Acronis

Acronis Backup Cloud
Version 7

Table of contents

1 Administrator's Guide

1.1 About this document

This document is intended for partners who want to provide backup as a service to their clients, as well as for client company administrators who want to use the backup service.

This document describes how to quickly set up the backup service and perform backup and recovery.

1.2 About the backup service

The backup service is provided at the partner level, down to the client company level and the end-user level.

The backup service management is available through a web interface.

1.2.1 Accounts and groups

There are two account types: **administrator accounts** and **user accounts**. Both the user and the administrators can manage backups of the user's data.

Each account belongs to a group. The group hierarchy is supposed to match the client/vendor relationships between the backup service users and providers.

A group type of **Customer** typically corresponds to organizations that use the backup service. A group type of **Unit** typically corresponds to units or departments within the organization.

An administrator can create and manage groups, administrator accounts, and user accounts on or below their level in the hierarchy.

Administrators at the customer level and higher can limit access to their groups for higher-level administrators. This is done by disabling the **Inherit administrator accounts from parent group** setting on the **Administrators** tab of the root group. When the inheritance is disabled, the parent group administrators can only modify the group properties. They do not see the accounts and child groups at all.

The following diagram illustrates three hierarchy levels—the partner, customer, and unit groups. At least one account (either an administrator or a user) must exist within a unit. If a customer group does not have units, at least one account must exist within the customer group.
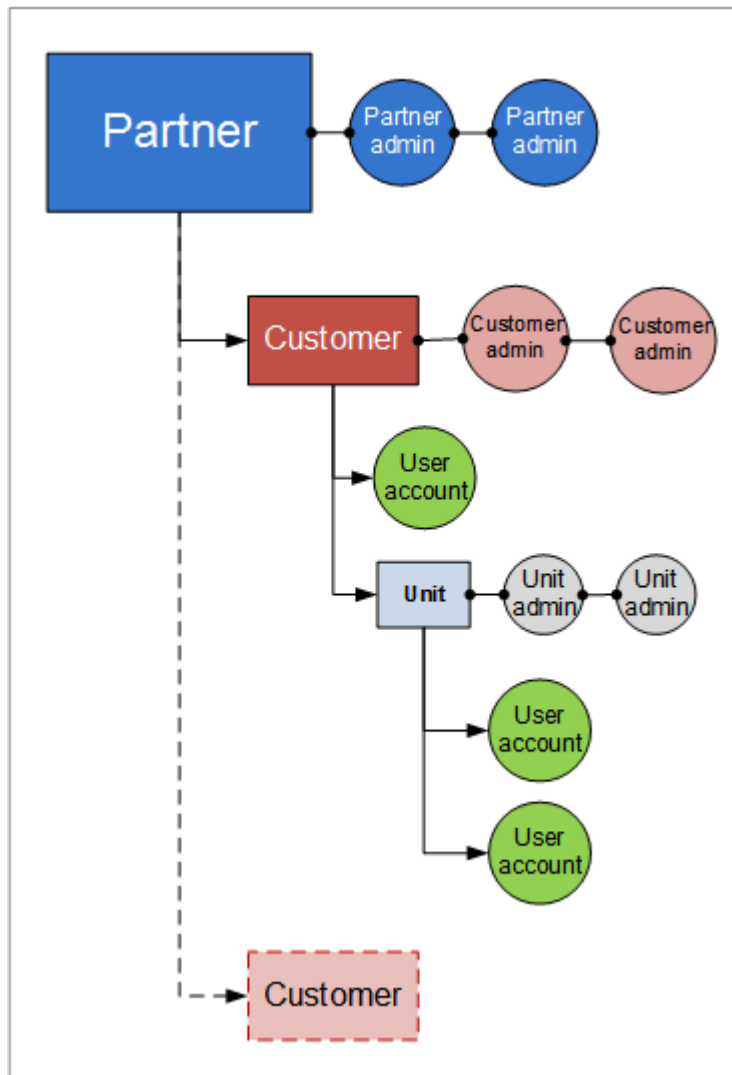
The following table summarizes operations that can be performed by the administrators and users.

Operation	Users	Customer and unit administrators	Partner administrators
Create groups	No	Yes	Yes
Create accounts	No	Yes	Yes
Download and install the backup software	Yes	Yes	No*
Manage backup	Yes	Yes	Yes
Manage recovery	Yes	Yes	Yes
Create reports about the service usage	No	Yes	Yes

*A partner administrator who needs to perform this operation can create a customer administrator or user account for themselves.

1.2.2   Components

This section describes the software components utilized by the backup service.

On the end-user side

At least one of the following components must be installed on the end-user side:

- **Agent for Windows** backs up disks, volumes, and files on a machine running Windows.
- **Agent for VMware** backs up ESXi virtual machines without installing agents into the guest systems. The agent is installed on a Windows machine that has network access to vCenter Server and to the storage where the backed-up virtual machines are stored.
- **Agent for Hyper-V** backs up Hyper-V virtual machines without installing agents into the guest systems. The agent is installed on a Hyper-V host.
- **Agent for Virtuozzo** backs up Virtuozzo virtual machines and containers without installing agents into the guest systems. The agent is installed on a Virtuozzo host.
- **Agent for Exchange** backs up Microsoft Exchange Server databases.
- **Agent for SQL** backs up Microsoft SQL Server databases.
- **Agent for Linux** backs up disks, volumes, and files on a machine running Linux.
- **Agent for Mac** backs up disks, volumes, and files on a machine running OS X.
- **Agent for Active Directory** backs up and ensures proper recovery of a domain controller.
- **Agent for Office 365** backs up Microsoft Office 365 mailboxes.

The agents can be installed by users or by administrators.

On the data-center side

The servers are located in Acronis data centers.

- **Account server** stores the user account hierarchy and enables administering the backup service from the **account management console.** Only administrators can access this console.
- **Backup management server** manages the agents. It enables users and administrators to set up and monitor backups from the **backup console.** Users, unit administrators, and customer administrators log in directly to this console. Partner administrators access it from the account management console.

The backup storages are located in Acronis data centers. Service providers can organize backup storages in their own data centers, by using the Acronis Storage or Acronis Storage Gateway software. End users have the option to store backups either in a data center or within their local networks.

The following diagram illustrates the default backup service architecture. Blue arrows (→) show the software component interactions. Black arrows (→) show how administrators and end users access the backup service.
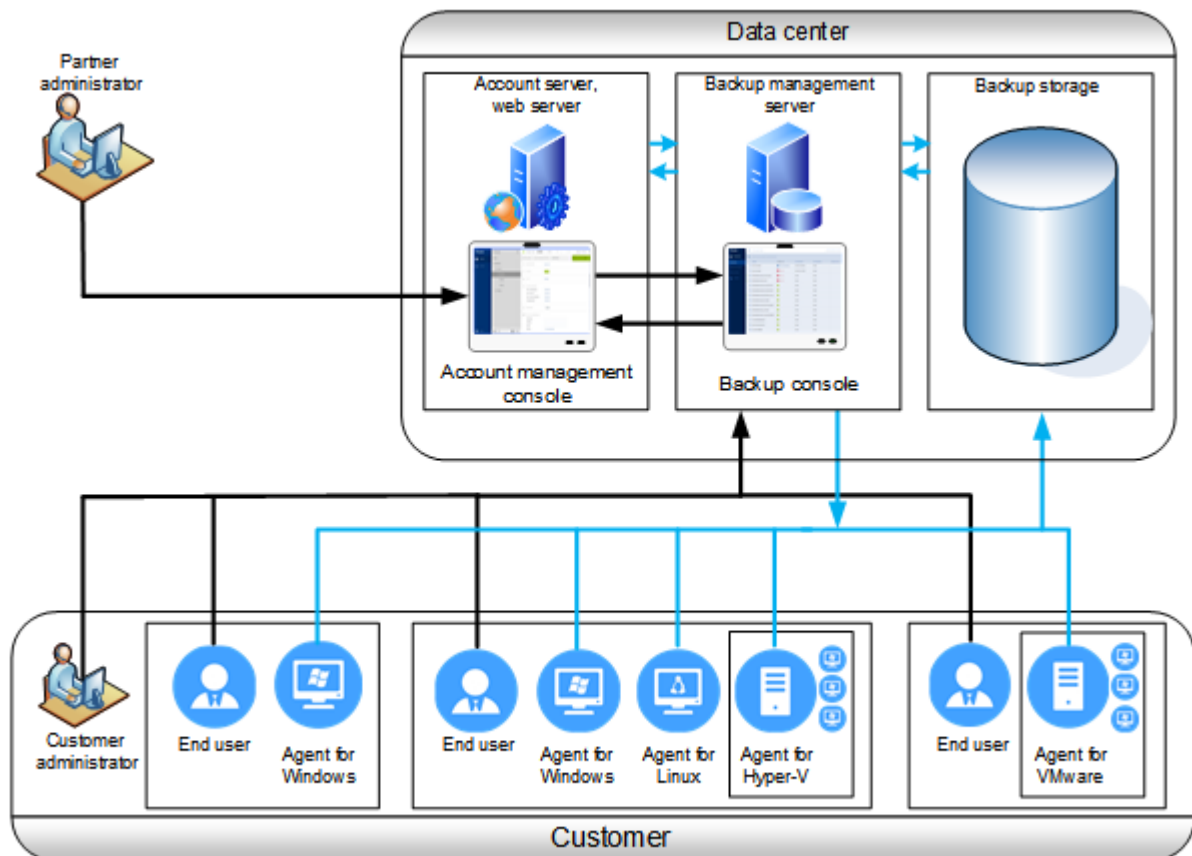
1.2.3　Supported web browsers

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 OS X 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.

1.3　Step-by-step instructions

The following steps will guide you through the installation and basic use of the backup service. They describe how to:

- Activate your administrator account
- Create a group

- Create an account
- Access the backup service
- Create a report about the service usage

For information about how to back up and recover data, refer to the User's Guide (p. 16).

1.3.1   Activating an administrator account

After signing the partnership agreement or signing up for the backup service, you will receive an email message containing the following information:

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

1.3.2   Accessing the backup service

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 password of the account.
3. Click **Log in**.

Unit administrators and customer administrators log in directly to the backup console. To access the account management console, they must click **Manage accounts**.

Partner administrators log in to the account management console. To access the backup console, they must select a customer or unit in the **Groups** list, and then click **Manage backups**.

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

For information about how to back up and recover data, refer to the User's Guide (p. 16).

1.3.3   Creating a group

A **Partner** group is normally created for each partner that signs the partnership agreement.

A **Customer** group is normally created for each organization that signs up for the backup service.

You may want to create a new **Unit** group within a customer group when expanding the backup service to a new organizational unit.

To create a group

1. Log in to the account management console.
2. Select a group in which you want to create the new group.
3. On the bottom of the **Groups** pane, click "**+**".
4. In **Name**, specify a name for the new group.
5. [Optional] In **Identifier**, type a string that will act as the identifier for the group. This identifier will appear in monthly reports, together with the group's usage data. You can use this identifier to refer to this group in other software, such as in your billing or monitoring systems.

The identifier can consist of up to 256 Unicode characters (for example, numbers and Latin letters). It does not need to be unique across groups.

6. In **Type**, select the type of the new group. The available types depend on the parent group type.

7. [Only when creating a customer group] In **Mode**, select whether the group is using the backup service in the trial mode or in the production mode. Monthly service usage reports do not include usage data for trial-mode groups.

   Important If you switch the mode from trial to production in the middle of a month, the entire month will be included in the monthly service usage report. For this reason, we recommend that you switch the mode on the 1st day of a month. The mode is automatically switched to production when a group remains in the backup service for one full month.

8. In **Default language**, select the default language of notifications, reports, and backup software that will be used within this group.

9. [Only when creating a customer group] In **Storage**, choose the data center where the backups will be kept.

   Detailed information about the data centers is available on the **Storage** tab, when the customer's parent group is selected in the **Groups** list. Click **Add** on the **Storage** tab to find information about organizing a backup storage in your own data center.

10. [Optional, only when creating a customer group] In **Pricing parameters**, select the currency that will be used for billing and **Backup price** of backup service per gigabyte per month.

11. [Optional, not applicable to a unit group] Specify the storage quota and the maximum number of machines/devices/mailboxes the group is allowed to protect. A machine/mailbox/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.

    - **Physical workstations**
    - **Physical servers**
    - **Virtual machines**
    - **Mobile devices**
    - **Office 365 mailboxes**
    - **Websites**
    - **Storage quota**

    These quotas are "soft". If any of these values are exceeded, an email notification is sent to the group administrators and the administrators of the parent group. Restrictions on using the backup service are not applied.

12. [Optional, only when creating a customer group] Specify the quota overages. An overage allows a customer group to exceed the quota by the specified value. When the overage is exceeded, backups fail.

    Important If you set both a quota and its overage to zero, the corresponding functionality will be hidden from the members of this group and its child groups.

13. [Optional] In **Backup locations**, select the backup locations for this group and its child groups. The following options are available:

    - **Local and cloud**
    - **Cloud only**

14. [Optional] Disable the **Agent auto update** switch. If you do this, the agents that are registered under the accounts within this group and its child groups will not be updated automatically when a new version is released.

15. [Optional] In **Contact information**, specify the contact information for the group.
16. Click **Create**.

The newly created group appears in the **Groups** tree.

If you want to specify the billing information for a group, select the group in the **Groups** list, click **Properties**, and then complete the billing information section.

1.3.4 Creating a partner account

Within a partner group, only administrator accounts can be created.

To create a partner account

1. Log in to the account management console.
2. Select a group in which you want to create the account.
3. Click the **Administrators** tab.
4. Click **Add account**.
5. Specify the following contact information for the account.
   - **Login**

     Important Each account must have a unique login. You can create multiple logins using the same email address.

   - **Email address**
   - [Optional] **First name**
   - [Optional] **Last name**
6. [Optional] Change the **Backup notifications** level. You can choose one of the following levels:
   - **Off**: No notifications (default)
   - **Less**: Notifications about backup failures
   - **More**: Notifications about backup failures and warnings
   - **All**: Notifications about backup failures, warnings, and successful backups

   All notifications are sent to the specified email address.
7. [Optional] Clear the **Send daily recap about active alerts** check box.

   The recap is sent at 10:00 (data center time). The recap informs about missed backups and other problems, in addition to failed backups.
8. [Optional] Disable **Business notifications**. If you do this, notifications about exceeded quotas will not be sent to the specified email address.
9. Click **Add**.

As a result:

- A new account appears in the **Administrators** tab.
- An email message containing the activation link is sent to the email address you specified.

1.3.5 Creating a customer account

At least one account (either an administrator or a user) must exist within a unit. If a customer group does not have units, at least one account must exist within the customer group.

To create an account within a unit or a customer group

1. Log in to the account management console.

2. Select a group in which you want to create the account.

3. Click the **Accounts** tab.

4. Click **Add account**.

5. Specify the following contact information for the account.

    - **Login**

      Important Each account must have a unique login. You can create multiple logins using the same email address.

    - **Email address**

    - [Optional] **First name**

    - [Optional] **Last name**

6. If you want this account to be an administrator account, enable the **Administrator privileges** switch.

7. [Optional] Disable the **Agent auto update** switch. If you do this, the agents that are registered under this account will not be updated automatically when a new version is released.

8. [Optional] Specify the storage quota and the maximum number of machines/devices/mailboxes the user is allowed to protect. A machine/mailbox/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.

    - **Physical workstations**

    - **Physical servers**

    - **Virtual machines**

    - **Mobile devices**

    - **Office 365 mailboxes**

    - **Websites**

    - **Storage quota**

    These quotas are "soft". If any of these values are exceeded, a notification will be sent to the email address specified in step 5. Restrictions on using the backup service are not applied.

9. [Optional] Specify the quota overages. An overage allows the user to exceed the quota by the specified value. When the overage is exceeded, backups fail.

    Important If you set both a quota and its overage to zero, the corresponding functionality will be hidden from the user.

10. [Optional] In **Backup locations**, select the backup locations for this account. The following options are available:

    - **Local and cloud**

    - **Cloud only**

11. [Optional] Change the **Backup notifications** level. You can choose one of the following levels:

    - **Off**: No notifications (default)

    - **Less**: Notifications about backup failures

    - **More**: Notifications about backup failures and warnings

    - **All**: Notifications about backup failures, warnings, and successful backups

    All notifications are sent to the specified email address.

12. [Optional] Clear the **Send daily recap about active alerts** check box.

    The recap is sent at 10:00 (data center time). The recap informs about missed backups and other problems, in addition to failed backups.

13. [Optional] Disable **Business notifications**. If you do this, notifications about exceeded quotas will not be sent to the specified email address.

14. Click **Add**.

As a result:

- A new account appears in the **Accounts** tab.
- An email message containing the activation link is sent to the email address you specified.

1.3.6 Creating a report about the service usage

Usage reports provide historical data about using the backup service. This data can be used to charge the customers.

Only administrators can create these reports.

Reporting parameters

The report includes the following data about a customer, units, and accounts:

- Size of backups by group, by account, by machine type.
- Amount of protected machines by group, by account, by machine type.
- Price value by group, by account, by machine type.
- The total size of backups.
- The total amount of protected machines.
- Total price value.

Report scope

You can select the scope of the report from the following values:

- **Direct customers and partners**

  The report will include the values of the reporting parameters only for the immediate child groups of your group.

- **All customers and partners**

  The report will include the values of the reporting parameters for all child groups of your group.

- **All customers and partners (including account details)**

  The report will include the values of the reporting parameters for all child groups of your group and for all user accounts within the groups.

Enabling or disabling scheduled usage reports

A scheduled report covers system usage data for the last full calendar month. The reports are generated at 23:59:59 by UTC time on the first day of a month and sent on the second day of that month to all administrators of your group.

1. In the account management console, click **Reports**.
2. Select the **Scheduled** tab.
3. Enable or disable the scheduled usage reports by clicking the on/off switch.
4. In **Level of detail**, select the report scope as described above.

Generating a custom usage report

This type of report can be generated on demand and cannot be scheduled. The report will be sent to your email address.

1. In the account management console, click **Reports**.
2. Select the **Custom** tab.
3. In **Period**, select the reporting period:
    -   **Current calendar month**
    -   **Previous calendar month**
    -   **Custom**
4. If you want to specify a custom reporting period, select the start and the end dates. Otherwise, skip this step.
5. In **Type**, select the report type:
    -   **Summary report**: The report will include the total values of the reporting parameters for the specified period, including the total price value.
    -   **Daily statistics**: The report will include the values of the reporting parameters for each day of the specified period, excluding the price values.
6. In **Level of detail**, select the report scope as described above.
7. To generate the report, click **Generate and send**.

1.4   Advanced scenarios

1.4.1   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: 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. Copy the setup program to the folder you created.
4. Start the setup program.
5. Click **Create .mst and .msi files for unattended installation**.
6. If prompted, specify the credentials of the account to which the machines should be assigned.
7. Review or modify the installation settings that will be added to the .mst file.
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. You can now move or delete the setup program .exe file.

Step 2: 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 and Windows Server 2012).

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 and Windows Server 2012:

   ▪ 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 and Windows Server 2012, 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:

   ▪ 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.

1.4.2   Limiting access to the web interface

You can limit access to the web interface by specifying a list of IP addresses from which the members of a group are allowed to log in.

This restriction is *not* applied to the members of the child groups.

To limit access to the web interface

1. Log in to the account management console.

2. Select a group for which you want to limit the access.

3. Click **Settings** > **Security**.

4. Select the **Enable logon control** check box.

5. In **Allowed IP addresses**, specify the allowed IP addresses.

   You can enter any of the following parameters, separated by a semicolon:

   - IP addresses, for example 192.0.2.0
   - IP ranges, for example 192.0.2.0-192.0.2.255
   - Subnets, for example 192.0.2.0/24

6. Click **Save**.

2 User's Guide

2.1 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.

2.2 Software requirements

2.2.1 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 OS X 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.

2.2.2 Supported operating systems and environments

Agent for Windows

Windows XP Professional SP3 (x86, x64)

Windows Server 2003/2003 R2 – 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

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 4.9 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

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

Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24

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

CentOS 5.x, 6.x, 7, 7.1, 7.2, 7.3

Oracle Linux 5.x, 6.x, 7.0, 7.1, 7.2, 7.3 – both Unbreakable Enterprise Kernel and Red Hat Compatible Kernel

CloudLinux 5.x, 6.x, 7, 7.1

ClearOS 5.x, 6.x, 7, 7.1

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 – Apple File System (APFS) is not supported

Agent for VMware

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, and 6.0

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

2.2.3   Supported Microsoft SQL Server versions

- 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

2.2.4   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.

2.2.5   Supported Microsoft SharePoint versions

Acronis Backup Cloud 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.

2.2.6 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 **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	+	+
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		Only fully virtualized (aka HVM) guests
Red Hat and Linux		

Platform	Backup at a hypervisor level (agentless backup)	Backup from inside a guest OS
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		+
Kernel-based Virtual Machines (KVM)		+
Parallels		
Parallels Workstation		+
Parallels Server 4 Bare Metal		+
Oracle		
Oracle VM Server 3.0 and 3.3		+
Oracle VM VirtualBox 4.x		+
Virtuozzo		
Virtuozzo 6.0.10, 6.0.11	+	(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.

2.2.7   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

2.3 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	-	+	
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

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.

2.4 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 future. The login and password are the same as in the previous step.

2.5 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 password of the account.
3. Click **Log in**.

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

2.6 Installing the software

2.6.1 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 OS X	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.
Machines running Active Directory Domain Services	Agent for Active Directory	On the domain controller.

What are you going to back up?	Which agent to install?	Where to install it?
Virtual machines		
VMware ESXi virtual machines	Agent for VMware	On a Windows machine that has network access to vCenter Server and to the virtual machine storage.*
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		
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. 109).

**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.

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 the Administrator's Guide (p. 13).

Installation in Linux and OS X 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. 25) section to understand whether you need to configure these settings on each machine that runs a backup agent.

2.6.2 Proxy server settings

The backup agents can transfer data through an HTTP proxy server.

The agent installation requires an Internet connection. 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. In Linux and OS X, you must specify the proxy settings before the installation.

Use the procedures below to specify the proxy settings before the agent installation or to change them at a later time.

In Linux

1. Create the file **/etc/Acronis/Global.config** and open it in a text editor.
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>
    </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. Save the file.

5. If the backup agent is not installed yet, you can now install it. Otherwise, restart the agent by executing the following command in any directory:

```
sudo service acronis_mms restart
```

In OS X

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>
    </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. Save the file.

5. 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
```

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
```

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. Save the document as **proxy.reg**.

5. Run the file as an administrator.

6. Confirm that you want to edit the Windows registry.

7. 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
```

2.6.3 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 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.

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**	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**	The setup program will download and install the packages automatically.
	perl	Run the following command: ```yum install perl```

Ubuntu	**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```

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.

2.6.4   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. Click **Install**.
4. Specify the credentials of the account to which the machine should be assigned.
5. Click **Show proxy settings** if you want to verify or change the proxy server host name/IP address and port. Otherwise, skip this step. If a proxy server is enabled in Windows, it is detected and used automatically.
6. [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. We recommend using an account that has the **Administrator** role assigned. Otherwise, provide an account with the necessary privileges (p. 112) on the vCenter Server or ESXi.
7. [Only when installing on a domain controller] Specify the user account under which the agent service will run. For security reasons, the setup program does not automatically create new accounts on a domain controller.
8. Click **Start installation**.

You can change the installation path and the account for the agent service by clicking **Customize installation settings** on the first step of the installation wizard.

In Linux

1. Ensure that the machine is connected to the Internet.
2. As the root user, run the installation file.
3. Specify the credentials of the account to which the machine should be assigned.
4. 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.
5. Complete the installation procedure.

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

In OS X

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 prompted, provide administrator credentials.

6. Specify the credentials of the account to which the machine should be assigned.

7. Complete the installation procedure.

2.6.5   Updating agents

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

- Agent for Windows, Agent for VMware, 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**.

If automatic update is enabled by a backup service administrator, the agents are updated automatically as soon as a new version is released. If automatic update is disabled or fails for any reason, use the procedure described below.

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**.

   The update progress is shown in the status column for each machine.

2.6.6   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 OS X

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**.

2.7   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.
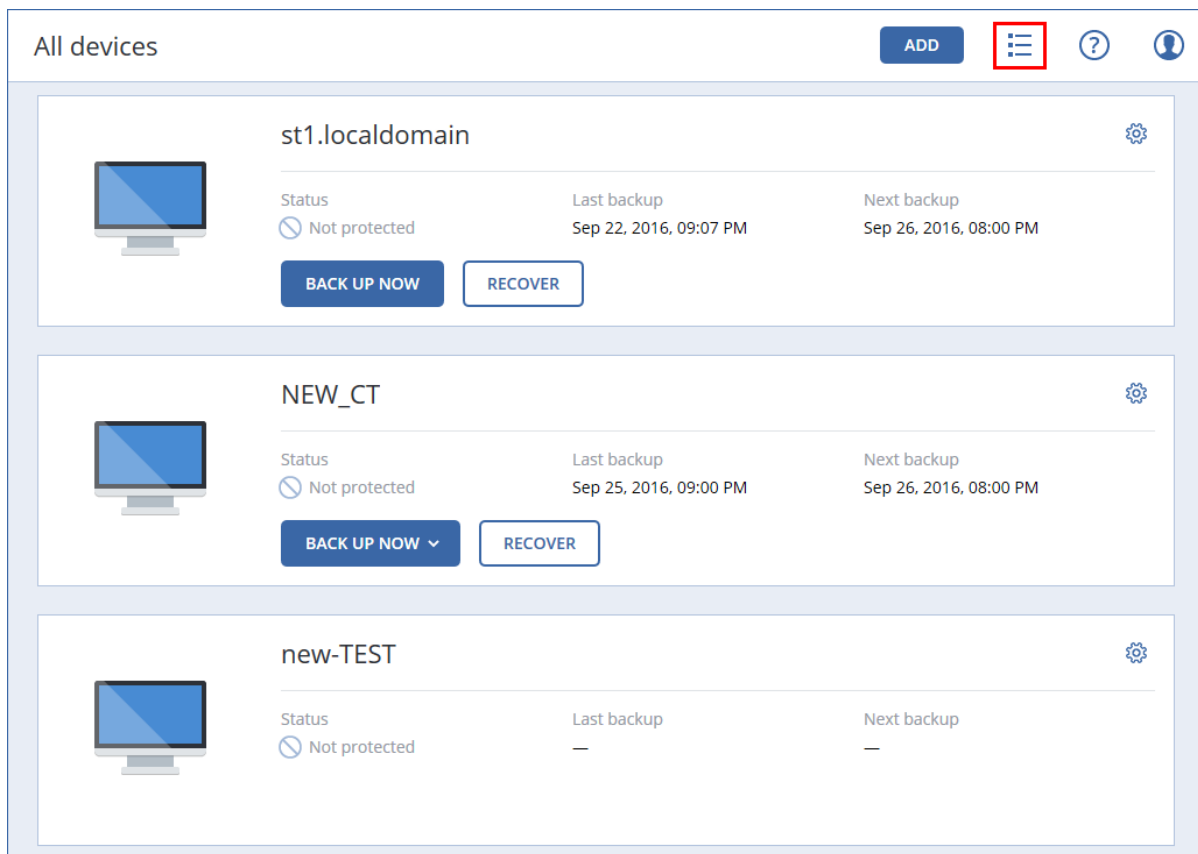
The table view is enabled automatically when the number of machines becomes large.
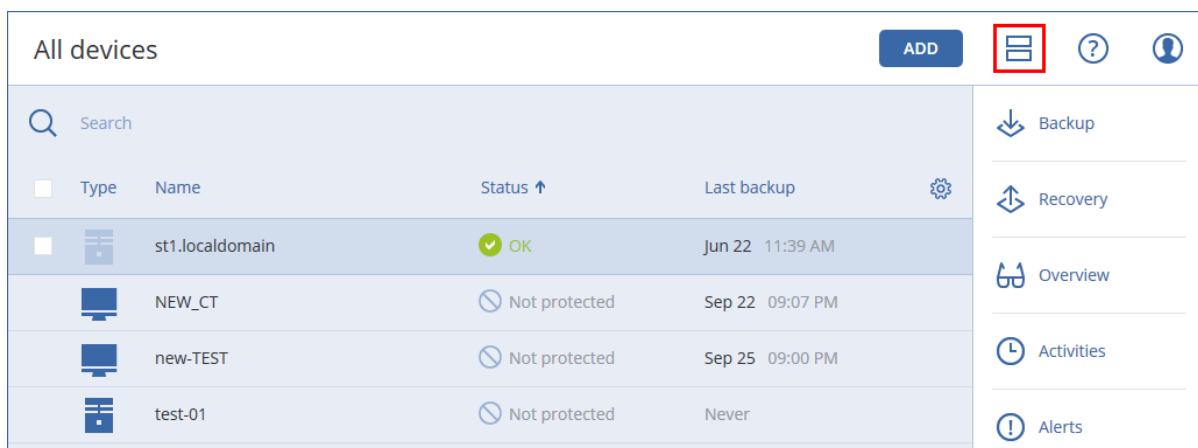
Both views provide access to the same features and operations. This document describes access to operations from the table view.

2.8 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.

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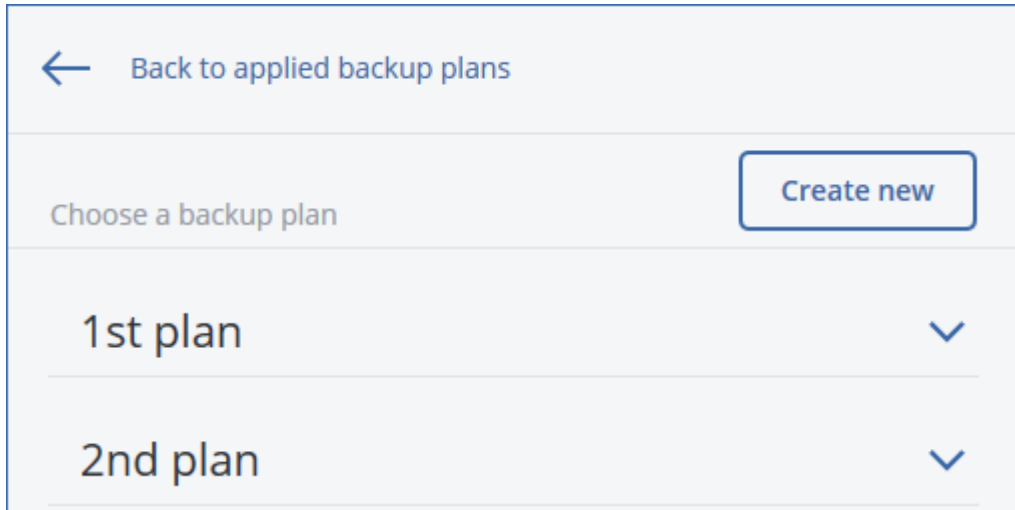
3. Select a backup plan to apply.
4. Click **Apply**.

2.8.1 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. 35) Policy rules (p. 35) File filters (p. 51)	Cloud (p. 40) Local folder (p. 40) Network folder (p. 40) NFS (p. 40)* Secure Zone (p. 40)**	Always incremental (Single-file) (p. 42) Always full (p. 42) Weekly full, daily incremental (p. 42) Custom (F-D-I) (p. 42)	By backup age (single rule/per backup set) (p. 43) By number of backups (p. 43) Keep indefinitely (p. 43)
Disks/volumes (virtual machines)	Policy rules (p. 35) File filters (p. 51)	Cloud (p. 40) Local folder (p. 40) Network folder (p. 40) NFS (p. 40)*		
Files (physical machines only)	Direct selection (p. 37) Policy rules (p. 37) File filters (p. 51)	Cloud (p. 40) Local folder (p. 40) Network folder (p. 40) NFS (p. 40)* Secure Zone (p. 40)**	Always full (p. 42) Weekly full, daily incremental (p. 42) Custom (F-D-I) (p. 42)	
ESXi configuration	Direct selection (p. 39)	Local folder (p. 40) Network folder (p. 40) NFS (p. 40)*		

Websites (files and MySQL databases)	Direct selection (p. 99)	Cloud (p. 40)	—	
System state	Direct selection (p. 39)	Cloud (p. 40) Local folder (p. 40) Network folder (p. 40)	Always full (p. 42) Weekly full, daily incremental (p. 42) Custom (F-I) (p. 42)	
SQL databases	Direct selection (p. 88)			
Exchange databases	Direct selection (p. 88)			
Office 365 mailboxes	Direct selection (p. 98)		Always incremental (Single-file) (p. 42)	By number of backups (p. 43) Keep indefinitely (p. 43)

* Backup to NFS shares is not available in Windows.

** Secure Zone cannot be created on a Mac.

2.8.2   Selecting data to back up

2.8.2.1   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. 51).

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 OS X

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

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 OS X

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

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. 59) 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. 60) 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.

2.8.2.2   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. 51).

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.

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 OS X

- 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**.

2.8.2.3   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

2.8.2.4   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.

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.

2.8.3   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.

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

  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. 40).

2.8.3.1   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. 115). 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.

2.8.4   Schedule

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.

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. 115).

  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.

Additional scheduling options

With any destination, you can 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. 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.

2.8.5   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. 115) 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**

Note A backup stored in a local or network folder cannot be deleted if it has dependent backups that are not subject to deletion. Such backup chains are deleted only when the lifetime of all their backups expires. This requires extra space for storing backups whose deletion is postponed. Also, the backup age and number of backups may exceed the values you specify.

2.8.6   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. 43).

2.8.7   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.

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.

After the settings are saved, they cannot be modified, but you can reset them as described below.

This option is available for machines running Windows or Linux. It is not supported for OS X.

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 kind of load balancing among them.

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>`

The backups will be encrypted using the AES algorithm with a 256-bit key.

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**

Important After you reset the encryption settings on a machine, the backups of this machine will fail. To continue backing up the machine, create a new backup plan.

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.

2.8.8   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.

2.8.9 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, OS X).
- 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	OS X	Windows	Linux	OS X	ESXi	Hyper-V	Virtuozzo	Windows
Alerts (p. 48)	+	+	+	+	+	+	+	+	+	+
Backup consolidation (p. 48)	+	+	+	+	+	+	+	+	+	-
Backup validation (p. 49)	+	+	+	+	+	+	+	+	+	+
Changed block tracking (CBT) (p. 49)	+	-	-	-	-	-	+	+	-	-
Compression level (p. 49)	+	+	+	+	+	+	+	+	+	+
Error handling (p. 50)										
Re-attempt, if an error occurs	+	+	+	+	+	+	+	+	+	+
Do not show messages and dialogs while processing (silent mode)	+	+	+	+	+	+	+	+	+	+
Ignore bad sectors	+	+	+	+	+	+	+	+	+	-

	Disk-level backup			File-level backup			Virtual machines			SQL and Exchange
	Windows	Linux	OS X	Windows	Linux	OS X	ESXi	Hyper-V	Virtuozzo	Windows
Re-attempt, if an error occurs during VM snapshot creation	-	-	-	-	-	-	+	+	+	-
Fast incremental/differential backup (p. 50)	+	+	+	-	-	-	-	-	-	-
File-level backup snapshot (p. 52)	-	-	-	+	+	+	-	-	-	-
File-level security (p. 52)	-	-	-	+	-	-	-	-	-	-
File filters (p. 51)	+	+	+	+	+	+	+	+	+	-
Log truncation (p. 53)	-	-	-	-	-	-	+	+	-	SQL only
LVM snapshotting (p. 53)	-	+	-	-	-	-	-	-	-	-
Mount points (p. 53)	-	-	-	+	-	-	-	-	-	-
Multi-volume snapshot (p. 54)	+	-	-	+	-	-	-	-	-	-
Performance (p. 54)	+	+	+	+	+	+	+	+	+	+
Pre/Post commands (p. 55)	+	+	+	+	+	+	+	+	+	+
Pre/Post data capture commands (p. 57)	+	+	+	+	+	+	-	-	-	+
Scheduling (p. 58)										
Distribute start times within a time window	+	+	+	+	+	+	+	+	+	+

	Disk-level backup			File-level backup			Virtual machines			SQL and Exchange
	Windows	Linux	OS X	Windows	Linux	OS X	ESXi	Hyper-V	Virtuozzo	Windows
Limit the number of simultaneously running backups	-	-	-	-	-	-	+	+	+	-
Sector-by-sector backup (p. 59)	+	+	-	-	-	-	+	+	+	-
Splitting (p. 59)	+	+	+	+	+	+	+	+	+	+
Task failure handling (p. 59)	+	+	+	+	+	+	+	+	+	+
Volume Shadow Copy Service (VSS) (p. 60)	+	-	-	+	-	-	-	+	-	+
Volume Shadow Copy Service (VSS) for virtual machines (p. 61)	-	-	-	-	-	-	+	+	-	-
Weekly backup (p. 61)	+	+	+	+	+	+	+	+	+	+
Windows event log (p. 61)	+	-	-	+	-	-	+	+	-	+

2.8.9.1   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.

2.8.9.2   Backup consolidation

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

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.

2.8.9.3   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. 101) in the ESXi or Hyper-V environment.

2.8.9.4   Changed block tracking (CBT)

This option is effective for disk-level backups of virtual machines and of physical machines running Windows.

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 content are continuously tracked at the block level. When a backup starts, the changes can be immediately saved to the backup.

2.8.9.5   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.

2.8.9.6 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.

Note If the cloud storage is selected as the primary or the second destination, the option value is automatically set to Enabled. Number of attempts: 300.

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.

2.8.9.7 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.

2.8.9.8 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 unless the backup destination is 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 OS X).

  Both in Windows and Linux/OS X, 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 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.

2.8.9.9   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: **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.

2.8.9.10   File-level security

This option is effective only for file-level backup in Windows.

This option defines whether to back up NTFS permissions for files along with the files.

The preset is: **Enabled.**

When this option is enabled, files and folders are backed up with the original permissions to read, write or execute the files for each user or user group. If you recover a secured file/folder on a machine without the user account specified in the permissions, you may not be able to read or modify this file.

If this option is disabled, the recovered files and folders will inherit the permissions from the folder to which they are recovered or from the disk, if recovered to the root.

Alternatively, you can disable recovery (p. 76) of the security settings. The result will be the same - the files will inherit the permissions from the parent folder.

2.8.9.11   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.

2.8.9.12   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.

2.8.9.13   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. 76) 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. 76).

The preset is: **Disabled**.

Copyright © Acronis International GmbH, 2002-2017

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. 76).

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.

2.8.9.14   Multi-volume snapshot

This option is effective only for Windows operating systems.

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. 52) 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: **Enabled**.

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.

2.8.9.15   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 OS X.
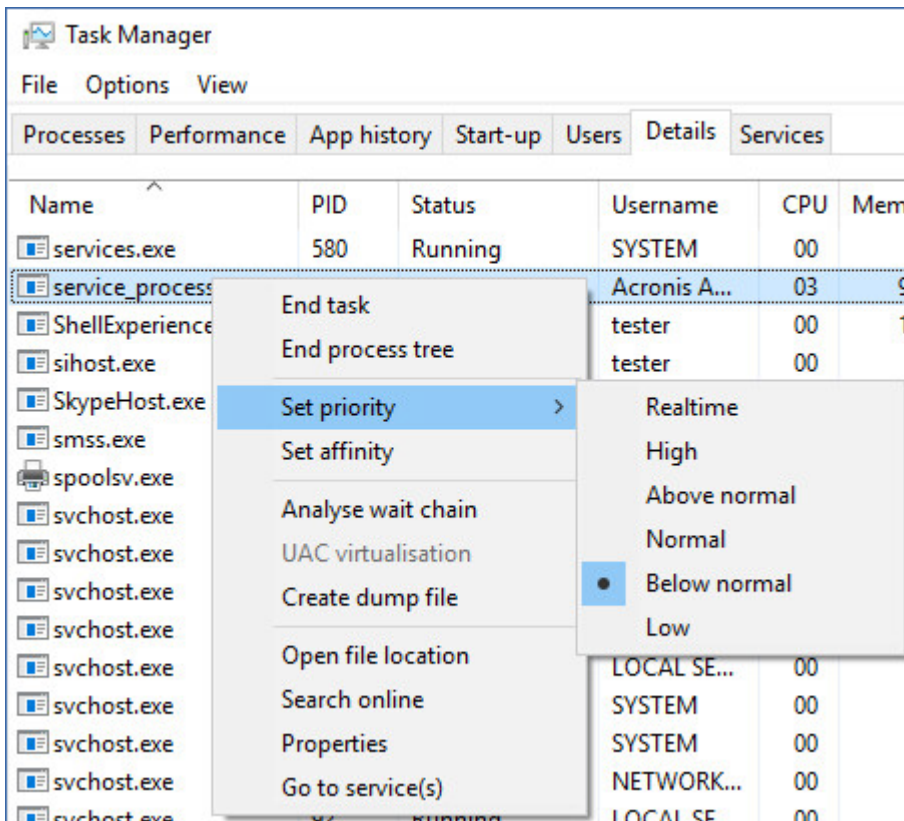
Output speed during backup

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.

2.8.9.16 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
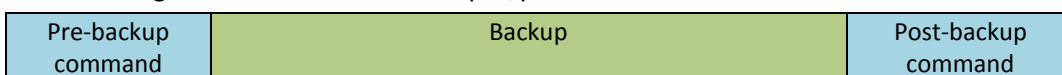
Examples of how you can use the pre/post commands:

- 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").

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.

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.
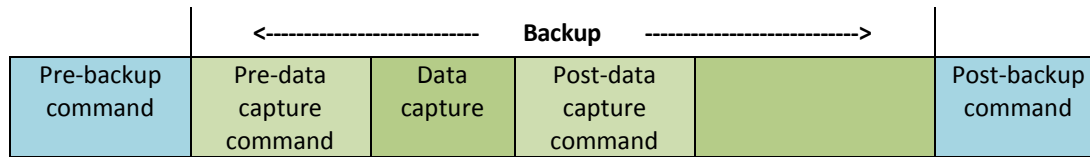6. Click **Done**.

2.8.9.17   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. 60) 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.

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.

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.

2.8.9.18   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.

Backups of physical machines will start exactly as scheduled.

2.8.9.19   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. 49) 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.

2.8.9.20   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.

2.8.9.21   Task failure handling

This option determines the program behavior when execution of a backup plan fails.

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**.

2.8.9.22   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. 57) 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. 53) backup option.

2.8.9.23 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. 50) 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.

2.8.9.24 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**.

2.8.9.25 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**.

2.9 Recovery

2.9.1 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. 63) Using bootable media (p. 67)
Physical machine (Mac)	Using bootable media (p. 67)
Virtual machine (VMware or Hyper-V)	Using the web interface (p. 65) Using bootable media (p. 67)
Virtual machine or container (Virtuozzo)	Using the web interface (p. 65)
ESXi configuration	Using bootable media (p. 73)
Files/Folders	Using the web interface (p. 70) Downloading files from the cloud storage (p. 71) Using bootable media (p. 71) Extracting files from local backups (p. 72)
System state	Using the web interface (p. 73)

SQL databases	Using the web interface (p. 90)
Exchange databases	Using the web interface (p. 92)
Exchange mailboxes	Using the web interface (p. 94)
Office 365 mailboxes	Using the web interface (p. 98)
Websites	Using the web interface (p. 101)

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.

2.9.2 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 OS X, create a separate media on a machine running OS X.

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. 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 OS X

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.

2.9.3   Recovering a machine

2.9.3.1   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:

- OS X
- 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. 79).
    - Recover the machine as described in "Recovering disks by using bootable media" (p. 67).
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. 67). The media enables you to choose disks for recovery and to map the disks manually.

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.

2.9.3.2   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.
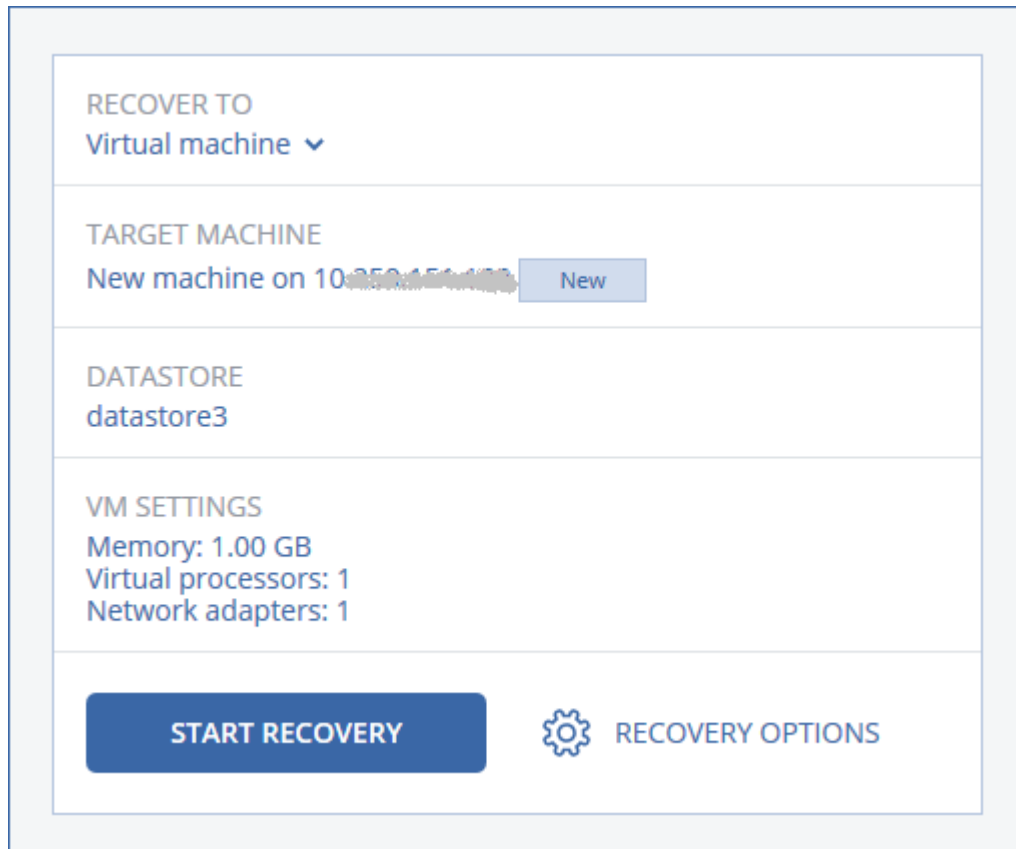
For more information about P2V migration, refer to "Machine migration" (p. 109).

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. 79).
    - Recover the machine as described in "Recovering disks by using bootable media" (p. 67).

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.~~350.454.4~~ [New]

DATASTORE
datastore3

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

[**START RECOVERY**]   ⚙ RECOVERY OPTIONS

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.

2.9.3.3   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**).
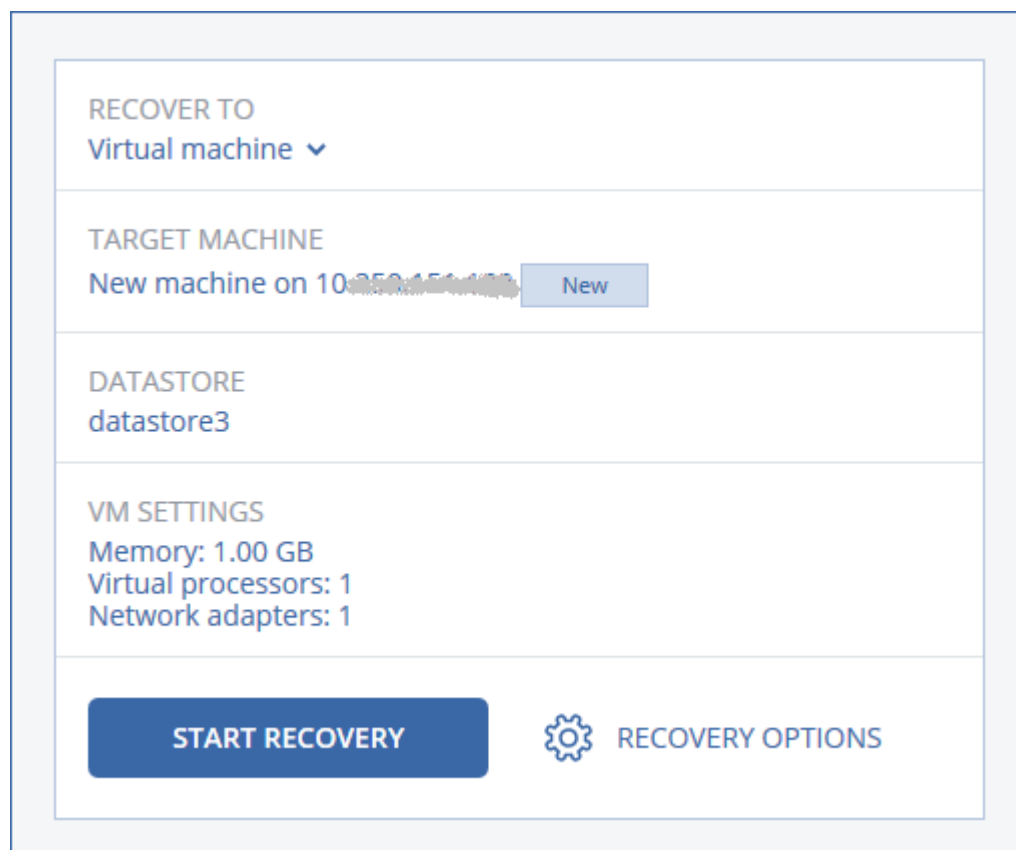
To recover a virtual machine

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. 79).

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. 63). Otherwise, we recommend that you perform the V2P migration by using bootable media (p. 67).

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. 109).

   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.

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.

2.9.3.4 Recovering disks by using bootable media

For information about how to create bootable media, refer to "Creating bootable media" (p. 62).

To recover disks by using bootable media

1. Boot the target machine by using 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 and port. Otherwise, skip this step.
4. On the welcome screen, click **Recover**.
5. Click **Select data**, and then click **Browse**.
6. 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.
   - 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.
7. Select the backup from which you want to recover the data. If prompted, type the password for the backup.
8. In **Backup contents**, select the disks that you want to recover. Click **OK** to confirm your selection.
9. 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.

10. [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.
11. [Optional] Click **Recovery options** to specify additional settings.
12. Click **OK** to start the recovery.

2.9.3.5 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. 68).

5. Click **OK**.

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.

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.

2.9.4   Recovering files

2.9.4.1   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. Select a recovery point on the Backups tab (p. 79) or use other ways to recover:
   - Download the files from the cloud storage (p. 71)
   - Use bootable media (p. 71)
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. 51).

   > ***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.
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.

2.9.4.2 Downloading files from the cloud storage

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

Limitation: Backups of system state, SQL databases, and Exchange databases cannot be browsed.

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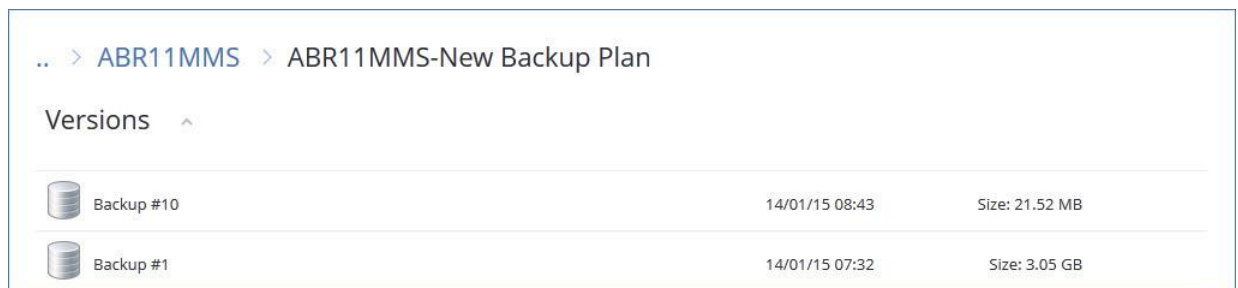
[When browsing file-level backups] You can select the backup date and time in the next step, under the gear icon located to the right of the selected file. By default, files are recovered from the latest backup.

5. Browse to the required folder or use search to obtain the list of the required files and folders.
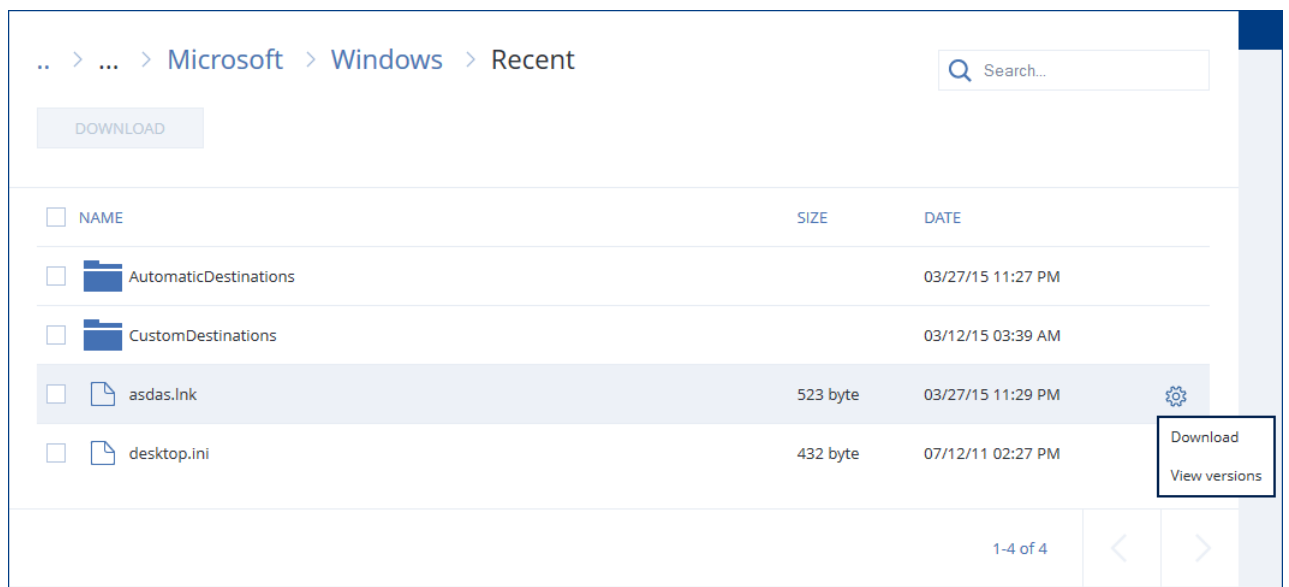
6. Select the check boxes for the items you need to recover, and then click **Download**.

    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**.

2.9.4.3 Recovering files by using bootable media

For information about how to create bootable media, refer to "Creating bootable media" (p. 62).

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 and port. Otherwise, skip this step.

4. On the welcome screen, click **Recover**.

5. Click **Select data**, and then click **Browse**.

6. 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.

    - 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.

7. Select the backup from which you want to recover the data. If prompted, type the password for the backup.

8. In **Backup contents**, select **Folders/files**.

9. Select the data that you want to recover. Click **OK** to confirm your selection.

10. Under **Where to recover**, specify a folder. Optionally, you can prohibit overwriting of newer versions of files or exclude some files from recovery.

11. [Optional] Click **Recovery options** to specify additional settings.

12. Click **OK** to start the recovery.

2.9.4.4   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, on a network share (SMB/CIFS), or in the Secure Zone.

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.

2.9.5   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.

2.9.6   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. 62).

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. If the backup is located in cloud storage that is accessed via a proxy server, click **Tools** > **Proxy server**, and then specify the proxy server host name/IP address and port. Otherwise, skip this step.

4. On the welcome screen, click **Recover**.

5. Click **Select data**, and then click **Browse**.

6. Specify the backup location:

    ▪ Browse to the folder under **Local folders** or **Network folders**.

    Click **OK** to confirm your selection.

7. In **Show**, select **ESXi configurations**.

8. Select the backup from which you want to recover the data. If prompted, type the password for the backup.

9. Click **OK**.

10. 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.

11. 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**.

12. [Optional] In **Network mapping**, change the result of automatic mapping of the virtual switches present in the backup to the physical network adapters.

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

2.9.7 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, OS X, 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	OS X	Bootable media	ESXi, Hyper-V, and Virtuozzo	Windows
Backup validation (p. 75)	+	+	+	+	+	+	+	+	+
Date and time for files (p. 75)	-	-	-	+	+	+	+	-	-
Error handling (p. 75)	+	+	+	+	+	+	+	+	+
File exclusions (p. 75)	-	-	-	+	+	+	+	-	-
File-level security (p. 76)	-	-	-	+	+	+	+	-	-
Flashback (p. 76)	-	-	-	-	-	-	-	+	-
Full path recovery (p. 76)	-	-	-	+	+	+	+	-	-
Mount points (p. 76)	-	-	-	+	-	-	-	-	-
Performance (p. 76)	+	+	-	+	+	+	-	+	+
Pre/post commands (p. 77)	+	+	-	+	+	+	-	+	+
SID changing (p. 78)	+	-	-	-	-	-	-	-	-
VM power management (p. 78)	-	-	-	-	-	-	-	+	-
Windows event log (p. 79)	+	-	-	+	-	-	-	Hyper-V only	+

2.9.7.1   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.

2.9.7.2   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**.

2.9.7.3   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.

2.9.7.4   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.

2.9.7.5   File-level security

This option is effective only for recovery from file-level backup of Windows files.

This option defines whether to recover NTFS permissions for files along with the files.

The preset is: **Enabled**.

If the file NTFS permissions were preserved during backup (p. 52), you can choose whether to recover the permissions or let the files inherit their NTFS permissions from the folder to which they are recovered.

2.9.7.6   Flashback

This option is effective when recovery to a virtual machine is performed by Agent for VMware, Agent for Hyper-V, or Agent for Virtuozzo.

The Flashback technology accelerates recovery of virtual machines. If the option is enabled, only the differences between backup and the target are recovered. Data is compared at the block level.

The preset is: **Enabled**.

2.9.7.7   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**.

2.9.7.8   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. 53) 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.

2.9.7.9   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.

2.9.7.10   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.

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.

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.*

2.9.7.11   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.

2.9.7.12   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.

2.9.7.13 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**.

2.10 Operations with backups

2.10.1 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 customer 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.

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.

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.

2.10.2 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.

2.10.3 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 recycle bin icon.
   - 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 recycle bin icon.
   - To delete the selected group, click **Delete**.
4. Confirm your decision.

2.11 Operations with backup plans

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.

2.12 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.
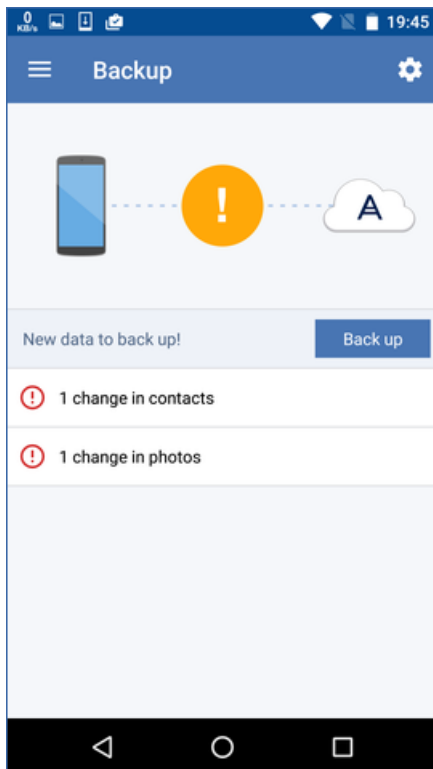
- The **Continuous backup** functionality is enabled by default. In this mode, the backup app checks for the data changes every six hours and runs a backup automatically if some data has changed. You can turn off continuous backup or change it to **Only when charging** in the app settings.
- You can 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.
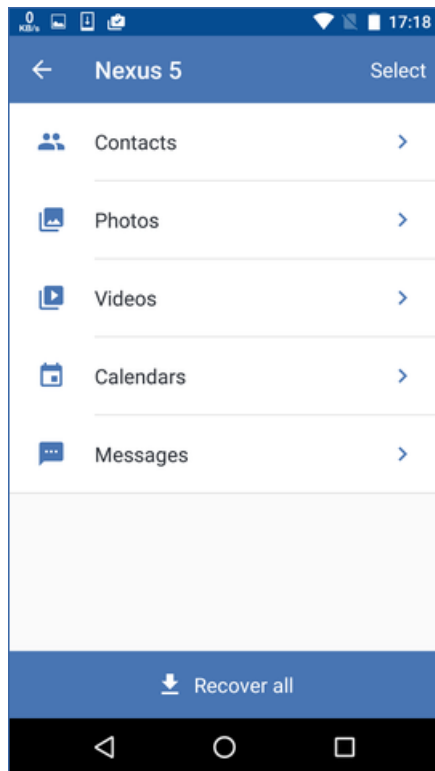

5. Do one of the following:
   - To recover a single data item, tap it.
   - To recover several data items, tap **Select**, and then tap the check boxes for the required data items.
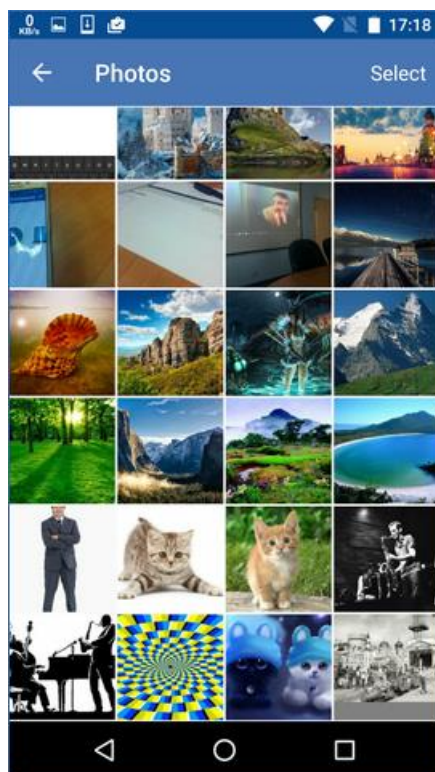
6. Tap **Recover**.

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**.
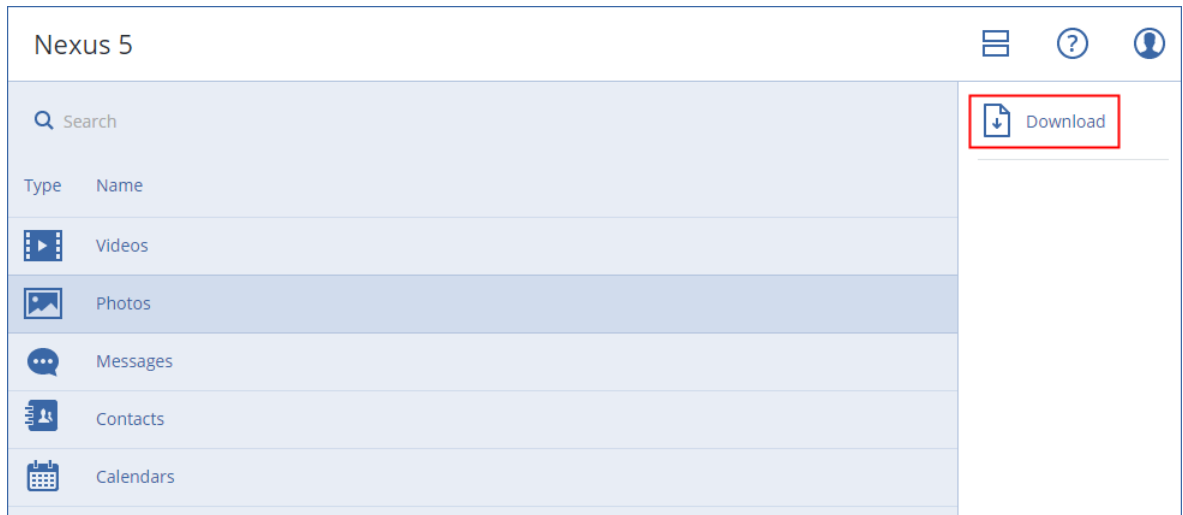
   - To download individual photos, videos, or contacts, click the respective data category name, and then select the check boxes for the required data items. Click **Download**.
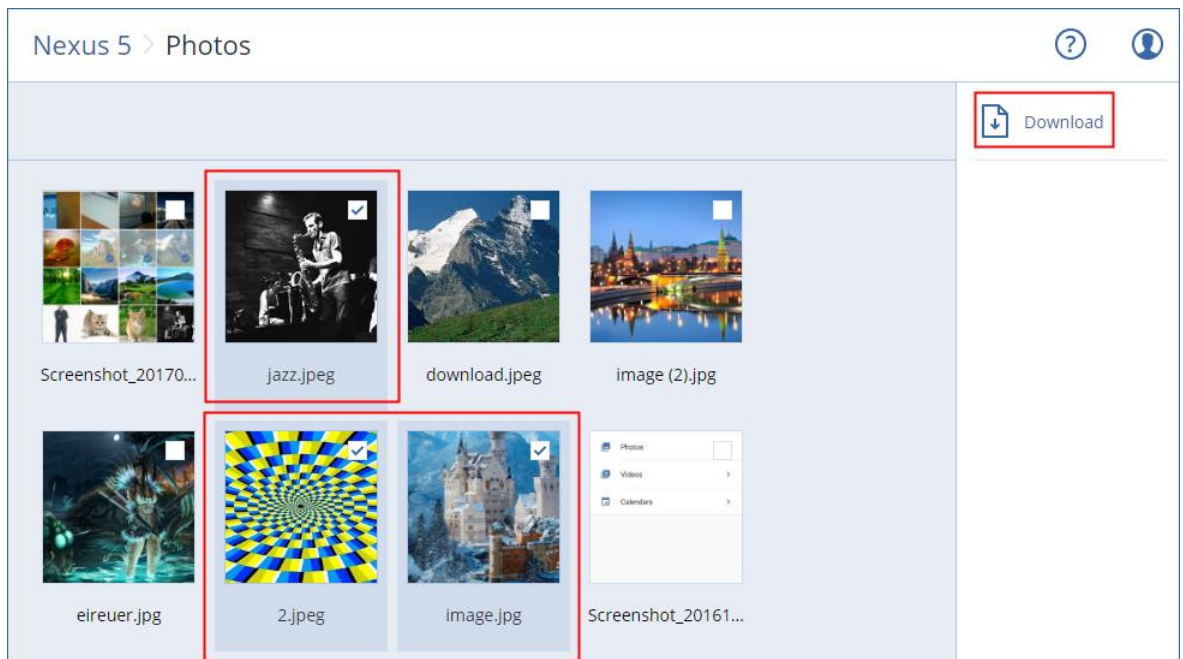
   - To preview a text message, a photo, or a contact, click the respective data category name, and then click the required data item.

For more information, refer to https://docs.acronis.com/mobile-backup. This help is also available in the backup app (tap **Settings** > **Help** on the app menu).

2.13 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. 90) Databases as files (p. 90)	Entire machine (p. 63) Databases to a live SQL Server instance (p. 90) Databases as files (p. 90)	Entire machine (p. 63)
Microsoft Exchange Server	Databases to a live Exchange (p. 92) Databases as files (p. 92) Granular recovery to a live Exchange (p. 94)	Entire machine (p. 63) Databases to a live Exchange (p. 92) Databases as files (p. 92) Granular recovery to a live Exchange (p. 94)	Entire machine (p. 63)

Microsoft SharePoint database servers	Databases to a live SQL Server instance (p. 90) Databases as files (p. 90) Granular recovery by using SharePoint Explorer	Entire machine (p. 63) Databases to a live SQL Server instance (p. 90) Databases as files (p. 90) Granular recovery by using SharePoint Explorer	Entire machine (p. 63)
Microsoft SharePoint front-end web servers	-	-	Entire machine (p. 63)
Active Directory Domain Services	-	Entire machine (p. 63)	-

2.13.1 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.
- SQL Server Browser Service and TCP/IP protocol are enabled. For instructions on how to start SQL Server Browser Service, refer to: http://msdn.microsoft.com/en-us/library/ms189093.aspx. You can enable the TCP/IP protocol by using a similar procedure.
- 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. 60) backup option is enabled.
- For virtual machines, the Volume Shadow Copy Service (VSS) for virtual machines (p. 61) 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://code.vmware.com/doc/preview?id=4076#https://vdc-repo.vmware.com/vmwb-repository/dcr-public/17aee92f-6920-4675-b03c-8c85de455bb3/5e2b0233-eea0-44c6-84aa-0d3a5aefe1a1/doc/vddkBkupVadp.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.

2.13.2   Database backup

Before backing up databases, ensure that the requirements listed in "Prerequisites" (p. 87) are met.

Select the databases as described below, and then specify other settings of the backup plan as appropriate (p. 34).

2.13.2.1   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. 53).

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.

2.13.2.2   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 **Organization 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**.

2.13.3 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.
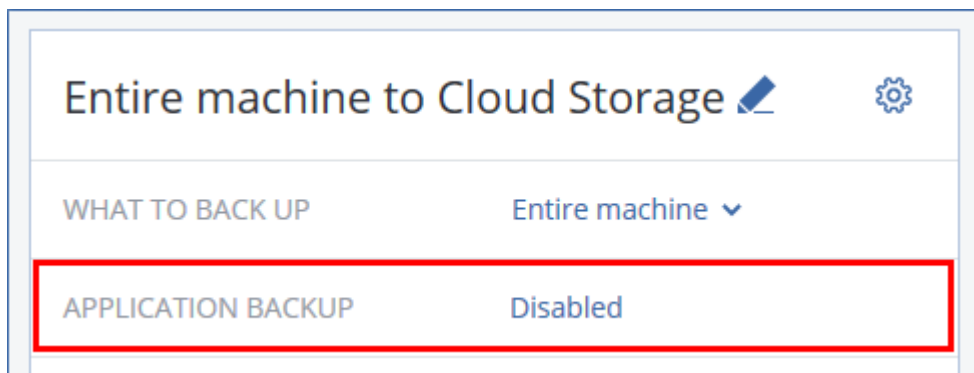
Why use application-aware backup?

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. 53). The Exchange transaction logs are truncated on virtual machines only. You can enable the VSS full backup option (p. 60) 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).

Other requirements are listed in the "Prerequisites" (p. 87) and "Required user rights" (p. 90) sections.

2.13.3.1   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.

2.13.4 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. 92).

If you use only Agent for VMware, recovering databases as files is the only available recovery method.

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. 92).

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. 79).

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 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.

2.13.4.1 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.

2.13.4.2 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**.

2.13.5 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 **Organization 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. 94).

If you use only Agent for VMware, recovering databases as files is the only available recovery method.

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. 79).

   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.

2.13.5.1   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 2016: http://technet.microsoft.com/en-us/library/aa998871.aspx
- Exchange 2013: http://technet.microsoft.com/en-us/library/aa998871(v=EXCHG.150).aspx
- Exchange 2010: http://technet.microsoft.com/en-us/library/aa998871(v=EXCHG.141).aspx
- Exchange 2007: http://technet.microsoft.com/en-us/library/aa998871(v=EXCHG.80).aspx

2.13.6   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.

2.13.6.1   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. 79).

    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.
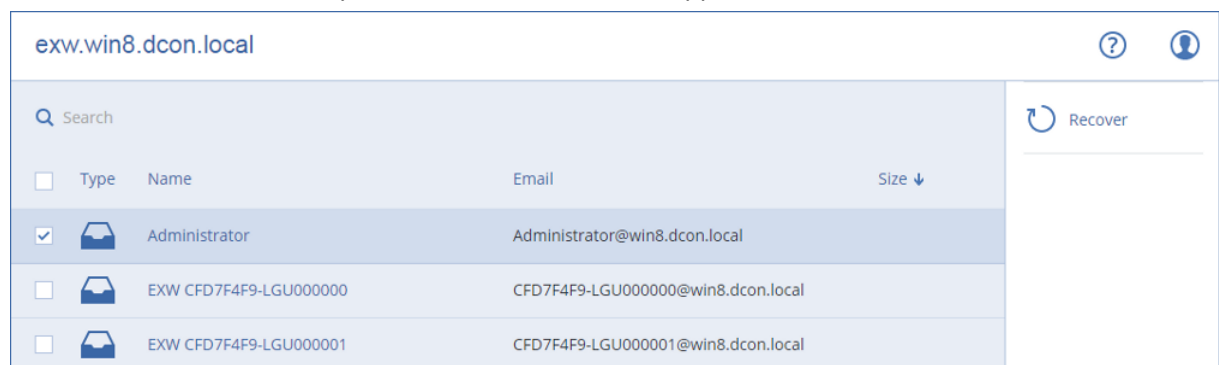
7. Click **Recover**.
8. Click **Target machine with Microsoft Exchange Server** to select or change the target machine.
    This step allows recovery to a machine that is not running Agent for Exchange.

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 is a member of the **Organization Management** role group.

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.

2.13.6.2   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. 79).

   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.
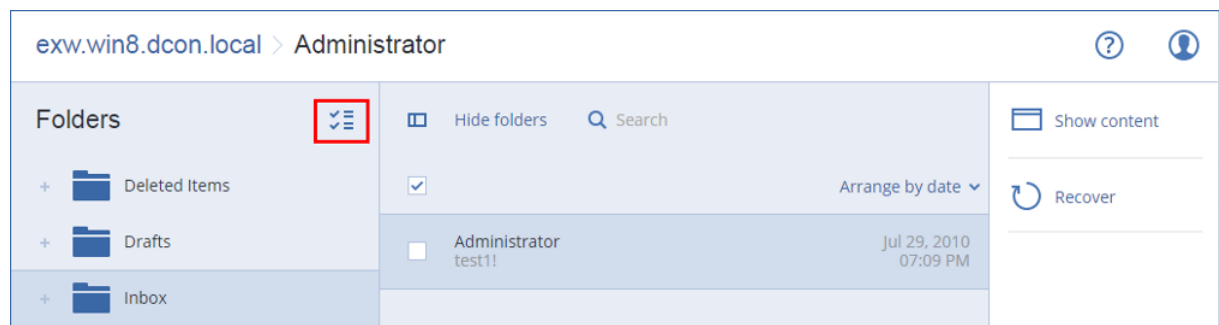
   When an email message is selected, you can click **Show content** to view its contents, including attachments.

   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 is a member of the **Organization Management** role group.

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.

2.14 Protecting Office 365 mailboxes

Why back up Office 365 mailboxes?

Even though Microsoft Office 365 is a cloud service, 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 Office 365 mailboxes if it is required by a regulatory compliance.

What do I need to back up the mailboxes?

To back up and recover Office 365 mailboxes, you must be assigned the global administrator role in Microsoft Office 365.

Install Agent for Office 365 on a Windows machine that is connected to the Internet. There must be only one Agent for Office 365 in an organization (customer group). The agent must be registered under the customer administrator account.

▪ Enter the customer administrator credentials during the agent installation and when logging in to the web interface.

▪ Enter the Office 365 global administrator credentials on the **Microsoft Office 365** page of the web interface.

  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.

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. The mailbox items are always recovered to the **Recovered items** folder of the target mailbox.

Limitations

- Archive mailboxes (**In-Place Archive**) cannot be backed up.
- Recovery to a new mailbox is not possible. You must first create a new Office 365 user manually, and then recover items to this user's mailbox.
- Recovery to a different Microsoft Office 365 organization or to an on-premises Microsoft Exchange Server is not supported.

2.14.1   Selecting Office 365 mailboxes

Select the mailboxes as described below, and then specify other settings of the backup plan as appropriate (p. 34).

To select Microsoft Office 365 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**.

2.14.2   Recovering Office 365 mailboxes and mailbox items

2.14.2.1   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. 79), 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**.

2.14.2.2   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. 79), 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.

2.15 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.

2.15.1 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**.

2.15.2   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. 51).

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.

2.16   Special operations with virtual machines

2.16.1   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.
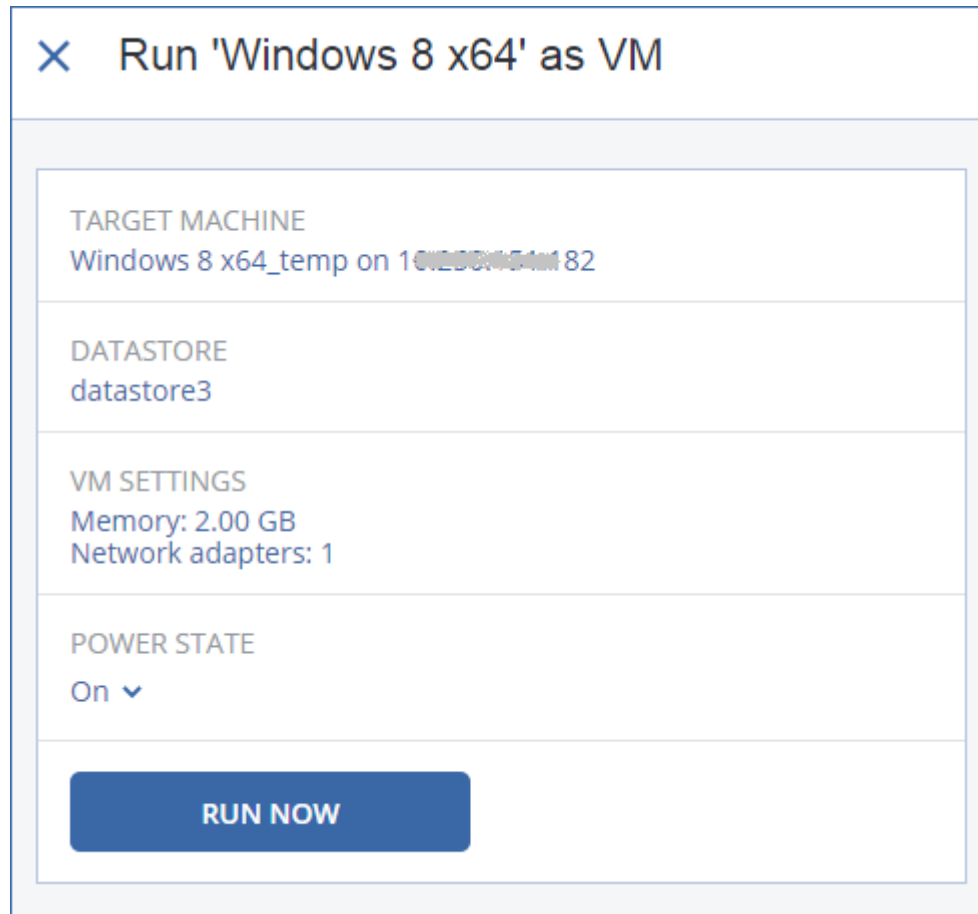
Prerequisites

- 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.

2.16.1.1   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. 79).

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░░░░░░░82

DATASTORE
datastore3

VM SETTINGS
Memory: 2.00 GB
Network adapters: 1

POWER STATE
On ⌄

RUN NOW

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

 . Such virtual machines cannot be selected for backup.

2.16.1.2 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.

2.16.1.3 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.

2.16.2 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. 108), 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. 106)

  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. 106)

  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.

2.16.2.1 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. 108).

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:

2.16.2.2   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.

2.16.2.3   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. 107)

    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. 107)

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. 107)

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.

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.

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**.

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. 108).
7. Click **Start recovery**.
8. Confirm your decision.

2.16.2.4   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. 49).

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. 50).

Pre/Post commands

This option is similar to the backup option "Pre/Post commands" (p. 55).

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. 61).

2.16.2.5   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. 75).

Performance

This option is similar to the recovery option "Performance" (p. 76).

Pre/Post commands

This option is similar to the recovery option "Pre/Post commands" (p. 77).

VM power management

This option is similar to the recovery option "VM power management" (p. 78).

2.16.3   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**.

2.16.4   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. 64)
- Virtual-to-virtual (V2V) - "Virtual machine" (p. 65)
- Virtual-to-physical (V2P) - "Virtual machine" (p. 65) or "Recovering disks by using bootable media" (p. 67)

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.
- Recreate logical volumes (LVM) or Linux Software RAID on the target machine.
- Provide drivers for specific hardware that is critical for the system bootability.

2.16.5   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.
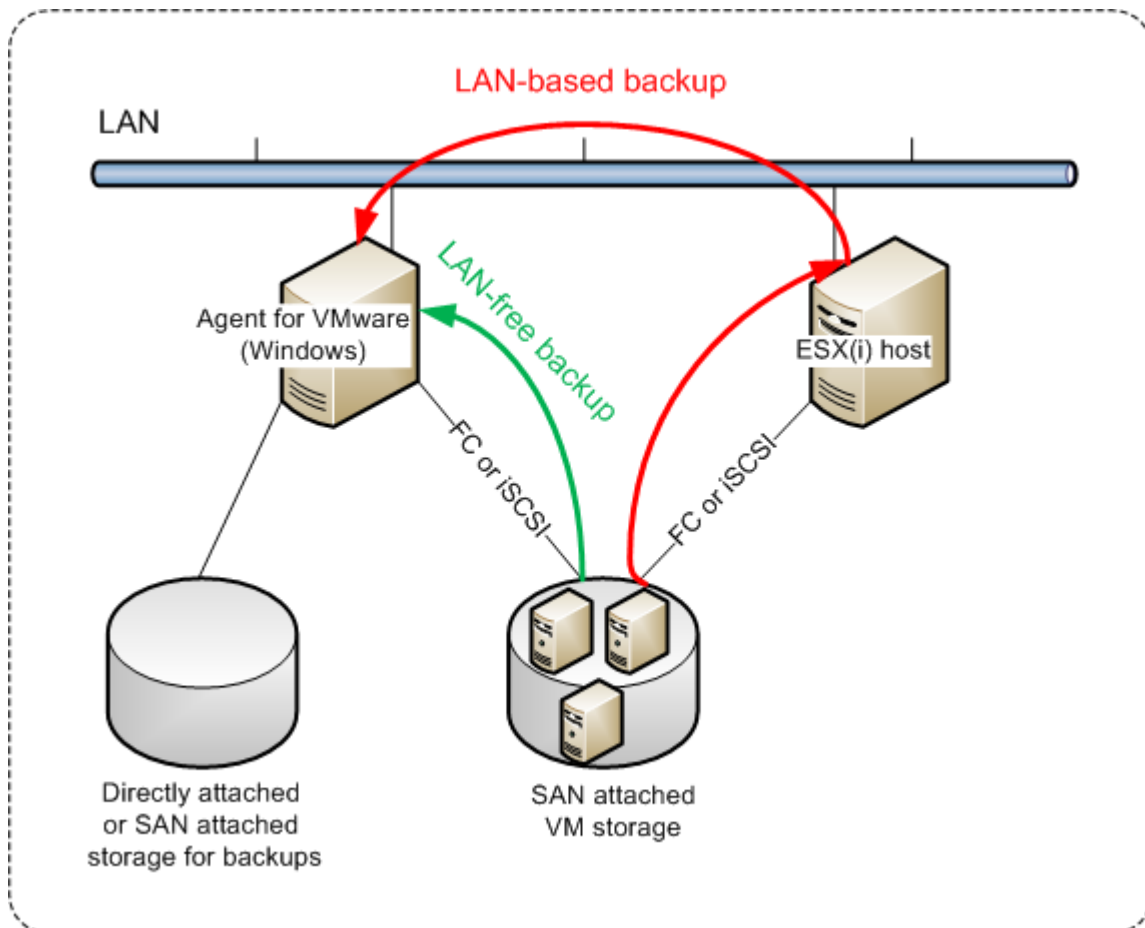
To enable the agent to access a datastore directly

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.

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.

Copyright © Acronis International GmbH, 2002-2017
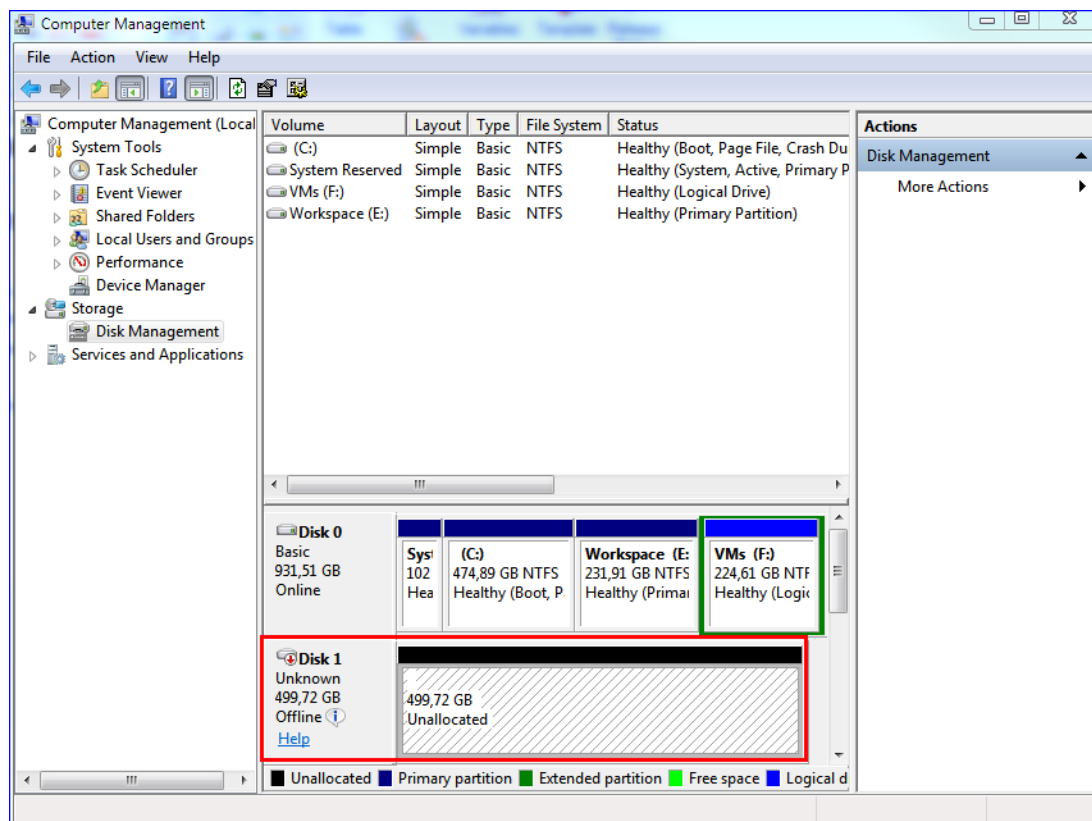
2.16.6 Agent for VMware - necessary privileges

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. 108) section.

Object	Privilege	Operation			
		Back up a VM	Recover to a new VM	Recover to an existing VM	Run VM from backup
Datastore	**Allocate space**		+	+	+
	Browse datastore				+
	Configure datastore	+	+	+	+
	Low level file operations				+
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		+		

Object	Privilege	Operation			
		Back up a VM	Recover to a new VM	Recover to an existing VM	Run VM from backup
	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		+	+	
	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	+		+	+

* This privilege is required for application-aware backups only.

2.16.7 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. 63). When configuring the recovery, select the new machine as the target machine.

2.17 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.

3 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**).
- A daily backup is the first backup created after a day starts.
- An hourly backup is the first backup created after an hour starts.

D

Differential backup

A differential backup stores changes to the data against the latest full backup (p. 115). 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.