# Table of contents

1 Administrator's Guide ..............................................................................................................3  
1.1 About this document .............................................................................................................3  
1.2 About the backup service ......................................................................................................3  
  1.2.1 Accounts and groups ......................................................................................................3  
  1.2.2 Components ...................................................................................................................4  
  1.2.3 Supported web browsers .................................................................................................6  
1.3 Step-by-step instructions .......................................................................................................6  
  1.3.1 Activating the backup service subscription ...................................................................7  
  1.3.2 Creating a group ............................................................................................................7  
  1.3.3 Creating an account ........................................................................................................8  
  1.3.4 Accessing the backup management console .................................................................8  
  1.3.5 Creating a report about the service usage .....................................................................9  
1.4 Advanced scenarios ..............................................................................................................9  
  1.4.1 Deploying agents on client machines ..........................................................................9  
2 User's Guide ...........................................................................................................................12  
  2.1 About the backup service ....................................................................................................12  
  2.2 Software requirements ......................................................................................................12  
    2.2.1 Supported web browsers .............................................................................................12  
    2.2.2 Supported operating systems and environments .......................................................12  
    2.2.3 Supported Microsoft SQL Server versions .................................................................13  
    2.2.4 Supported Microsoft Exchange Server versions .......................................................13  
  2.3 Activating the backup account ............................................................................................14  
  2.4 Accessing the backup service .............................................................................................14  
  2.5 Installing the software .....................................................................................................14  
    2.5.1 Preparation ................................................................................................................14  
    2.5.2 Linux packages ...........................................................................................................16  
    2.5.3 Installing agents ..........................................................................................................18  
    2.5.4 Updating agents ..........................................................................................................19  
  2.6 Backup console views ..........................................................................................................19  
  2.7 Backup .............................................................................................................................20  
    2.7.1 Backup plan cheat sheet .............................................................................................21  
    2.7.2 Selecting data to back up ..........................................................................................21  
    2.7.3 Selecting a destination ...............................................................................................26  
    2.7.4 Schedule ....................................................................................................................27  
    2.7.5 Retention rules ...........................................................................................................28  
    2.7.6 Starting a backup manually .......................................................................................28  
  2.8 Recovery ...........................................................................................................................28  
    2.8.1 Recovery cheat sheet ..................................................................................................28  
    2.8.2 Creating bootable media ............................................................................................29  
    2.8.3 Recovering a machine ...............................................................................................29  
    2.8.4 Recovering files .........................................................................................................31  
    2.8.5 Recovering system state ............................................................................................34  
    2.8.6 Recovering SQL databases .........................................................................................34  
    2.8.7 Recovering Exchange data .........................................................................................35  
  2.9 Operations with backups and backup plans .....................................................................37  
    2.9.1 Operations with backups ..........................................................................................37  
    2.9.2 Operations with backup plans ..................................................................................37  
  2.10 Troubleshooting ................................................................................................................38  
3 Glossary ..................................................................................................................................39
1 Administrator's Guide

1.1 About this document
This document is intended for organization administrators and end users who want to use Acronis 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 management is available through a web interface.

1.2.1 Accounts and groups
There are two account types: administrator accounts and backup accounts.

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

A backup account enables backing up physical and virtual machines. It is created by an administrator and typically corresponds to an end user. Both the end user and the administrators can manage backups of the end users' data.

Each account belongs to a group. The organization group is automatically created for your organization. Optionally, you can create unit groups, which typically correspond to units or departments of the organization.
The following diagram illustrates two hierarchy levels—the organization and unit groups. Optional groups and accounts are shown by a dotted line.

The following table summarizes operations that can be performed by the administrators and the end users.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Administrators</th>
<th>End users (using the backup account credentials)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create groups</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Create administrator accounts</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Create backup accounts</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Download and install the backup software</td>
<td>Yes, using the backup account credentials</td>
<td>Yes</td>
</tr>
<tr>
<td>Manage backup</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Manage recovery</td>
<td>Yes, using the backup account credentials</td>
<td>Yes</td>
</tr>
<tr>
<td>Create reports about the service usage</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

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 ESX(i) 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 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.

The agents can be installed by the end users or by the administrators and registered on the backup management server by using the backup account credentials.

**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 management console**. End users log in directly to this console by using their backup account credentials. Administrators access it from the account management console.

The backup storages are located in Acronis data centers. 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 backup service 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
- Safari 5.1.7 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 the backup service subscription
- Create a group
- Create a backup account and, optionally, an administrator account
- Access the backup management console
- Create a report about the service usage

For information about how to back up and recover data, refer to the User's Guide (p. 12).

### 1.3.1 Activating the backup service subscription

2. Log in to your Acronis account. If you do not have an Acronis account, create one.
3. Enter the backup service registration codes.
4. Click Register.
5. To access the account management console, click Manage your backups.
   At a later time, you can access the management console at [https://backup.acronis.com/](https://backup.acronis.com/).

### 1.3.2 Creating a group

Skip this step if you do not want to organize accounts into groups.

You may want to create a new Unit group within an EUC 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 Language, select the default language of notifications, reports, and backup software that will be used within this group.
7. [Optional] Specify the storage quota and the maximum number of machines the unit is allowed to back up.
   - Physical workstations
   - Physical servers
   - Virtual machines
   - Storage quota
   If any of these values are exceeded, the group administrator and the administrators of the parent group will receive an email notification. Restrictions on using the backup service are not applied.
8. [Optional] In Contact information, specify the contact information for the group.
9. 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.

1.3.3 Creating an account

You must create at least one backup account.

You may want to create an administrator within an organization or a unit group as well.

To create an account

1. Log in to the account management console.
2. Select a group in which you want to create the account.
3. Click the Backup accounts or Administrators tab, and then click "+".
4. Specify the following contact information for the backup 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
5. [Optional, for backup accounts only] Specify the storage quota and the maximum number of machines the user is allowed to back up.
   - Physical workstations
   - Physical servers
   - Virtual machines
   - Storage quota
     If any of these values are exceeded, a notification will be sent to the email address specified in step 4. Restrictions on using the backup service are not applied.
6. [Optional] Change the Backup notifications level. If you disable backup notifications, the notifications about backup failures, warnings, and successful backups will not be sent to the specified email address.
7. [Optional] Disable Business notifications. If you do this, notifications about exceeded quotas will not be sent to the specified email address.
8. Click Add.

As a result:
   - A new account appears in the Backup accounts or Administrators tab.
   - An email message containing the activation link is sent to the email address you specified.

1.3.4 Accessing the backup management console

Administrators can access the backup management console from the account management console. End users log in directly to the backup management console.

To access the backup management console as an administrator

1. Log in to the account management console.
2. [Optional] Select the group that contains the machines you want to back up.
3. Click Manage backups. For information about how to back up and recover data, refer to the User's Guide (p. 12).

1.3.5 Creating a report about the service usage

Usage reports provide historical data about using the backup service.

Only administrators can create these reports. The report data differs, depending on who created the report.

- Reports created by organization administrators contain statistics for each of the units.
- Reports created by unit administrators contain statistics for each of end users in the unit.

Reporting parameters

The report includes the following data about a unit and its backup accounts:

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

Enabling or disabling scheduled usage reports

Scheduled report covers system usage data for the last full calendar month. The reports will be generated and sent on the second day of every month to all administrators of your group.

1. In the account management console, click Reports.
2. Select the Scheduled tab.
3. In Status, enable or disable the scheduled usage reports by clicking the on/off switch.
4. [Optional] To generate a report immediately, click Send report now.

Enabling or disabling ad-hoc usage reports

Ad-hoc report covers system usage data for the specified period with one-day interval. This type of report can be generated on demand and cannot be scheduled. The report will be sent to the email address of your administrator account.

1. In the account management console, click Reports.
2. Select the Ad-hoc tab.
3. In Reporting period, select start and end dates of reporting period.
4. To generate a report immediately, click Send report now.

1.4 Advanced scenarios

1.4.1 Deploying agents on client machines

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 on the machine and the machine is registered in the backup service.

**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 machine page in the backup management 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. Specify the credentials of the backup account. This account will be used to register machines with installed agents in the backup service.
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 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.
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.
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 backup service 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
- Safari 5.1.7 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 SP2+ (x86, x64)
- Windows 2000 SP4 – all editions except for the Datacenter edition
- Windows Server 2003/2003 R2 – Standard and Enterprise editions (x86, x64)
- 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 Small Business Server 2011 – all editions
- Windows 8/8.1 – all editions except for the Windows RT editions (x86, x64)
- Windows Server 2012/2012 R2 – all editions

Agent for Linux

- Linux with kernel from 2.4.20 to 3.18 and glibc 2.3.2 or later
- Various x86 and x86_64 Linux distributions, including:
Red Hat Enterprise Linux 4.x, 5.x, 6.x, and 7.x
Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, and 21
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, and 7.7
CentOS 5.x, 6.x, and 7.0
Oracle Linux 5.x, 6.x, and 7.0 – both Unbreakable Enterprise Kernel and Red Hat Compatible Kernel
CloudLinux 6.x

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 Mountain Lion 10.8
OS X Mavericks 10.9
OS X Yosemite 10.10

Agent for VMware
This agent is delivered as a Windows application for running in any operating system listed above for Agent for Windows.
VMware ESXi(i) 4.0, 4.1, 5.0, 5.1, 5.5, and 6.0

Agent for Hyper-V
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

2.2.3 Supported Microsoft SQL Server versions
Agent for SQL supports the following versions of Microsoft SQL Server:
- Microsoft SQL Server 2005
- Microsoft SQL Server 2008
- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2012
- Microsoft SQL Server 2014

2.2.4 Supported Microsoft Exchange Server versions
Agent for Exchange supports the following versions of Microsoft Exchange Server:
- Microsoft Exchange Server 2013 – all editions, Cumulative Update 1 (CU1) and later.
Microsoft Exchange Server 2003 – all editions, SP2 or later.
Hotfix http://support.microsoft.com/kb/908072 must be installed.

2.3 Activating the backup account

When an administrator creates a backup 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 backup account. Remember your login that is shown on the account activation page.

  *Important* You must provide these credentials when installing the agents on the machines that are associated with this backup account.

- **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.

2.4 Accessing the backup service

You can log in to the backup service if you activated your backup 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 backup account.
3. Click **Log in**.

2.5 Installing the software

2.5.1 Preparation

**Step 1**

Choose the 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 any other agent installed in Windows (Agent for VMware, Agent for Hyper-V, Agent for Exchange, Agent for SQL). If you install, for example, Agent for SQL, you also will be able to back up the entire machine where the agent is installed.

<table>
<thead>
<tr>
<th>What are you going to back up?</th>
<th>Which agent do I need?</th>
<th>Where to install it?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical machines running Windows</td>
<td>Agent for Windows</td>
<td>On the machine that will be backed up.</td>
</tr>
<tr>
<td>Physical machines running Linux</td>
<td>Agent for Linux</td>
<td>On the machine that will be backed up.</td>
</tr>
<tr>
<td>Physical machines running OS X</td>
<td>Agent for Mac</td>
<td>On the machine that will be backed up.</td>
</tr>
<tr>
<td>VMware ESX(i) virtual machines</td>
<td>Agent for VMware</td>
<td>On a Windows machine that has network access to vCenter Server and to the virtual machine storage.*</td>
</tr>
<tr>
<td>Hyper-V virtual machines</td>
<td>Agent for Hyper-V</td>
<td>On the Hyper-V host.</td>
</tr>
</tbody>
</table>
SQL databases | Agent for SQL | On the machine running Microsoft SQL Server.
---|---|---
Exchange databases | Agent for Exchange | On the machine running Microsoft Exchange Server.
Virtual machines hosted on Windows Azure | The same as for physical machines** | On the machine that will be backed up.

*If your ESX(i) 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 ESX(i) host and LAN.

**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 machine appears as a physical machine.

**Step 2**

Review the system requirements for the agents.

<table>
<thead>
<tr>
<th>Agent</th>
<th>Disk space occupied by the agent(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent for Windows</td>
<td>550 MB</td>
</tr>
<tr>
<td>Agent for Linux</td>
<td>500 MB</td>
</tr>
<tr>
<td>Agent for Mac</td>
<td>450 MB</td>
</tr>
<tr>
<td>Agent for VMware</td>
<td>700 MB (150 MB + 550 MB Agent for Windows)</td>
</tr>
<tr>
<td>Agent for Hyper-V</td>
<td>600 MB (50 MB + 550 MB Agent for Windows)</td>
</tr>
<tr>
<td>Agent for Exchange</td>
<td>750 MB (200 MB + 550 MB Agent for Windows)</td>
</tr>
<tr>
<td>Agent for SQL</td>
<td>600 MB (50 MB + 550 MB Agent for Windows)</td>
</tr>
</tbody>
</table>

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 machines > Add machine.

The Add machine 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 the All agents for installation in Windows, 64-bit package (a package for 32-bit systems is not available). This package also enables unattended installation, for example, via Group Policy. This advanced scenario is described in the Administrator’s Guide (p. 9).

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 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.
2.5.2 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:
   ```bash
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:
   ```bash
   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:
     ```bash
     yum list installed | grep kernel-devel
     ```
   - In Ubuntu, run the following commands:
     ```bash
     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:
   ```bash
   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.
<table>
<thead>
<tr>
<th>Linux distribution</th>
<th>Package names</th>
<th>How to install</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat Enterprise Linux</td>
<td>kernel-devel gcc make</td>
<td>The setup program will download and install the packages automatically by using your Red Hat subscription.</td>
</tr>
<tr>
<td></td>
<td>perl</td>
<td>Run the following command:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>yum install perl</td>
</tr>
<tr>
<td></td>
<td>kernel-devel gcc make</td>
<td>The setup program will download and install the packages automatically.</td>
</tr>
<tr>
<td></td>
<td>perl</td>
<td>Run the following command:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>yum install perl</td>
</tr>
<tr>
<td></td>
<td>linux-headers</td>
<td>Run the following commands:</td>
</tr>
<tr>
<td></td>
<td>linux-image</td>
<td>sudo apt-get update</td>
</tr>
<tr>
<td></td>
<td>gcc</td>
<td>sudo apt-get install linux-headers-<code>uname -r</code></td>
</tr>
<tr>
<td></td>
<td>make</td>
<td>sudo apt-get install linux-image-<code>uname -r</code></td>
</tr>
<tr>
<td></td>
<td>perl</td>
<td>sudo apt-get install gcc-&lt;package version&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>sudo apt-get install make</td>
</tr>
<tr>
<td></td>
<td></td>
<td>sudo apt-get install perl</td>
</tr>
</tbody>
</table>

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:
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-4.5.1-4.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.

### 2.5.3 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 backup account that the machine is assigned to.
5. [Only when installing Agent for VMware] Specify the address and access credentials for the vCenter Server or ESX(i) host whose virtual machines the agent will back up.
6. [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.
7. 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 backup account that the machine is assigned to.
4. 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. Inside the image, run the .pkg file.
5. If prompted, provide administrator credentials.
6. Specify the credentials of the backup account that the machine is assigned to.
7. Complete the installation procedure.

2.5.4 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
- Agent for Mac, Agent for SQL, Agent for Exchange: any version

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

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

To update an agent by using the web interface

1. Click Updates.
   The software displays the machines with outdated agent versions.
2. Select the machines on which you want to update the agents. The machines must be online.
3. Click Update agent.
   The update progress is shown in the status column for each machine.

2.6 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 up to five machines.
The table view is enabled automatically if the number of machines to display exceeds five.

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

### 2.7 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 apply a backup plan to machines**

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, if any, or a new backup plan template.
3. [Optional] To select another backup plan or to create a new backup plan, click the arrow next to the backup plan name.
4. [Optional] To modify the plan parameters, click the corresponding section of the backup plan panel.
5. Click **Apply**.
6. Specify a name for the new backup plan or confirm changes to the existing backup plan (if any).
2.7.1 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.

<table>
<thead>
<tr>
<th>WHAT TO BACK UP</th>
<th>ITEMS TO BACK UP Selection methods</th>
<th>WHERE TO BACK UP</th>
<th>SCHEDULE Backup schemes (not for Cloud)</th>
<th>HOW LONG TO KEEP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disks/volumes (physical machines)</td>
<td>Direct selection (p. 21) Policy rules (p. 21) File filters (p. 25)</td>
<td>Single-file (p. 27)</td>
<td>Always full (p. 27) Weekly full, daily incremental (p. 27) Custom (F-D-I) (p. 27)</td>
<td>By backup age (single rule/per backup set) (p. 28) By number of backups (p. 28) Keep indefinitely (p. 28)</td>
</tr>
<tr>
<td>Disks/volumes (virtual machines)</td>
<td>Policy rules (p. 21) File filters (p. 25)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Files (physical machines only)</td>
<td>Direct selection (p. 22) Policy rules (p. 22) File filters (p. 25)</td>
<td>Cloud (p. 26)</td>
<td>Always full (p. 27) Weekly full, daily incremental (p. 27) Custom (F-I) (p. 27)</td>
<td></td>
</tr>
<tr>
<td>System state</td>
<td>Direct selection (p. 24)</td>
<td>Local folder (p. 26) Network folder (p. 26)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SQL databases</td>
<td>Direct selection (p. 24)</td>
<td></td>
<td>Always full (p. 27) Weekly full, daily incremental (p. 27) Custom (F-I) (p. 27)</td>
<td></td>
</tr>
<tr>
<td>Exchange databases</td>
<td>Direct selection (p. 25)</td>
<td></td>
<td>Always full (p. 27) Weekly full, daily incremental (p. 27) Custom (F-I) (p. 27)</td>
<td></td>
</tr>
</tbody>
</table>

2.7.2 Selecting data to back up

2.7.2.1 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. 25).

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.

2.7.2.2 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. 25).

**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 share*.
      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.
- \texttt{/etc} selects the directory for system configuration files.

**Selection rules for OS X**

Full path to a file or directory.

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

2.7.2.3 **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

2.7.2.4 **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.

**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.
2.7.2.5 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.

<table>
<thead>
<tr>
<th>Exchange version</th>
<th>Data items</th>
<th>User rights</th>
</tr>
</thead>
<tbody>
<tr>
<td>2003</td>
<td>Storage groups</td>
<td>Membership in the Organization Management role group.</td>
</tr>
<tr>
<td>2007</td>
<td>Storage groups</td>
<td>Membership in the Exchange Organization Administrators role group</td>
</tr>
<tr>
<td>2010/2013</td>
<td>Databases</td>
<td>Membership in the Organization Management role group.</td>
</tr>
</tbody>
</table>

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.

2.7.2.6 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.

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.
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.

- **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.

### 2.7.3 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.

[Optional] To copy the backups to the cloud storage, select the Copy backups to Cloud Storage check box.

- **Network folder**

  Browse to the required shared folder or enter the path and click the arrow button. If prompted, specify the user name and password for the shared folder.

  [Optional] To copy the backups to the cloud storage, select the Copy backups to Cloud Storage check box.

### 2.7.4 Schedule

#### 2.7.4.1 Disk-level backups

By default, backups are performed on a daily basis. You can select the days of the week and 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 saved in a local or network folder, disk-level backups use the new single-file backup format (p. 39).

---

You can set a date range for when the schedule is effective. Select the Run backup plan within a date range check box, and then specify the date range.

#### 2.7.4.2 File-level backups

The scheduling parameters of a file-level backup depend on the backup destination.

With any destination, you can set a date range for when the schedule is effective. Select the Run backup plan within a date range check box, and then specify the date range.

**When backing up to cloud storage**

By default, backups are performed on a daily basis. You can select the days of the week and 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 a local or network folder**

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:

- **Always full**

  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.
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** (default)
  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.

### 2.7.5 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. 39) 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.

### 2.7.6 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 Recovery

#### 2.8.1 Recovery cheat sheet

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

<table>
<thead>
<tr>
<th>What to recover</th>
<th>Recovery method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical machine</td>
<td>Using the web interface (p. 29)</td>
</tr>
<tr>
<td>(Windows or Linux)</td>
<td>Using bootable media (p. 30)</td>
</tr>
</tbody>
</table>
### 2.8.2 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 Rescue Media Builder on the Applications menu.
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.

### 2.8.3 Recovering a machine

#### 2.8.3.1 Physical machine

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

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

### Table

<table>
<thead>
<tr>
<th>Physical machine (Mac)</th>
<th>Using bootable media (p. 30)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual machine</td>
<td>Using the web interface (p. 30) (only to the original machine) Using bootable media (p. 30)</td>
</tr>
<tr>
<td>Files/Folders</td>
<td>Using the web interface (p. 31) (only from a local/network folder) Downloading files from the cloud storage (p. 32) Using bootable media (p. 33)</td>
</tr>
<tr>
<td>System state</td>
<td>Using the web interface (p. 34)</td>
</tr>
<tr>
<td>SQL databases</td>
<td>Using the web interface (p. 34)</td>
</tr>
<tr>
<td>Exchange databases</td>
<td>Using the web interface (p. 35)</td>
</tr>
</tbody>
</table>
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.
   - If the backup is located in the cloud storage, click Select machine, select a target machine that is online, and then select a recovery point.
   - Otherwise, recover the machine as described in "Recovering disks by using bootable media" (p. 30).
4. Click Recover machine.
   The software automatically maps the disks from the backup to the target disks.
   - If the disk mapping fails, recover the machine as described in "Recovering disks by using bootable media" (p. 30). The media enables you to choose disks for recovery and to map the disks manually.
   - If the disk mapping succeeds, click Recover.
5. 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 in the Status column for the machine.

2.8.3.2 Virtual machine

The backup service web interface enables you to overwrite a virtual machine with its backed-up version.

Overwriting a machine means that only the content of its original disks is overwritten. The content of disks that were added after the backup will remain the same.

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.

To recover a virtual machine
1. Select the machine that you want to recover.
2. Click Recovery.
3. Select a recovery point. Note that recovery points are filtered by location.
4. Click Recover machine.
5. Confirm that you want to overwrite the machine with its backed-up version.

The recovery progress is shown in the Status column for the machine.

2.8.3.3 Recovering disks by using bootable media

For information about how to create bootable media, refer to "Creating bootable media" (p. 29).
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. On the welcome screen, click Recover.
4. Click Select data, and then click Browse.
5. Specify the backup location:
   - To recover from cloud storage, select Cloud storage. Enter the credentials of the backup account to which the backed up machine was 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.
6. Select the backup from which you want to recover the data. If prompted, type the password for the backup.
7. In Backup contents, select the disks that you want to recover. Click OK to confirm your selection.
8. 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.

9. [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.
10. If you are recovering an operating system to dissimilar hardware, choose to use the Universal Restore feature.
     [When recovering Windows] Click Add folder and specify the path to the location where drivers for the motherboard, mass storage, and network adapter are stored. If the target hardware has a specific mass storage controller, such as RAID (especially NVIDIA RAID) or a fibre channel adapter, explicitly specify the mass storage drivers for them. To do this, in Mass storage drivers to install anyway, click Add driver, and then specify the drivers.
11. [Optional] Click Recovery options to specify additional settings.
12. Click OK to start the recovery.

2.8.4 Recovering files

2.8.4.1 Recovering files by using the web interface

Use this method to recover files from backups stored in a local/network folder.

To recover files by using the web interface

1. Select the machine which 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 machine is offline, the recovery points are not displayed. Recover the files by using bootable media (p. 33).

4. Click Recover files.
5. Select the files that you want to recover.
6. Click Recover.
7. Select the recovery destination. You can select the original location or any local or network folder.
8. Click Recover.
9. If the files are recovered to the original location, 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 in the Status column for the machine.

2.8.4.2 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. Log in with your backup account credentials.
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**.

### 2.8.4.3 Recovering files by using bootable media

For information about how to create bootable media, refer to "Creating bootable media" (p. 29).

**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. On the welcome screen, click **Recover**.
4. Click **Select data**, and then click **Browse**.
5. Specify the backup location:
   - To recover from cloud storage, select **Cloud storage**. Enter the credentials of the backup account to which the backed up machine was 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.
6. Select the backup from which you want to recover the data. If prompted, type the password for the backup.
7. In **Backup contents**, select **Folders/files**.
8. Select the data that you want to recover. Click **OK** to confirm your selection.
9. Under **Where to recover**, specify a folder. Optionally, you can prohibit overwriting of newer versions of files or exclude some files from recovery.
10. [Optional] Click **Recovery options** to specify additional settings.
11. Click **OK** to start the recovery.
2.8.5 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 in the Status column for the machine.

2.8.6 Recovering SQL databases

The backup service enables you to 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 recover databases to a machine where Agent for SQL is not installed, or you need to extract data for data mining, audit, or further processing by third-party tools.

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. 35).

To recover SQL databases

1. Click Microsoft SQL.
   Machines with Agent for SQL installed are shown.
2. Select the machine which 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.
5. Click Recover database.
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 machine or 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 **Recover**.
12. If the original databases were selected as the destination, confirm overwriting the databases with their backed-up versions.

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

### 2.8.6.1 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.

### 2.8.7 Recovering Exchange data

The backup service enables you to recover Exchange Server data to the original Exchange Server.

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
--- | --- | ---
2003 | Storage groups | Membership in the **Organization Management role group.**
2007 | Storage groups | Membership in the **Exchange Organization Administrators role group.**
2010/2013 | 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. 36).

**To recover Exchange data**

We will refer to both databases and storage groups as "databases" throughout this procedure.

1. Click **Microsoft Exchange.**
   Machines with Agent for Exchange installed are shown.
2. Select the machine which 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.
5. Click **Recover Exchange data.**
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.**
11. If the databases are recovered to the original ones, confirm overwriting the databases with their backed-up versions.

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

#### 2.8.7.1 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:


### 2.9 Operations with backups and backup plans

#### 2.9.1 Operations with backups

**To delete all backups of a machine from a given location**

1. Select a machine whose backups you want to delete.
2. Click **Recovery**.
3. Select the location to delete the backups from.
4. Click **Delete all**.
5. Confirm your decision.

#### 2.9.2 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 resources**.

**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.

### 2.10 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. 39). 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 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.