you need to recover, and then click **Download**.

   If you select a single file, it will be downloaded as is. Otherwise, the selected data will be archived into a .zip file.

7. Select the location to save the data to, and then click **Save**.

9.4.3 Signing a file with ASign

ASign is a service that allows multiple people to sign a backed-up file electronically. This feature is available only for file-level backups stored in the cloud storage.

Only one file version can be signed at a time. If the file was backed up multiple times, you must choose the version to sign, and only this version will be signed.

For example, ASign can be used for electronic signing of the following files:

- Rental or lease agreements
- Sales contracts
- Asset purchase agreements
- Loan agreements
- Permission slips
- Financial documents
- Insurance documents
- Liability waivers
- Healthcare documents
- Research papers
- Certificates of product authenticity
- Nondisclosure agreements
- Offer letters
- Confidentiality agreements
- Independent contractor agreements

To sign a file version

1. Select the file as described in steps 1-6 of the "Recovering files by using the web interface" (p. 82) section.
2. Ensure that the correct date and time is selected on the left panel.
3. Click **Sign this file version**.
4. Specify the password for the cloud storage account under which the backup is stored. The login of the account is displayed in the prompt window.

   The ASign service interface is opened in a web browser window.
5. Add other signees by specifying their email addresses. It is not possible to add or remove signees after sending invitations, so ensure that the list includes everyone whose signature is required.
6. Click **Invite to sign** to send invitations to the signees.

   Each signee receives an email message with the signature request. When all the requested signees sign the file, it is notarized and signed through the notary service.

   You will receive notifications when each signee signs the file and when the entire process is complete. You can access the ASign web page by clicking **View details** in any of the email messages that you receive.
7. Once the process is complete, go to the ASign web page and click **Get document** to download a .pdf document that contains:
   - The Signature Certificate page with the collected signatures.
   - The Audit Trail page with history of activities: when the invitation was sent to the signees, when each signee signed the file, and so on.

9.4.4 Recovering files by using bootable media

For information about how to create bootable media, refer to "Creating bootable media" (p. 74).

To recover files by using bootable media

1. Boot the target machine by using the bootable media.
2. Click **Manage this machine locally** or click **Rescue Bootable Media** twice, depending on the media type you are using.
3. If a proxy server is enabled in your network, click **Tools** > **Proxy server**, and then specify the proxy server host name/IP address, port, and credentials. Otherwise, skip this step.
4. [Optional] When recovering Windows or Linux, click **Tools** > **Register media in the backup service**, and then specify the registration token that you obtained when downloading the media. If you do this, you will not need to enter credentials or a registration code to access the cloud storage, as described in step 7.
5. On the welcome screen, click **Recover**.
6. Click **Select data**, and then click **Browse**.
7. Specify the backup location:
   - To recover from cloud storage, select **Cloud storage**. Enter the credentials of the account to which the backed up machine is assigned.

     When recovering Windows or Linux, you have the option to request a registration code and use it instead of the credentials. Click **Use registration code** > **Request the code**. The software shows the registration link and the registration code. You can copy them and perform the registration steps on a different machine. The registration code is valid for one hour.

- To recover from a local or a network folder, browse to the folder under **Local folders** or **Network folders**.

  Click **OK** to confirm your selection.

8. Select the backup from which you want to recover the data. If prompted, type the password for the backup.
9. In **Backup contents**, select **Folders/files**.
10. Select the data that you want to recover. Click **OK** to confirm your selection.
11. Under **Where to recover**, specify a folder. Optionally, you can prohibit overwriting of newer versions of files or exclude some files from recovery.
12. [Optional] Click **Recovery options** to specify additional settings.
13. Click **OK** to start the recovery.

9.4.5 Extracting files from local backups

You can browse the contents of backups and extract files that you need.

Requirements

- This functionality is available only in Windows by using File Explorer.
- A backup agent must be installed on the machine from which you browse a backup.
- The backed-up file system must be one of the following: FAT16, FAT32, NTFS, ReFS, Ext2, Ext3, Ext4, XFS, or HFS+.
- The backup must be stored in a local folder or on a network share (SMB/CIFS).

To extract files from a backup

1. Browse to the backup location by using File Explorer.
2. Double-click the backup file. The file names are based on the following template:

   ```
   <machine name> - <backup plan GUID>
   ```
3. If the backup is encrypted, enter the encryption password. Otherwise, skip this step.

   File Explorer displays the recovery points.
4. Double-click the recovery point.

   File Explorer displays the backed-up data.
5. Browse to the required folder.
6. Copy the required files to any folder on the file system.

9.5 Recovering system state

1. Select the machine for which you want to recover the system state.
2. Click **Recovery**.
3. Select a system state recovery point. Note that recovery points are filtered by location.
4. Click **Recover system state**.
5. Confirm that you want to overwrite the system state with its backed-up version.

The recovery progress is shown on the **Activities** tab.

9.6 Recovering ESXi configuration

To recover an ESXi configuration, you need Linux-based bootable media. For information about how to create bootable media, refer to "Creating bootable media" (p. 74).

If you are recovering an ESXi configuration to a non-original host and the original ESXi host is still connected to the vCenter Server, disconnect and remove this host from the vCenter Server to avoid unexpected issues during the recovery. If you want to keep the original host along with the recovered one, you can add it again after the recovery is complete.

The virtual machines running on the host are not included in an ESXi configuration backup. They can be backed up and recovered separately.

To recover an ESXi configuration

1. Boot the target machine by using the bootable media.
2. Click **Manage this machine locally**.
3. On the welcome screen, click **Recover**.
4. Click **Select data**, and then click **Browse**.
5. Specify the backup location:
   - Browse to the folder under **Local folders** or **Network folders**.

   Click **OK** to confirm your selection.
6. In **Show**, select **ESXi configurations**.
7. Select the backup from which you want to recover the data. If prompted, type the password for the backup.
8. Click **OK**.
9. In **Disks to be used for new datastores**, do the following:
   - Under **Recover ESXi to**, select the disk where the host configuration will be recovered. If you are recovering the configuration to the original host, the original disk is selected by default.
   - [Optional] Under **Use for new datastore**, select the disks where new datastores will be created. Be careful because all data on the selected disks will be lost. If you want to preserve the virtual machines in the existing datastores, do not select any disks.
10. If any disks for new datastores are selected, select the datastore creation method in **How to create new datastores**: **Create one datastore per disk** or **Create one datastore on all selected HDDs**.
11. [Optional] In **Network mapping**, change the result of automatic mapping of the virtual switches present in the backup to the physical network adapters.
12. [Optional] Click **Recovery options** to specify additional settings.
13. Click **OK** to start the recovery.

9.7 Recovery options

To modify the recovery options, click **Recovery options** when configuring recovery.

Availability of the recovery options

The set of available recovery options depends on:

- The environment the agent that performs recovery operates in (Windows, Linux, macOS, or bootable media).
- The type of data being recovered (disks, files, virtual machines, application data).

The following table summarizes the availability of the recovery options.

	Disks			Files				Virtual machines	SQL and Exchange
	Windows	Linux	Bootable media	Windows	Linux	macOS	Bootable media	ESXi, Hyper-V, and Virtuozzo	Windows
Backup validation (p. 88)	+	+	+	+	+	+	+	+	+
Date and time for files (p. 89)	-	-	-	+	+	+	+	-	-
Error handling (p. 89)	+	+	+	+	+	+	+	+	+
File exclusions (p. 89)	-	-	-	+	+	+	+	-	-
File-level security (p. 89)	-	-	-	+	-	-	-	-	-
Flashback (p. 90)	+	+	+	-	-	-	-	+	-
Full path recovery (p. 90)	-	-	-	+	+	+	+	-	-
Mount points (p. 90)	-	-	-	+	-	-	-	-	-
Performance (p. 90)	+	+	-	+	+	+	-	+	+
Pre/post commands (p. 91)	+	+	-	+	+	+	-	+	+
SID changing (p. 92)	+	-	-	-	-	-	-	-	-
VM power management (p. 92)	-	-	-	-	-	-	-	+	-
Windows event log (p. 92)	+	-	-	+	-	-	-	Hyper-V only	+

9.7.1 Backup validation

This option defines whether to validate a backup to ensure that the backup is not corrupted, before data is recovered from it.

The preset is: **Disabled**.

Validation calculates a checksum for every data block saved in the backup. The only exception is validation of file-level backups that are located in the cloud storage. These backups are validated by checking consistency of the meta information saved in the backup.

Validation is a time-consuming process, even for an incremental or differential backup, which are small in size. This is because the operation validates not only the data physically contained in the backup, but all of the data recoverable by selecting the backup. This requires access to previously created backups.

9.7.2 Error handling

These options enable you to specify how to handle errors that might occur during recovery.

Re-attempt, if an error occurs

The preset is: **Enabled. Number of attempts: 30. Interval between attempts: 30 seconds.**

When a recoverable error occurs, the program re-attempts to perform the unsuccessful operation. You can set the time interval and the number of attempts. The attempts will be stopped as soon as the operation succeeds OR the specified number of attempts are performed, depending on which comes first.

Do not show messages and dialogs while processing (silent mode)

The preset is: **Disabled**.

With the silent mode enabled, the program will automatically handle situations requiring user interaction where possible. If an operation cannot continue without user interaction, it will fail. Details of the operation, including errors, if any, can be found in the operation log.

9.7.3 Date and time for files

This option is effective only when recovering files.

This option defines whether to recover the files' date and time from the backup or assign the files the current date and time.

If this option is enabled, the files will be assigned the current date and time.

The preset is: **Enabled**.

9.7.4 File exclusions

This option is effective only when recovering files.

The option defines which files and folders to skip during the recovery process and thus exclude from the list of recovered items.

Note *Exclusions override the selection of data items to recover. For example, if you select to recover file MyFile.tmp and to exclude all .tmp files, file MyFile.tmp will not be recovered.*

9.7.5 File-level security

This option is effective when recovering files from disk- and file-level backups of NTFS-formatted volumes.

This option defines whether to recover NTFS permissions for files along with the files.

The preset is: **Enabled**.

You can choose whether to recover the permissions or let the files inherit their NTFS permissions from the folder to which they are recovered.

9.7.6 Flashback

This option is effective when recovering disks and volumes on physical and virtual machines, except for Mac.

This option works only if the volume layout of the disk being recovered exactly matches that of the target disk.

If the option is enabled, only the differences between the data in the backup and the target disk data are recovered. This accelerates recovery of physical and virtual machines. The data is compared at the block level.

When recovering a physical machine, the preset is: **Disabled**.

When recovering a virtual machine, the preset is: **Enabled**.

9.7.7 Full path recovery

This option is effective only when recovering data from a file-level backup.

If this option is enabled, the full path to the file will be re-created in the target location.

The preset is: **Disabled**.

9.7.8 Mount points

This option is effective only in Windows for recovering data from a file-level backup.

Enable this option to recover files and folders that were stored on the mounted volumes and were backed up with the enabled Mount points (p. 64) option.

The preset is: **Disabled**.

This option is effective only when you select for recovery a folder that is higher in the folder hierarchy than the mount point. If you select for recovery folders within the mount point or the mount point itself, the selected items will be recovered regardless of the **Mount points** option value.

***Note** Please be aware that if the volume is not mounted at the moment of recovery, the data will be recovered directly to the folder that has been the mount point at the time of backing up.*

9.7.9 Performance

This option defines the priority of the recovery process in the operating system.

The available settings are: **Low**, **Normal**, **High**.

The preset is: **Normal**.

The priority of a process running in a system determines the amount of CPU and system resources allocated to that process. Decreasing the recovery priority will free more resources for other applications. Increasing the recovery priority might speed up the recovery process by requesting the operating system to allocate more resources to the application that will perform the recovery. However, the resulting effect will depend on the overall CPU usage and other factors like disk I/O speed or network traffic.

9.7.10 Pre/Post commands

The option enables you to define the commands to be automatically executed before and after the data recovery.

Example of how you can use the pre/post commands:

- Launch the **Checkdisk** command in order to find and fix logical file system errors, physical errors or bad sectors to be started before the recovery starts or after the recovery ends.

The program does not support interactive commands, i.e. commands that require user input (for example, "pause".)

A post-recovery command will not be executed if the recovery proceeds with reboot.

9.7.10.1 Pre-recovery command

To specify a command/batch file to be executed before the recovery process starts

1. Enable the **Execute a command before the recovery** switch.
2. In the **Command...** field, type a command or browse to a batch file. The program does not support interactive commands, i.e. commands that require user input (for example, "pause".)
3. In the **Working directory** field, specify a path to a directory where the command/batch file will be executed.
4. In the **Arguments** field specify the command's execution arguments, if required.
5. Depending on the result you want to obtain, select the appropriate options as described in the table below.
6. Click **Done**.

Check box	**Selection**			
Fail the recovery if the command execution fails*	Selected	Cleared	Selected	Cleared
Do not recover until the command execution is complete	Selected	Selected	Cleared	Cleared
Result				
	Preset Perform the recovery only after the command is successfully executed. Fail the recovery if the command execution failed.	Perform the recovery after the command is executed despite execution failure or success.	N/A	Perform the recovery concurrently with the command execution and irrespective of the command execution result.

* A command is considered failed if its exit code is not equal to zero.

9.7.10.2 Post-recovery command

To specify a command/executable file to be executed after the recovery is completed

1. Enable the **Execute a command after the recovery** switch.
2. In the **Command...** field, type a command or browse to a batch file.

3. In the **Working directory** field, specify a path to a directory where the command/batch file will be executed.
4. In the **Arguments** field, specify the command execution arguments, if required.
5. Select the **Fail the recovery if the command execution fails** check box if successful execution of the command is critical for you. The command is considered failed if its exit code is not equal to zero. If the command execution fails, the recovery status will be set to **Error**.

   When the check box is not selected, the command execution result does not affect the recovery failure or success. You can track the command execution result by exploring the **Activities** tab.
6. Click **Done**.

Note *A post-recovery command will not be executed if the recovery proceeds with reboot.*

9.7.11 SID changing

This option is effective when recovering Windows 8.1/Windows Server 2012 R2 or earlier.

This option is not effective when recovery to a virtual machine is performed by Agent for VMware or Agent for Hyper-V.

The preset is: **Disabled**.

The software can generate a unique security identifier (Computer SID) for the recovered operating system. You only need this option to ensure operability of third-party software that depends on Computer SID.

Microsoft does not officially support changing SID on a deployed or recovered system. So use this option at your own risk.

9.7.12 VM power management

These options are effective when recovery to a virtual machine is performed by Agent for VMware, Agent for Hyper-V, or Agent for Virtuozzo.

Power off target virtual machines when starting recovery

The preset is: **Enabled**.

Recovery to an existing virtual machine is not possible if the machine is online, and so the machine is powered off automatically as soon as the recovery starts. Users will be disconnected from the machine and any unsaved data will be lost.

Clear the check box for this option if you prefer to power off virtual machines manually before the recovery.

Power on the target virtual machine when recovery is complete

The preset is: **Disabled**.

After a machine is recovered from a backup to another machine, there is a chance the existing machine's replica will appear on the network. To be on the safe side, power on the recovered virtual machine manually, after you take the necessary precautions.

9.7.13 Windows event log

This option is effective only in Windows operating systems.

This option defines whether the agents have to log events of the recovery operations in the Application Event Log of Windows (to see this log, run eventvwr.exe or select **Control Panel** > **Administrative tools** > **Event Viewer**). You can filter the events to be logged.

The preset is: **Disabled**.

10 Disaster recovery

The disaster recovery functionality enables you to own a virtual machine in the cloud. In case of a disaster, the workload can be instantly switched (failed over) from a corrupted machine to the cloud virtual machine.

To include the cloud machine in your local TCP/IP network, you need to extend the network to the cloud via a secure VPN tunnel. This can be easily done by installing the VPN appliance that is delivered in two flavors: for VMware ESXi and for Hyper-V.

Once the VPN connection is configured and the virtual machine is created in the cloud, you can access the virtual machine directly from the backup console. You can also use the RDP or SSH connection.

The disaster recovery functionality is available only for administrators at the company level. The administrators are responsible for providing user access to the cloud virtual machine and for instructing the users on how to access this machine in case of a disaster.

The paid resources controlled by quotas

Having a virtual machine in the cloud, you do not need to care about spare hardware, but you do need to pay for the computing resources consumed by the virtual machine. These include CPU and RAM calculated in compute points; the datastore space occupied by the virtual machine files; and a public IP address if it is necessary.

The datastore space is referred to as "disaster recovery storage". This fast storage is more expensive than ordinary cloud storage where backups are stored. The cost of the disaster recovery storage also includes the cost of the infrastructure that is required for disaster recovery.

Recovery servers

The cloud virtual machine may be a copy of your local server, based on the server backups stored in the cloud. This machine is named a **recovery server**.

A recovery server is stopped most of the time. You start it only for testing or when a failover is required. Because the CPU and RAM resources are consumed for a relatively short time, you pay mostly for the cloud storage where the backups are kept and for reservation of the disaster recovery storage. Other advantages of a recovery server are as follows:

- Deep knowledge of the software installed on the server is not required.
- Long-term data retention. You can go back to a recovery point that is years in the past, and view the data changes or access deleted data.
- Additional recovery capabilities. You can recover the machine or perform granular recovery from the same backup that is used for disaster recovery.

Primary servers

Another type of a cloud virtual machine is a **primary server**. It is simply an additional server in your network. The service enables you to create a virtual machine based on one of the provided templates. Further maintenance of the server is your responsibility.

Typically, a primary server is used for real-time data replication across servers running crucial applications. You set up the replication by yourself, using the application's native tools. For example, Active Directory replication or SQL replication can be configured among the local servers and the primary server.

Alternatively, a primary server can be included in an AlwaysOn Availability Group (AAG) or Database Availability Group (DAG).

Both methods require a deep knowledge of the application and the administrator rights for it. A primary server constantly consumes computing resources and space on the fast disaster recovery storage. It needs maintenance on your side: monitoring the replication, installing software updates, backing up. The benefits are the minimal RPO and RTO with a minimal load on the production environment (as compared to backing up entire servers to the cloud).

Limitations

Disaster recovery is not supported:

- For Virtuozzo virtual machines and containers
- For Mac machines
- For Linux machines that have logical volumes (LVM) or volumes formatted with the XFS file system or disks without a partition table.
- For Windows machines that have dynamic disks
- If the backups of the original machine are encrypted

A recovery server has one network interface. If the original machine has several network interfaces, only one is emulated.

Cloud servers are not encrypted.

10.1 Software requirements

Supported operating systems

Protection with a recovery server has been tested for the following operating systems:

- Centos 6.6, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6
- Debian 9
- Ubuntu 16.04, 18.04
- Windows Server 2008/2008 R2
- Windows Server 2012/2012 R2
- Windows Server 2016 – all installation options, except for Nano Server

Windows desktop operating systems are not supported due to Microsoft product terms.

The software may work with other Windows operating systems and Linux distributions, but this is not guaranteed.

Supported virtualization platforms

Protection of virtual machines with a recovery server has been tested for the following virtualization platforms:

- VMware ESXi 5.1, 5.5, 6.0, 6.5
- Windows Server 2008 R2 with Hyper-V
- Windows Server 2012/2012 R2 with Hyper-V

- Microsoft Hyper-V Server 2012/2012 R2
- Windows Server 2016 with Hyper-V – all installation options, except for Nano Server
- Microsoft Hyper-V Server 2016
- Kernel-based Virtual Machines (KVM)
- Red Hat Enterprise Virtualization (RHEV) 3.6
- Red Hat Virtualization (RHV) 4.0
- Citrix XenServer: 6.5, 7.0, 7.1, 7.2
- Azure virtual machines

The VPN appliance has been tested for the following virtualization platforms:

- VMware ESXi 5.1, 5.5, 6.0, 6.5
- Windows Server 2008 R2 with Hyper-V
- Windows Server 2012/2012 R2 with Hyper-V
- Microsoft Hyper-V Server 2012/2012 R2
- Windows Server 2016 with Hyper-V – all installation options, except for Nano Server
- Microsoft Hyper-V Server 2016

The software may work with other virtualization platforms and versions, but this is not guaranteed.

10.2 Configuring a VPN connection

Before creating a recovery server or a primary server, a VPN connection to the cloud recovery site must be set up. The VPN connection uses two virtual machines:

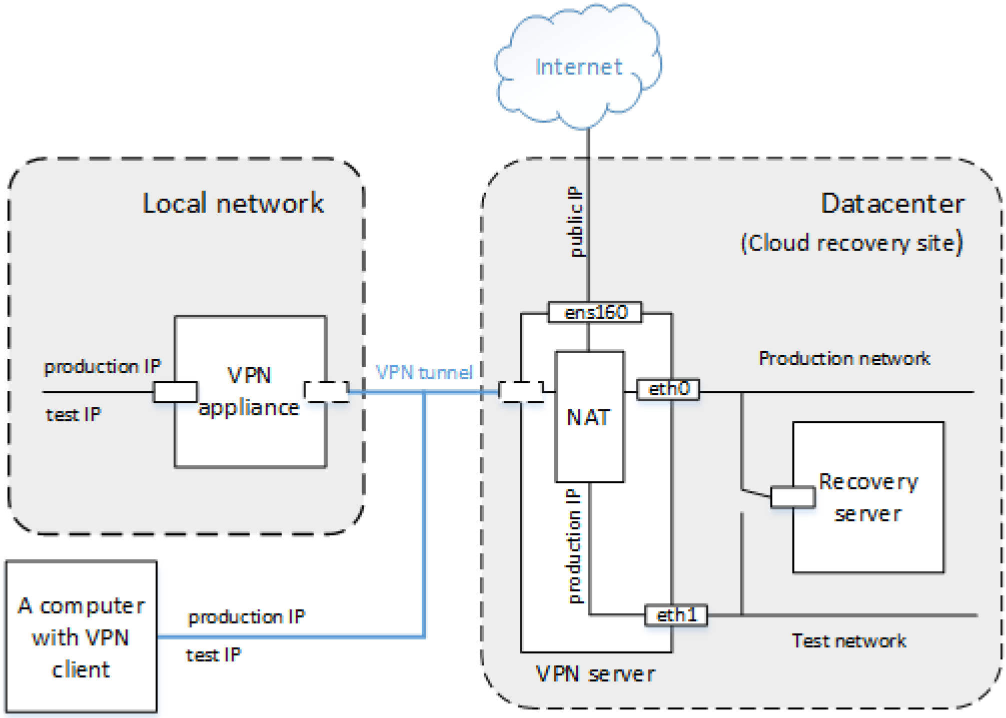
- A VPN appliance, located on your premises.
- A VPN server, located on the cloud recovery site.

The VPN appliance enables connection between the cloud recovery site and your local network. In case the local network is down, you need the capability to connect directly to the VPN server.

The diagram below illustrates the methods of connection to the cloud recovery site and translation of IP addresses in the failover and test failover modes.

- In the failover mode (as shown), a recovery server is connected to the production network and assigned the production IP address.
- In the test failover mode, a recovery server is connected to the isolated test network and also assigned the production IP address. However, to access the server via VPN, you must use the test IP address. The VPN server replaces the test IP address with the production IP address within the test network.

- If the recovery server has a public IP address, it is also translated to the production IP address in both the failover and test failover modes.



10.2.1 Requirements for the VPN appliance

System requirements

- 1 CPU
- 1 GB RAM
- 8 GB disk space

Ports

- TCP 443 (outbound) - for VPN connection
- TCP 80 (outbound) - for automatic update of the appliance (p. 99)

Ensure that your firewalls and other components of your network security system allow connections through these ports to any IP address.

10.2.2 Connection via the VPN appliance

The VPN appliance extends your local network to the cloud via a secure VPN tunnel. This kind of connection is often referred to as a "site-to-site" (S2S) connection.

To set up a connection via the VPN appliance

1. Click **Devices** > **Cloud recovery site**.
2. Click **Start** on the welcome page.

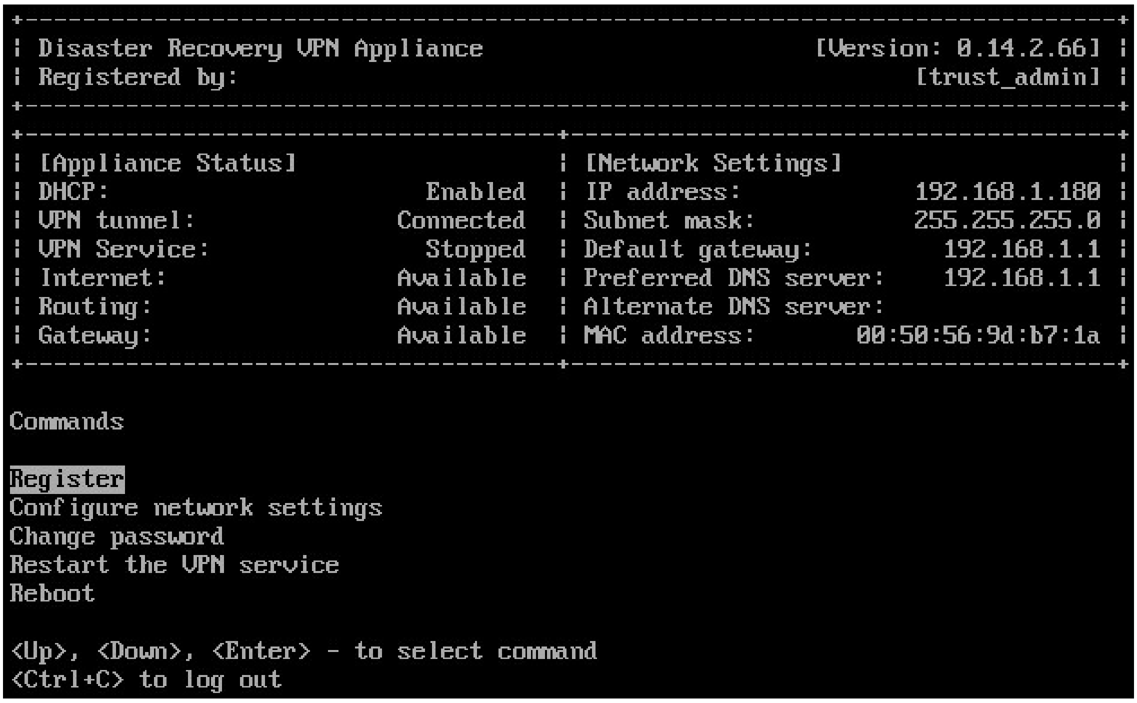
   The system starts deploying the VPN server in the cloud, this will take some time. Meanwhile, you can proceed to the next step.

   Note *The VPN server is provided without additional charge. It will be deleted if the disaster recovery functionality is not used, i.e. no primary or recovery server is present in the cloud for seven days.*

3. Depending on the virtualization platform you are using, download the VPN appliance for VMware vSphere or Microsoft Hyper-V.
4. Deploy the appliance and connect it to the production network.

   In vSphere, ensure that **Promiscuous mode** is enabled and set to **Accept** for all virtual switches that connect the VPN appliance to the production network. To access this setting, in vSphere Client, select the host > **Summary** > **Network** > select the switch > **Edit settings...** > **Security**.

   In Hyper-V, create a Generation 1 virtual machine with 1024 MB of memory. We also recommend enabling Dynamic Memory for the machine. Once the machine is created, go to **Settings** > **Hardware** > **Network Adapter** > **Advanced Features** and select the **Enable MAC address spoofing** check box.
5. Power on the appliance.
6. Open the appliance console and log on with the "admin"/"admin" user name and password.

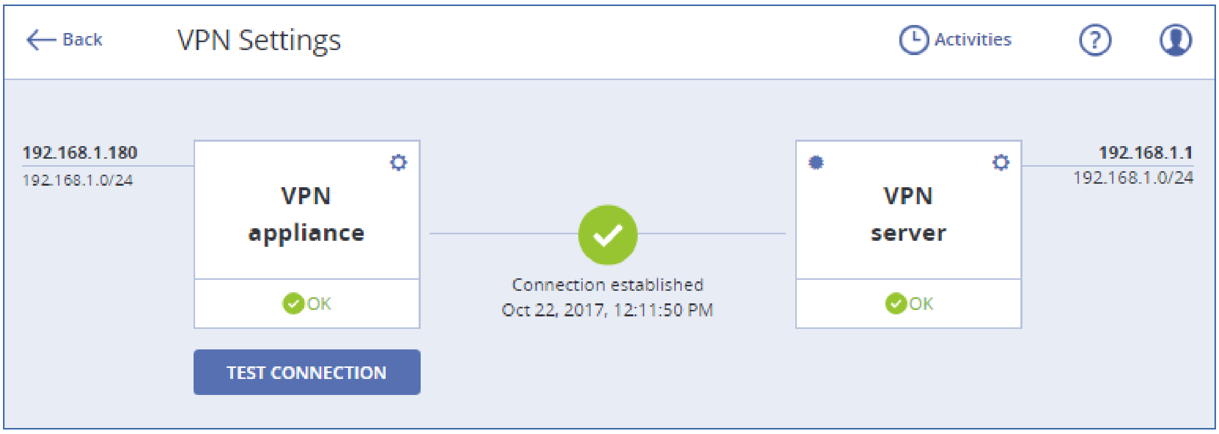


```
+----------------------------------------------------------------------------+
| Disaster Recovery VPN Appliance                      [Version: 0.14.2.66] |
| Registered by:                                              [trust_admin] |
+----------------------------------------------------------------------------+
+--------------------------------------+-------------------------------------+
| [Appliance Status]                   | [Network Settings]                  |
| DHCP:                        Enabled | IP address:           192.168.1.180 |
| VPN tunnel:                Connected | Subnet mask:          255.255.255.0 |
| VPN Service:                 Stopped | Default gateway:        192.168.1.1 |
| Internet:                  Available | Preferred DNS server:   192.168.1.1 |
| Routing:                   Available | Alternate DNS server:               |
| Gateway:                   Available | MAC address:       00:50:56:9d:b7:1a |
+--------------------------------------+-------------------------------------+

Commands

Register
Configure network settings
Change password
Restart the VPN service
Reboot

<Up>, <Down>, <Enter> - to select command
<Ctrl+C> to log out
```

7. [Optional] Change the password.
8. [Optional] Change the network settings. You may want to assign the appliance a static IP address.
9. Register the appliance in the backup service by using the credentials of the company administrator.

   These credentials are only used once to retrieve the certificate. The datacenter URL is predefined.

The appliance connects to the VPN server. Once the configuration is complete, the appliance will show the **OK** status.



To test the VPN connection

1. Click **Devices** > **Cloud recovery site**.
2. Click **VPN settings**.
3. Ensure that the VPN appliance and the VPN server have the **OK** status.
4. Click **Test**.

   The VPN appliance checks the connectivity to the VPN server. You see the list of tests being performed and their results.

10.2.3 Operations with VPN appliance

In the backup console (**Devices** > **Cloud recovery site** > **VPN settings**), you can:

- Connect/disconnect the appliance
- Unregister the appliance

To access these settings, click the gear icon on the VPN appliance image.

In the appliance console you can:

- Change the password for the appliance
- View and change the network settings
- Register/change the registration account (by repeating the registration)
- Restart the VPN service
- Reboot the appliance
- Ping a network address for troubleshooting

Updating the VPN appliance

The VPN appliance automatically checks for updates once a day. When a new version is detected, the update is applied automatically without a reboot or stopping the VPN service.

10.2.4 Point-to-site connection

The VPN appliance enables connection between the cloud recovery site and your local network. In case the local network is down, you need the capability to connect directly to the cloud recovery site. This kind of connection is often referred to as a "point-to-site" (P2S) connection, in contrast to the "site-to-site" (S2S) connection.

To set user name and password for the point-to-site connection

1. In the backup console (**Devices** > **Cloud recovery site** > **VPN settings**), click the gear icon on the VPN server image.
2. Click **Change credentials**.
3. Create and type in the user name.
4. Create and type in the password.
5. Confirm the password.
6. Click **OK**.

To establish the point-to-site connection

1. Install the OpenVPN client on the machine that you want to connect to the cloud recovery site.

   Supported OpenVPN client versions: 2.4.0 and later.
2. In the backup console, click **Devices** > **Cloud recovery site** > **VPN settings**.
3. Click the gear icon in upper left corner of the VPN server.
4. Click **Download configuration for OpenVPN**.
5. Import the configuration to OpenVPN.
6. When the connection is initiated, enter the user name and password that were set up as described above.

10.2.5 Point-to-site connection parameters

In the backup console (**Devices** > **Cloud recovery site** > **VPN settings**), click the gear icon on the VPN server image. The software displays the user name that is set for the point-to-site connection and the following menu items.

Download configuration for OpenVPN

This will download the configuration file for the OpenVPN client. The file is required to establish a point-to-site connection to the cloud recovery site (p. 99).

Change credentials

You can change the user name and/or password that are used for the point-to-site connection.

This is required in the following cases:

- During the initial configuration of the point-to-site connection (p. 99).
- To perform a planned password change according to the security policy set in your organization.
- In order to restrict access to the cloud recovery site for some users (for example, former employees).

After the credentials have been changed, make sure to inform the users that they need to use different credentials.

Re-generate config file

You can re-generate the configuration file for the OpenVPN client.

This is required in the following cases:

- If the VPN client certificate is about to expire. To view the expiration date, click the (i) icon on the VPN server image.
- If you suspect that the configuration file is compromised.

As soon as the configuration file is updated, the connection by means of the old configuration file becomes not possible. Make sure to distribute the new file among the users who are allowed to use the point-to-site connection.

10.3 Working with a recovery server

10.3.1 Creating a recovery server

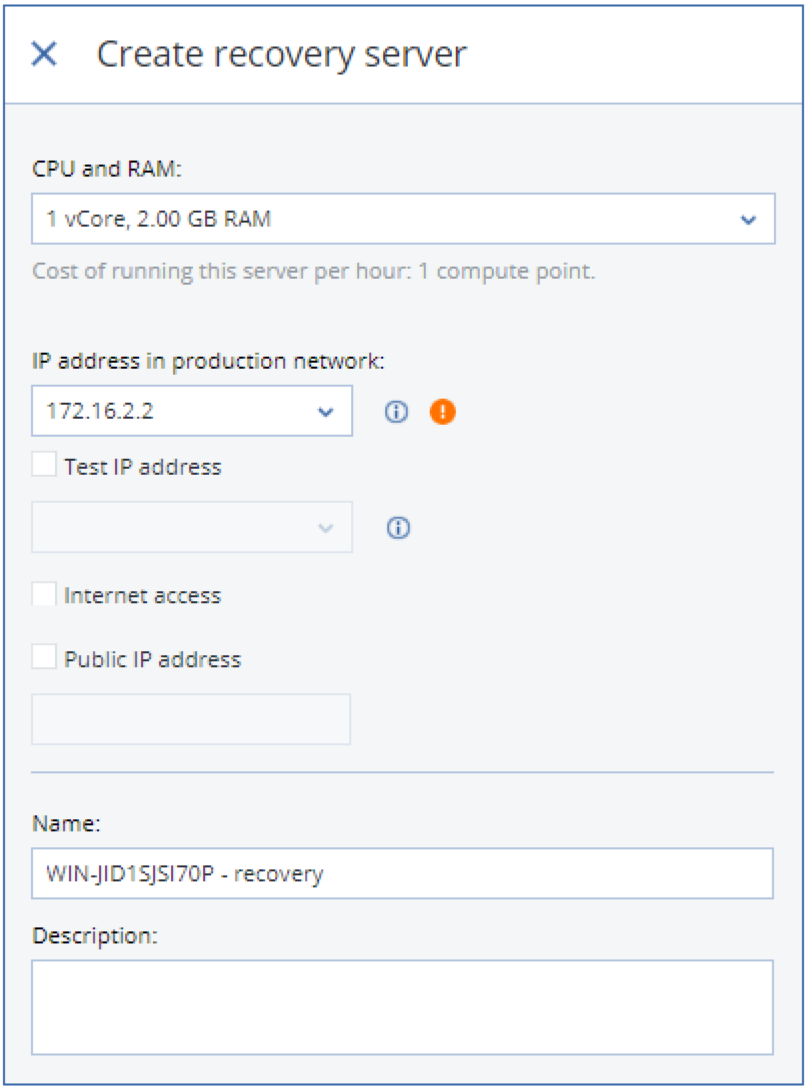
Prerequisites

- A backup plan must be applied to the machine that you want to protect.
  - You can back up the entire machine, or only the disks required for booting up and providing the necessary services.
  - The cloud storage must be selected as a destination.
  - Encryption of backups must be disabled.
  - We recommend that you run the backup plan at least once prior to creating the recovery server, to ensure that cloud backups are successfully created.
- A VPN connection to the cloud recovery site must be set.

To create a recovery server

1. Select the machine that you want to protect.

2. Click **Disaster recovery**, and then click **Create recovery server**.



Create recovery server

CPU and RAM: 1 vCore, 2.00 GB RAM

Cost of running this server per hour: 1 compute point.

IP address in production network: 172.16.2.2

□ Test IP address

□ Internet access

□ Public IP address

Name: WIN-JID1SJSI70P - recovery

Description:

3. Select the number of virtual cores and the size of RAM.

   Be aware of the compute points next to every option. The number of compute points reflects the cost of running the recovery server per hour.

4. Specify the IP address that the server will have in the production network. By default, the IP address of the original machine is set.

   Note *If you use a DHCP server, add this IP address to the server exclusion list in order to avoid IP address conflicts.*

5. [Optional] Select the **Test IP address** check box, and then specify the IP address.

   This will give you the capability to connect to the recovery server via RDP or SSH during a test failover. In the test failover mode, the VPN server will replace the test IP address with the production IP address by using the NAT protocol.

   If you leave the check box cleared, the console will be the only way to access the server during a test failover.

   Note *If you use a DHCP server, add this IP address to the server exclusion list in order to avoid IP address conflicts.*

   You can select one of the proposed IP addresses or type in a different one.

6. [Optional] Select the **Internet access** check box.

This will enable the recovery server to access the Internet during a real or test failover.

7. [Optional] Select the **Public IP address** check box.

   Having a public IP address makes the recovery server available from the Internet during a failover or test failover. If you leave the check box cleared, the server will be available only in your production network.

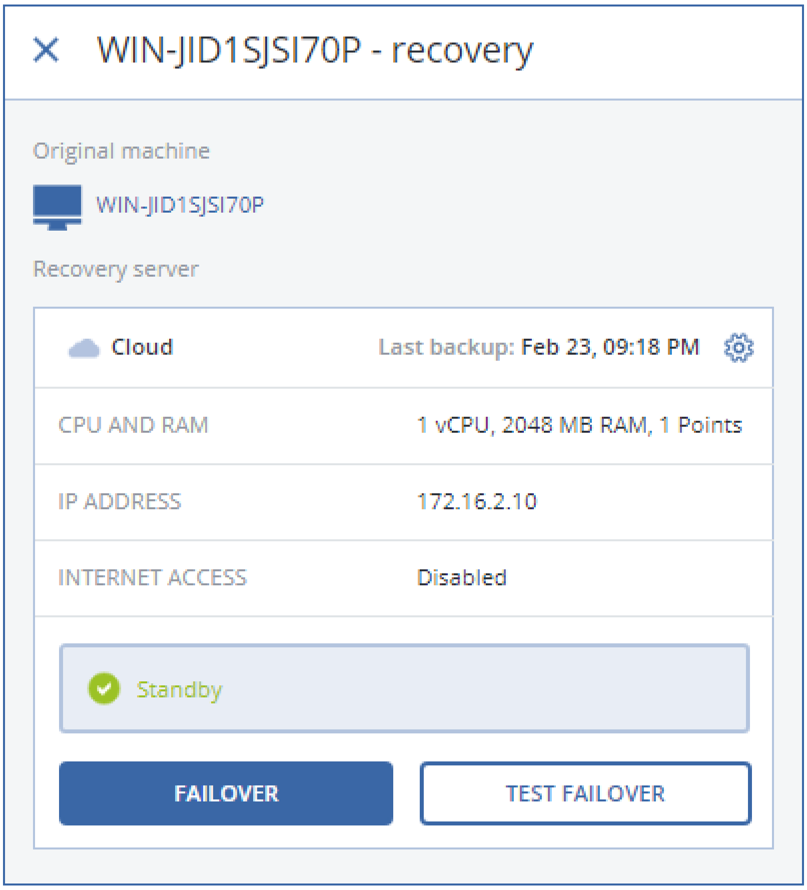
   The public IP address will be shown after you complete the configuration. The following ports are open for inbound connections to public IP addresses:

   TCP: 80, 443, 8088, 8443

   UDP: 1194

   If you need other ports to be open, contact the support team.
8. [Optional] Change the recovery server name.
9. [Optional] Type a description for the recovery server.
10. Click **Done**.

The recovery server appears in the **Cloud recovery site** section of the backup console. You can also access its settings by selecting the original machine and clicking **Disaster recovery**.


WIN-JID1SJSI70P - recovery

Original machine

WIN-JID1SJSI70P

Recovery server

Cloud — Last backup: Feb 23, 09:18 PM

CPU AND RAM	1 vCPU, 2048 MB RAM, 1 Points
IP ADDRESS	172.16.2.10
INTERNET ACCESS	Disabled

Standby

10.3.2 How a failover works

The failover operation employs the "run VM from a backup" (p. 161) functionality.

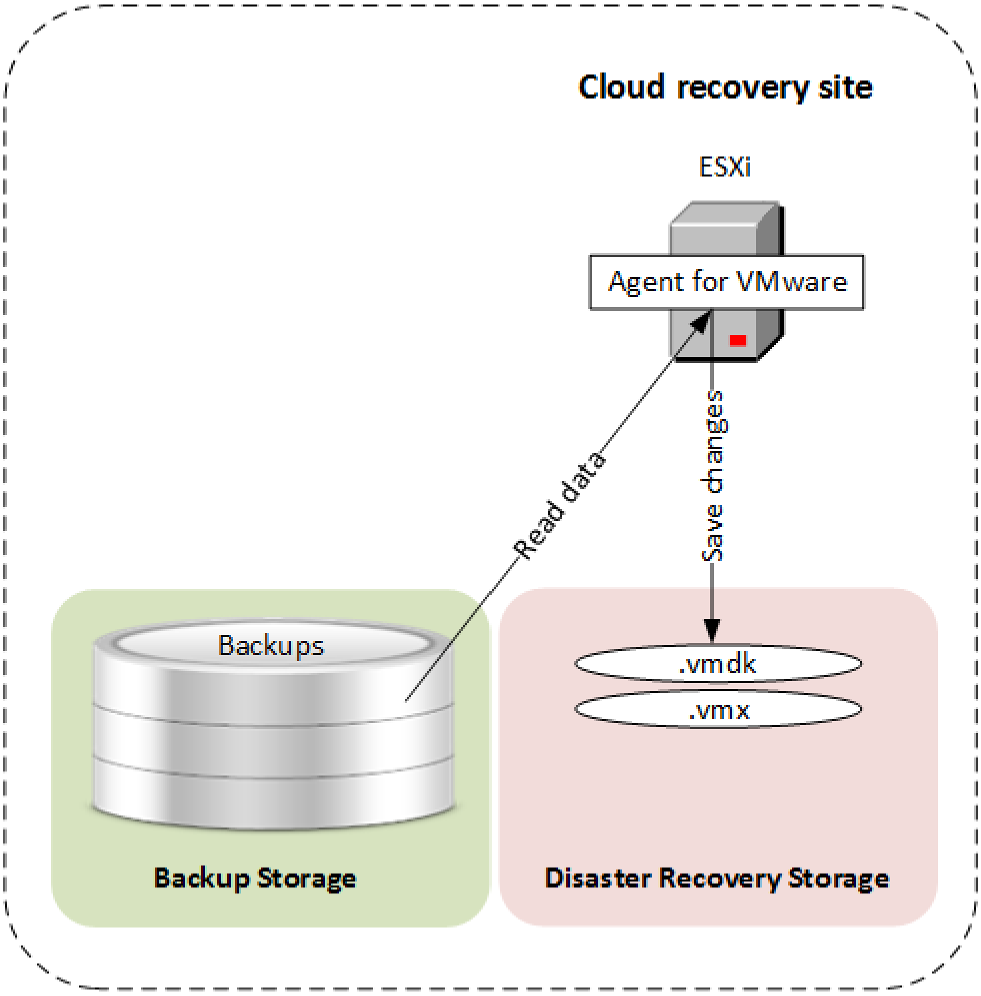
When we say "a recovery server starts", it means that a virtual machine with predefined parameters is run from one of the backups of the original machine.

During a **test failover**, the virtual machine is not finalized. This means that the agent reads the virtual disks' content directly from the backup, i.e. performs random access to different parts of the backup. Therefore, the server may work slower, but occupies little space on the datastore (the disaster recovery storage).

During a **real failover**, the virtual machine is finalized as soon as possible, to achieve the best performance. Once a recovery server starts, its state changes to **Finalization**. This process transfers the server's virtual disks from the backup to the disaster recovery storage. In fact, the virtual machine recovery takes place while the machine is running. Because of this process, the server may work slower. When the finalization is completed, the server performance reaches its normal value. The server state changes to **Failover**.

If the recovery server has a backup agent inside, the agent service is stopped to avoid undesired activity such as starting a backup or reporting outdated statuses to the backup service.

The following diagram illustrates running a recovery server, including storage consumption.



10.3.3 Testing a failover

Testing a failover means starting a recovery server in the test VLAN that is isolated from your production network. You can test several recovery servers at a time in order to check their interaction. In the test network, the servers communicate using their production IP addresses, but they cannot initiate TCP or UDP connections to the machines in your local network.

Though testing a failover is optional, we recommend that you make it a regular process with a frequency that you find adequate in terms of cost and safety. A good practice is creating a runbook—a set of instructions describing how to spin up the production environment in the cloud.

To run a test failover

1. Select the original machine or select the recovery server that you want to test.
2. Click **Disaster Recovery**.

   The description of the recovery server opens.
3. Click **Test failover**.
4. Select the recovery point, and then click **Test failover**.

   When the recovery server starts, its state changes to **Testing failover**.
5. Test the recovery server by using any of the following methods:
   - In the backup console, click **Devices** > **Cloud recovery site**, select the recovery server, and then click **Console** on the right panel.
   - Connect to the recovery server by using RDP or SSH, and the test IP address that you specified when creating the recovery server. Try the connection from both inside and outside the production network (as described in "Point-to-site connection" (p. 99)).
   - Run a script within the recovery server.

     The script may check the logon screen, whether applications are started, the Internet connection, and the ability of other machines to connect to the recovery server.
   - If the recovery server has access to the Internet and a public IP, you may want to use TeamViewer.
6. When the test is complete, click **Stop testing** in the backup console.

   The recovery server is stopped. All changes made to the recovery server during the test failover are lost.

10.3.4 Performing a failover

A failover is a process of moving a workload from your premises to the cloud, and also the state when the workload remains in the cloud.

When you initiate a failover, the recovery server starts in the production network. All backup plans are revoked from the original machine. A new backup plan is automatically created and applied to the recovery server.

To perform a failover

1. Ensure that the original machine is not available on the network.
2. In the backup console, select the original machine or select the recovery server that corresponds to this machine.
3. Click **Disaster Recovery**.

   The description of the recovery server opens.
4. Click **Failover**.
5. Select the recovery point, and then click **Failover**.

   When the recovery server starts, its state changes to **Finalization**, and after some time to **Failover.** It is critical to understand that the server is available in both states, despite the spinning progress indicator. For details, refer to the "How a failover works" (p. 103) section.
6. Ensure that the recovery server is started by viewing its console. Click **Devices** > **Cloud recovery site**, select the recovery server, and then click **Console** on the right panel.

7. Ensure that the recovery server can be accessed using the production IP that you specified when creating the recovery server.

Once the recovery server is finalized, a new backup plan is automatically created and applied to it. This backup plan is based on the backup plan that was used for creating the recovery server, with certain limitations. In this plan, you can change only the schedule and retention rules. For more information, refer to "Backing up the cloud servers" (p. 107).

The only way to get out of the failover state is a failback.

10.3.5 Performing a failback

A failback is a process of moving the workload from the cloud back to your premises.

During this process, the server being moved is unavailable. The length of the maintenance window is approximately equal to the duration of a backup and the subsequent recovery of the server.

To perform a failback

1. Select the recovery server that is in the **Failover** state.
2. Click **Disaster Recovery**.

   The description of the recovery server opens.
3. Click **Prepare failback**.

   The recovery server will be stopped and backed up to the cloud storage. Wait for the backup to complete.

   At this time, two actions become available: **Cancel failback** and **Commit failback**. If you click **Cancel failback**, the recovery server will start and the failover will continue.
4. Recover the server from this backup to hardware or to a virtual machine on your premises.
   - When using bootable media, proceed as described in "Recovering disks by using bootable media" (p. 79). Ensure that you sign in to the cloud with the account for which the server is registered and that you select the most recent backup.
   - If the target machine is online or is a virtual machine, you can use the backup console. On the **Backups** tab, select the cloud storage. In **Machine to browse from**, select the target physical machine or the machine running the agent, if the target machine is virtual. The selected machine must be registered for the same account for which the server is registered. Find the most recent backup of the server, click **Recover entire machine**, and then set up other recovery parameters. For the detailed instructions, refer to "Recovering a machine" (p. 75).

   Ensure that the recovery is completed and the recovered machine works properly.
5. Return to the recovery server in the backup console, and then click **Commit failback**.

   The recovery server and recovery points become ready for a next failover. To create new recovery points, apply a backup plan to the new local server.

10.4 Working with a primary server

10.4.1 Creating a primary server

Prerequisites

- A VPN connection to the cloud recovery site must be set.

To create a primary server

1. Click **Devices** > **Cloud**.

2. Click **New**.
3. Select a template for the new virtual machine.
4. Select the number of virtual cores and the size of RAM.

   Pay attention to the compute points next to every option. The number of compute points reflects the cost of running the primary server per hour.
5. Specify the IP address that the server will have in the production network. By default, the first free IP address from your production network is set.

   Note *If you use a DHCP server, add this IP address to the server exclusion list in order to avoid IP address conflicts.*
6. [Optional] Select the **Internet access** check box.

   This will enable the primary server to access the Internet.
7. [Optional] Select the **Public IP address** check box.

   Having a public IP address makes the primary server available from the Internet. If you leave the check box cleared, the server will be available only in your production network.

   The public IP address will be shown after you complete the configuration. The following ports are open for inbound connections to public IP addresses:

   TCP: 80, 443, 8088, 8443

   UDP: 1194

   If you need other ports to be open, contact the support team.
8. [Optional] Change the virtual disk size. If you need more than one hard disk, click **Add disk**, and then specify the new disk size.
9. Create and type in the primary server name.
10. [Optional] Type a description for the primary server.
11. Click **Done**.

The primary server becomes available in the production network. You can manage the server by using its console, RDP, SSH, or TeamViewer.

10.4.2 Operations with a primary server

The primary server appears in the **Cloud recovery site** section of the backup console.

To start or stop the server, click **Start** or **Stop** on the right panel.

To edit the primary server settings, stop the server, click **Info**, and then click **Edit**.

To apply a backup plan to the primary server, click **Backup**. You will see a predefined backup plan where you can change only the schedule and retention rules. For more information, refer to "Backing up the cloud servers" (p. 107).

10.5 Backing up the cloud servers

Primary and recovery servers are backed up by Agent for VMware, which is installed on the cloud recovery site. In the initial release, this backup is somewhat restricted in functionality as compared to backup performed by local agents. These limitations are temporary and will be removed in future releases.

- The only possible backup location is the cloud storage.

- A backup plan cannot be applied to multiple servers. Each server must have its own backup plan, even if all of the backup plans have the same settings.
- Only one backup plan can be applied to a server.
- Application-aware backup is not supported.
- Encryption is not available.
- Backup options are not available.

When you delete a primary server, its backups are also deleted.

A recovery server is backed up only in the failover state. Its backups continue the backup sequence of the original server. When a failback is performed, the original server can continue this backup sequence. So, the backups of the recovery server can only be deleted manually or as a result of applying the retention rules. When a recovery server is deleted, its backups are always kept.

10.6 Using runbooks

A runbook is a set of instructions describing how to spin up the production environment in the cloud. You can create runbooks in the backup console. To access the **Runbooks** tab, select **Disaster recovery** > **Runbooks**.

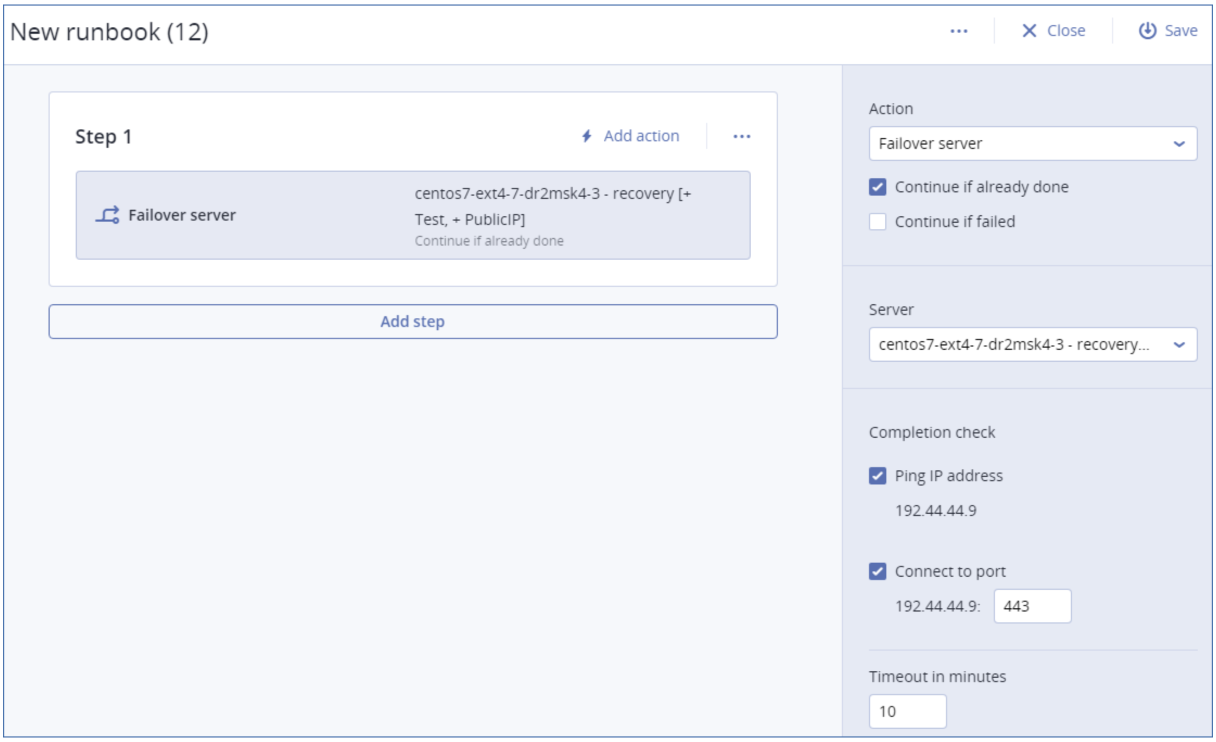
Why use runbooks?

Runbooks let you:

- Automate a failover of one or multiple servers
- Automatically check the failover result by pinging the server IP and checking the connection to the port you specify
- Set the sequence of operations for servers running distributed applications
- Include manual operations in the workflow
- Verify the integrity of your disaster recovery solution, by executing runbooks in the test mode

10.6.1 Creating a runbook

To start creating a runbook, click **Create runbook** > **Add step** > **Add action**. You can use drag and drop to move actions and steps. Do not forget to give a distinctive name to the runbook. While creating a long runbook, click **Save** from time to time. Once you are finished, click **Close**.



New runbook (12)

Step 1

Failover server — centos7-ext4-7-dr2msk4-3 - recovery [+ Test, + PublicIP]
Continue if already done

Action: Failover server

☑ Continue if already done

☐ Continue if failed

Server: centos7-ext4-7-dr2msk4-3 - recovery...

Completion check

☑ Ping IP address

192.44.44.9

☑ Connect to port

192.44.44.9: 443

Timeout in minutes: 10

Steps and actions

A runbook consists of steps that are executed consecutively. A step consists of actions that start simultaneously. An action may consist of:

- An operation to be performed with a cloud server (**Failover server**, **Start server**, **Stop server**, **Failback server**). To define this operation, you need to choose the operation, the cloud server, and the operation parameters.
- A manual operation that you need to describe verbally. Once the operation is completed, a user must click the confirmation button to allow the runbook to proceed.
- Execution of another runbook. To define this operation, you need to choose the runbook.

  A runbook can include only one execution of a given runbook. For example, if you added the action "execute Runbook A", you can add the action "execute Runbook B", but cannot add another action "execute Runbook A".

***Note** In this product version a user has to perform a failback manually. A runbook shows the prompt when it is required.*

Action parameters

All operations with cloud servers have the following parameters:

- **Continue if already done** (enabled by default)

  This parameter defines the runbook behavior when the required operation is already done (for example, a failover has already been performed or a server is already running). When enabled, the runbook issues a warning and proceeds. When disabled, the operation fails and the runbook fails.

- **Continue if failed** (disabled by default)

  This parameter defines the runbook behavior when the required operation fails. When enabled, the runbook issues a warning and proceeds. When disabled, the operation fails and the runbook fails.

Completion check

You can add completion checks to the **Failover server** and **Start server** actions, to ensure that the server is available and provides the necessary services. If any of the checks fail, the action is considered failed.

- **Ping IP address**

  The software will ping the production IP address of the cloud server until the server replies or the timeout expires, whichever comes first.
- **Connect to port** (443 by default)

  The software will try to connect to the cloud server by using its production IP address and the port you specify, until the connection is established or the timeout expires, whichever comes first. This way, you can check if the application that listens on the specified port is running.

The default timeout is 10 minutes. You can change it if you wish.

10.6.2 Operations with runbooks

To access the list of operations, hover on a runbook and click the ellipsis icon. When a runbook is not running, the following operations are available:

- **Execute**
- **Edit**
- **Clone**
- **Delete**

Executing a runbook

Every time you click **Execute**, you are prompted for the execution parameters. These parameters apply to all failover and failback operations included in the runbook. The runbooks specified in the **Execute runbook** operations inherit these parameters from the main runbook.

- **Failover and failback mode**

  Choose whether you want to run a test failover (by default) or a real (production) failover. The failback mode will correspond to the chosen failover mode.
- **Failover recovery point**

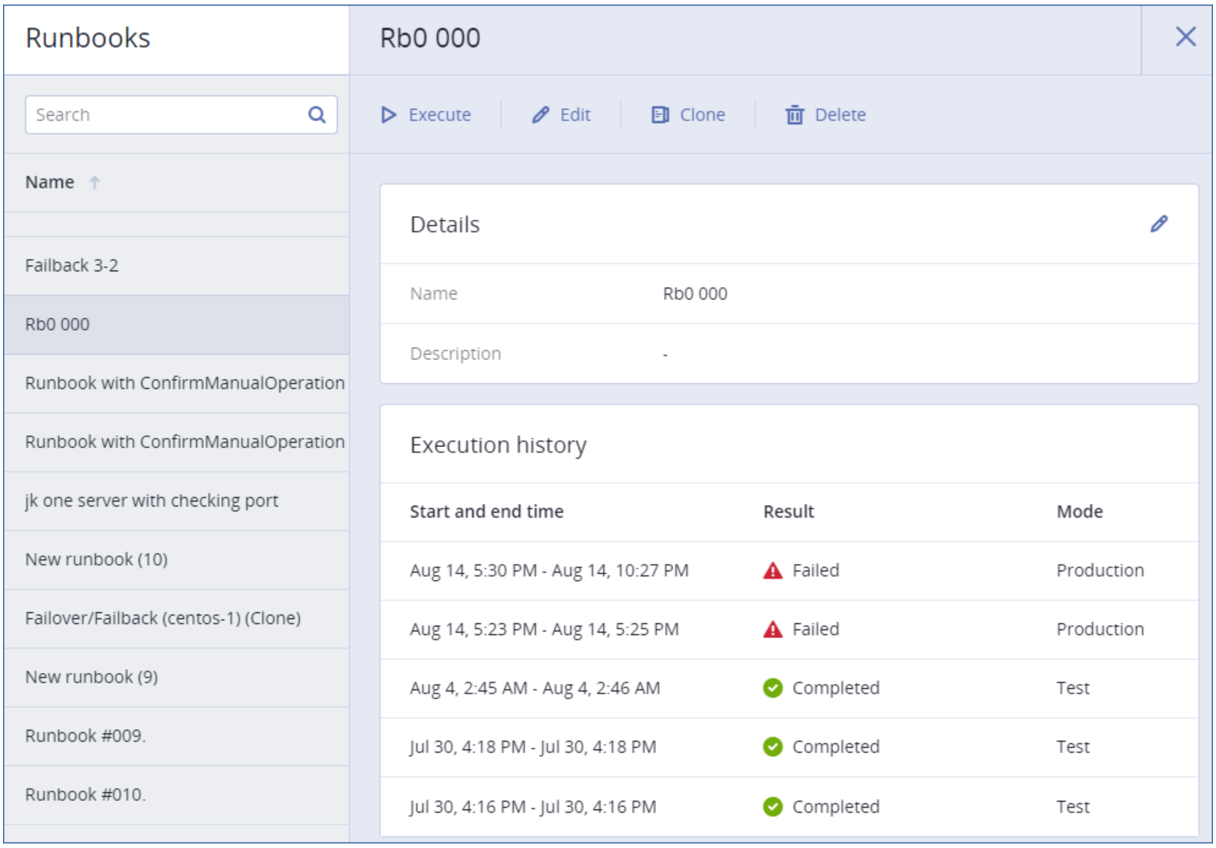
  Choose the most recent recovery point (by default) or select a point in time in the past. If the latter is the case, the recovery points closest before the specified date and time will be selected for each server.

Stopping a runbook execution

During a runbook execution, you can select **Stop** in the list of operations. The software will complete all of the already started actions except for those that require user interaction.

Viewing the execution history

When you select a runbook on the **Runbooks** tab, the software displays the runbook details and execution history. Click the line corresponding to a specific execution to view the execution log.



- Failback 3-2
- Rb0 000
- Runbook with ConfirmManualOperation
- Runbook with ConfirmManualOperation
- jk one server with checking port
- New runbook (10)
- Failover/Failback (centos-1) (Clone)
- New runbook (9)
- Runbook #009.
- Runbook #010.

Name Rb0 000

Description -

Start and end time	Result	Mode
Aug 14, 5:30 PM - Aug 14, 10:27 PM	⚠ Failed	Production
Aug 14, 5:23 PM - Aug 14, 5:25 PM	⚠ Failed	Production
Aug 4, 2:45 AM - Aug 4, 2:46 AM	✓ Completed	Test
Jul 30, 4:18 PM - Jul 30, 4:18 PM	✓ Completed	Test
Jul 30, 4:16 PM - Jul 30, 4:16 PM	✓ Completed	Test

11 Operations with backups

11.1 The Backups tab

The **Backups** tab provides access to all backups, including backups of offline machines and machines that are no longer registered in the backup service.

Backups that are stored in a shared location (such as an SMB or NFS share) are visible to all users that have the read permission for the location.

In the cloud storage, users have access only to their own backups. An administrator can view backups on behalf of any account that belongs to the given unit or company and its child groups. This account is indirectly chosen in **Machine to browse from**. The **Backups** tab shows backups of all machines ever registered under the same account as this machine is registered.

Backups created by the *cloud* Agent for Office 365 and backups of G Suite data are shown not in the **Cloud storage** location, but in a separate section named **Cloud applications backups**.

Backup locations that are used in backup plans are automatically added to the **Backups** tab. To add a custom folder (for example, a detachable USB device) to the list of backup locations, click **Browse** and specify the folder path.

If you added or removed some backups by using a file manager, click the gear icon next to the location name, and then click **Refresh**.

A backup location (except for the cloud storage) disappears from the **Backups** tab if all machines that had ever backed up to the location were deleted from the backup service. This ensures that you do not have to pay for the backups stored in this location. As soon as a backup to this location occurs, the location is re-added along with all backups that are stored in it.

To select a recovery point by using the Backups tab

1. On the **Backups** tab, select the location where the backups are stored.

   The software displays all backups that your account is allowed to view in the selected location. The backups are combined in groups. The group names are based on the following template:

   ```
   <machine name> - <backup plan name>
   ```
2. Select a group from which you want to recover the data.
3. [Optional] Click **Change** next to **Machine to browse from**, and then select another machine. Some backups can only be browsed by specific agents. For example, you must select a machine running Agent for SQL to browse the backups of Microsoft SQL Server databases.

   > ***Important*** *Please be aware that the **Machine to browse from** is a default destination for recovery from a physical machine backup. After you select a recovery point and click **Recover**, double check the **Target machine** setting to ensure that you want to recover to this specific machine. To change the recovery destination, specify another machine in **Machine to browse from**.*
4. Click **Show backups**.
5. Select the recovery point.

11.2 Mounting volumes from a backup

Mounting volumes from a disk-level backup lets you access the volumes as though they were physical disks. Volumes are mounted in the read-only mode.

Requirements

- This functionality is available only in Windows by using File Explorer.
- Agent for Windows must be installed on the machine that performs the mount operation.
- The backed-up file system must be supported by the Windows version that the machine is running.
- The backup must be stored in a local folder, on a network share (SMB/CIFS), or in the Secure Zone.

To mount a volume from a backup

1. Browse to the backup location by using File Explorer.
2. Double-click the backup file. The file names are based on the following template:

   ```
   <machine name> - <backup plan GUID>
   ```
3. If the backup is encrypted, enter the encryption password. Otherwise, skip this step.

   File Explorer displays the recovery points.
4. Double-click the recovery point.

   File Explorer displays the backed-up volumes.

   > ***Tip*** *Double-click a volume to browse its content. You can copy files and folders from the backup to any folder on the file system.*
5. Right-click a volume to mount, and then click **Mount in read-only mode**.

6. If the backup is stored on a network share, provide access credentials. Otherwise, skip this step.

   The software mounts the selected volume. The first unused letter is assigned to the volume.

To unmount a volume

1. Browse to **Computer** (**This PC** in Windows 8.1 and later) by using File Explorer.
2. Right-click the mounted volume.
3. Click **Unmount**.

   The software unmounts the selected volume.

11.3 Deleting backups

To delete backups of a machine that is online and present in the backup console

1. On the **All devices** tab, select a machine whose backups you want to delete.
2. Click **Recovery**.
3. Select the location to delete the backups from.
4. Do one of the following:
   - To delete a single backup, select the backup to delete, and then click the X sign.
   - To delete all backups in the selected location, click **Delete all**.
5. Confirm your decision.

To delete backups of any machine

1. On the **Backups** tab, select the location from which you want to delete the backups.

   The software displays all backups that your account is allowed to view in the selected location. The backups are combined in groups. The group names are based on the following template:

   ```
   <machine name> - <backup plan name>
   ```
2. Select a group.
3. Do one of the following:
   - To delete a single backup, click **Show backups**, select the backup to delete, and then click the X sign.
   - To delete the selected group, click **Delete**.
4. Confirm your decision.

To delete backups directly from the cloud storage

1. Log in to the cloud storage, as described in "Downloading files from the cloud storage" (p. 83).
2. Click the name of the machine whose backups you want to delete.

   The software displays one or more backup groups.
3. Click the gear icon corresponding to the backup group that you want to delete.
4. Click **Remove**.
5. Confirm the operation.

What to do if you deleted local backups by using a file manager

We recommend that you delete backups by using the backup console, whenever possible. If you deleted local backups by using a file manager, do the following:

1. On the **Backups** tab, click the gear icon next to the location name.
2. Click **Refresh**.

This way you will inform the backup service that the local storage usage is decreased.

12 Operations with backup plans

For information about how to create a backup plan, refer to "Backup" (p. 33).

To edit a backup plan

1. If you want to edit the backup plan for all machines to which it is applied, select one of these machines. Otherwise, select the machines for which you want to edit the backup plan.
2. Click **Backup**.
3. Select the backup plan that you want to edit.
4. Click the gear icon next to the backup plan name, and then click **Edit**.
5. To modify the plan parameters, click the corresponding section of the backup plan panel.
6. Click **Save changes**.
7. To change the backup plan for all machines to which it is applied, click **Apply the changes to this backup plan**. Otherwise, click **Create a new backup plan only for the selected devices**.

To revoke a backup plan from machines

1. Select the machines that you want to revoke the backup plan from.
2. Click **Backup**.
3. If several backup plans are applied to the machines, select the backup plan that you want to revoke.
4. Click the gear icon next to the backup plan name, and then click **Revoke**.

To delete a backup plan

1. Select any machine to which the backup plan that you want to delete is applied.
2. Click **Backup**.
3. If several backup plans are applied to the machine, select the backup plan that you want to delete.
4. Click the gear icon next to the backup plan name, and then click **Delete**.

   As a result, the backup plan is revoked from all of the machines and completely removed from the web interface.

13 Protecting mobile devices

To back up and recover the data on your mobile devices, use the backup app.

Supported mobile devices

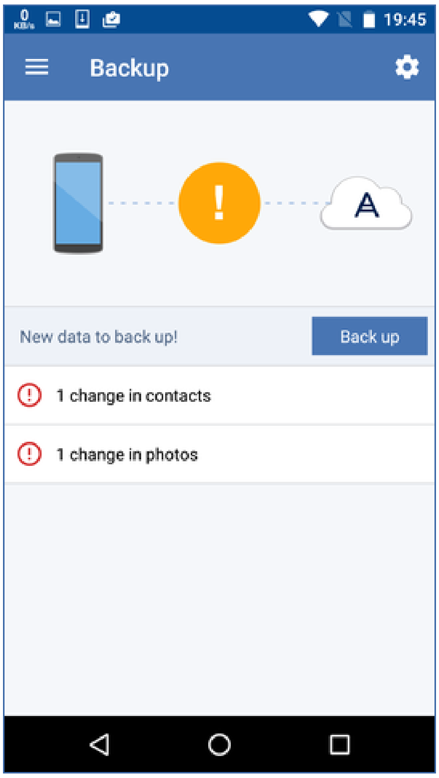
- Smartphones and tablets running Android 4.1 or later.
- iPhones, iPads, and iPods running iOS 8 or later.

What you can back up

- Contacts
- Photos
- Videos
- Calendars
- Text messages (only on Android devices)
- Reminders (only on iOS devices)

What you need to know

- You can back up the data only to the cloud storage.
- Any time you open the app, you see the summary of data changes and can start a backup manually.



New data to back up!

1 change in contacts

1 change in photos

- The **Continuous backup** functionality is enabled by default. In this mode, the backup app checks for the data changes every six hours and runs a backup automatically if some data has changed. You can turn off continuous backup or change it to **Only when charging** in the app settings.
- You can access the backed-up data from any mobile device registered under your account. This helps you transfer the data from an old mobile device to a new one. Contacts and photos from an Android device can be recovered to an iOS device and vice versa. You can also download a photo, video, or contact to a computer by using the backup console.
- The data backed up from mobile devices registered under your account is available only under this account. Nobody else can view or recover your data.
- In the backup app, you can recover the data only from the latest backup. If you need to recover from older backups, use the backup console on either a tablet or a computer.
- Retention rules are not applied to backups of mobile devices.
- If an SD card is present during a backup, the data stored on this card is also backed up. The data will be recovered to an SD card if it is present during recovery, or to the internal storage otherwise.
- Regardless of whether the original data was stored in the internal storage of the device or on a SIM card, the data will be recovered to the internal storage.

Step-by-step instructions

To get the backup app

1. On the mobile device, open a browser and type the backup console URL.
2. Sign in with your account.
3. Click **All devices** > **Add**.

4. Under **Mobile devices**, select the device type.

   Depending on the device type, you will be redirected to the App Store or to the Google Play Store.
5. [Only on iOS devices] Click **Get**.
6. Click **Install** to install the backup app.

To start backing up an iOS device

1. Open the backup app.
2. Sign in with your account.
3. Select the data categories that you want to back up. By default, all categories are selected.
4. Tap **Back up now**.
5. Allow the app access to your personal data. If you deny access to some data categories, they will not be backed up.

The backup starts.

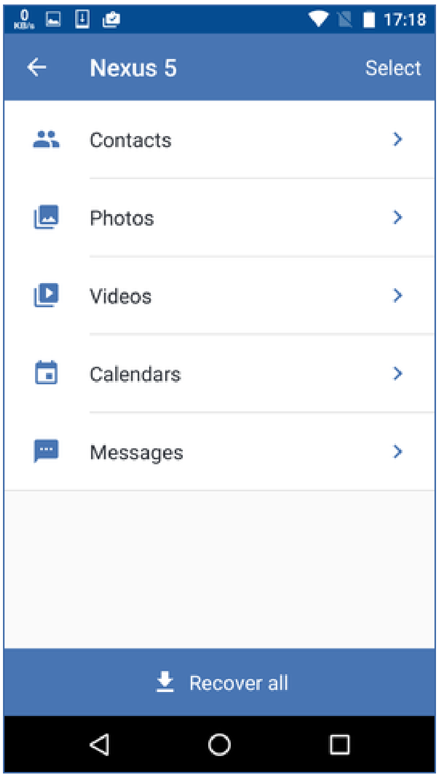
To start backing up an Android device

1. Open the backup app.
2. Sign in with your account.
3. [In Android 6.0 and later] Allow the app access to your personal data. If you deny access to some data categories, they will not be backed up.
4. [Optional] Specify the data categories that you do not want to back up. To do this, tap the gear icon, tap the sliders for the data categories to be excluded from backup, and then tap the back arrow.
5. Tap **Back up**.

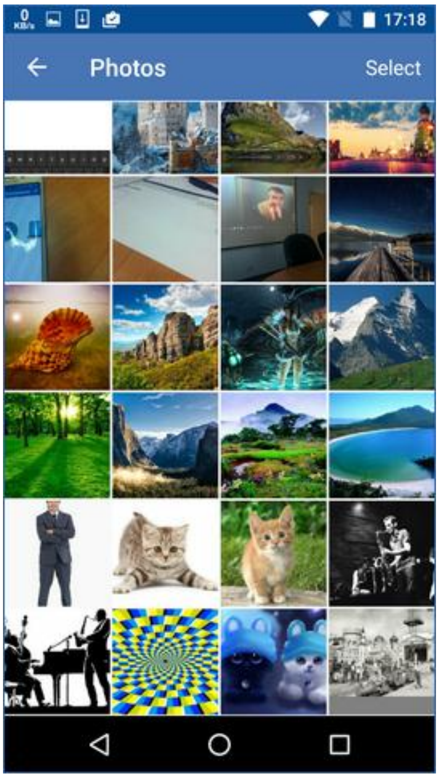
To recover data to a mobile device

1. Open the backup app.
2. Swipe to the right, and then tap **Access and Recovery**.
3. Tap the device name.
4. Do one of the following:
   - To recover all of the backed-up data, tap **Recover all**. No more actions are required.
   - To recover one or more data categories, tap **Select**, and then tap the check boxes for the required data categories. Tap **Recover**. No more actions are required.

- To recover one or more data items belonging to the same data category, tap the data category. Proceed to further steps.



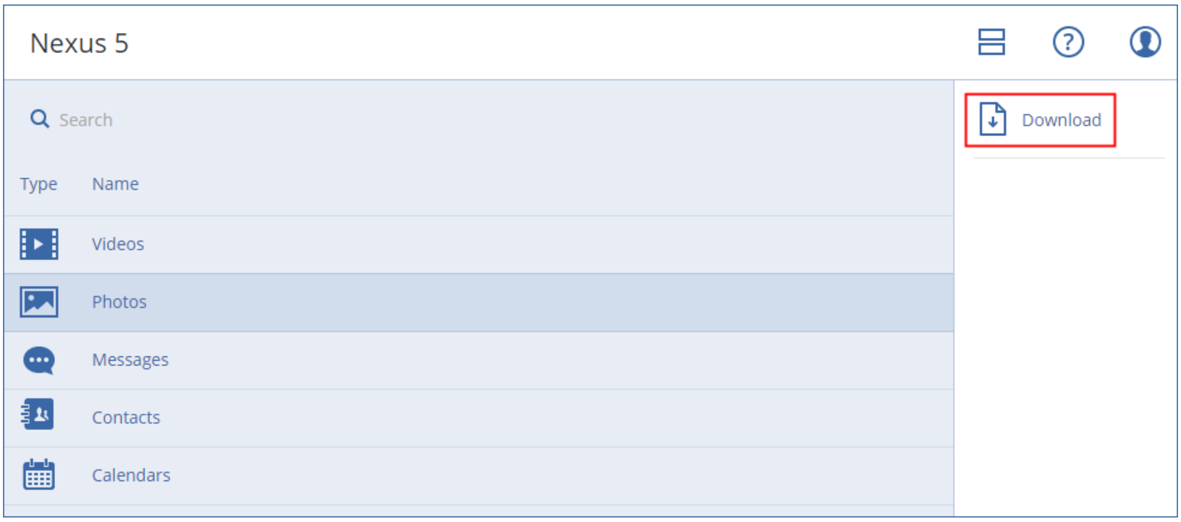
5. Do one of the following:
   - To recover a single data item, tap it.
   - To recover several data items, tap **Select**, and then tap the check boxes for the required data items.



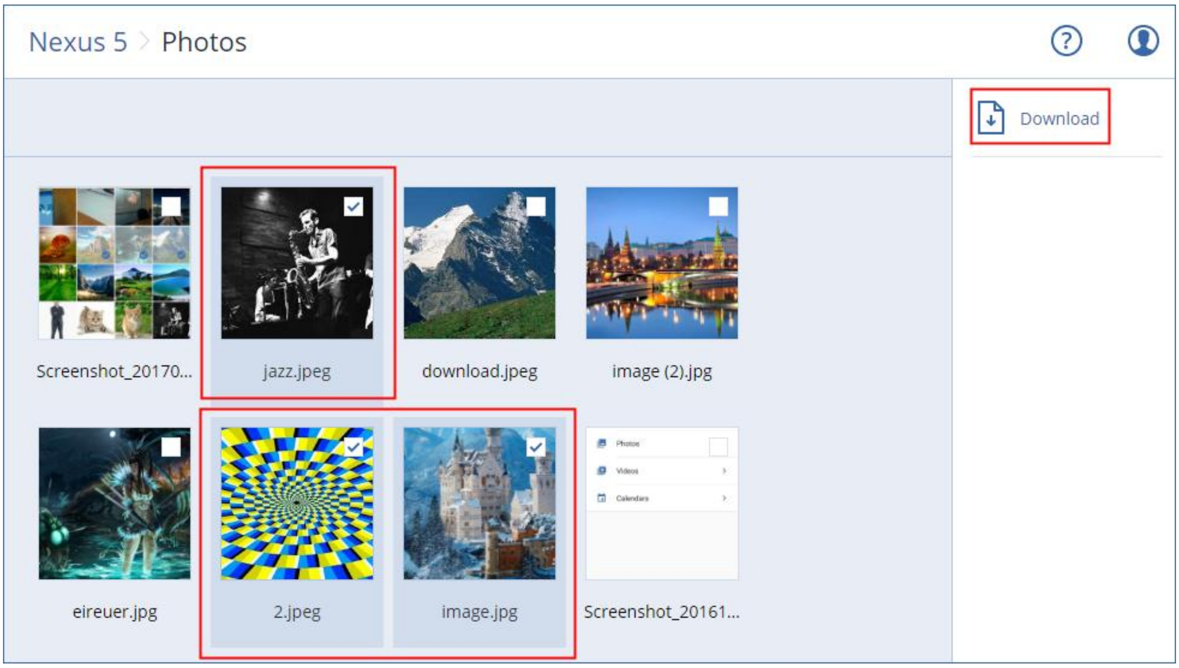
6. Tap **Recover**.

To access data via the backup console

1. On a computer, open a browser and type the backup console URL.
2. Sign in with your account.
3. In **All devices**, select your mobile device name, and then click **Recovery**.
4. Select the recovery point.
5. Do any of the following:
   - To download all photos, videos, or contacts, select the respective data category. Click **Download**.



   - To download individual photos, videos, or contacts, click the respective data category name, and then select the check boxes for the required data items. Click **Download**.



   - To preview a text message, a photo, or a contact, click the respective data category name, and then click the required data item.

For more information, refer to http://www.acronis.com/redirector/products/atimobile/docs/?lang=en. This help is also available in the backup app (tap **Settings** > **Help** on the app menu).

14 Protecting applications

Protecting Microsoft SQL Server and Microsoft Exchange Server

There are two methods of protecting these applications:

- **Database backup**

  This is a file-level backup of the databases and the metadata associated with them. The databases can be recovered to a live application or as files.

- **Application-aware backup**

  This is a disk-level backup that also collects the applications' metadata. This metadata enables browsing and recovery of the application data without recovering the entire disk or volume. The disk or volume can also be recovered as a whole. This means that a single solution and a single backup plan can be used for both disaster recovery and data protection purposes.

Protecting Microsoft SharePoint

A Microsoft SharePoint farm consists of front-end servers that run SharePoint services, database servers that run Microsoft SQL Server, and (optionally) application servers that offload some SharePoint services from the front-end servers. Some front-end and application servers may be identical to each other.

To protect an entire SharePoint farm:

- Back up all of the database servers with application-aware backup.
- Back up all of the unique front-end servers and application servers with usual disk-level backup.

The backups of all servers should be done on the same schedule.

To protect only the content, you can back up the content databases separately.

Protecting a domain controller

A machine running Active Directory Domain Services can be protected by application-aware backup. If a domain contains more than one domain controller, and you recover one of them, a nonauthoritative restore is performed and a USN rollback will not occur after the recovery.

Recovering applications

The following table summarizes the available application recovery methods.

	From a database backup	From an application-aware backup	From a disk backup
Microsoft SQL Server	Databases to a live SQL Server instance (p. 123) Databases as files (p. 123)	Entire machine (p. 75) Databases to a live SQL Server instance (p. 123) Databases as files (p. 123)	Entire machine (p. 75)
Microsoft Exchange Server	Databases to a live Exchange (p. 126) Databases as files (p. 126) Granular recovery to a live Exchange (p. 127)	Entire machine (p. 75) Databases to a live Exchange (p. 126) Databases as files (p. 126) Granular recovery to a live Exchange (p. 127)	Entire machine (p. 75)

Microsoft SharePoint database servers	Databases to a live SQL Server instance (p. 123) Databases as files (p. 123) Granular recovery by using SharePoint Explorer	Entire machine (p. 75) Databases to a live SQL Server instance (p. 123) Databases as files (p. 123) Granular recovery by using SharePoint Explorer	Entire machine (p. 75)
Microsoft SharePoint front-end web servers	-	-	Entire machine (p. 75)
Active Directory Domain Services	-	Entire machine (p. 75)	-

14.1 Prerequisites

Before configuring the application backup, ensure that the requirements listed below are met.

To check the VSS writers state, use the **`vssadmin list writers`** command.

Common requirements

For Microsoft SQL Server, ensure that:

- At least one Microsoft SQL Server instance is started.
- The SQL writer for VSS is turned on.

For Microsoft Exchange Server, ensure that:

- The Microsoft Exchange Information Store service is started.
- Windows PowerShell is installed. For Exchange 2010 or later, the Windows PowerShell version must be at least 2.0.
- Microsoft .NET Framework is installed.

  For Exchange 2007, the Microsoft .NET Framework version must be at least 2.0.

  For Exchange 2010 or later, the Microsoft .NET Framework version must be at least 3.5.
- The Exchange writer for VSS is turned on.

On a domain controller, ensure that:

- The Active Directory writer for VSS is turned on.

When creating a backup plan, ensure that:

- For physical machines, the Volume Shadow Copy Service (VSS) (p. 72) backup option is enabled.
- For virtual machines, the Volume Shadow Copy Service (VSS) for virtual machines (p. 73) backup option is enabled.

Additional requirements for application-aware backups

When creating a backup plan, ensure that **Entire machine** is selected for backup.

If the applications run on virtual machines that are backed up by Agent for VMware, ensure that:

- The virtual machines being backed up meet the requirements for application-consistent quiescing listed in the following VMware knowledge base article: https://pubs.vmware.com/vsphere-6-5/index.jsp?topic=%2Fcom.vmware.vddk.pg.doc%2FvddkBkupVadp.9.6.html
- VMware Tools is installed and up-to-date on the machines.

- User Account Control (UAC) is disabled on the machines. If you do not want to disable UAC, you must provide the credentials of a built-in domain administrator (DOMAIN\Administrator) when enabling application backup.

14.2 Database backup

Before backing up databases, ensure that the requirements listed in "Prerequisites" (p. 120) are met.

Select the databases as described below, and then specify other settings of the backup plan as appropriate (p. 34).

14.2.1 Selecting SQL databases

A backup of an SQL database contains the database files (.mdf, .ndf), log files (.ldf), and other associated files. The files are backed with the help of the SQL Writer service. The service must be running at the time that the Volume Shadow Copy Service (VSS) requests a backup or recovery.

The SQL transaction logs are truncated after each successful backup. SQL log truncation can be disabled in the backup plan options (p. 64).

To select SQL databases

1. Click **Microsoft SQL**.

   Machines with Agent for SQL installed are shown.
2. Browse to the data that you want to back up.

   Double-click a machine to view the SQL Server instances it contains. Double-click an instance to view the databases it contains.
3. Select the data that you want to back up. You can select entire instances or individual databases.
   - If you select entire SQL Server instances, all current databases and all databases that are added to the selected instances in the future will be backed up.
   - If you select databases directly, only the selected databases will be backed up.
4. Click **Backup**. If prompted, provide credentials to access the SQL Server data. The account must be a member of the **Backup Operators** or **Administrators** group on the machine and a member of the **sysadmin** role on each of the instances that you are going to back up.

14.2.2 Selecting Exchange Server data

The following table summarizes the Microsoft Exchange Server data that you can select for backup and the minimal user rights required to back up the data.

Exchange version	Data items	User rights
2007	Storage groups	Membership in the **Exchange Organization Administrators** role group
2010/2013/2016	Databases	Membership in the **Server Management** role group.

A full backup contains all of the selected Exchange Server data.

An incremental backup contains the changed blocks of the database files, the checkpoint files, and a small number of the log files that are more recent than the corresponding database checkpoint. Because changes to the database files are included in the backup, there is no need to back up all the transaction log records since the previous backup. Only the log that is more recent than the checkpoint needs to be replayed after a recovery. This makes for faster recovery and ensures successful database backup, even with circular logging enabled.

The transaction log files are truncated after each successful backup.

To select Exchange Server data

1. Click **Microsoft Exchange**.

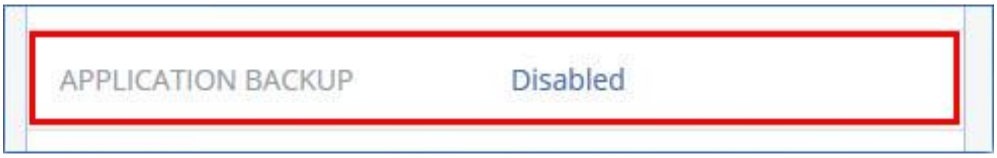
   Machines with Agent for Exchange installed are shown.
2. Browse to the data that you want to back up.

   Double-click a machine to view the databases (storage groups) it contains.
3. Select the data that you want to back up. If prompted, provide the credentials to access the data.
4. Click **Backup**.

14.3 Application-aware backup

Application-aware disk-level backup is available for physical machines and for ESXi virtual machines.

When you back up a machine running Microsoft SQL Server, Microsoft Exchange Server, or Active Directory Domain Services, enable **Application backup** for additional protection of these applications' data.



APPLICATION BACKUP Disabled

Why use application-aware backup?

By using application-aware backup, you ensure that:

1. The applications are backed up in a consistent state and thus will be available immediately after the machine is recovered.
2. You can recover the SQL and Exchange databases, mailboxes, and mailbox items without recovering the entire machine.
3. The SQL transaction logs are truncated after each successful backup. SQL log truncation can be disabled in the backup plan options (p. 64). The Exchange transaction logs are truncated on virtual machines only. You can enable the VSS full backup option (p. 72) if you want to truncate Exchange transaction logs on a physical machine.
4. If a domain contains more than one domain controller, and you recover one of them, a nonauthoritative restore is performed and a USN rollback will not occur after the recovery.

What do I need to use application-aware backup?

On a physical machine, Agent for SQL and/or Agent for Exchange must be installed, in addition to Agent for Windows.

On a virtual machine, no agent installation is required; it is presumed that the machine is backed up by Agent for VMware (Windows).

Agent for VMware (Virtual Appliance) can create application-aware backups, but cannot recover application data from them. To recover application data from backups created by this agent, you need Agent for VMware (Windows), Agent for SQL, or Agent for Exchange on a machine that has access to the location where the backups are stored. When configuring recovery of application data, select the recovery point on the **Backups** tab, and then select this machine in **Machine to browse from**.

Other requirements are listed in the "Prerequisites" (p. 120) and "Required user rights" (p. 123) sections.

14.3.1 Required user rights

An application-aware backup contains metadata of VSS-aware applications that are present on the disk. To access this metadata, the agent needs an account with the appropriate rights, which are listed below. You are prompted to specify this account when enabling application backup.

- For SQL Server:

  The account must be a member of the **Backup Operators** or **Administrators** group on the machine, and a member of the **sysadmin** role on each of the instances that you are going to back up.
- For Exchange Server:

  Exchange 2007: The account must be a member of the **Exchange Organization Administrators** role group.

  Exchange 2010 and later: The account must be a member of the **Organization Management** role group.
- For Active Directory:

  The account must be a domain administrator.

14.4 Recovering SQL databases

This section describes recovery from both database backups and application-aware backups.

You can recover SQL databases to a SQL Server instance, if Agent for SQL is installed on the machine running the instance. You will need to provide credentials for an account that is a member of the **Backup Operators** or **Administrators** group on the machine and a member of the **sysadmin** role on the target instance.

Alternatively, you can recover the databases as files. This can be useful if you need to extract data for data mining, audit, or further processing by third-party tools. You can attach the SQL database files to a SQL Server instance, as described in "Attaching SQL Server databases" (p. 125).

If you use only Agent for VMware (Windows), recovering databases as files is the only available recovery method. Recovering databases by using Agent for VMware (Virtual Appliance) is not possible.

System databases are basically recovered in the same way as user databases. The peculiarities of system database recovery are described in "Recovering system databases" (p. 125).

To recover SQL databases

1. When recovering from a database backup, click **Microsoft SQL**. Otherwise, skip this step.
2. Select the machine that originally contained the data that you want to recover.
3. Click **Recovery**.
4. Select a recovery point. Note that recovery points are filtered by location.

   If the machine is offline, the recovery points are not displayed. Do one of the following:

- If the backup location is cloud or shared storage (i.e. other agents can access it), click **Select machine**, select an online machine that has Agent for SQL, and then select a recovery point.
- Select a recovery point on the Backups tab (p. 111).

The machine chosen for browsing in either of the above actions becomes a target machine for the SQL databases recovery.

5. Do one of the following:
   - When recovering from a database backup, click **Recover SQL databases**.
   - When recovering from an application-aware backup, click **Recover** > **SQL databases**.
6. Select the data that you want to recover. Double-click an instance to view the databases it contains.
7. If you want to recover the databases as files, click **Recover as files**, select a local or a network folder to save the files to, and then click **Recover**. Otherwise, skip this step.
8. Click **Recover**.
9. By default, the databases are recovered to the original ones. If the original database does not exist, it will be recreated. You can select another SQL Server instance (running on the same machine) to recover the databases to.

   To recover a database as a different one to the same instance:

   a. Click the database name.
   b. In **Recover to**, select **New database**.
   c. Specify the new database name.
   d. Specify the new database path and log path. The folder you specify must not contain the original database and log files.
10. [Optional] To change the database state after recovery, click the database name, and then choose one of the following states:
    - **Ready to use (RESTORE WITH RECOVERY)** (default)

      After the recovery completes, the database will be ready for use. Users will have full access to it. The software will roll back all uncommitted transactions of the recovered database that are stored in the transaction logs. You will not be able to recover additional transaction logs from the native Microsoft SQL backups.
    - **Non-operational (RESTORE WITH NORECOVERY)**

      After the recovery completes, the database will be non-operational. Users will have no access to it. The software will keep all uncommitted transactions of the recovered database. You will be able to recover additional transaction logs from the native Microsoft SQL backups and thus reach the necessary recovery point.
    - **Read-only (RESTORE WITH STANDBY)**

      After the recovery completes, users will have read-only access to the database. The software will undo any uncommitted transactions. However, it will save the undo actions in a temporary standby file so that the recovery effects can be reverted.

      This value is primarily used to detect the point in time when a SQL Server error occurred.
11. Click **Start recovery**.

The recovery progress is shown on the **Activities** tab.

14.4.1 Recovering system databases

All system databases of an instance are recovered at once. When recovering system databases, the software automatically restarts the destination instance in the single-user mode. After the recovery completes, the software restarts the instance and recovers other databases (if any).

Other things to consider when recovering system databases:

- System databases can only be recovered to an instance of the same version as the original instance.
- System databases are always recovered in the "ready to use" state.

Recovering the master database

System databases include the **master** database. The **master** database records information about all databases of the instance. Hence, the **master** database in a backup contains information about databases which existed in the instance at the time of the backup. After recovering the **master** database, you may need to do the following:

- Databases that have appeared in the instance after the backup was done are not visible by the instance. To bring these databases back to production, attach them to the instance manually by using SQL Server Management Studio.
- Databases that have been deleted after the backup was done are displayed as offline in the instance. Delete these databases by using SQL Server Management Studio.

14.4.2 Attaching SQL Server databases

This section describes how to attach a database in SQL Server by using SQL Server Management Studio. Only one database can be attached at a time.

Attaching a database requires any of the following permissions: **CREATE DATABASE**, **CREATE ANY DATABASE**, or **ALTER ANY DATABASE**. Normally, these permissions are granted to the **sysadmin** role of the instance.

To attach a database

1. Run Microsoft SQL Server Management Studio.
2. Connect to the required SQL Server instance, and then expand the instance.
3. Right-click **Databases** and click **Attach**.
4. Click **Add**.
5. In the **Locate Database Files** dialog box, find and select the .mdf file of the database.
6. In the **Database Details** section, make sure that the rest of database files (.ndf and .ldf files) are found.

   Details. SQL Server database files may not be found automatically, if:

   - They are not in the default location, or they are not in the same folder as the primary database file (.mdf). Solution: Specify the path to the required files manually in the **Current File Path** column.
   - You have recovered an incomplete set of files that make up the database. Solution: Recover the missing SQL Server database files from the backup.
7. When all of the files are found, click **OK**.

14.5 Recovering Exchange databases

This section describes recovery from both database backups and application-aware backups.

You can recover Exchange Server data to a live Exchange Server. This may be the original Exchange Server or an Exchange Server of the same version running on the machine with the same fully qualified domain name (FQDN). Agent for Exchange must be installed on the target machine.

The following table summarizes the Exchange Server data that you can select for recovery and the minimal user rights required to recover the data.

Exchange version	Data items	User rights
2007	Storage groups	Membership in the **Exchange Organization Administrators** role group.
2010/2013/2016	Databases	Membership in the **Server Management** role group.

Alternatively, you can recover the databases (storage groups) as files. The database files, along with transaction log files, will be extracted from the backup to a folder that you specify. This can be useful if you need to extract data for an audit or further processing by third-party tools, or when the recovery fails for some reason and you are looking for a workaround to mount the databases manually (p. 127).

If you use only Agent for VMware (Windows), recovering databases as files is the only available recovery method. Recovering databases by using Agent for VMware (Virtual Appliance) is not possible.

To recover Exchange data

We will refer to both databases and storage groups as "databases" throughout this procedure.

1. When recovering from a database backup, click **Microsoft Exchange**. Otherwise, skip this step.
2. Select the machine that originally contained the data that you want to recover.
3. Click **Recovery**.
4. Select a recovery point. Note that recovery points are filtered by location.

   If the machine is offline, the recovery points are not displayed. Use other ways to recover:

   - If the backup location is cloud or shared storage (i.e. other agents can access it), click **Select machine**, select an online machine that has Agent for Exchange, and then select a recovery point.
   - Select a recovery point on the Backups tab (p. 111).

   The machine chosen for browsing in either of the above actions becomes a target machine for the Exchange data recovery.
5. Click **Recover** > **Exchange databases**.
6. Select the data that you want to recover.
7. If you want to recover the databases as files, click **Recover as files**, select a local or a network folder to save the files to, and then click **Recover**. Otherwise, skip this step.
8. Click **Recover**. If prompted, provide credentials to access the Exchange Server.
9. By default, the databases are recovered to the original ones. If the original database does not exist, it will be recreated.

   To recover a database as a different one:

   a. Click the database name.

b. In **Recover to**, select **New database**.

c. Specify the new database name.

d. Specify the new database path and log path. The folder you specify must not contain the original database and log files.

10. Click **Start recovery**.

The recovery progress is shown on the **Activities** tab.

14.5.1 Mounting Exchange Server databases

After recovering the database files, you can bring the databases online by mounting them. Mounting is performed by using Exchange Management Console, Exchange System Manager, or Exchange Management Shell.

The recovered databases will be in a Dirty Shutdown state. A database that is in a Dirty Shutdown state can be mounted by the system if it is recovered to its original location (that is, information about the original database is present in Active Directory). When recovering a database to an alternate location (such as a new database or as the recovery database), the database cannot be mounted until you bring it to a Clean Shutdown state by using the **`Eseutil /r <Enn>`** command. **`<Enn>`** specifies the log file prefix for the database (or storage group that contains the database) into which you need to apply the transaction log files.

The account you use to attach a database must be delegated an Exchange Server Administrator role and a local Administrators group for the target server.

For details about how to mount databases, see the following articles:

- Exchange 2010 or later: http://technet.microsoft.com/en-us/library/aa998871.aspx
- Exchange 2007: http://technet.microsoft.com/en-us/library/aa998871(v=EXCHG.80).aspx

14.6 Recovering Exchange mailboxes and mailbox items

This section describes how to recover Exchange mailboxes and mailbox items from database backups and from application-aware backups.

Overview

Granular recovery can be performed to Microsoft Exchange Server 2010 Service Pack 1 (SP1) and later. The source backup may contain databases of any supported Exchange version.

Granular recovery can be performed by Agent for Exchange or Agent for VMware (Windows). The target Exchange Server and the machine running the agent must belong to the same Active Directory forest.

The following items can be recovered:

- Mailboxes (except for archive mailboxes)
- Public folders
- Public folder items
- Email folders
- Email messages
- Calendar events
- Tasks

- Contacts
- Journal entries
- Notes

You can use search to locate the items.

When a mailbox is recovered to an existing mailbox, the existing items with matching IDs are overwritten.

Recovery of mailbox items does not overwrite anything. The mailbox items are always recovered to the **Recovered items** folder of the target mailbox.

Requirements on user accounts

A mailbox being recovered from a backup must have an associated user account in Active Directory.

User mailboxes and their contents can be recovered only if their associated user accounts are *enabled*. Shared, room, and equipment mailboxes can be recovered only if their associated user accounts are *disabled*.

A mailbox that does not meet the above conditions is skipped during recovery.

If some mailboxes are skipped, the recovery will succeed with warnings. If all mailboxes are skipped, the recovery will fail.

14.6.1 Recovering mailboxes

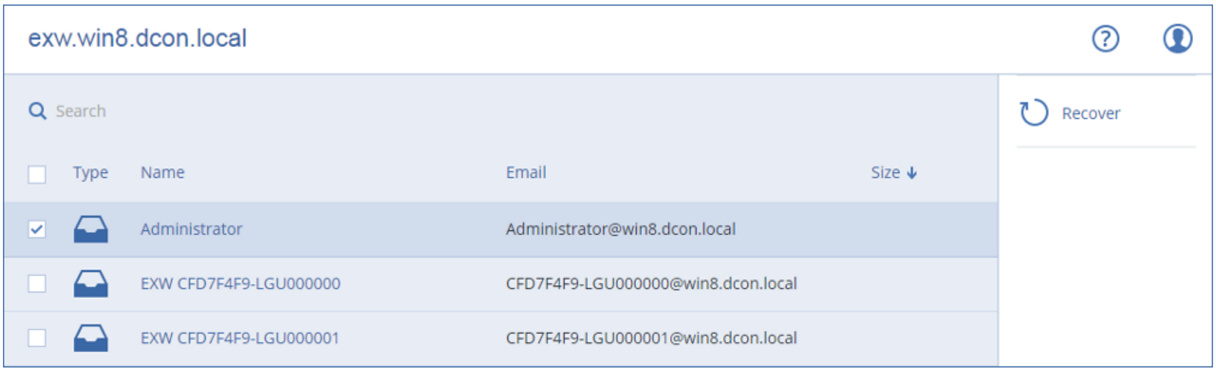
1. When recovering from a database backup, click **Microsoft Exchange**. Otherwise, skip this step.
2. Select the machine that originally contained the data that you want to recover.
3. Click **Recovery**.
4. Select a recovery point. Note that recovery points are filtered by location.

   If the machine is offline, the recovery points are not displayed. Use other ways to recover:

   - If the backup location is cloud or shared storage (i.e. other agents can access it), click **Select machine**, select an online machine that has Agent for Exchange or Agent for VMware, and then select a recovery point.
   - Select a recovery point on the Backups tab (p. 111).

   The machine chosen for browsing in either of the above actions will perform the recovery instead of the original machine that is offline.
5. Click **Recover** > **Exchange mailboxes**.
6. Select the mailboxes that you want to recover.

   You can search mailboxes by name. Wildcards are not supported.



exw.win8.dcon.local

□	Type	Name	Email	Size
☑		Administrator	Administrator@win8.dcon.local	
□		EXW CFD7F4F9-LGU000000	CFD7F4F9-LGU000000@win8.dcon.local	
□		EXW CFD7F4F9-LGU000001	CFD7F4F9-LGU000001@win8.dcon.local	

7. Click **Recover**.
8. Click **Target machine with Microsoft Exchange Server** to select or change the target machine. This step allows recovery to a machine that is not running Agent for Exchange.

   Specify the fully qualified domain name (FQDN) of the machine where the **Client Access** role of Microsoft Exchange Server is enabled. The machine must belong to the same Active Directory forest as the machine that performs the recovery.

   If prompted, provide the credentials of an account that will be used to access the machine. The requirements for this account are listed in "Required user rights" (p. 130).
9. [Optional] Click **Database to re-create any missing mailboxes** to change the automatically selected database.
10. Click **Start recovery**.
11. Confirm your decision.

The recovery progress is shown on the **Activities** tab.

14.6.2 Recovering mailbox items

1. When recovering from a database backup, click **Microsoft Exchange**. Otherwise, skip this step.
2. Select the machine that originally contained the data that you want to recover.
3. Click **Recovery**.
4. Select a recovery point. Note that recovery points are filtered by location.

   If the machine is offline, the recovery points are not displayed. Use other ways to recover:

   - If the backup location is cloud or shared storage (i.e. other agents can access it), click **Select machine**, select an online machine that has Agent for Exchange or Agent for VMware, and then select a recovery point.
   - Select a recovery point on the Backups tab (p. 111).

   The machine chosen for browsing in either of the above actions will perform the recovery instead of the original machine that is offline.
5. Click **Recover** > **Exchange mailboxes**.
6. Click the mailbox that originally contained the items that you want to recover.
7. Select the items that you want to recover.

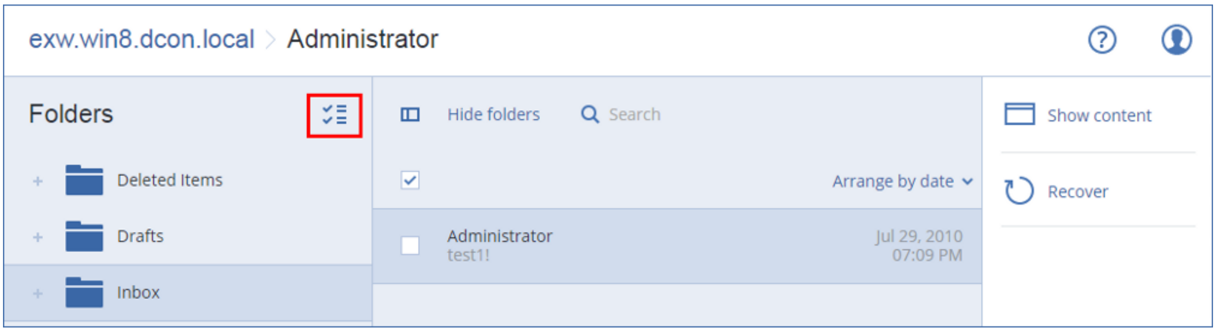
   The following search options are available. Wildcards are not supported.

   - For email messages: search by subject, sender, recipient, and date.
   - For events: search by title and date.
   - For tasks: search by subject and date.
   - For contacts: search by name, email address, and phone number.

   When an email message is selected, you can click **Show content** to view its contents, including attachments.

   Tip *Click the name of an attached file to download it.*

To be able to select folders, click the recover folders icon.



8. Click **Recover**.
9. Click **Target machine with Microsoft Exchange Server** to select or change the target machine. This step allows recovery to a machine that is not running Agent for Exchange.

   Specify the fully qualified domain name (FQDN) of the machine where the **Client Access** role of Microsoft Exchange Server is enabled. The machine must belong to the same Active Directory forest as the machine that performs the recovery.

   If prompted, provide the credentials of an account that will be used to access the machine. The requirements for this account are listed in "Required user rights" (p. 130).
10. In **Target mailbox**, view, change, or specify the target mailbox.

    By default, the original mailbox is selected. If this mailbox does not exist or a non-original target machine is selected, you must specify the target mailbox.
11. Click **Start recovery**.
12. Confirm your decision.

The recovery progress is shown on the **Activities** tab.

14.6.3 Required user rights

To access mailboxes, Agent for Exchange needs an account with the appropriate rights. You are prompted to specify this account when configuring various operations with mailboxes.

Membership of the account in the **Organization Management** role group enables access to any mailbox, including mailboxes that will be created in the future.

The minimum required user rights are as follows:

- The account must be a member of the **Recipient Management** role group.
- The account must have the **ApplicationImpersonation** management role enabled for all users or groups of users whose mailboxes the agent will access.

  For information about configuring the **ApplicationImpersonation** management role, refer to the following Microsoft knowledge base article: https://msdn.microsoft.com/en-us/library/office/dn722376.aspx.

15 Protecting Office 365 data

Why back up Office 365 data?

Even though Microsoft Office 365 is a set of cloud services, regular backups provide an additional layer of protection from user errors and intentional malicious actions. You can recover deleted items from a backup even after the Office 365 retention period has expired. Also, you can keep a local copy of the Exchange Online mailboxes if it is required for regulatory compliance.

Agent for Office 365

Depending on the desired functionality, you can choose to install Agent for Office 365 locally, use the agent installed in the cloud, or both. The following table summarizes the functionality of the local and the cloud agent.

	Local Agent for Office 365	**Cloud Agent for Office 365**
Data items that can be backed up	**Exchange Online:** user and shared mailboxes	▪ **Exchange Online**: user, shared, and group mailboxes ▪ **OneDrive**: user files and folders ▪ **SharePoint Online**: classic site collections, group (team) sites, communication sites, individual data items
Backup of archive mailboxes (**In-Place Archive**)	No	Yes
Backup schedule	User-defined (p. 43)	Cannot be changed. Each backup plan runs daily at the same time of day.*
Backup locations	Cloud storage, local folder, network folder	Cloud storage only
Automatic protection of new Office 365 users, groups, sites	No	Yes, by applying a backup plan to the **All users**, **All groups**, **All sites** groups
Protecting more than one Office 365 organization	No	Yes
Granular recovery	Yes	Yes
Recovery to another user within one organization	Yes	Yes
Recovery to another organization	No	Yes
Recovery to an on-premises Microsoft Exchange Server	No	No
Maximum number of items that can be backed up without performance degradation	When backing up to the cloud storage: 5000 mailboxes per company When backing up to other destinations: 2000 mailboxes per backup plan (no limitation for number of mailboxes per company)	5000 protected items (mailboxes, OneDrives, or sites) per company

* Because a cloud agent serves multiple customers, it determines the start time for each backup plan on its own, to ensure even load during a day and the equal quality of service for all of the customers.

Limitation

Automatic creation of users, groups, or sites during a recovery is not possible. For example, if you want to recover a deleted SharePoint Online site, first create a new site manually, and then specify it as the target site during a recovery.

Required user rights

In the backup service

Any Agent for Office 365, either local or cloud, must be registered under a customer administrator account.

In Microsoft Office 365

Your account must be assigned the global administrator role in Microsoft Office 365.

- The local agent will log in to Office 365 by using this account. To enable the agent to access the contents of all mailboxes, this account will be assigned the **ApplicationImpersonation** management role. If you change this account password, update the password in the backup console, as described in "Changing the Office 365 access credentials" (p. 134).
- The cloud agent does not log in to Office 365. The agent is given the necessary permissions directly by Microsoft Office 365. You only need to confirm granting these permissions once, being signed in as a global administrator. The agent does not store your account credentials and does not use them to perform backup and recovery. Changing this account password in Office 365 does not affect agent operation.

15.1 Using the locally installed Agent for Office 365

15.1.1 Adding a Microsoft Office 365 organization

To add a Microsoft Office 365 organization

1. Sign in to the backup console as a company administrator.
2. Click the account icon in the top-right corner, and then click **Downloads** > **Agent for Office 365**.
3. Download the agent and install it on a Windows machine that is connected to the Internet.
4. After the installation is complete, click **Devices** > **Microsoft Office 365**, and then enter the Office 365 global administrator credentials.

   Important *There must be only one locally installed Agent for Office 365 in an organization (company group).*

As a result, your organization data items appear in the backup console on the **Microsoft Office 365** page.

15.1.2 Protecting Exchange Online mailboxes

What items can be backed up?

You can back up user mailboxes and shared mailboxes. Group mailboxes and archive mailboxes (**In-Place Archive**) cannot be backed up.

What items can be recovered?

The following items can be recovered from a mailbox backup:

- Mailboxes
- Email folders
- Email messages
- Calendar events
- Tasks

- Contacts
- Journal entries
- Notes

You can use search to locate the items.

When a mailbox is recovered to an existing mailbox, the existing items with matching IDs are overwritten.

Recovery of mailbox items does not overwrite anything. Instead, the full path to a mailbox item is recreated in the target folder.

15.1.2.1 Selecting mailboxes

Select the mailboxes as described below, and then specify other settings of the backup plan as appropriate (p. 34).

To select mailboxes

1. Click **Microsoft Office 365**.
2. If prompted, sign in as a global administrator to Microsoft Office 365.
3. Select the mailboxes that you want to back up.
4. Click **Backup**.

15.1.2.2 Recovering mailboxes and mailbox items

Recovering mailboxes

1. Click **Microsoft Office 365**.
2. Select the mailbox to recover, and then click **Recovery**.

   You can search mailboxes by name. Wildcards are not supported.

   If the mailbox was deleted, select it on the Backups tab (p. 111), and then click **Show backups**.
3. Select a recovery point. Note that recovery points are filtered by location.
4. Click **Recover** > **Mailbox**.
5. In **Target mailbox**, view, change, or specify the target mailbox.

   By default, the original mailbox is selected. If this mailbox does not exist, you must specify the target mailbox.
6. Click **Start recovery**.

Recovering mailbox items

1. Click **Microsoft Office 365**.
2. Select the mailbox that originally contained the items that you want to recover, and then click **Recovery**.

   You can search mailboxes by name. Wildcards are not supported.

   If the mailbox was deleted, select it on the Backups tab (p. 111), and then click **Show backups**.
3. Select a recovery point. Note that recovery points are filtered by location.
4. Click **Recover** > **Email messages**.
5. Select the items that you want to recover.

   The following search options are available. Wildcards are not supported.

    - For email messages: search by subject, sender, recipient, and date.
    - For events: search by title and date.
    - For tasks: search by subject and date.
    - For contacts: search by name, email address, and phone number.

    When an email message is selected, you can click **Show content** to view its contents, including attachments.

    ***Tip** Click the name of an attached file to download it.*

    When an email message is selected, you can click **Send as email** to send the message to an email address. The message is sent from your administrator account's email address.

    To be able to select folders, click the "recover folders" icon: ☑

6. Click **Recover**.
7. In **Target mailbox**, view, change, or specify the target mailbox.

   By default, the original mailbox is selected. If this mailbox does not exist, you must specify the target mailbox.
8. Click **Start recovery**.
9. Confirm your decision.

The mailbox items are always recovered to the **Recovered items** folder of the target mailbox.

15.1.2.3 Changing the Office 365 access credentials

You can change access credentials for Office 365 without re-installing the agent.

To change the Office 365 access credentials

1. Click **Devices** > **Microsoft Office 365**.
2. Click **Specify credentials**.
3. Enter the Office 365 global administrator credentials, and then click **OK**.

   The agent will log in to Office 365 by using this account. To enable the agent to access the contents of all mailboxes, this account will be assigned the **ApplicationImpersonation** management role.

15.2 Using the cloud Agent for Office 365

15.2.1 Adding a Microsoft Office 365 organization

To add a Microsoft Office 365 organization

1. Sign in to the backup console as a company administrator.
2. Click **Devices** > **Add** > **Microsoft Office 365 for Business**.
3. Select the Microsoft data center used by your organization.

   The software redirects you to the Microsoft Office 365 login page.
4. Sign in with the Office 365 global administrator credentials.

   Microsoft Office 365 displays a list of permissions that are necessary to back up and recover your organization's data.
5. Confirm that you grant the backup service these permissions.

As a result, your organization's data items appear in the backup console on the **Microsoft Office 365** page.

Tips for further usage

- The cloud agent synchronizes with Office 365 every 24 hours, starting from the moment when the organization is added to the backup service. If you add or remove a user, group, or site, you will not see this change in the backup console immediately. To forcibly synchronize the cloud agent with Office 365, select the organization on the **Microsoft Office 365** page, and then click **Refresh**.
- If you applied a backup plan to the **All users**, **All groups**, or **All sites** group, the newly added items will be included in the backup only after the synchronization.
- According to Microsoft policy, after a user, group, or site is removed from Office 365 GUI, it remains available for a few days via the API. During these days, the removed item is inactive (grayed out) in the backup console and is not backed up. When the removed item becomes unavailable via the API, it disappears from the backup console. Its backups (if any) can be found at **Backups** > **Cloud applications backups**.

15.2.2 Protecting Exchange Online mailboxes

What items can be backed up?

You can back up user mailboxes, shared mailboxes, and group mailboxes. Optionally, you can choose to back up the archive mailboxes (**In-Place Archive**) of the selected mailboxes.

What items can be recovered?

The following items can be recovered from a mailbox backup:

- Mailboxes
- Email folders
- Email messages
- Calendar events
- Tasks
- Contacts
- Journal entries
- Notes

You can use search to locate the items.

When recovering mailboxes and mailbox items, you can select whether to overwrite the items in the target location.

15.2.2.1 Selecting mailboxes

Select the mailboxes as described below, and then specify other settings of the backup plan as appropriate (p. 34).

To select Exchange Online mailboxes

1. Click **Microsoft Office 365**.
2. If multiple Office 365 organizations were added to the backup service, select the organization whose users' data you want to back up. Otherwise, skip this step.
3. Do one of the following:

- To back up the mailboxes of all users and all shared mailboxes (including mailboxes that will be created in the future), expand the **Users** node, select **All users**, and then click **Group backup**.
- To back up individual user or shared mailboxes, expand the **Users** node, select **All users**, select the users whose mailboxes you want to back up, and then click **Backup**.
- To back up all group mailboxes (including mailboxes of groups that will be created in the future), expand the **Groups** node, select **All groups**, and then click **Group backup**.
- To back up individual group mailboxes, expand the **Groups** node, select **All groups**, select the groups whose mailboxes you want to back up, and then click **Backup**.

4. On the backup plan panel:
    - Ensure that the **Mailboxes** item is selected in **What to back up**.
    - If you do not want to backup the archive mailboxes, disable the **Archive mailbox** switch.

15.2.2.2 Recovering mailboxes and mailbox items

Recovering mailboxes

1. Click **Microsoft Office 365**.
2. If multiple Office 365 organizations were added to the backup service, select the organization whose backed-up data you want to recover. Otherwise, skip this step.
3. Do one of the following:
    - To recover a user mailbox, expand the **Users** node, select **All users**, select the user whose mailbox you want to recover, and then click **Recovery**.
    - To recover a shared mailbox, expand the **Users** node, select **All users**, select the shared mailbox that you want to recover, and then click **Recovery**.
    - To recover a group mailbox, expand the **Groups** node, select **All groups**, select the group whose mailbox you want to recover, and then click **Recovery**.
    - If the user, group, or the shared mailbox was deleted, select the item in the **Cloud applications backups** section of the Backups tab (p. 111), and then click **Show backups**.

    You can search users and groups by name. Wildcards are not supported.
4. Select a recovery point.

    Tip. *To see only the recovery points that contain mailboxes, select **Mailboxes** in **Filter by content**.*
5. Click **Recover** > **Entire mailbox**.
6. If multiple Office 365 organizations are added to the backup service, click **Office 365 organization** to view, change, or specify the target organization.

    By default, the original organization is selected. If this organization is no longer registered in the backup service, you must specify the target organization.
7. In **Recover to mailbox**, view, change, or specify the target mailbox.

    By default, the original mailbox is selected. If this mailbox does not exist or a non-original organization is selected, you must specify the target mailbox.
8. Click **Start recovery**.
9. Select one of the overwriting options:
    - **Overwrite existing items**
    - **Do not overwrite existing items**
10. Click **Proceed** to confirm your decision.

Recovering mailbox items

1. Click **Microsoft Office 365**.
2. If multiple Office 365 organizations were added to the backup service, select the organization whose backed-up data you want to recover. Otherwise, skip this step.
3. Do one of the following:
   - To recover items from a user mailbox, expand the **Users** node, select **All users**, select the user whose mailbox originally contained the items that you want to recover, and then click **Recovery**.
   - To recover items from a shared mailbox, expand the **Users** node, select **All users**, select the shared mailbox that originally contained the items that you want to recover, and then click **Recovery**.
   - To recover items from a group mailbox, expand the **Groups** node, select **All groups**, select the group whose mailbox originally contained the items that you want to recover, and then click **Recovery**.
   - If the user, group, or the shared mailbox was deleted, select the item in the **Cloud applications backups** section of the Backups tab (p. 111), and then click **Show backups**.

   You can search users and groups by name. Wildcards are not supported.
4. Select a recovery point.

   Tip. *To see only the recovery points that contain mailboxes, select **Mailboxes** in **Filter by content**.*
5. Click **Recover** > **Email messages**.
6. Browse to the required folder or use search to obtain the list of the required items.

   The following search options are available. Wildcards are not supported.
   - For email messages: search by subject, sender, recipient, and date.
   - For events: search by title and date.
   - For tasks: search by subject and date.
   - For contacts: search by name, email address, and phone number.
7. Select the items that you want to recover. To be able to select folders, click the "recover folders" icon: ✓☰

   Additionally, you can do any of the following:
   - When an item is selected, click **Show content** to view its contents, including attachments. Click the name of an attached file to download it.
   - When an email message or a calendar item is selected, click **Send as email** to send the item to the specified email addresses. You can select the sender and write a text to be added to the forwarded item.
   - Only if the backup is not encrypted, you used search, and selected a single item in the search results: click **Show versions** to select the item version to recover. You can select any backed-up version, earlier or later than the selected recovery point.
8. Click **Recover**.
9. If multiple Office 365 organizations were added to the backup service, click **Office 365 organization** to view, change, or specify the target organization.

   By default, the original organization is selected. If this organization is no longer registered in the backup service, you must specify the target organization.
10. In **Recover to mailbox**, view, change, or specify the target mailbox.

By default, the original mailbox is selected. If this mailbox does not exist or a non-original organization is selected, you must specify the target mailbox.

11. [Only when recovering to a user or a shared mailbox] In **Path**, view or change the target folder in the target mailbox. By default, the **Recovered items** folder is selected.

    Group mailbox items are always recovered to the **Inbox** folder.
12. Click **Start recovery**.
13. Select one of the overwriting options:
    - **Overwrite existing items**
    - **Do not overwrite existing items**
14. Click **Proceed** to confirm your decision.

15.2.3 Protecting OneDrive files

What items can be backed up?

You can back up an entire OneDrive, or individual files and folders.

Files are backed up together with their sharing permissions. Advanced permission levels (**Design**, **Full**, **Contribute**) are not backed up.

What items can be recovered?

You can recover an entire OneDrive or any file or folder that was backed up.

You can use search to locate the items.

You can choose whether to recover the sharing permissions or let the files inherit the permissions from the folder to which they are recovered.

Sharing links for files and folders are not recovered.

15.2.3.1 Selecting OneDrive files

Select the files as described below, and then specify other settings of the backup plan as appropriate (p. 34).

To select OneDrive files

1. Click **Microsoft Office 365**.
2. If multiple Office 365 organizations were added to the backup service, select the organization whose users' data you want to back up. Otherwise, skip this step.
3. Do one of the following:
    - To back up the files of all users (including users that will be created in the future), expand the **Users** node, select **All users**, and then click **Group backup**.
    - To back up the files of individual users, expand the **Users** node, select **All users**, select the users whose files you want to back up, and then click **Backup**.
4. On the backup plan panel:
    - Ensure that the **OneDrive** item is selected in **What to back up**.
    - In **Items to back up**, do one of the following:
        - Keep the default setting **[All]** (all files).
        - Specify the files and folders to back up by adding their names or paths.

You can use wildcard characters (*, **, and ?). For more details about specifying paths and using wildcards, refer to "File filters" (p. 62).

- Specify the files and folders to back up by browsing.

  The **Browse** link is available only when creating a backup plan for a single user.

- [Optional] In **Items to back up**, click **Show exclusions** to specify the files and folders to skip during the backup.

  File exclusions override the file selection; i.e. if you specify the same file in both fields, this file will be skipped during a backup.

15.2.3.2 Recovering OneDrive and OneDrive files

Recovering an entire OneDrive

1. Click **Microsoft Office 365**.
2. If multiple Office 365 organizations were added to the backup service, select the organization whose backed-up data you want to recover. Otherwise, skip this step.
3. Expand the **Users** node, select **All users**, select the user whose OneDrive you want to recover, and then click **Recovery**.

   If the user was deleted, select the user in the **Cloud applications backups** section of the Backups tab (p. 111), and then click **Show backups**.

   You can search users by name. Wildcards are not supported.
4. Select a recovery point.

   Tip. *To see only the recovery points that contain OneDrive files, select **OneDrive** in **Filter by content**.*
5. Click **Recover** > **Entire OneDrive**.
6. If multiple Office 365 organizations were added to the backup service, click **Office 365 organization** to view, change, or specify the target organization.

   By default, the original organization is selected. If this organization is no longer registered in the backup service, you must specify the target organization.
7. In **Recover to drive**, view, change, or specify the target user.

   By default, the original user is selected. If this user does not exist or a non-original organization is selected, you must specify the target user.
8. Select whether to recover the sharing permissions for the files.
9. Click **Start recovery**.
10. Select one of the overwriting options:
    - **Overwrite existing files**
    - **Overwrite an existing file if it is older**
    - **Do not overwrite existing files**
11. Click **Proceed** to confirm your decision.

Recovering OneDrive files

1. Click **Microsoft Office 365**.
2. If multiple Office 365 organizations were added to the backup service, select the organization whose backed-up data you want to recover. Otherwise, skip this step.
3. Expand the **Users** node, select **All users**, select the user whose OneDrive files you want to recover, and then click **Recovery**.

If the user was deleted, select the user in the **Cloud Applications Backups** section of the Backups tab (p. 111), and then click **Show backups**.

You can search users by name. Wildcards are not supported.

4. Select a recovery point.

   Tip. *To see only the recovery points that contain OneDrive files, select* ***OneDrive*** *in* ***Filter by content****.*

5. Click **Recover** > **Files/folders**.
6. Browse to the required folder or use search to obtain the list of the required files and folders.

   You can use one or more wildcard characters (* and ?). For more details about using wildcards, refer to "File filters" (p. 62).

   The search is not available if the backup is encrypted.
7. Select the files that you want to recover.

   If the backup is not encrypted and you selected a single file, you can click **Show versions** to select the file version to recover. You can select any backed-up version, earlier or later than the selected recovery point.
8. If you want to download a file, select the file, click **Download**, select the location to save the file to, and then click **Save**. Otherwise, skip this step.
9. Click **Recover**.
10. If multiple Office 365 organizations were added to the backup service, click **Office 365 organization** to view, change, or specify the target organization.

    By default, the original organization is selected. If this organization is no longer registered in the backup service, you must specify the target organization.
11. In **Recover to drive**, view, change, or specify the target user.

    By default, the original user is selected. If this user does not exist or a non-original organization is selected, you must specify the target user.
12. In **Path**, view or change the target folder in the target user's OneDrive. By default, the original location is selected.
13. Select whether to recover the sharing permissions for the files.
14. Click **Start recovery**.
15. Select one of the file overwriting options:
    - **Overwrite existing files**
    - **Overwrite an existing file if it is older**
    - **Do not overwrite existing files**
16. Click **Proceed** to confirm your decision.

15.2.4 Protecting SharePoint Online sites

What items can be backed up?

You can back up SharePoint classic site collections, group (team) sites, and communication sites. Also, it is possible to choose individual subsites, lists, and libraries for backup.

The following items are *skipped* during a backup:

- The **Look and Feel** site settings (except for **Title, description, and logo**).
- Site page comments and page comments settings (comments **On**/**Off**).
- The **Site features** site settings.

- Web part pages and web parts embedded in the wiki pages (due to SharePoint Online API limitations).
- OneNote files (due to SharePoint Online API limitations).
- External data and Managed Metadata types of columns.
- The default site collection "domain-my.sharepoint.com". This is a collection where all of the organization users' OneDrive files reside.
- The contents of the recycle bin.

Limitations

- Titles and descriptions of sites/subsites/lists/columns are truncated during a backup if the title/description size is greater than 10000 bytes.

What items can be recovered?

The following items can be recovered from a site backup:

- Entire site
- Subsites
- Lists
- List items
- Document libraries
- Documents
- List item attachments
- Site pages and wiki pages

You can use search to locate the items.

Items can be recovered to the original or a non-original site. The path to a recovered item is the same as the original one. If the path does not exist, it is created.

You can choose whether to recover the sharing permissions or let the items inherit the permissions from the parent object after the recovery.

The following items cannot be recovered:

- Subsites based on the **Visio Process Repository** template.
- Lists of the following types: **Survey list**, **Task list**, **Picture library**, **Links**, **Calendar**, **Discussion Board**, **External**, and **Import Spreadsheet**.
- Lists for which multiple content types are enabled.

15.2.4.1 Selecting SharePoint Online data

Select the data as described below, and then specify other settings of the backup plan as appropriate (p. 34).

To select SharePoint Online data

1. Click **Microsoft Office 365**.
2. If multiple Office 365 organizations were added to the backup service, select the organization whose users' data you want to back up. Otherwise, skip this step.
3. Do one of the following:

- To back up all classic SharePoint sites in the organization (including sites that will be created in the future), expand the **Site collections** node, select **All site collections**, and then click **Group backup**.
- To back up individual classic sites, expand the **Site collections** node, select **All site collections**, select the sites that you want to back up, and then click **Backup**.
- To back up all group sites (including sites that will be created in the future), expand the **Groups** node, select **All groups**, and then click **Group backup**.
- To back up individual group sites, expand the **Groups** node, select **All groups**, select the groups whose sites you want to back up, and then click **Backup**.

4. On the backup plan panel:
   - Ensure that the **SharePoint sites** item is selected in **What to back up**.
   - In **Items to back up**, do one of the following:
     - Keep the default setting **[All]** (all items of the selected sites).
     - Specify the subsites, lists, and libraries to back up by adding their names or paths.

       To back up a subsite or a top-level site list/library, specify its display name in the following format: `/display name/**`

       To back up a subsite list/library, specify its display name in the following format: `/subsite display name/list display name/**`

       The display names of subsites, lists, and libraries are shown on the **Site contents** page of a SharePoint site or subsite.
     - Specify the subsites to back up by browsing.

       The **Browse** link is available only when creating a backup plan for a single site.
   - [Optional] In **Items to back up**, click **Show exclusions** to specify the subsites, lists, and libraries to skip during the backup.

     Item exclusions override the item selection; i.e. if you specify the same subsite in both fields, this subsite will be skipped during a backup.

15.2.4.2 Recovering SharePoint Online data

1. Click **Microsoft Office 365**.
2. If multiple Office 365 organizations were added to the backup service, select the organization whose backed-up data you want to recover. Otherwise, skip this step.
3. Do one of the following:
   - To recover data from a group site, expand the **Groups** node, select **All groups**, select the group whose site originally contained the items that you want to recover, and then click **Recovery**.
   - To recover data from a classic site, expand the **Site Collections** node, select **All site collections**, select the site that originally contained the items that you want to recover, and then click **Recovery**.
   - If the site was deleted, select it in the **Cloud applications backups** section of the Backups tab (p. 111), and then click **Show backups**.

   You can search groups and sites by name. Wildcards are not supported.
4. Select a recovery point.

   Tip. *To see only the recovery points that contain SharePoint sites, select **SharePoint sites** in **Filter by content**.*
5. Click **Recover SharePoint files**.

6. Browse to the required folder or use search to obtain the list of the required data items.

   You can use one or more wildcard characters (* and ?). For more details about using wildcards, refer to "File filters" (p. 62).

   The search is not available if the backup is encrypted.
7. Select the items that you want to recover.

   If the backup is not encrypted, you used search, and selected a single item in the search results, you can click **Show versions** to select the item version to recover. You can select any backed-up version, earlier or later than the selected recovery point.
8. If you want to download an item, select the item, click **Download**, select the location to save the item to, and click **Save**. Otherwise, skip this step.
9. Click **Recover**.
10. If multiple Office 365 organizations were added to the backup service, click **Office 365 organization** to view, change, or specify the target organization.

    By default, the original organization is selected. If this organization is no longer registered in the backup service, you must specify the target organization.
11. In **Recover to site**, view, change, or specify the target site.

    By default, the original site is selected. If this site does not exist or a non-original organization is selected, you must specify the target site.
12. Select whether to recover the sharing permissions of the recovered items.
13. Click **Start recovery**.
14. Select one of the overwriting options:
    - **Overwrite existing files**
    - **Overwrite an existing file if it is older**
    - **Do not overwrite existing files**
15. Click **Proceed** to confirm your decision.

15.2.5 Upgrading the cloud agent

This section describes how to upgrade to the current version of the backup solution for Microsoft Office 365. This version supports OneDrive and SharePoint Online backup, and provides improved backup and recovery performance.

The upgrade availability depends on the data center readiness and the settings made by your service provider. If the upgrade is available, the backup console shows a notification at the top of the **Microsoft Office 365 (v1)** tab.

The upgrade process

During the upgrade, your Office 365 organization users are added to the new backup solution. The backup plans are migrated and applied to the appropriate users.

The earlier created backups are copied from one location in the cloud to another. On the **Backups** tab, the copied backups are shown in a separate section named **Cloud applications backups**, while the original backups remain in the **Cloud storage** location. When the upgrade process is complete, the original backups are deleted from the **Cloud storage** location.

The upgrade may take several hours, or even days, depending on the number of users in the organization, the number of backups, and the Office 365 access speed. During the upgrade, recovery from the earlier created backups is possible. However, backups and backup plans created during the upgrade will be lost.

In the unlikely case of an upgrade failure, the backup solution remains fully operational and the upgrade can be restarted from the point of failure.

To start the upgrade process

1. Click **Microsoft Office 365 (v1)**.
2. Click **Upgrade** in the notification at the top of the screen.
3. Confirm that you want to start the upgrade process.
4. Select the Microsoft data center used by your organization.

   The software redirects you to the Microsoft Office 365 login page.
5. Sign in with the Office 365 global administrator credentials.

   Microsoft Office 365 displays a list of permissions that are necessary to back up and recover your organization's data.
6. Confirm that you grant the backup service these permissions.

   You are redirected to the backup console and the upgrade process begins. The upgrade progress is shown on the **Microsoft Office 365** > **Activities** panel.

16 Protecting G Suite data

What does G Suite protection mean?

- Cloud-to-cloud backup and recovery of G Suite user data (Gmail mailboxes, Calendars, Contacts, Google Drives) and G Suite Team Drives.
- Granular recovery of emails, files, contacts, and other items.
- Support for several G Suite organizations and cross-organization recovery.
- Optional notarization of the backed-up files by means of the Ethereum blockchain database. When enabled, you can prove that a file is authentic and unchanged since it was backed up.
- Optional full-text search. When enabled, you can search emails by their content.
- Up to 5000 items (mailboxes, Google Drives, and Team Drives) per company can be protected without performance degradation.

Required user rights

To add your G Suite organization to the backup service, you must be signed in as a Super Admin.

The Super Admin password is not stored anywhere and is not used to perform backup and recovery. Changing this password in G Suite does not affect backup service operation.

If the Super Admin who added the G Suite organization is deleted from G Suite or assigned a role with less privileges, the backups will fail with an error like "access denied". In this case, repeat the "Adding a G Suite organization" (p. 145) procedure and specify valid Super Admin credentials. To avoid this situation, we recommend creating a dedicated Super Admin user for backup and recovery purposes.

In the backup service, you need to be a company administrator. Unit administrators and users cannot back up or recover G Suite.

About the backup schedule

Because the cloud agent serves multiple customers, it determines the start time for each backup plan on its own, to ensure an even load during a day and an equal quality of service for all of the customers.

Each backup plan runs daily at the same time of day.

Limitations

Search in encrypted backups is not supported.

16.1 Adding a G Suite organization

To add a G Suite organization

1. Sign in to the backup console as a company administrator.
2. Click **Devices** > **Add** > **G Suite**.
3. Follow the instructions displayed by the software:
    a. Click **Open marketplace**.
    b. Sign in with the Super Admin credentials.
    c. Click **Domain install**.
    d. Confirm the domain-wide installation.

       G Suite displays a list of permissions that are necessary to back up and recover your organization's data.
    e. Confirm that you grant the backup service these permissions.
    f. Complete the installation wizard.
    g. Click **Launch**.

You are redirected back to the backup console. Your organization's data items appear in the backup console on the **G Suite** page.

Tips for further usage

- The cloud agent synchronizes with G Suite every 24 hours, starting from the moment when the organization is added to the backup service. If you add or remove a user or Team Drive, you will not see this change in the backup console immediately. To forcibly synchronize the cloud agent with G Suite, select the organization on the **G Suite** page, and then click **Refresh**.
- If you applied a backup plan to the **All users** or **All Team Drives** group, the newly added items will be included in the backup only after the synchronization.
- According to Google policy, after a user or Team Drive is removed from the G Suite GUI, it remains available for a few days via the API. During these days, the removed item is inactive (grayed out) in the backup console and is not backed up. When the removed item becomes unavailable via the API, it disappears from the backup console. Its backups (if any) can be found at **Backups** > **Cloud Applications Backups**.

16.2 Protecting Gmail data

What items can be backed up?

You can back up Gmail users' mailboxes. A mailbox backup also includes the Calendar and Contacts data. Optionally, you can choose to back up the shared calendars.

The following items are *skipped* during a backup:

- The **Birthdays**, **Reminders**, **Tasks** calendars
- Folders attached to calendar events
- The **Directory** folder in Contacts

The following Calendar items are *skipped,* due to Google Calendar API limitations:

- Appointment slots
- The conferencing field of an event
- The calendar setting **All-day event notifications**
- The calendar setting **Auto-accept invitations** (in calendars for rooms or shared spaces)

The following Contacts items are *skipped,* due to Google People API limitations:

- The **Other contacts** folder
- The external profiles of a contact (**Directory profile**, **Google profile**)
- The contact field **File as**

What items can be recovered?

The following items can be recovered from a mailbox backup:

- Mailboxes
- Email folders (According to Google terminology, "labels". **Labels** are presented in the backup software as folders, for consistency with other data presentation.)
- Email messages
- Calendar events
- Contacts

You can use search to locate items in a backup, unless the backup is encrypted. Search in encrypted backups is not supported.

When recovering mailboxes and mailbox items, you can select whether to overwrite the items in the target location.

Limitations

- Contact photos cannot be recovered
- The **Out of office** calendar item is recovered as a regular calendar event, due to Google Calendar API limitations

16.2.1 Selecting mailboxes

Select the mailboxes as described below, and then specify other settings of the backup plan as appropriate (p. 34).

To select Gmail mailboxes

1. Click **G Suite**.
2. If multiple G Suite organizations were added to the backup service, select the organization whose users' data you want to back up. Otherwise, skip this step.
3. Do one of the following:
   - To back up the mailboxes of all users (including mailboxes that will be created in the future), expand the **Users** node, select **All users**, and then click **Group backup**.
   - To back up individual user mailboxes, expand the **Users** node, select **All users**, select the users whose mailboxes you want to back up, and then click **Backup**.
4. On the backup plan panel:
   - Ensure that the **Gmail** item is selected in **What to back up**.

- If you want to back up calendars that are shared with the selected users, enable the **Include shared calendars** switch.
- Decide whether you need full-text search (p. 147) through the backed-up email messages. To access this option, click the gear icon > **Backup options** > **Full-text search**.

16.2.1.1 Full-text search

This option defines whether the email messages content is indexed by the cloud agent.

The preset is: **Enabled**.

If this option is enabled, the messages content is indexed and you can search messages by their content. Otherwise, only searching by subject, sender, recipient, or date is available.

***Note** Search in encrypted backups is not supported.*

The indexing process does not affect the backup performance because it is performed by a different software component. Indexing of the first (full) backup may take some time, therefore, there may be a delay between the backup completion and the content appearing in the search results.

The index occupies 10-30 percent of storage space occupied by the mailbox backups. To learn the exact value, click **Backups** > **Cloud applications backups** and view the **Index size** column. You may want to disable full-text search in order to save this space. The value in the **Index size** column will decrease to a few megabytes after the next backup. This minimal amount of metadata is necessary to perform a search by subject, sender, recipient, or date.

When you re-enable full-text search, the software indexes all of the backups previously created by the backup plan. This also takes some time.

16.2.2 Recovering mailboxes and mailbox items

16.2.2.1 Recovering mailboxes

1. Click **G Suite**.
2. If multiple G Suite organizations were added to the backup service, select the organization whose backed-up data you want to recover. Otherwise, skip this step.
3. Expand the **Users** node, select **All users**, select the user whose mailbox you want to recover, and then click **Recovery**.

   If the user was deleted, select the user in the **Cloud applications backups** section of the Backups tab (p. 111), and then click **Show backups**.

   You can search users and groups by name. Wildcards are not supported.
4. Select a recovery point.

   ***Tip.** To see only the recovery points that contain mailboxes, select **Gmail** in **Filter by content**.*
5. Click **Recover** > **Entire mailbox**.
6. If multiple G Suite organizations are added to the backup service, click **G Suite organization** to view, change, or specify the target organization.

   By default, the original organization is selected. If this organization is no longer registered in the backup service, you must specify the target organization.
7. In **Recover to mailbox**, view, change, or specify the target mailbox.

By default, the original mailbox is selected. If this mailbox does not exist or a non-original organization is selected, you must specify the target mailbox.

8. Click **Start recovery**.
9. Select one of the overwriting options:
   - **Overwrite existing items**
   - **Do not overwrite existing items**
10. Click **Proceed** to confirm your decision.

16.2.2.2 Recovering mailbox items

1. Click **G Suite**.
2. If multiple G Suite organizations were added to the backup service, select the organization whose backed-up data you want to recover. Otherwise, skip this step.
3. Expand the **Users** node, select **All users**, select the user whose mailbox originally contained the items that you want to recover, and then click **Recovery**.

   If the user was deleted, select the user in the **Cloud applications backups** section of the Backups tab (p. 111), and then click **Show backups**.

   You can search users and groups by name. Wildcards are not supported.
4. Select a recovery point.

   Tip. *To see only the recovery points that contain mailboxes, select **Gmail** in **Filter by content**.*
5. Click **Recover** > **Email messages**.
6. Browse to the required folder. If the backup is not encrypted, you can use search to obtain the list of the required items.

   The following search options are available. Wildcards are not supported.
   - For email messages: search by subject, sender, recipient, date, attachment name, and message content. The last two options yield results only if the **Full-text search** option was enabled during backup. The language of the message fragment being searched can be specified as an additional parameter.
   - For events: search by title and date.
   - For contacts: search by name, email address, and phone number.
7. Select the items that you want to recover. To be able to select folders, click the "recover folders" icon:

   Additionally, you can do any of the following:
   - When an item is selected, click **Show content** to view its contents, including attachments. Click the name of an attached file to download it.
   - Only if the backup is not encrypted, you used search, and selected a single item in the search results: click **Show versions** to select the item version to recover. You can select any backed-up version, earlier or later than the selected recovery point.
8. Click **Recover**.
9. If multiple G Suite organizations were added to the backup service, click **G suite organization** to view, change, or specify the target organization.

   By default, the original organization is selected. If this organization is no longer registered in the backup service, you must specify the target organization.
10. In **Recover to mailbox**, view, change, or specify the target mailbox.

By default, the original mailbox is selected. If this mailbox does not exist or a non-original organization is selected, you must specify the target mailbox.

11. In **Path**, view or change the target folder in the target mailbox. By default, the original folder is selected.
12. Click **Start recovery**.
13. Select one of the overwriting options:
    - **Overwrite existing items**
    - **Do not overwrite existing items**
14. Click **Proceed** to confirm your decision.

16.3 Protecting Google Drive files

What items can be backed up?

You can back up an entire Google Drive, or individual files and folders. Optionally, you can choose to back up files that are shared with the Google Drive user.

Files are backed up together with their sharing permissions.

The following items are *skipped* during a backup:

- A shared file, if the user has a commenter or viewer access to the file and the file owner disabled the options to download, print, and copy for commenters and viewers.
- The **Computers** folder (created by the Backup and Sync client)

Limitations

- Out of Google-specific file formats, only Google docs, Google sheets, Google slides, and Google Drawings are backed up.

What items can be recovered?

You can recover an entire Google Drive, or any file or folder that was backed up.

You can use search to locate items in a backup, unless the backup is encrypted. Search in encrypted backups is not supported.

You can choose whether to recover the sharing permissions or let the files inherit the permissions from the folder to which they are recovered.

Limitations

- Comments in files are not recovered.
- Sharing links for files and folders are not recovered.
- The read-only **Owner settings** for shared files (**Prevent editors from changing access and adding new people** and **Disable options to download, print and copy for commenters and viewers**) cannot be changed during a recovery.
- Ownership of a shared folder cannot be changed during a recovery if the **Prevent editors from changing access and adding new people** option is enabled for this folder. This setting prevents the Google Drive API from listing the folder permissions. Ownership of the files in the folder is recovered correctly.

16.3.1 Selecting Google Drive files

Select the files as described below, and then specify other settings of the backup plan as appropriate (p. 34).

To select Google Drive files

1. Click **G Suite**.
2. If multiple G Suite organizations were added to the backup service, select the organization whose users' data you want to back up. Otherwise, skip this step.
3. Do one of the following:
   - To back up the files of all users (including users that will be created in the future), expand the **Users** node, select **All users**, and then click **Group backup**.
   - To back up the files of individual users, expand the **Users** node, select **All users**, select the users whose files you want to back up, and then click **Backup**.
4. On the backup plan panel:
   - Ensure that the **Google Drive** item is selected in **What to back up**.
   - In **Items to back up**, do one of the following:
     - Keep the default setting **[All]** (all files).
     - Specify the files and folders to back up by adding their names or paths.

       You can use wildcard characters (*, **, and ?). For more details about specifying paths and using wildcards, refer to "File filters" (p. 62).
     - Specify the files and folders to back up by browsing.

       The **Browse** link is available only when creating a backup plan for a single user.
   - [Optional] In **Items to back up**, click **Show exclusions** to specify the files and folders to skip during the backup.

     File exclusions override the file selection; i.e. if you specify the same file in both fields, this file will be skipped during a backup.
   - If you want to back up the files that are shared with the selected users, enable the **Include shared files** switch.
   - If you want to enable notarization of all files selected for backup, enable the **Notarization** switch. For more information about notarization, refer to "Notarization" (p. 155).

16.3.2 Recovering Google Drive and Google Drive files

16.3.2.1 Recovering an entire Google Drive

1. Click **G Suite**.
2. If multiple G Suite organizations were added to the backup service, select the organization whose backed-up data you want to recover. Otherwise, skip this step.
3. Expand the **Users** node, select **All users**, select the user whose Google Drive you want to recover, and then click **Recovery**.

   If the user was deleted, select the user in the **Cloud applications backups** section of the Backups tab (p. 111), and then click **Show backups**.

   You can search users by name. Wildcards are not supported.
4. Select a recovery point.

   ***Tip.** To see only the recovery points that contain Google Drive files, select **Google Drive** in **Filter by content**.*

5. Click **Recover** > **Entire Drive**.
6. If multiple G Suite organizations were added to the backup service, click **G Suite organization** to view, change, or specify the target organization.

   By default, the original organization is selected. If this organization is no longer registered in the backup service, you must specify the target organization.
7. In **Recover to drive**, view, change, or specify the target user or the target Team Drive.

   By default, the original user is selected. If this user does not exist or a non-original organization is selected, you must specify the target user or the target Team Drive.

   If the backup contains shared files, the files will be recovered to the root folder of the target drive.
8. Select whether to recover the sharing permissions for the files.
9. Click **Start recovery**.
10. Select one of the overwriting options:
    - **Overwrite existing files**
    - **Overwrite an existing file if it is older**
    - **Do not overwrite existing files**
11. Click **Proceed** to confirm your decision.

16.3.2.2 Recovering Google Drive files

1. Click **G Suite**.
2. If multiple G Suite organizations were added to the backup service, select the organization whose backed-up data you want to recover. Otherwise, skip this step.
3. Expand the **Users** node, select **All users**, select the user whose Google Drive files you want to recover, and then click **Recovery**.

   If the user was deleted, select the user in the **Cloud applications backups** section of the Backups tab (p. 111), and then click **Show backups**.

   You can search users by name. Wildcards are not supported.
4. Select a recovery point.

   Tip. *To see only the recovery points that contain Google Drive files, select **Google Drive** in **Filter by content**.*
5. Click **Recover** > **Files/folders**.
6. Browse to the required folder or use search to obtain the list of the required files and folders.

   You can use one or more wildcard characters (* and ?). For more details about using wildcards, refer to "File filters" (p. 62).

   The search is not available if the backup is encrypted.
7. Select the files that you want to recover.

   If the backup is not encrypted and you selected a single file, you can click **Show versions** to select the file version to recover. You can select any backed-up version, earlier or later than the selected recovery point.
8. If you want to download a file, select the file, click **Download**, select the location to save the file to, and then click **Save**. Otherwise, skip this step.
9. Click **Recover**.
10. If multiple G Suite organizations were added to the backup service, click **G Suite organization** to view, change, or specify the target organization.

By default, the original organization is selected. If this organization is no longer registered in the backup service, you must specify the target organization.

11. In **Recover to drive**, view, change, or specify the target user or the target Team Drive.

    By default, the original user is selected. If this user does not exist or a non-original organization is selected, you must specify the target user or the target Team Drive.
12. In **Path**, view or change the target folder in the target user's Google Drive or in the Target Team drive. By default, the original location is selected.
13. Select whether to recover the sharing permissions for the files.
14. Click **Start recovery**.
15. Select one of the file overwriting options:
    - **Overwrite existing files**
    - **Overwrite an existing file if it is older**
    - **Do not overwrite existing files**
16. Click **Proceed** to confirm your decision.

16.4 Protecting Team Drive files

What items can be backed up?

You can back up an entire Team Drive, or individual files and folders.

Files are backed up together with their sharing permissions.

Limitations

- A Team Drive without members cannot be backed up, due to Google Drive API limitations.
- Out of Google-specific file formats only Google docs, Google sheets, Google slides, and Google Drawings are backed up.

What items can be recovered?

You can recover an entire Team Drive, or any file or folder that was backed up.

You can use search to locate items in a backup, unless the backup is encrypted. Search in encrypted backups is not supported.

You can choose whether to recover the sharing permissions or let the files inherit the permissions from the folder to which they are recovered.

The following items are not recovered:

- Sharing permissions for a file that was shared with a user outside the organization are not recovered if sharing outside the organization is disabled in the target Team Drive.
- Sharing permissions for a file that was shared with a user who is not a member of the target Team Drive are not recovered if **Sharing with non-members** is disabled in the target Team Drive.

Limitations

- Comments in files are not recovered.
- Sharing links for files and folders are not recovered.

16.4.1 Selecting Team Drive files

Select the files as described below, and then specify other settings of the backup plan as appropriate (p. 34).

To select Team Drive files

1. Click **G Suite**.
2. If multiple G Suite organizations were added to the backup service, select the organization whose users' data you want to back up. Otherwise, skip this step.
3. Do one of the following:
   - To back up the files of all Team Drives (including Team Drives that will be created in the future), expand the **Team Drives** node, select **All Team Drives**, and then click **Group backup**.
   - To back up the files of individual Team Drives, expand the **Team Drives** node, select **All Team Drives**, select the Team Drives to back up, and then click **Backup**.
4. On the backup plan panel:
   - In **Items to back up**, do one of the following:
     - Keep the default setting **[All]** (all files).
     - Specify the files and folders to back up by adding their names or paths.

       You can use wildcard characters (*, **, and ?). For more details about specifying paths and using wildcards, refer to "File filters" (p. 62).
     - Specify the files and folders to back up by browsing.

       The **Browse** link is available only when creating a backup plan for a single Team Drive.
   - [Optional] In **Items to back up**, click **Show exclusions** to specify the files and folders to skip during the backup.

     File exclusions override the file selection; i.e. if you specify the same file in both fields, this file will be skipped during a backup.
   - If you want to enable notarization of all files selected for backup, enable the **Notarization** switch. For more information about notarization, refer to "Notarization" (p. 155).

16.4.2 Recovering Team Drive and Team Drive files

16.4.2.1 Recovering an entire Team Drive

1. Click **G Suite**.
2. If multiple G Suite organizations were added to the backup service, select the organization whose backed-up data you want to recover. Otherwise, skip this step.
3. Expand the **Team Drives** node, select **All Team Drives**, select the Team Drive that you want to recover, and then click **Recovery**.

   If the Team Drive was deleted, select it in the **Cloud applications backups** section of the Backups tab (p. 111), and then click **Show backups**.

   You can search Team Drives by name. Wildcards are not supported.
4. Select a recovery point.
5. Click **Recover** > **Entire Team Drive**.
6. If multiple G Suite organizations were added to the backup service, click **G Suite organization** to view, change, or specify the target organization.

   By default, the original organization is selected. If this organization is no longer registered in the backup service, you must specify the target organization.

7. In **Recover to drive**, view, change, or specify the target Team Drive or the target user. If you specify a user, the data will be recovered to this user's Google Drive.

   By default, the original Team Drive is selected. If this Team Drive does not exist or a non-original organization is selected, you must specify the target Team Drive or the target user.
8. Select whether to recover the sharing permissions for the files.
9. Click **Start recovery**.
10. Select one of the overwriting options:
    - **Overwrite existing files**
    - **Overwrite an existing file if it is older**
    - **Do not overwrite existing files**
11. Click **Proceed** to confirm your decision.

16.4.2.2 Recovering Team Drive files

1. Click **G Suite**.
2. If multiple G Suite organizations were added to the backup service, select the organization whose backed-up data you want to recover. Otherwise, skip this step.
3. Expand the **Team Drives** node, select **All Team Drives**, select the Team Drive that originally contained the files you want to recover, and then click **Recovery**.

   If the Team Drive was deleted, select it in the **Cloud applications backups** section of the Backups tab (p. 111), and then click **Show backups**.

   You can search Team Drives by name. Wildcards are not supported.
4. Select a recovery point.
5. Click **Recover** > **Files/folders**.
6. Browse to the required folder or use search to obtain the list of the required files and folders.

   You can use one or more wildcard characters (* and ?). For more details about using wildcards, refer to "File filters" (p. 62).

   The search is not available if the backup is encrypted.
7. Select the files that you want to recover.

   If the backup is not encrypted and you selected a single file, you can click **Show versions** to select the file version to recover. You can select any backed-up version, earlier or later than the selected recovery point.
8. If you want to download a file, select the file, click **Download**, select the location to save the file to, and then click **Save**. Otherwise, skip this step.
9. Click **Recover**.
10. If multiple G Suite organizations were added to the backup service, click **G Suite organization** to view, change, or specify the target organization.

    By default, the original organization is selected. If this organization is no longer registered in the backup service, you must specify the target organization.
11. In **Recover to drive**, view, change, or specify the target Team Drive or the target user. If you specify a user, the data will be recovered to this user's Google Drive.

    By default, the original Team Drive is selected. If this Team Drive does not exist or a non-original organization is selected, you must specify the target Team Drive or the target user.
12. In **Path**, view or change the target folder in the target Team Drive or the target user's Google Drive. By default, the original location is selected.
13. Select whether to recover the sharing permissions for the files.

14. Click **Start recovery**.
15. Select one of the file overwriting options:
    - **Overwrite existing files**
    - **Overwrite an existing file if it is older**
    - **Do not overwrite existing files**
16. Click **Proceed** to confirm your decision.

16.5 Notarization

Notarization enables you to prove that a file is authentic and unchanged since it was backed up. We recommend that you enable notarization when backing up your legal document files or other files that require proved authenticity.

Notarization is available only for backups of Google Drive files and G Suite Team Drive files.

How to use notarization

To enable notarization of all files selected for backup, enable the **Notarization** switch when creating a backup plan.

When configuring recovery, the notarized files will be marked with a special icon, and you can verify the file authenticity.

How it works

During a backup, the agent calculates the hash codes of the backed-up files, builds a hash tree (based on the folder structure), saves the tree in the backup, and then sends the hash tree root to the notary service. The notary service saves the hash tree root in the Ethereum blockchain database to ensure that this value does not change.

When verifying the file authenticity, the agent calculates the hash of the file, and then compares it with the hash that is stored in the hash tree inside the backup. If these hashes do not match, the file is considered not authentic. Otherwise, the file authenticity is guaranteed by the hash tree.

To verify that the hash tree itself was not compromised, the agent sends the hash tree root to the notary service. The notary service compares it with the one stored in the blockchain database. If the hashes match, the selected file is guaranteed to be authentic. Otherwise, the software displays a message that the file is not authentic.

16.5.1 Verifying file authenticity with Notary Service

If notarization was enabled during backup, you can verify the authenticity of a backed-up file.

To verify the file authenticity

1. Do one of the following:
    - To verify the authenticity of a Google Drive file, select the file as described in steps 1-7 of the "Recovering Google Drive files" (p. 151) section.
    - To verify the authenticity of a G Suite Team Drive file, select the file as described in steps 1-7 of the "Recovering Team Drive files" (p. 154) section.
2. Ensure that the selected file is marked with the following icon: 📄. This means that the file is notarized.

3. Do one of the following:
   - Click **Verify**.

     The software checks the file authenticity and displays the result.
   - Click **Get certificate**.

     A certificate that confirms the file notarization is opened in a web browser window. The window also contains instructions that allow you to verify the file authenticity manually.

17 Active Protection

Active Protection protects a system from ransomware and cryptocurrency mining malware. Ransomware encrypts files and demands a ransom for the encryption key. Cryptomining malware performs mathematical calculations in the background, thus stealing the processing power and network traffic.

Active Protection is available for machines running Windows 7 and later, Windows Server 2008 R2 and later. Agent for Windows must be installed on the machine.

Active Protection is available for agents starting with version 12.0.4290. To update an agent, follow the instructions in "Updating agents" (p. 29).

How it works

Active Protection monitors processes running on the protected machine. When a third-party process tries to encrypt files or mine cryptocurrency, Active Protection generates an alert and performs additional actions, if those are specified by the configuration.

In addition, Active Protection prevents unauthorized changes to the backup software's own processes, registry records, executable and configuration files, and backups located in local folders.

To identify malicious processes, Active Protection uses behavioral heuristics. Active Protection compares the chain of actions performed by a process with the chains of events recorded in the database of malicious behavior patterns. This approach enables Active Protection to detect new malware by its typical behavior.

Active Protection settings

To minimize resources consumed by the heuristic analysis, and to eliminate so-called false positives, when a trusted program is considered as ransomware, you can define the following settings:

- Trusted processes that are never considered ransomware. Processes signed by Microsoft are always trusted.
- Harmful processes that are always considered ransomware. These processes will not be able to start as long as Active Protection is enabled on the machine.
- Folders where file changes will not be monitored.

Specify the full path to the process executable, starting with the drive letter. For example: `C:\Windows\Temp\er76s7sdkh.exe`.

For specifying folders, you can use the wildcard characters * and ?. The asterisk (*) substitutes for zero or more characters. The question mark (?) substitutes for exactly one character. Environment variables, such as %AppData%, cannot be used.

Active Protection plan

All settings of Active Protection are contained in the Active Protection plan. This plan can be applied to multiple machines.

There can be only one Active Protection plan in an organization (company group). Only company administrators and administrators of the upper levels are allowed to apply, edit, or revoke the plan.

Applying the Active Protection plan

1. Select the machines for which you want to enable Active Protection.
2. Click **Active Protection**.
3. [Optional] Click **Edit** to modify the following settings:
   - In **Action on detection**, select the action that the software will perform when detecting a ransomware activity, and then click **Done**. You can select one of the following:
     - **Notify only**

       The software will generate an alert about the process.
     - **Stop the process** (default)

       The software will generate an alert and stop the process.
     - **Revert using cache**

       The software will generate an alert, stop the process, and revert the file changes by using the service cache.
   - In **Harmful processes**, specify harmful processes that will always be considered ransomware, and then click **Done**.
   - In **Trusted processes**, specify trusted processes that will never be considered ransomware, and then click **Done**. Processes signed by Microsoft are always trusted.
   - In **Folder exclusions**, specify a list of folders where file changes will not be monitored, and then click **Done**.
   - Disable the **Self-protection** switch.

     Self-protection prevents unauthorized changes to the software's own processes, registry records, executable and configuration files, and backups located in local folders. We do not recommend disabling this feature.
   - Change **Protection options** (p. 157).
4. If you modified the settings, click **Save changes**. The changes will be applied to all machines where Active Protection is enabled.
5. Click **Apply**.

17.1 Protection options

Backups

This option is effective when **Self-protection** is enabled in the Active Protection plan.

This option applies to files that have extensions .tibx, .tib, .tia, and are located in local folders.

This option lets you specify the processes that are allowed to modify the backup files, even though these files are protected by self-protection. This comes in handy, for example, if you delete backup files or move them to a different location by using a script.

The preset is: **Enabled**.

If this option is enabled, the backup files can be modified only by processes signed by the backup software vendor. This allows the software to apply retention rules and to delete backups when a user requests this from the web interface. Other processes, no matter suspicious or not, cannot modify the backups.

If this option is disabled, you can allow other processes to modify the backups. Specify the full path to the process executable, starting with the drive letter.

Cryptomining protection

This option defines whether Active Protection detects potential cryptomining malware.

The preset is: **Disabled**.

If a cryptomining activity is detected, the selected **Action on detection** is performed (except reverting files from cache, as there is nothing to revert).

Cryptomining malware degrades performance of useful applications, increases electricity bills, may cause system crashes and even hardware damage due to abuse. We recommend that you add cryptomining malware to the **Harmful processes** list to prevent it from running.

Mapped drives

This option defines whether Active Protection protects network folders that are mapped as local drives.

This option applies to folders shared via SMB or NFS.

The preset is: **Enabled**.

If a file was originally located on a mapped drive, it cannot be saved to the original location when extracted from the cache by the **Revert using cache** action. Instead, it will be saved to the folder specified in this option's settings. The default folder is **C:\ProgramData\Acronis\Restored Network Files**. If this folder does not exist, it will be created. If you want to change this path, be sure to specify a local folder. Network folders, including folders on mapped drives, are not supported.

18 Protecting websites and hosting servers

18.1 Protecting websites

A website can be corrupted as a result of unauthorized access or a malware attack. Back up your website if you want to easily revert it to a healthy state, in case of corruption.

What do I need to back up a website?

The website must be accessible via the SFTP or SSH protocol. You do not need to install an agent, just add a website as described later in this section.

What items can be backed up?

You can back up the following items:

- **Website content files**

  All files accessible to the account you specify for the SFTP or SSH connection.
- **Linked databases (if any) hosted on MySQL servers.**

All databases accessible to the MySQL account you specify.

If your website employs databases, we recommend that you back up both the files and the databases, to be able to recover them to a consistent state.

Limitations

- The only backup location available for website backup is the cloud storage.
- A backup plan cannot be applied to multiple websites. Each website must have its own backup plan, even if all of the backup plans have the same settings.
- Only one backup plan can be applied to a website.
- Backup options are not available.

18.1.1 Backing up a website

To add a website and configure its backup

1. Click **Devices** > **Add**.
2. Click **Website**.
3. Configure the following access settings for the website:
   - In **Website name**, create and type a name for your website. This name will be displayed in the backup console.
   - In **Host**, specify the host name or IP address that will be used to access the website via SFTP or SSH. For example, `my.server.com` or `10.250.100.100`.
   - In **Port**, specify the port number.
   - In **User name** and **Password**, specify the credentials of the account that can be used to access the website via SFTP or SSH.

   Important *Only the files that are accessible to the specified account will be backed up.*

   Instead of a password, you can specify your private SSH key. To do this, select the **Use SSH private key instead of password** check box, and then specify the key.
4. Click **Next**.
5. If your website uses MySQL databases, configure the access settings for the databases. Otherwise, click **Skip**.
   a. In **Connection type**, select how to access the databases from the cloud:
      - **Via SSH from host**—The databases will be accessed via the host specified in step 3.
      - **Direct connection**—The databases will be accessed directly. Choose this setting only if the databases are accessible from the Internet.

   b. In **Host**, specify the name or IP address of the host where the MySQL server is running.

   c. In **Port**, specify the port number for the TCP/IP connection to the server. The default port number is 3306.

   d. In **User name** and **Password**, specify the MySQL account credentials.

   Important *Only the databases that are accessible to the specified account will be backed up.*

   e. Click **Create**.
6. The software shows a new backup plan template. Change the settings if necessary, and then click **Apply**.

To change the connection settings

1. Select the website under **Devices** > **Websites**.
2. Click **Overview**.

3. Click the pencil icon next to the website or the database connection settings.
4. Do the necessary changes, and then click **Save**.

To edit the backup plan

1. Select the website under **Devices** > **Websites**.
2. Click **Backup**.
3. Click the gear icon next to the backup plan name, and then click **Edit**.
4. Do the necessary changes, and then click **Save changes**.

18.1.2 Recovering a website

To recover a website

1. Under **Devices** > **Websites**, select the website that you want to recover.

   You can search websites by name. Wildcards are not supported.
2. Click **Recovery**.
3. Select the recovery point.
4. Click **Recover**, and then select what you want to recover: **Files/folders** or **SQL databases** (if any).

   To ensure that your website is in a consistent state, we recommend recovering both files and databases, in any order.
5. Depending on your choice, follow one of the procedures described below.

To recover the website files/folders

1. Browse to the required folder or use search to obtain the list of the required files and folders.

   You can use one or more wildcard characters (* and ?). For details about using wildcards, refer to "File filters" (p. 62).
2. Select the files that you want to recover.
3. If you want to save the files as a .zip file, click **Download**, select the location to save the data to, and click **Save**. Otherwise, skip this step.
4. Click **Recover**, and then confirm the action.

   The selected files and folders will be recovered to the original location.

To recover the databases

1. Select the databases that you want to recover.
2. If you want to save the databases as a .zip file, click **Download**, select the location to save the data to, and click **Save**. Otherwise, skip this step.
3. Click **Recover**, and then confirm the action.

   The selected databases will be recovered to the original location.

18.2 Protecting web hosting servers

Web hosting administrators that use the Plesk or cPanel platforms can integrate these platforms with the backup service.

The integration enables an administrator to do the following:

- Back up an entire Plesk or cPanel server to the cloud storage, with disk-level backup
- Recover the entire server, including all of the websites
- For Plesk: perform granular recovery of websites, individual files, mailboxes, or databases

- For cPanel: perform granular recovery of websites, individual files, mailboxes, mail filters, mail forwarders, databases, and accounts
- Enable self-service recovery for Plesk and cPanel customers

The integration is performed by using the backup service extension. If you need the extension for Plesk or cPanel, contact the provider of the backup service.

Supported Plesk and cPanel versions

- Plesk for Linux 17.0 and later
- Any cPanel version with PHP 5.6 and later

Quotas

Each backed-up Plesk or cPanel server consumes the **Web hosting servers** quota. If this quota is disabled or the overage for this quota is exceeded, the following will happen:

- If the server is physical, the **Servers** quota will be used. If this quota is disabled or the overage for this quota is exceeded, the backup will fail.
- If the server is virtual, the **Virtual machines** quota will be used. If this quota is disabled or the overage for this quota is exceeded, the **Servers** quota will be used. If this quota is disabled or the overage for this quota is exceeded, the backup will fail.

19 Special operations with virtual machines

19.1 Running a virtual machine from a backup (Instant Restore)

You can run a virtual machine from a disk-level backup that contains an operating system. This operation, also known as instant recovery, enables you to spin up a virtual server in seconds. The virtual disks are emulated directly from the backup and thus do not consume space on the datastore (storage). The storage space is required only to keep changes to the virtual disks.

We recommend running this temporary virtual machine for up to three days. Then, you can completely remove it or convert it to a regular virtual machine (finalize) without downtime.

As long as the temporary virtual machine exists, retention rules cannot be applied to the backup being used by that machine. Backups of the original machine can continue to run.

Usage examples

- **Disaster recovery**

  Instantly bring a copy of a failed machine online.
- **Testing a backup**

  Run the machine from the backup and ensure that the guest OS and applications are functioning properly.
- **Accessing application data**

  While the machine is running, use application's native management tools to access and extract the required data.

Prerequisites

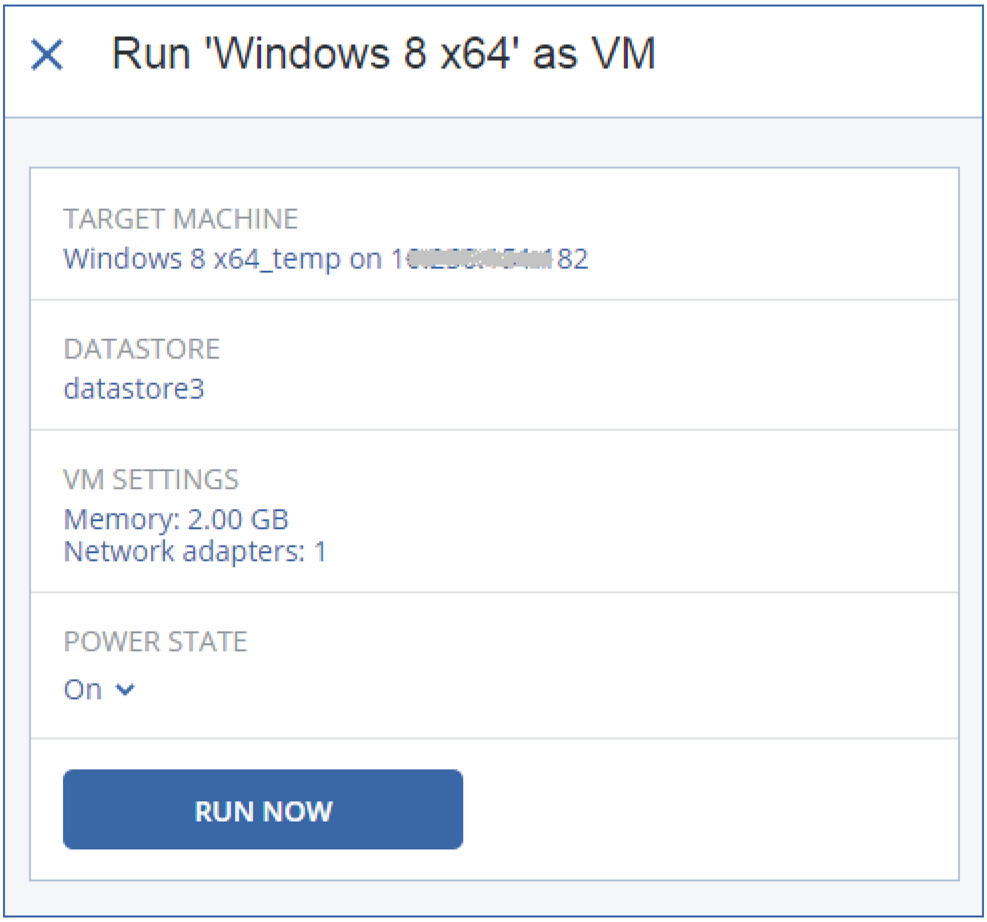
- At least one Agent for VMware or Agent for Hyper-V must be registered in the backup service.

- The backup can be stored in a network folder or in a local folder of the machine where Agent for VMware or Agent for Hyper-V is installed. If you select a network folder, it must be accessible from that machine. A virtual machine can also be run from a backup stored in the cloud storage, but it works slower because this operation requires intense random-access reading from the backup.
- The backup must contain an entire machine or all of the volumes that are required for the operating system to start.
- Backups of both physical and virtual machines can be used. Backups of Virtuozzo *containers* cannot be used.
- Backups that contain Linux logical volumes (LVM) must be created by Agent for VMware or Agent for Hyper-V. The virtual machine must be of the same type as the original machine (ESXi or Hyper-V).

19.1.1 Running the machine

1. Do one of the following:
   - Select a backed-up machine, click **Recovery**, and then select a recovery point.
   - Select a recovery point on the Backups tab (p. 111).
2. Click **Run as VM**.

   The software automatically selects the host and other required parameters.



Run 'Windows 8 x64' as VM

TARGET MACHINE
Windows 8 x64_temp on 1[redacted]82

DATASTORE
datastore3

VM SETTINGS
Memory: 2.00 GB
Network adapters: 1

POWER STATE
On

3. [Optional] Click **Target machine**, and then change the virtual machine type (ESXi or Hyper-V), the host, or the virtual machine name.
4. [Optional] Click **Datastore** for ESXi or **Path** for Hyper-V, and then select the datastore for the virtual machine.

Changes to the virtual disks accumulate while the machine is running. Ensure that the selected datastore has enough free space.

5. [Optional] Click **VM settings** to change the memory size and network connections of the virtual machine.
6. [Optional] Select the VM power state (**On**/**Off**).
7. Click **Run now**.

As a result, the machine appears in the web interface with one of the following icons: or HYPER-V. Such virtual machines cannot be selected for backup.

19.1.2 Deleting the machine

We do not recommend to delete a temporary virtual machine directly in vSphere/Hyper-V. This may lead to artifacts in the web interface. Also, the backup from which the machine was running may remain locked for a while (it cannot be deleted by retention rules).

To delete a virtual machine that is running from a backup

1. On the **All devices** tab, select a machine that is running from a backup.
2. Click **Delete**.

The machine is removed from the web interface. It is also removed from the vSphere or Hyper-V inventory and datastore (storage). All changes that occurred to the data while the machine was running are lost.

19.1.3 Finalizing the machine

While a virtual machine is running from a backup, the virtual disks' content is taken directly from that backup. Therefore, the machine will become inaccessible or even corrupted if the connection is lost to the backup location or to the backup agent.

For an ESXi machine, you have the option to make this machine permanent, i.e. recover all of its virtual disks, along with the changes that occurred while the machine was running, to the datastore that stores these changes. This process is named finalization.

Finalization is performed without downtime. The virtual machine will *not* be powered off during finalization.

To finalize a machine that is running from a backup

1. On the **All devices** tab, select a machine that is running from a backup.
2. Click **Finalize**.
3. [Optional] Specify a new name for the machine.
4. [Optional] Change the disk provisioning mode. The default setting is **Thin**.
5. Click **Finalize**.

The machine name changes immediately. The recovery progress is shown on the **Activities** tab. Once the recovery is completed, the machine icon changes to that of a regular virtual machine.

What you need to know about finalization

Finalization vs. regular recovery

The finalization process is slower than a regular recovery for the following reasons:

- During a finalization, the agent performs random access to different parts of the backup. When an entire machine is being recovered, the agent reads data from the backup sequentially.
- If the virtual machine is running during the finalization, the agent reads data from the backup more often, to maintain both processes simultaneously. During a regular recovery, the virtual machine is stopped.

Finalization of machines running from cloud backups

Because of intensive access to the backed-up data, the finalization speed highly depends on the connection bandwidth between the backup location and the agent. The finalization will be slower for backups located in the cloud as compared to local backups. If the Internet connection is very slow or unstable, the finalization of a machine running from a cloud backup may fail. We recommend to run virtual machines from local backups if you are planning to perform finalization and have the choice.

19.2 Replication of virtual machines

Replication is available only for VMware ESXi virtual machines.

Replication is the process of creating an exact copy (replica) of a virtual machine, and then maintaining the replica in sync with the original machine. By replicating a critical virtual machine, you will always have a copy of this machine in a ready-to-start state.

The replication can be started manually or on the schedule you specify. The first replication is full (copies the entire machine). All subsequent replications are incremental and are performed with Changed Block Tracking (p. 167), unless this option is disabled.

Replication vs. backing up

Unlike scheduled backups, a replica keeps only the latest state of the virtual machine. A replica consumes datastore space, while backups can be kept on a cheaper storage.

However, powering on a replica is much faster than a recovery and faster than running a virtual machine from a backup. When powered on, a replica works faster than a VM running from a backup and does not load the Agent for VMware.

Usage examples

- **Replicate virtual machines to a remote site.**

  Replication enables you to withstand partial or complete datacenter failures, by cloning the virtual machines from a primary site to a secondary site. The secondary site is usually located in a remote facility that is unlikely to be affected by environmental, infrastructure, or other factors that might cause the primary site failure.

- **Replicate virtual machines within a single site (from one host/datastore to another).**

  Onsite replication can be used for high availability and disaster recovery scenarios.

What you can do with a replica

- **Test a replica** (p. 166)

  The replica will be powered on for testing. Use vSphere Client or other tools to check if the replica works correctly. Replication is suspended while testing is in progress.

- **Failover to a replica** (p. 166)

  Failover is a transition of the workload from the original virtual machine to its replica. Replication is suspended while a failover is in progress.

- **Back up the replica**

  Both backup and replication require access to virtual disks, and thus impact the performance of the host where the virtual machine is running. If you want to have both a replica and backups of a virtual machine, but don't want to put additional load on the production host, replicate the machine to a different host, and set up backups of the replica.

Restrictions

The following types of virtual machines cannot be replicated:

- Fault-tolerant machines running on ESXi 5.5 and lower.
- Machines running from backups.
- Replicas of virtual machines.

19.2.1 Creating a replication plan

A replication plan must be created for each machine individually. It is not possible to apply an existing plan to other machines.

To create a replication plan

1. Select a virtual machine to replicate.
2. Click **Replication**.

   The software displays a new replication plan template.
3. [Optional] To modify the replication plan name, click the default name.
4. Click **Target machine**, and then do the following:
   a. Select whether to create a new replica or use an existing replica of the original machine.
   b. Select the ESXi host and specify the new replica name, or select an existing replica.

      The default name of a new replica is **[Original Machine Name]_replica**.
   c. Click **OK**.
5. [Only when replicating to a new machine] Click **Datastore**, and then select the datastore for the virtual machine.
6. [Optional] Click **Schedule** to change the replication schedule.

   By default, replication is performed on a daily basis, Monday to Friday. You can select the time to run the replication.

   If you want to change the replication frequency, move the slider, and then specify the schedule.

   You can also do the following:

   - Set a date range for when the schedule is effective. Select the **Run the plan within a date range** check box, and then specify the date range.
   - Disable the schedule. In this case, replication can be started manually.
7. [Optional] Click the gear icon to modify the replication options (p. 167).
8. Click **Apply**.
9. [Optional] To run the plan manually, click **Run now** on the plan panel.

As a result of running a replication plan, the virtual machine replica appears in the **All devices** list with the following icon: R

19.2.2 Testing a replica

To prepare a replica for testing

1. Select a replica to test.
2. Click **Test replica**.
3. Click **Start testing**.
4. Select whether to connect the powered-on replica to a network. By default, the replica will not be connected to a network.
5. [Optional] If you chose to connect the replica to the network, select the **Stop original virtual machine** check box to stop the original machine before powering on the replica.
6. Click **Start**.

To stop testing a replica

1. Select a replica for which testing is in progress.
2. Click **Test replica**.
3. Click **Stop testing**.
4. Confirm your decision.

19.2.3 Failing over to a replica

To failover a machine to a replica

1. Select a replica to failover to.
2. Click **Replica actions**.
3. Click **Failover**.
4. Select whether to connect the powered-on replica to a network. By default, the replica will be connected to the same network as the original machine.
5. [Optional] If you chose to connect the replica to the network, clear the **Stop original virtual machine** check box to keep the original machine online.
6. Click **Start**.

While the replica is in a failover state, you can choose one of the following actions:

- **Stop failover** (p. 167)

  Stop failover if the original machine was fixed. The replica will be powered off. Replication will be resumed.
- **Perform permanent failover to the replica** (p. 167)

  This instant operation removes the 'replica' flag from the virtual machine, so that replication to it is no longer possible. If you want to resume replication, edit the replication plan to select this machine as a source.
- **Failback** (p. 167)

  Perform failback if you failed over to the site that is not intended for continuous operations. The replica will be recovered to the original or a new virtual machine. Once the recovery to the original machine is complete, it is powered on and replication is resumed. If you choose to recover to a new machine, edit the replication plan to select this machine as a source.

19.2.3.1 Stopping failover

To stop a failover

1. Select a replica that is in the failover state.
2. Click **Replica actions**.
3. Click **Stop failover**.
4. Confirm your decision.

19.2.3.2 Performing a permanent failover

To perform a permanent failover

1. Select a replica that is in the failover state.
2. Click **Replica actions**.
3. Click **Permanent failover**.
4. [Optional] Change the name of the virtual machine.
5. [Optional] Select the **Stop original virtual machine** check box.
6. Click **Start**.

19.2.3.3 Failing back

To failback from a replica

1. Select a replica that is in the failover state.
2. Click **Replica actions**.
3. Click **Failback from replica**.

   The software automatically selects the original machine as the target machine.
4. [Optional] Click **Target machine**, and then do the following:
   a. Select whether to failback to a new or existing machine.
   b. Select the ESXi host and specify the new machine name, or select an existing machine.
   c. Click **OK**.
5. [Optional] When failing back to a new machine, you can also do the following:
   - Click **Datastore** to select the datastore for the virtual machine.
   - Click **VM settings** to change the memory size, the number of processors, and the network connections of the virtual machine.
6. [Optional] Click **Recovery options** to modify the failback options (p. 168).
7. Click **Start recovery**.
8. Confirm your decision.

19.2.4 Replication options

To modify the replication options, click the gear icon next to the replication plan name, and then click **Replication options**.

Changed Block Tracking (CBT)

This option is similar to the backup option "Changed Block Tracking (CBT)" (p. 60).

Disk provisioning

This option defines the disk provisioning settings for the replica.

The preset is: **Thin provisioning**.

The following values are available: **Thin provisioning**, **Thick provisioning**, **Keep the original setting**.

Error handling

This option is similar to the backup option "Error handling" (p. 61).

Pre/Post commands

This option is similar to the backup option "Pre/Post commands" (p. 67).

Volume Shadow Copy Service VSS for virtual machines

This option is similar to the backup option "Volume Shadow Copy Service VSS for virtual machines" (p. 73).

19.2.5 Failback options

To modify the failback options, click **Recovery options** when configuring failback.

Error handling

This option is similar to the recovery option "Error handling" (p. 89).

Performance

This option is similar to the recovery option "Performance" (p. 90).

Pre/Post commands

This option is similar to the recovery option "Pre/Post commands" (p. 91).

VM power management

This option is similar to the recovery option "VM power management" (p. 92).

19.2.6 Seeding an initial replica

To speed up replication to a remote location and save network bandwidth, you can perform replica seeding.

Important *To perform replica seeding, Agent for VMware (Virtual Appliance) must be running on the target ESXi.*

To seed an initial replica

1. Do one of the following:
   - If the original virtual machine can be powered off, power it off, and then skip to step 4.
   - If the original virtual machine cannot be powered off, continue to the next step.
2. Create a replication plan (p. 165).

   When creating the plan, in **Target machine**, select **New replica** and the ESXi that hosts the original machine.
3. Run the plan once.

A replica is created on the original ESXi.

4. Export the virtual machine (or the replica) files to an external hard drive.
   a. Connect the external hard drive to the machine where vSphere Client is running.
   b. Connect vSphere Client to the original vCenter\ESXi.
   c. Select the newly created replica in the inventory.
   d. Click **File** > **Export** > **Export OVF template**.
   e. In **Directory**, specify the folder on the external hard drive.
   f. Click **OK**.
5. Transfer the hard drive to the remote location.
6. Import the replica to the target ESXi.
   a. Connect the external hard drive to the machine where vSphere Client is running.
   b. Connect vSphere Client to the target vCenter\ESXi.
   c. Click **File** > **Deploy OVF template**.
   d. In **Deploy from a file or URL**, specify the template that you exported in step 4.
   e. Complete the import procedure.
7. Edit the replication plan that you created in step 2. In **Target machine**, select **Existing replica**, and then select the imported replica.

As a result, the software will continue updating the replica. All replications will be incremental.

19.3 Managing virtualization environments

You can view the vSphere, Hyper-V, and Virtuozzo environments in their native presentation. Once the corresponding agent is installed and registered, the **VMware**, **Hyper-V**, or **Virtuozzo** tab appears under **Devices**.

The **VMware** tab enables you to change access credentials for the vCenter Server or stand-alone ESXi host without re-installing the agent.

To change the vCenter Server or ESXi host access credentials

1. Under **Devices**, click **VMware**.
2. Click **Hosts and Clusters**.
3. In the **Hosts and Clusters** list (to the right of the **Hosts and Clusters** tree), select the vCenter Server or stand-alone ESXi host that was specified during the Agent for VMware installation.
4. Click **Overview**.
5. Under **Credentials**, click the user name.
6. Specify the new access credentials, and then click **OK**.

19.4 Machine migration

You can perform machine migration by recovering its backup to a non-original machine.

The following table summarizes the available migration options.

Backed-up machine type	**Available recovery destinations**				
	Physical machine	ESXi virtual machine	Hyper-V virtual machine	Virtuozzo virtual machine	Virtuozzo container
Physical machine	+	+	+	-	-
VMware ESXi virtual machine	+	+	+	-	-
Hyper-V virtual machine	+	+	+	-	-
Virtuozzo virtual machine	+	+	+	+	-
Virtuozzo container	-	-	-	-	+

For instructions on how to perform migration, refer to the following sections:

- Physical-to-virtual (P2V) - "Physical machine to virtual" (p. 76)
- Virtual-to-virtual (V2V) - "Virtual machine" (p. 77)
- Virtual-to-physical (V2P) - "Virtual machine" (p. 77) or "Recovering disks by using bootable media" (p. 79)

Although it is possible to perform V2P migration in the web interface, we recommend using bootable media in specific cases. Sometimes, you may want to use the media for migration to ESXi or Hyper-V.

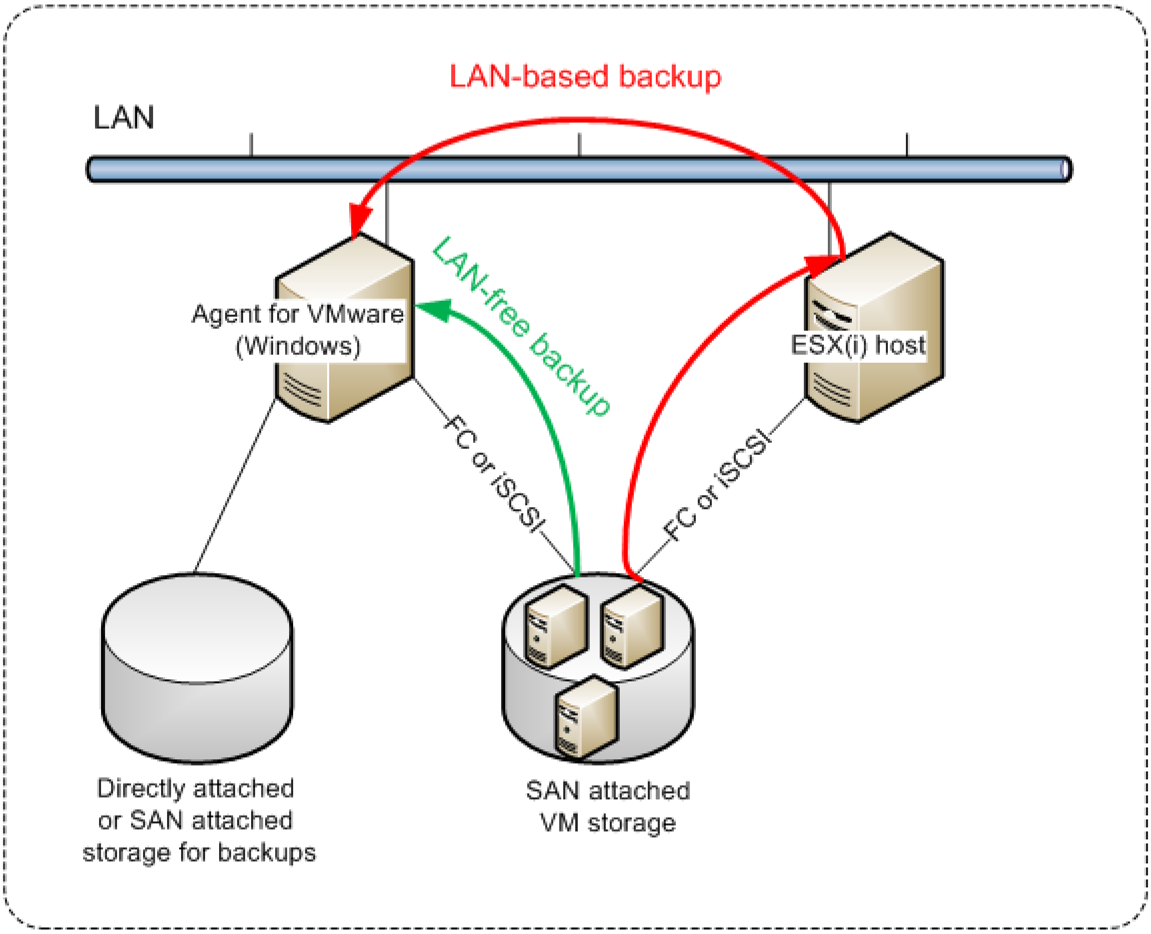
The media enables you to do the following:

- Choose individual disks or volumes for recovery.
- Manually map the disks from the backup to the target machine disks.
- Perform P2V migration or V2P migration or V2V migration from Virtuozzo, of a Linux machine containing logical volumes (LVM). Use Agent for Linux to create the backup and bootable media to recover.
- Provide drivers for specific hardware that is critical for the system bootability.

19.5 Agent for VMware - LAN-free backup

If your ESXi uses a SAN attached storage, install the agent on a machine connected to the same SAN. The agent will back up the virtual machines directly from the storage rather than via the ESXi host and LAN. This capability is called a LAN-free backup.

The diagram below illustrates a LAN-based and a LAN-free backup. LAN-free access to virtual machines is available if you have a fibre channel (FC) or iSCSI Storage Area Network. To completely eliminate transferring the backed-up data via LAN, store the backups on a local disk of the agent's machine or on a SAN attached storage.



To enable the agent to access a datastore directly

1. Install Agent for VMware on a Windows machine that has network access to the vCenter Server.
2. Connect the logical unit number (LUN) that hosts the datastore to the machine. Consider the following:
   - Use the same protocol (i.e. iSCSI or FC) that is used for the datastore connection to the ESXi.
   - The LUN *must not* be initialized and must appear as an "offline" disk in **Disk Management**. If Windows initializes the LUN, it may become corrupted and unreadable by VMware vSphere.

As a result, the agent will use the SAN transport mode to access the virtual disks, i.e. it will read raw LUN sectors over iSCSI/FC without recognizing the VMFS file system (which Windows is not aware of).

Limitations

- In vSphere 6.0 and later, the agent cannot use the SAN transport mode if some of the VM disks are located on a VMware Virtual Volume (VVol) and some are not. Backups of such virtual machines will fail.
- Encrypted virtual machines, introduced in VMware vSphere 6.5, will be backed up via LAN, even if you configure the SAN transport mode for the agent. The agent will fall back on the NBD transport because VMware does not support SAN transport for backing up encrypted virtual disks.

Example

If you are using an iSCSI SAN, configure the iSCSI initiator on the machine running Windows where Agent for VMware is installed.

To configure the SAN policy

1. Log on as an administrator, open the command prompt, type `diskpart`, and then press **Enter**.
2. Type `san`, and then press **Enter**. Ensure that **SAN Policy : Offline All** is displayed.
3. If another value for SAN Policy is set:
   a. Type `san policy=offlineall`.
   b. Press **Enter**.
   c. To check that the setting has been applied correctly, perform step 2.
   d. Restart the machine.

To configure an iSCSI initiator

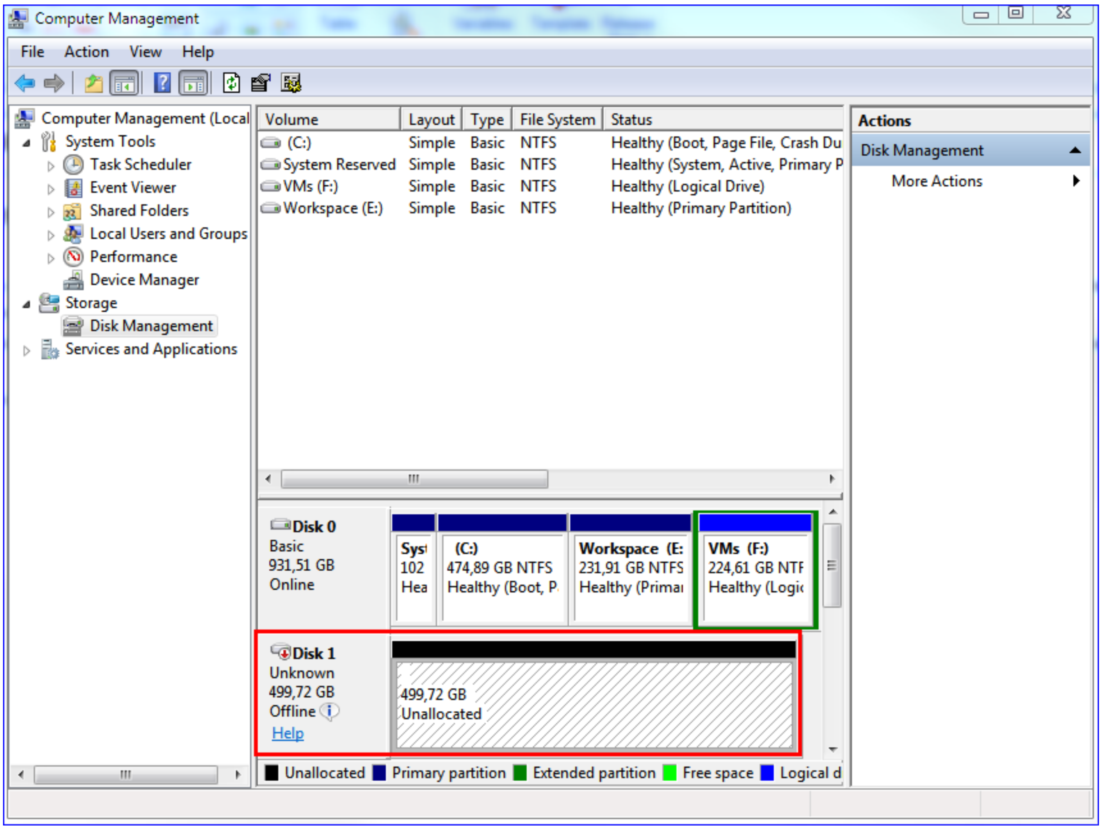
1. Go to **Control Panel** > **Administrative Tools** > **iSCSI Initiator**.

   Tip. *To find the* ***Administrative Tools*** *applet, you may need to change the* ***Control Panel*** *view to something other than* ***Home*** *or* ***Category****, or use search.*

2. If this is the first time that Microsoft iSCSI Initiator is launched, confirm that you want to start the Microsoft iSCSI Initiator service.
3. On the **Targets** tab, type the fully qualified domain name (FQDN) name or the IP address of the target SAN device, and then click **Quick Connect**.
4. Select the LUN that hosts the datastore, and then click **Connect**.

   If the LUN is not displayed, ensure that the zoning on the iSCSI target enables the machine running the agent to access the LUN. The machine must be added to the list of allowed iSCSI initiators on this target.
5. Click **OK**.

The ready SAN LUN should appear in **Disk Management** as shown in the screenshot below.



Volume	Layout	Type	File System	Status
(C:)	Simple	Basic	NTFS	Healthy (Boot, Page File, Crash Du
System Reserved	Simple	Basic	NTFS	Healthy (System, Active, Primary P
VMs (F:)	Simple	Basic	NTFS	Healthy (Logical Drive)
Workspace (E:)	Simple	Basic	NTFS	Healthy (Primary Partition)

19.6 Agent for VMware - necessary privileges

To perform operations on all hosts and clusters managed by a vCenter Server, Agent for VMware needs the privileges on the vCenter Server. If you want the agent to operate on a specific ESXi host only, provide the agent with the same privileges on the host.

Specify the account with the necessary privileges during Agent for VMware installation or configuration. If you need to change the account at a later time, refer to the "Managing virtualization environments" (p. 169) section.

		Operation			
Object	**Privilege**	**Back up a VM**	**Recover to a new VM**	**Recover to an existing VM**	**Run VM from backup**
Cryptographic operations (starting with vSphere 6.5)	**Add disk**	+*			
	Direct Access	+*			
Datastore	**Allocate space**		+	+	+
	Browse datastore				+
	Configure datastore	+	+	+	+
	Low level file operations				+

		Operation			
Object	Privilege	Back up a VM	Recover to a new VM	Recover to an existing VM	Run VM from backup
Global	**Licenses**	+	+	+	+
	Disable methods	+	+	+	
	Enable methods	+	+	+	
Host > **Configuration**	**Storage partition configuration**				+
Host > **Local operations**	**Create VM**				+
	Delete VM				+
	Reconfigure VM				+
Network	**Assign network**		+	+	+
Resource	**Assign VM to resource pool**		+	+	+
Virtual machine > **Configuration**	**Add existing disk**	+	+		+
	Add new disk		+	+	+
	Add or remove device		+		+
	Advanced	+	+	+	
	Change CPU count		+		
	Disk change tracking	+		+	
	Disk lease	+		+	
	Memory		+		
	Remove disk	+	+	+	+
	Rename		+		
	Set annotation				+
	Settings		+	+	+
Virtual machine > **Guest Operations**	**Guest Operation Program Execution**	+**			
	Guest Operation Queries	+**			
	Guest Operation Modifications	+**			
Virtual machine > **Interaction**	**Acquire guest control ticket** (in vSphere 4.1 and 5.0)				+
	Configure CD media		+	+	

		Operation			
Object	**Privilege**	**Back up a VM**	**Recover to a new VM**	**Recover to an existing VM**	**Run VM from backup**
	Guest operating system management by VIX API (in vSphere 5.1 and later)				+
	Power off			+	+
	Power on		+	+	+
Virtual machine > Inventory	**Create from existing**		+	+	+
	Create new		+	+	+
	Register				+
	Remove		+	+	+
	Unregister				+
Virtual machine > Provisioning	**Allow disk access**		+	+	+
	Allow read-only disk access	+		+	
	Allow virtual machine download	+	+	+	+
Virtual machine > State	**Create snapshot**	+		+	+
	Remove snapshot	+		+	+
vApp	**Add virtual machine**				+

* This privilege is required for backing up encrypted machines only.

** This privilege is required for application-aware backups only.

19.7 Windows Azure and Amazon EC2 virtual machines

To back up a Windows Azure or Amazon EC2 virtual machine, install a backup agent on the machine. The backup and recovery operations are the same as with a physical machine. Nevertheless, the machine is counted as virtual when you set quotas for the number of machines.

The difference from a physical machine is that Windows Azure and Amazon EC2 virtual machines cannot be booted from bootable media. If you need to recover to a new Windows Azure or Amazon EC2 virtual machine, follow the procedure below.

To recover a machine as a Windows Azure or Amazon EC2 virtual machine

1. Create a new virtual machine from an image/template in Windows Azure or Amazon EC2. The new machine must have the same disk configuration as the machine that you want to recover.
2. Install Agent for Windows or Agent for Linux on the new machine.

3. Recover the backed-up machine as described in "Physical machine" (p. 75). When configuring the recovery, select the new machine as the target machine.

19.8 Limiting the total number of simultaneously backed-up virtual machines

The **Scheduling** (p. 70) backup option defines how many virtual machines an agent can back up simultaneously when executing the given backup plan.

When multiple backup plans overlap in time, the numbers specified in their backup options are added up. Even though the resulting total number is programmatically limited to 10, overlapping plans can affect the backup performance and overload both the host and the virtual machine storage.

You can further reduce the total number of virtual machines that an Agent for VMware or Agent for Hyper-V can back up simultaneously.

To limit the total number of virtual machines that Agent for VMware (Windows) or Agent for Hyper-V can back up

1. On the machine running the agent, create a new text document and open it in a text editor, such as Notepad.
2. Copy and paste the following lines into the file:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\MMS\Configuration\ManagedMachine\SimultaneousBackupsLimits]
"MaxNumberOfSimultaneousBackups"=dword:00000001
```

3. Replace `00000001` with the hexadecimal value of the limit that you want to set. For example, `00000001` is 1 and `0000000A` is 10.
4. Save the document as **limit.reg**.
5. Run the file as an administrator.
6. Confirm that you want to edit the Windows registry.
7. Do the following to restart the agent:
    a. In the **Start** menu, click **Run**, and then type: **cmd**
    b. Click **OK**.
    c. Run the following commands:

```
net stop mms
net start mms
```

To limit the total number of virtual machines that Agent for VMware (Virtual Appliance) can back up

1. To start the command shell, press CTRL+SHIFT+F2 while in the virtual appliance UI.
2. Open the file **/etc/Acronis/MMS.config** in a text editor, such as **vi**.
3. Locate the following section:

```
<key name="SimultaneousBackupsLimits">
    <value name="MaxNumberOfSimultaneousBackups" type="Tdword">"10"</value>
</key>
```

4. Replace `10` with the decimal value of the limit that you want to set.
5. Save the file.

6. Execute the **`reboot`** command to restart the agent.

20 Administering user accounts and organization units

Administering user accounts and organization units is available in the management portal. To access the management portal, click **Management Portal** when logging in to the backup service or click the ⊞ icon in the top-right corner, and then click **Management portal**. Only users that have administrative privileges can access this portal.

For information about administering user accounts and organization units, refer to the Management Portal Administrator's Guide. To access this document, click the question mark icon in the management portal.

This section provides additional information related to managing the backup service.

20.1 Quotas

Quotas enable you to limit the users' ability to use the service. To set the quotas, select the user on the **Users** tab, and then click the pencil icon in the **Quotas** section.

When a quota is exceeded, a notification is sent to the user's email address. If you do not set a quota overage, the quota is considered "soft". This means that restrictions on using the backup service are not applied.

You can also specify the quota overages. An overage allows the user to exceed the quota by the specified value. When the overage is exceeded, restrictions on using the backup service are applied.

Managed-service providers can also specify quotas for their customer companies in a similar way.

20.1.1 Backup

You can specify the cloud storage quota, the quota for local backup, and the maximum number of machines/devices/websites a user is allowed to protect. The following quotas are available.

Quotas for devices

- **Workstations**
- **Servers**
- **Virtual machines**
- **Mobile devices**
- **Web hosting servers**
- **Websites**

A machine/device/website is considered protected as long as at least one backup plan is applied to it. A mobile device becomes protected after the first backup.

When the overage for a number of devices is exceeded, the user cannot apply a backup plan to more devices.

Quotas for cloud data sources

- **Office 365 seats**

  This quota is applied by the service provider to the entire company. The company can be allowed to protect **Mailboxes**, **OneDrive** files, or both. Company administrators can view the quota and the usage in the management portal, but cannot set the quota for a user.

- **Office 365 SharePoint Online**

  This quota is applied by the service provider to the entire company. This quota enables or disables the ability to protect SharePoint Online sites. If the quota is enabled, any number of SharePoint Online sites can be protected. Company administrators cannot view the quota in the management portal, but can view the amount of storage occupied by SharePoint Online backups in the usage reports.

- **G Suite seats**

  This quota is applied by the service provider to the entire company. The company can be allowed to protect **Gmail** mailboxes (including calendar and contacts), **Google Drive** files, or both. Company administrators can view the quota and the usage in the management portal, but cannot set the quota for a user.

- **G Suite Team Drive**

  This quota is applied by the service provider to the entire company. This quota enables or disables the ability to protect G Suite Team Drives. If the quota is enabled, any number of Team Drives can be protected. Company administrators cannot view the quota in the management portal, but can view the amount of storage occupied by SharePoint Online backups in the usage reports.

An Office 365 seat is considered protected as long as at least one backup plan is applied to the user's mailbox or OneDrive. A G Suite seat is considered protected as long as at least one backup plan is applied to the user's mailbox or Google Drive.

When the overage for a number of seats is exceeded, a company administrator cannot apply a backup plan to more seats.

Quotas for storage

- **Local backup**

  The **Local backup** quota limits the total size of local backups that are created by using the cloud infrastructure. An overage cannot be set for this quota.

- **Cloud resources**

  The **Cloud resources** quota combines the quota for backup storage and quotas for disaster recovery. The backup storage quota limits the total size of backups located in the cloud storage. When the backup storage quota overage is exceeded, backups fail.

20.1.2 Disaster recovery

These quotas are applied by the service provider to the entire company. Company administrators can view the quotas and the usage in the management portal, but cannot set quotas for a user.

- **Disaster recovery storage**

  This storage is used by primary and recovery servers. If the overage for this quota is reached, it is not possible to create primary and recovery servers, or add/extend disks of the existing primary servers. If the overage for this quota is exceeded, it is not possible to initiate a failover or just start a stopped server. The running servers continue to run.

When the quota is disabled, all of the servers are deleted. The **Cloud recovery site** tab disappears from the backup console.

- **Compute points**

  This quota limits the CPU and RAM resources that are consumed by primary and recovery servers during a billing period. If the overage for this quota is reached, all primary and recovery servers are shut down. It is not possible to use these servers until the beginning of the next billing period. The default billing period is a full calendar month.

  When the quota is disabled, the servers cannot be used regardless of the billing period.

- **Public IP addresses**

  This quota limits the number of public IP addresses that can be assigned to primary and recovery servers. If the overage for this quota is reached, it is not possible to enable public IP addresses for more servers. You can disallow a server to use a public IP address, by clearing the **Public IP address** check box in the server settings. After that, you can allow another server to use a public IP address, which usually will not be the same one.

  When the quota is disabled, all of the servers stop using public IP addresses, and thus become not reachable from the Internet.

- **Cloud servers**

  This quota limits the total number of primary and recovery servers. If the overage for this quota reached, it is not possible to create primary or recovery servers.

  When the quota is disabled, the servers are visible in the backup console, but the only available operation is **Delete**.

- **Internet access**

  This quota enables or disables the Internet access from primary and recovery servers.

  When the quota is disabled, the primary and recovery servers are disconnected from the Internet immediately. The **Internet access** switch in the servers' properties becomes cleared and disabled.

20.2 Notifications

To change the notifications settings for a user, select the user on the **Users** tab, and then click the pencil icon in the **Settings** section. The following notifications settings are available:

- **Quota overuse notifications** (enabled by default)

  The notifications about exceeded quotas.

- **Scheduled usage reports**

  The usage reports described below that are sent on the first day of each month.

- **Failure notifications**, **Warning notifications**, and **Success notifications** (disabled by default)

  The notifications about the execution results of backup plans and the results of disaster recovery operations for each device.

- **Daily recap about active alerts** (enabled by default)

  The recap that informs about failed backups, missed backups, and other problems. The recap is sent at 10:00 (data center time). If there are no problems by this moment, the recap is not sent.

All notifications are sent to the user's email address.

20.3 Usage reports

The report about using the backup service includes the following data about a company or a unit:

- Size of backups by unit, by user, by device type.
- Number of protected devices by unit, by user, by device type.
- Price value by unit, by user, by device type.
- The total size of backups.
- The total amount of protected devices.
- Total price value.

21 Troubleshooting

This section describes how to save an agent log to a .zip file. If a backup fails for an unclear reason, this file will help the technical support personnel to identify the problem.

To collect logs

1. Select the machine that you want to collect the logs from.
2. Click **Activities**.
3. Click **Collect system information**.
4. If prompted by your web browser, specify where to save the file.

22 Glossary

B

Backup set

A group of backups to which an individual retention rule can be applied.

For the **Custom** backup scheme, the backup sets correspond to the backup methods (**Full**, **Differential**, and **Incremental**).

In all other cases, the backup sets are **Monthly**, **Daily**, **Weekly**, and **Hourly**.

- A monthly backup is the first backup created after a month starts.
- A weekly backup is the first backup created on the day of the week selected in the **Weekly backup** option (click the gear icon, then **Backup options** > **Weekly backup**).

  If a weekly backup is the first backup created after a month starts, this backup is considered monthly. In this case, a weekly backup will be created on the selected day of the next week.
- A daily backup is the first backup created after a day starts, unless this backup falls within the definition of a monthly or weekly backup.
- An hourly backup is the first backup created after an hour starts, unless this backup falls within the definition of a monthly, weekly, or daily backup.

D

Differential backup

A differential backup stores changes to the data against the latest full backup (p. 181). You need access to the corresponding full backup to recover the data from a differential backup.

F

Full backup

A self-sufficient backup containing all data chosen for backup. You do not need access to any other backup to recover the data from a full backup.

I

Incremental backup

A backup that stores changes to the data against the latest backup. You need access to other backups to recover data from an incremental backup.

S

Single-file backup format

A new backup format, in which the initial full and subsequent incremental backups are saved to a single .tib or .tibx file, instead of a chain of files. This format leverages the speed of the incremental backup method, while avoiding its main disadvantage–difficult deletion of outdated backups. The software marks the blocks used by outdated backups as "free" and writes new backups to these blocks. This results in extremely fast cleanup, with minimal resource consumption.

The single-file backup format is not available when backing up to locations that do not support random-access reads and writes.