Acronis

Acronis Backup plugin for WHM and cPanel

INTEGRATION GUIDE

Revision: 7/14/2020

Table of contents

1 Introduction

This document describes how to install and use the Acronis Backup plugin for WHM and cPanel. The plugin integrates WHM and cPanel with Acronis Backup or Acronis Cyber Cloud.

With the plugin, a WHM user can:

- Back up an entire cPanel server to the cloud storage with the disk-level backup
- Recover the entire server including all of the websites
- Perform granular recovery of websites, individual files, mailboxes, mail filters, mail forwarders, accounts, and databases, including the databases created outside of WHM
- Enable self-service recovery for cPanel accounts

Once the plugin is installed and configured, the server is backed up on a predefined schedule. A backup can also be started on demand. The backup schedule can be configured in the Acronis web console.

Recovery can be performed from the WHM and cPanel interfaces.

It is not possible to back up individual websites. However, the rights for self-service recovery can be granted to each account separately.

2 System requirements

- PHP version 5.6 or later.
- Granular recovery of databases is supported only for local MySQL. Granular recovery of PostgreSQL databases is not supported.
- Besides the plugin, a backup agent must be installed on the same machine. If cPanel is running on a Virtuozzo container, the backup agent must be installed on the Virtuozzo host instead of the container.
- The list of supported operating systems for the backup agent (Agent for Linux) is available at https://www.acronis.com/en-us/support/documentation/BackupService/index.html#33496.html
- The list of supported virtualization platforms is available at https://www.acronis.com/en-us/support/documentation/BackupService/index.html#37870.html

  The agentless backup of VMware vSphere and Microsoft Hyper-V is not supported.

3 Obtaining the Acronis product

An Acronis Cyber Cloud or Acronis Backup 12.5 subscription is required to use the plugin.

You can purchase an Acronis Cyber Cloud subscription from service providers.

To purchase an Acronis Backup 12.5 subscription, visit https://www.acronis.com/business/backup/linux-server

A 30-day trial is available.

You will obtain a link and user name and password for the Acronis web console.

4 Installing the plugin

To install the Acronis Backup plugin for WHM and cPanel, run the following command:

```
sh <(curl -L
https://download.acronis.com/ci/cpanel/stable/install_acronis_cpanel.sh ||
wget -O -
https://download.acronis.com/ci/cpanel/stable/install_acronis_cpanel.sh)
```

This command runs the installation script.

5 Installing the backup agent

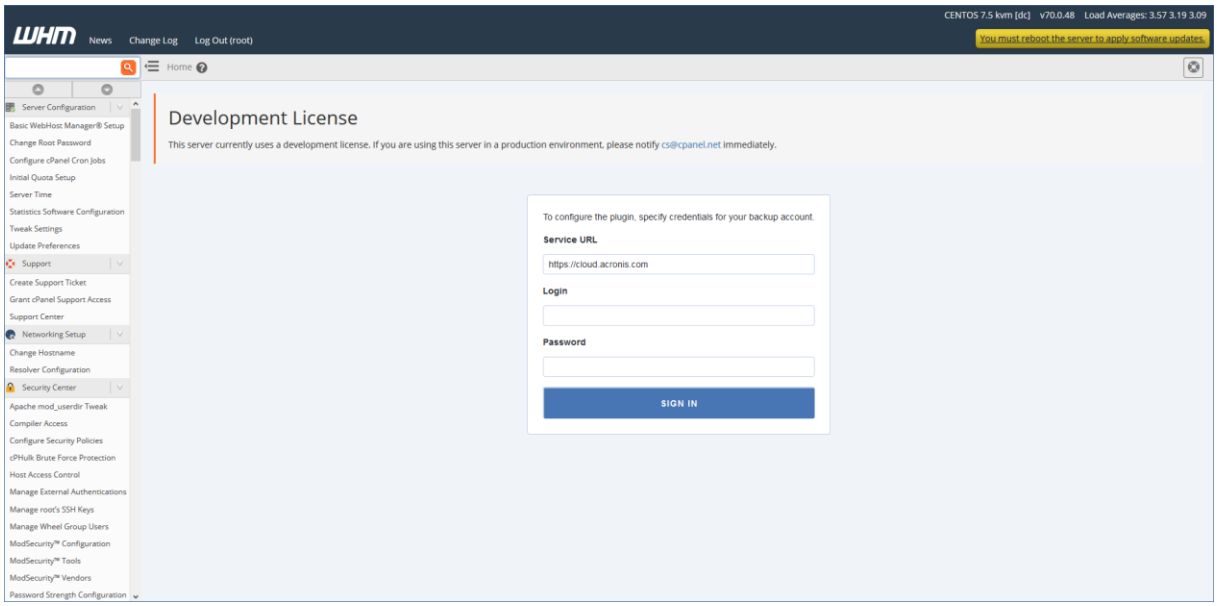
To back up the Virtuozzo container, the backup agent must be installed on its host as described in the Installing the backup agent on Virtuozzo host (p. 15) section.

To install the backup agent:

1. Log in to WHM UI.
2. Click **Plugins** > **Acronis Backup**.
3. Specify the credentials of the account to which the machine should be assigned.

   If you have enabled two-factor authentication (2FA) for your Acronis Cyber Cloud account, the backup agent must be installed according to the instruction provided in the Installing the backup agent using a registration token (p. 17) section.

   Make sure that you specify the credentials of an account created within the customer group (Customer administrator, Unit administrator, or User). Do not specify partner administrator credentials.



4. To encrypt your backups, enable the Encryption switch and specify the corresponding settings in the wizard.

   Be aware that there is no way to recover encrypted backups if you lose or forget the password.

   After a backup plan is created and applied, the encryption settings cannot be modified. To use different encryption settings, create a new backup plan in the Acronis backup console.

If you need to enforce encryption of backups, regardless of the backup plan encryption settings, save the encryption settings on each machine individually. The backups will be encrypted using the AES algorithm with a 256-bit key. In this case, the lock icon won't be shown on the Dashboard in the Backup section, as it represents an applied backup plan setting, not a machine one.

For more information on how to enable encryption per machine, check the following reference: https://www.acronis.com/support/documentation/AcronisBackup_12.5/#37608.html .

5. Follow the installation wizard.

   During the installation, the software checks if the ports required for communication with the cloud are open. If some of the ports are closed, the software shows numbers of these ports and the hostnames for which a port should be open. Open the ports, close the wizard and restart the installation.

   Completing the installation may take several minutes. You can leave the page during this process.

The backup agent can also be installed by using the command line.

For more details, see https://kb.acronis.com/content/61525

6 Uninstalling the plugin

To uninstall the Acronis Backup plugin for WHM and cPanel, run the following command:

```
yum remove acronis-backup-cpanel
```

Removing the extension will also uninstall the backup agent from the cPanel server. The backup accounts you created and the backed-up data will be left intact.

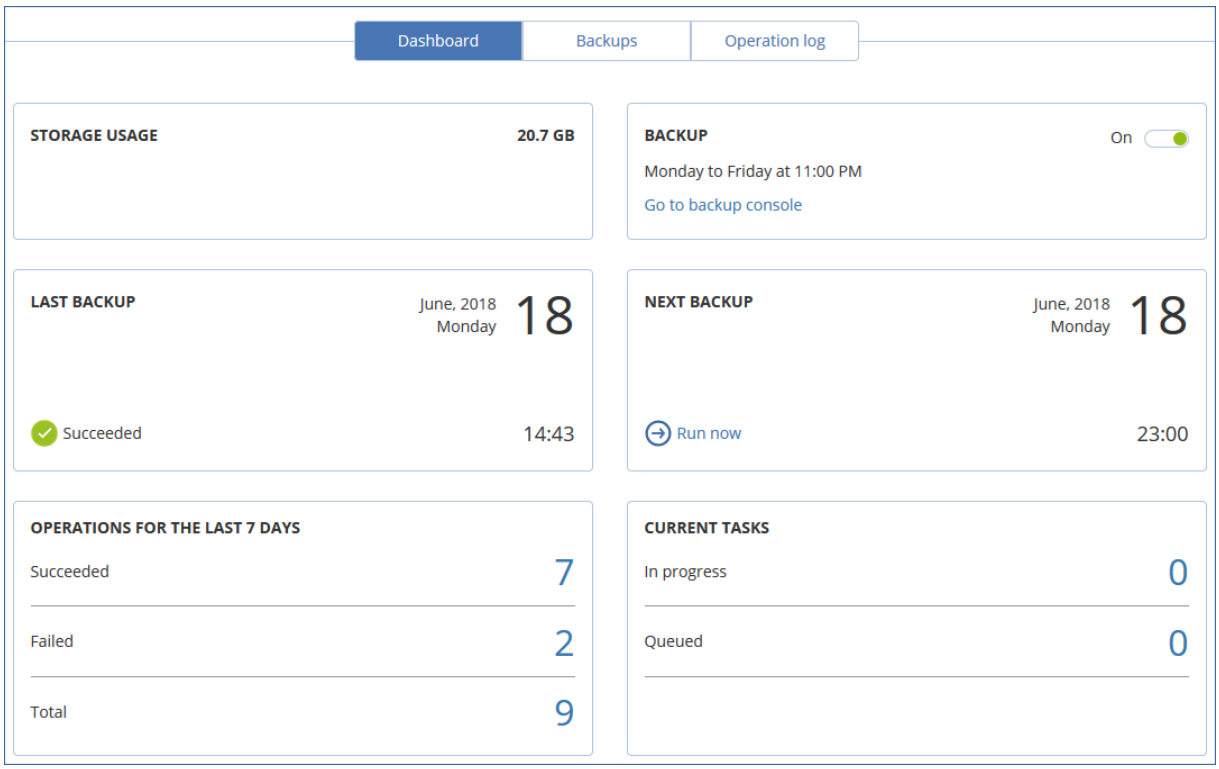
7 Backup

The following operations are available in WHM UI.

7.1 Enabling backup for a server

1. Click **Plugins** > **Acronis Backup**.

2. Enable the backup switch.



For cPanel server backup, a backup plan with the specific configuration is required.

- Avoid exclusion. Otherwise it will dramatically slow down mounting\recovery process.
- Do not change the parameters described in "Configuring a backup plan for a cPanel server" (p. 16). Otherwise, granular recovery in WHM and cPanel UI will not work.
- Do not apply to the cPanel server other plans that do not meet the above requirements. Otherwise, granular recovery in WHM and cPanel UI will not work either.

When you enable backup, the plugin attempts to find and apply a suitable backup plan. If several plans are found, a randomly selected one is applied. If no suitable plans are found, the default backup plan with “Webcp” name is created and applied to the cPanel server.

If you want to change the backup schedule or other parameters of the backup plan, do this in the Acronis web console.

7.2 Running a backup on demand

1. Click **Plugins** > **Acronis Backup**.
2. Click **Run now**.

7.3 Accessing the backup console

1. Click **Plugins** > **Acronis Backup**.
2. Click **Go to backup console**.

   The backup console opens in a new page. In the backup console you can adjust backup schedule and other backup parameters.

8 Enabling self-service for cPanel accounts

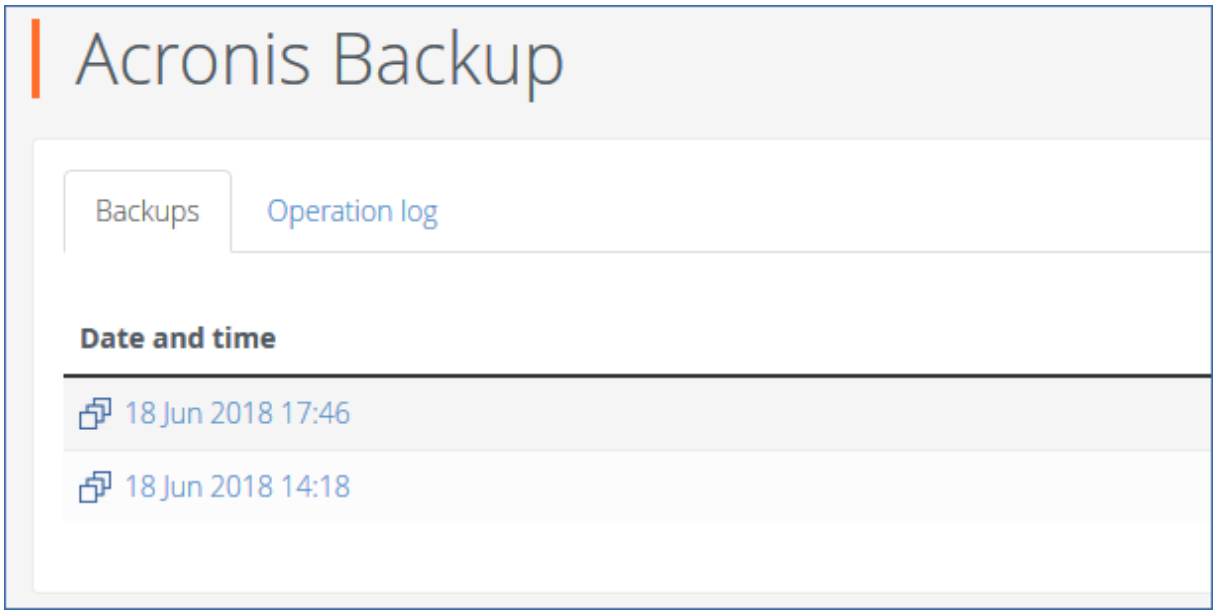
1. Click **Feature Manager**.
2. Select a feature list and click **Edit**.
3. Select the **Acronis Backup** check box.
4. Click **Save**.

9 Recovery in the cPanel UI

Accounts with the enabled Acronis Backup privilege can browse backups in their cPanel interface and download or recover files, folders, databases, mailboxes, mail filters, mail forwarders, and entire account.

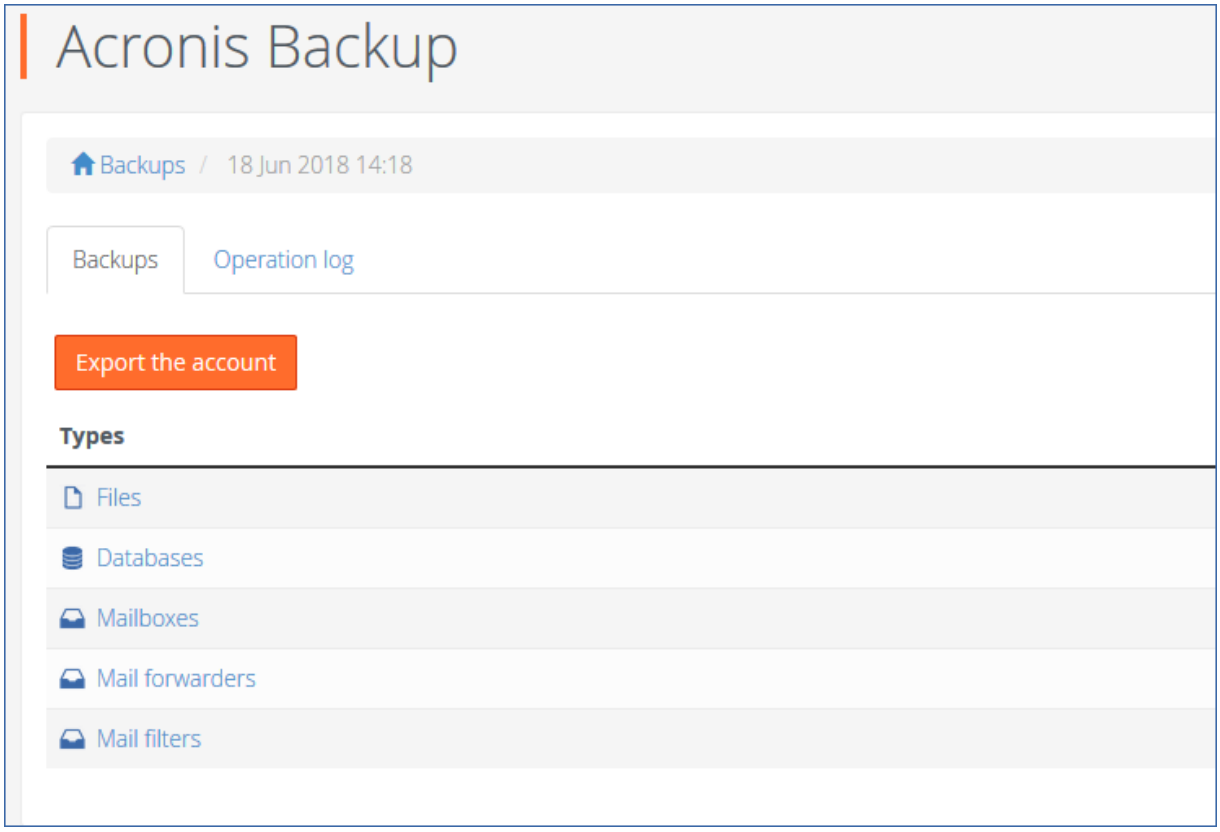
9.1 Downloading files

1. Click **Acronis Backup**.
2. Open the **Backups** tab.

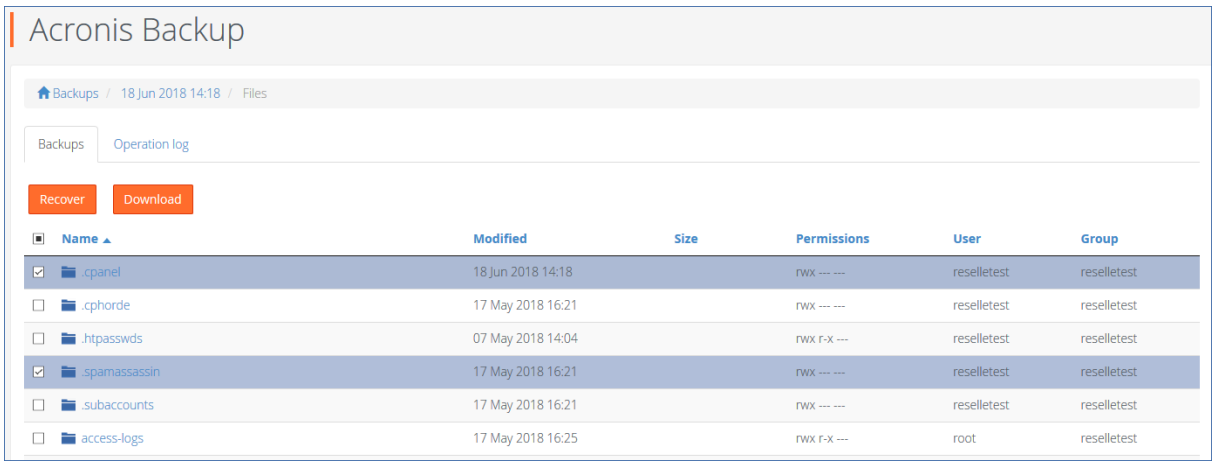


3. Select a recovery point.

After you select the recovery point, the corresponding backup is mounted to the cPanel server. The process may take up to a few minutes.



4. Click **Files**.
5. Select the files and folders to download.



6. Click **Download**.

If you choose to download a single file, the download will start immediately.

If you request to download several files, a .zip archive will be prepared and placed into your home folder. Once the archive is ready, download it by using the link in the notification bar or in the **Operation Log**, or by using the **File Manager**.

9.2 Recovering files to the original location

1. Click **Acronis Backup**.

2. Open the **Backups** tab.
3. Select a recovery point.

   After you select the recovery point, the corresponding backup is mounted to the cPanel server. The process may take up to a few minutes.
4. Click **Files**.
5. Select the files and folders to recover.
6. Click **Recover**.
7. If at least one folder is selected, you can select the **Delete any files in the original location that were created after the backup** option. If this option is enabled, all files from selected folders will be deleted before the recovery.

   This option may be useful if your website were hacked, to ensure that all malicious files are deleted.
8. Click **Recover**.

As a result, the selected files on the cPanel server are replaced with their copies from the backup.

9.3 Downloading database dumps

1. Click **Acronis Backup**.
2. Open the **Backups** tab.
3. Select a recovery point.
4. Click **Databases**.
5. Select the databases to download.
6. Click **Download**.

As result, a .zip archive with SQL dumps is prepared and placed into your home folder.

9.4 Recovering databases to the original location

1. Click **Acronis Backup**.
2. Open the **Backups** tab.
3. Select a recovery point.
4. Click **Databases**.
5. Select databases to recover.
6. Click **Recover**.
7. Make sure that the **Add suffix to the recovered database name** check box is cleared.
8. Click **Recover**.

As a result, the selected databases are recovered to the original location. The existing databases are overwritten. If a database no longer exists, it is recreated automatically.

9.5 Recovering databases as new ones

1. Click **Acronis Backup**.
2. Open the **Backups** tab.
3. Select a recovery point.
4. Click **Databases**.
5. Select databases to recover.

6. Click **Recover**.
7. Select the **Add suffix to the recovered database name** check box.
8. Click **Recover**.

As a result, new databases with the “%original_name%%suffix%” name is created in cPanel. The existing databases are not affected.

9.6 Downloading mailboxes

1. Click **Acronis Backup**.
2. Open the **Backups** tab.
3. Select a recovery point.
4. Click **Mailboxes**.
5. Select the mailboxes to download.
6. Click **Download**.

As a result, a .zip archive with the mailboxes content will be prepared and placed into your home folder.

9.7 Recovering mailboxes to the original location

1. Click **Acronis Backup**.
2. Open the **Backups** tab.
3. Select a recovery point.
4. Click **Mailboxes**.
5. Select the mailboxes to recover.
6. Click **Recover** and confirm.

As a result, the selected mailboxes are recovered to the original location. If the selected mailbox no longer exists on the server, it is recreated automatically.

9.8 Downloading mail filters

1. Click **Acronis Backup**.
2. Open the **Backups** tab.
3. Select a recovery point.
4. Click **Mail filters**.
5. Select the mail filters to download.
6. Click **Download**.

9.9 Recovering mail filters to the original location

1. Click **Acronis Backup**.
2. Open the **Backups** tab.
3. Select a recovery point.
4. Click **Mail filters**.
5. Select the mail filters to recover.
6. Click **Recover** and confirm.

9.10 Downloading mail forwarders

1. Click **Acronis Backup**.
2. Open the **Backups** tab.
3. Select a recovery point.
4. Click **Mail forwarders**.
5. Select the mail forwarders to download.
6. Click **Download**.

9.11 Recovering mail forwarders to the original location

1. Click **Acronis Backup**.
2. Open the **Backups** tab.
3. Select a recovery point.
4. Click **Mail forwarders**.
5. Select the mail forwarders to recover.
6. Click **Recover** and confirm.

9.12 Exporting the entire account

1. Click **Acronis Backup**.
2. Open the **Backups** tab.
3. Select a recovery point.
4. Click **Export the account**.
5. [Optional] Select **Skip export of databases** and **Skip export of home directory** check boxes.
6. Check the results in the **Operation log** tab. If the account was exported successfully, you can download the archive.

10 Recovering from WHM interface

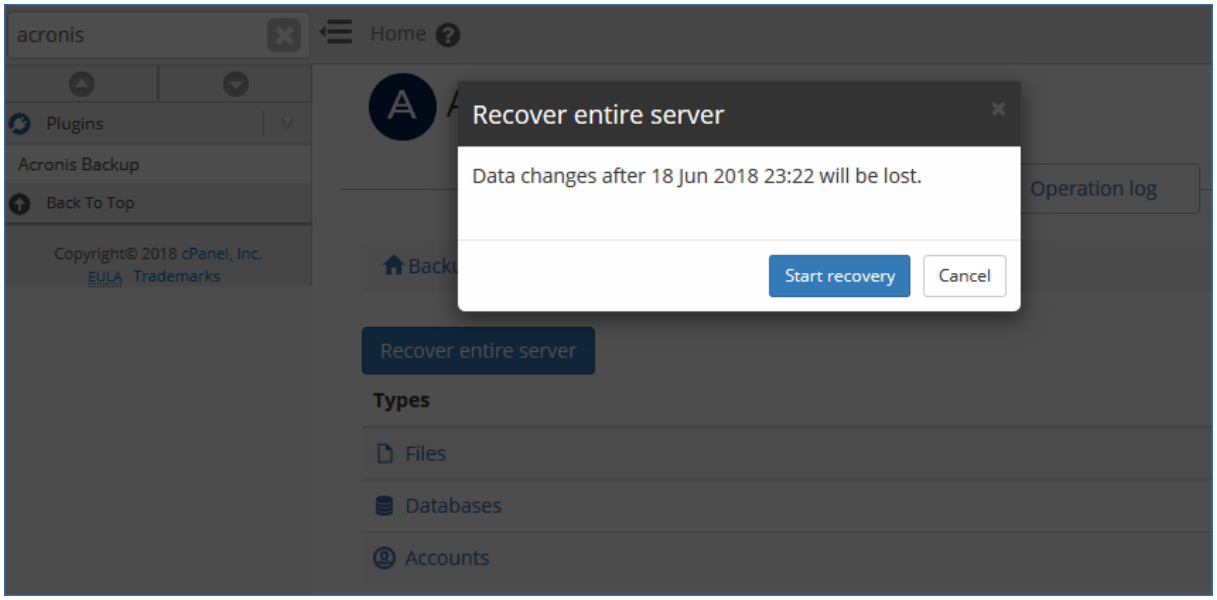
The recovery is similar to what is described in Recovery in the cPanel UI (p. 8). The differences are as follows:

- When you request to download .zip archive, the archive is placed in the `/root/backup_cloud/` folder.
  To change the archive location:
  - Open /usr/local/cpanel/base/3rdparty/acronisbackup/srv/config.ini
  - In section [app], add downloads_path = /root/new_path_to_archives/
  - Restart the Python service: /usr/local/cpanel/base/3rdparty/acronisbackup/scripts/acronis-backup-srv.sh restart
- These archives are stored for seven days by default.
  To change the retention period:
  - Open /usr/local/cpanel/base/3rdparty/acronisbackup/srv/config.ini
  - In section [app], add downloads_retention_days = 1
  - Restart the Python service: /usr/local/cpanel/base/3rdparty/acronisbackup/scripts/acronis-backup-srv.sh restart

- When you recover a user database as a new one, it is created under the user the original database belongs to.
- You can recover the entire server.
- You can recover or download accounts. When recovering individual accounts, you can configure several recovery options (p. 13).

10.1 Reverting a running cPanel server to a previous state

1. Click **Plugins** > **Acronis Backup**.
2. Open the **Backups** tab.
3. Select a recovery point.
4. Click **Recover entire server** and confirm.



As result, the entire server is reverted to the selected recovery point. All changes made after the backup will be lost.

The progress of the operation can be tracked in the Acronis web console.

If the WHM UI is not available as a result of the server failure, recover the server by using the Acronis web console or Acronis bootable media.

10.2 Options for recovering individual accounts via WHM UI

When you are recovering individual accounts from WHM UI, you can configure the following recovery options:

- **Overwrite the existing account**

  Use this option when another account with the same name exists. The existing account will be overwritten.
- **Change the user name**

Use this option to change the name of the recovered account. The maximum account name length is 16 alphanumeric characters.

- **Assign a dedicated IP address**

  Use this option to assign a spare dedicated IP address for the recovered account. You can configure the list of IPs in the **IP functions** section of WHM.

- **Skip recovery of databases**

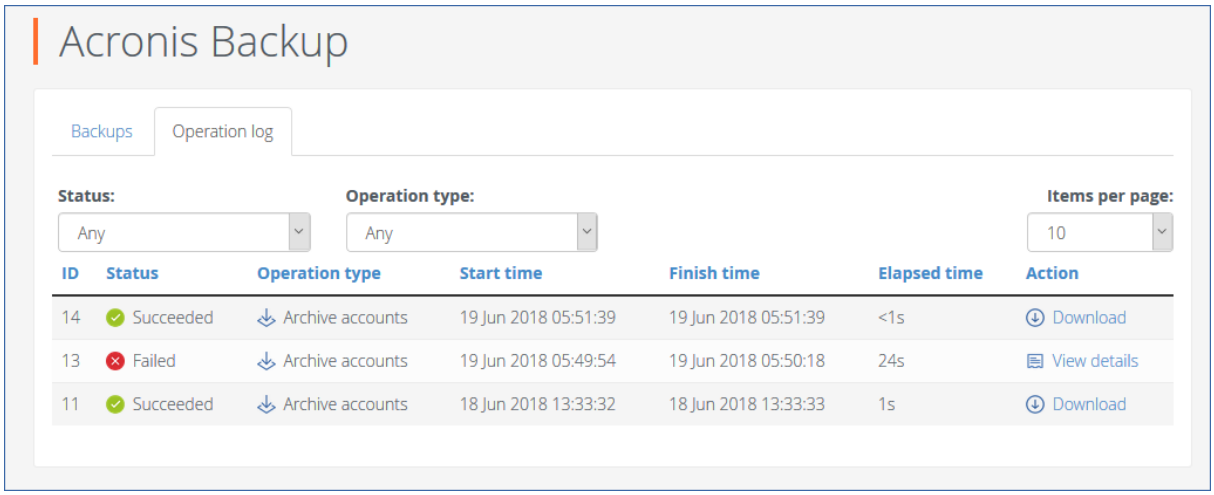
  Use this option to skip the recovery of databases.

- **Skip recovery of home directory**

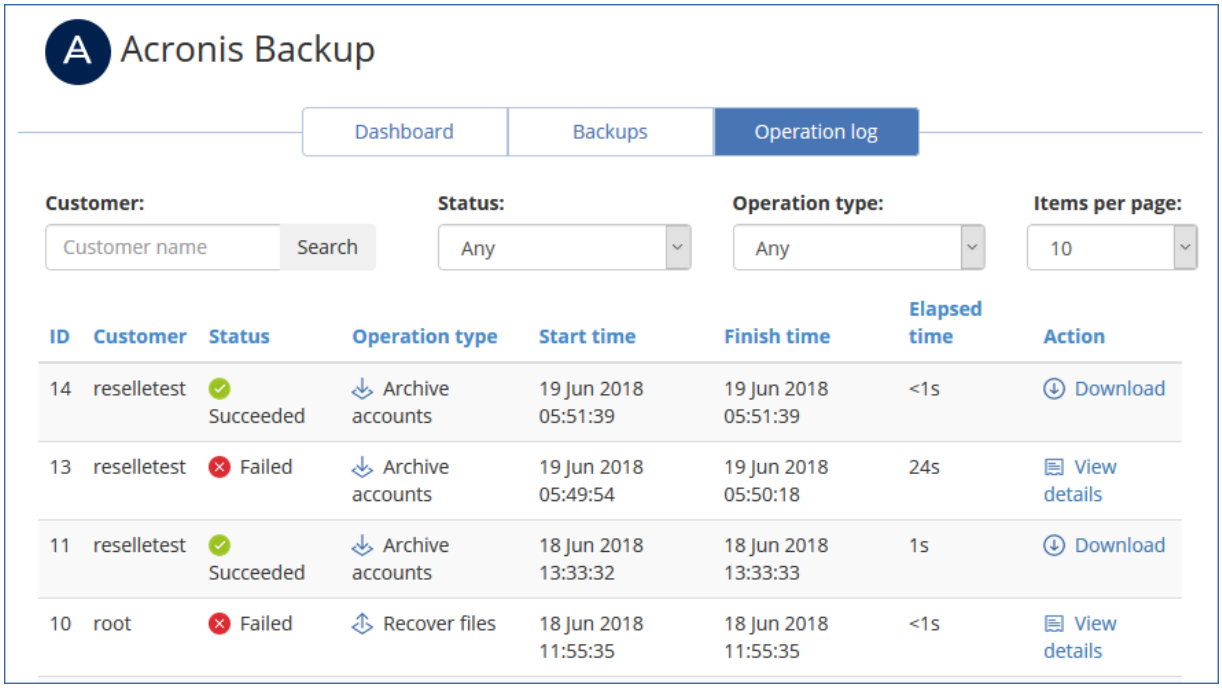
  Use this option to skip the recovery of files in the user home directory.

11 Tracking recovery progress

A cPanel user can see information about the recovery operations in the **Operation Log**. The log can be filtered by operation status and type. The log also contains download links for the download operations.



In the WHM UI, you can see the same information across all customers.



For detailed information about a failed operation, click **View details**. From there you can send the failure report so that the plugin vendor can improve the plugin in future versions. Please note that this option is not a call to support, if you need an assistance to solve the issue, please contact your service provider.

Recovery operations performed from the WHM and cPanel interfaces do not appear in the Acronis web console.

12 Appendix

12.1 Installing the backup agent on a Virtuozzo host

1. Log on to the host as the root user.
2. Run the installation file:

   `./Backup_Agent_for_Linux_x86_64.bin --register-with-credentials`

   *If you have enabled two-factor authentication (2FA) for your Acronis Cyber Cloud account, use the **`./Backup_Agent_for_Linux_x86_64.bin --token=%generated token%`** command instead. To obtain a registration token, use the instruction provided in the Installing the backup agent using a registration token (p. 17) section.*
3. Specify the credentials of the account to which the machine should be assigned.

   This account must be created within a customer tenant (Customer administrator, Unit administrator, or User). Do not specify the credentials of a partner administrator.
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

6. Open the */etc/Acronis/BackupAndRecovery.config* file and find the *Webcp* key.

This key determines whether backup is allowed for all containers, and whether backups of a container can be started on demand. By default, both options are set to "No".

- Set "*EnableBackupForAll*" = "Yes" if you want to make the backup service available for all cPanel containers.

  If *EnableBackupForAll* value is set to "No", you can enable backup for individual containers in the Acronis web console or using REST API. You will also need to create a backup plan that meets certain requirements described in the Configuring a backup plan for a cPanel server (p. 16) section.
- Set "*RunBackupForAll*" = "Yes" if you want to allow cPanel owners to run backups of a container on demand.

  If *RunBackupForAll* value is set to "No", backups of all containers (for which the backup is enabled) will run on the predefined schedule.

Example:

```
<key name="Webcp">
        <value name="EnableBackupForAll" type="TString">
              "Yes"
        </value>
        <value name="EnableWebcp" type="TString">
              "Yes"
        </value>
        <value name="RunBackupForAll" type="TString">
             "Yes"
        </value>
</key>
```

In a Virtuozzo cluster, the agent must be installed on each host registered in the cluster.

12.2 Configuring a backup plan for a cPanel server

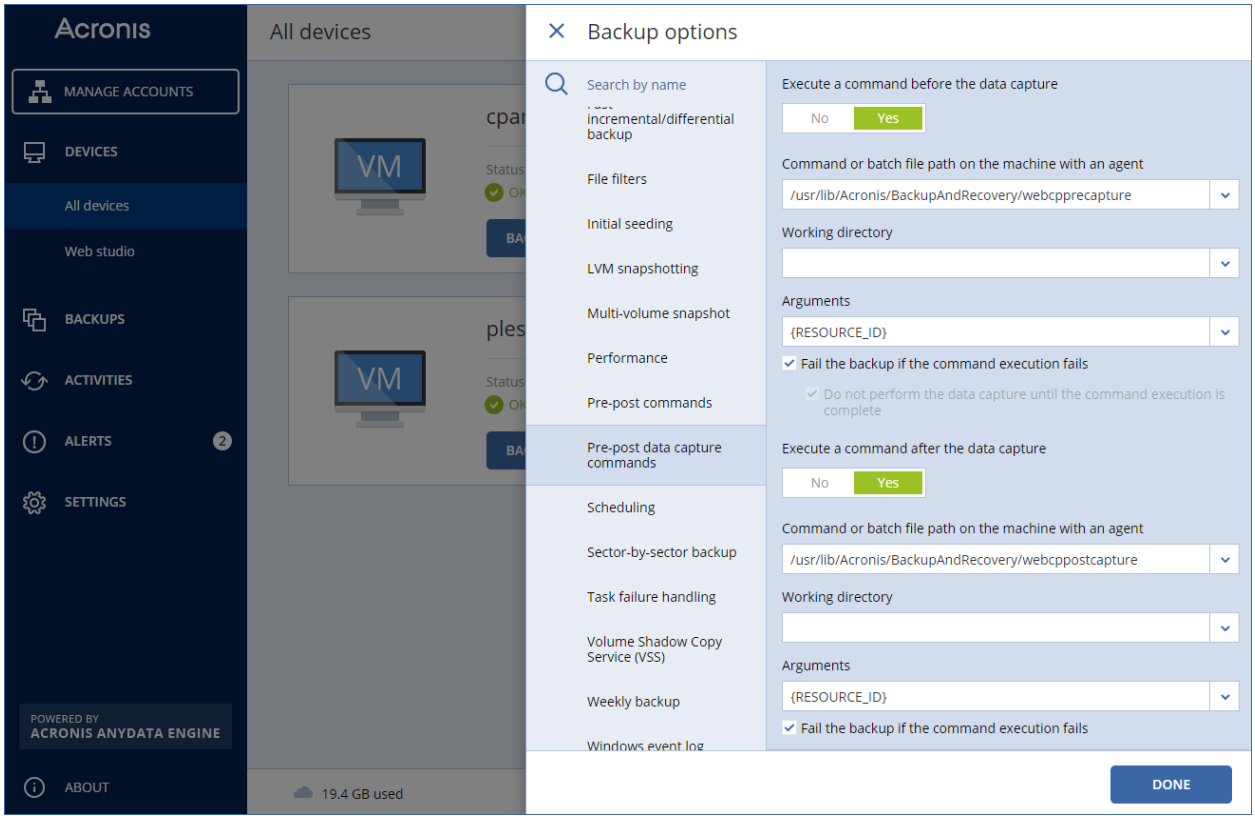
You can change parameters of the default backup plan or create a new plan for your cPanel server.

The backup plan must satisfy the following requirements:

1. It must back up the entire server or all volumes that contain cPanel data.
2. **Multi-volume snapshot** option must be enabled.
3. It must have **Pre-post data capture commands** configured:
   - Set **Execute a command before the data capture** to **Yes**
   - Set **Command or batch file path on the machine with an agent** to **/usr/lib/Acronis/BackupAndRecovery/webcpprecapture**
   - Leave **Working directory** empty
   - Set **Arguments** to **{RESOURCE_ID}**
   - Set **Fail the backup if the command execution fails** to **Yes**
   - Set **Execute a command after the data capture** to **Yes**

- Set **Command or batch file path on the machine with an agent** to **/usr/lib/Acronis/BackupAndRecovery/webcppostcapture**
- Leave **Working directory** empty
- Set **Arguments** to **{RESOURCE_ID}**
- Set **Fail the backup if the command execution fails** to **Yes**

4. Encryption can be enabled. For more information on the encryption options, please check the Acronis Backup guide.



12.3 Installing the backup agent using a registration token

1. To obtain a registration token, log in to the Acronis backup console with your credentials. Then go to **Devices** and click **Add**.
2. Scroll down to the **Registration token** section and click **GENERATE**.
3. Set up token lifetime if necessary, click **GENERATE TOKEN**, then click **COPY**.
4. Log on to the host as the root user.
5. Run the installation file, insert the registration token value generated earlier:
   `./Backup_Agent_for_Linux_x86_64.bin --token=%generated token%`
6. Select the respective check boxes for the agents that you want to install. The following agents are available:
   - Agent for Linux
7. Complete the installation procedure.
8. Troubleshooting information is provided in the following file:
   `/usr/lib/Acronis/BackupAndRecovery/HOWTO.INSTALL`

12.4 Unattended plugin configuration

1. Log on to the host as the root user.
2. If you haven't installed the plugin yet, run the following command:

   ```
   sh <(curl -L https://download.acronis.com/ci/cpanel/stable/install_acronis_cpanel.sh || wget -O - https://download.acronis.com/ci/cpanel/stable/install_acronis_cpanel.sh )
   ```

   Otherwise just skip this step.
3. Modify the following file:

   ```
   /usr/local/cpanel/base/3rdparty/acronisbackup/python/site-packages/acronis_backup_srv/bash_scripts/configurator.ini
   ```

Parameter name	Required	Value
acronis_cyber_cloud_login	YES	Tenant login name
acronis_cyber_cloud_password	YES	Tenant password
encryption_password	NO	This password will be used to create an encrypted backup plan for your machine. If empty – regular backup plan will be created, encryption will not be enabled.
encryption_type	NO	This parameter will be used to create an encrypted backup plan for your machine. Available values are: **aes256** **aes192** **aes128**
run_backup	YES	1 - run backup, 0 – do not run backup

Two-factor authentication (2FA) must be disabled while using unattended configuration script.

4. Run a script for unattended configuration:

   ```
   /usr/local/cpanel/base/3rdparty/acronisbackup/python/site-packages/acronis_backup_srv/bash_scripts/configurator.sh
   ```

   If your configuration file is located in another folder, use the following parameter:

   ```
   -c / --config
   ```

   to pass it to the script below:

   ```
   > ./configurator.sh -c=/DIR/configurator.ini
   > ./configurator.sh --config=/DIR/configurator.ini
   ```

   The following scenarios are supported:

   - If the backup agent is not installed, the script will:
     - Install the backup agent
     - Register the backup agent in Acronis Cyber Cloud
     - Apply encrypted or not backup plan (depending on the options, specified in the **configurator.ini** file) to the machine
     - Run the first backup (if **run_backup=1**)

- If the backup agent is installed, but not yet registered in Acronis Cyber Cloud, the script will:
  - Register the backup agent in Acronis Cyber Cloud and update it to the latest version, if necessary
  - Apply encrypted or not backup plan (depending on the options, specified in the **`configurator.ini`** file) to the machine
  - Run the first backup (if **`run_backup=1`**)
- If the backup agent is already both installed and registered in Acronis Cyber Cloud, the script will:
  - Apply standard backup plan to the machine. Encrypted backup plan can be created and applied only in case there were no suitable plans, applied to this machine before.
  - Run the first backup (if **`run_backup=1`**)

12.5 Advanced plugin configuration

A few configuration options are available for freezing MySQL, prior to taking a snapshot. These options are added to the following configuration file:

```
/var/lib/Acronis/AgentCommData/capture-data-config.sh
```

You can configure the below-listed parameters:

1. MYSQL_FREEZE
   - 0 - don't lock mysql tables before backup.
   - 1 - lock mysql tables before backup.

   If MYSQL_FREEZE is set to 1, databases will be switched to Read Only mode, while taking a snapshot to perform a backup in a consistent state. If this option is turned off, databases won't be locked during the backup and some data can be lost.
2. MYSQL_FREEZE_TIMEOUT
   - Specified in seconds.
3. MYSQL_FREEZE_SNAPSHOT_TIMEOUT
   - Specified in seconds.
4. MYSQL_FREEZE_ONLY_MYISAM
   - 0 - lock all tables before backup.
   - 1 - lock only MyISAM tables before backup.