

Acronis

[acronis.com](https://www.acronis.com)

Acronis Backup plugin for WHM and cPanel

Table of contents

1 System requirements	4
2 Obtaining the Acronis product	4
3 Installing the plugin	4
4 Installing the backup agent	4
5 Uninstalling the plugin	6
6 Backup	6
6.1 Enabling backup for a server	7
6.2 Running a backup on demand	8
6.3 Accessing the backup console	8
7 Enabling self-service for cPanel accounts	8
7.1 Setting up different service levels for cPanel accounts	8
8 Enabling self-service for WHM Resellers	10
9 Recovery in the cPanel UI	11
9.1 Downloading domains	11
9.2 Recovering domains to the original location	13
9.3 Downloading files	13
9.4 Recovering files to the original location	13
9.5 Downloading database dumps	14
9.6 Recovering databases to the original location	14
9.7 Recovering databases as new ones	14
9.8 Downloading mailboxes	15
9.9 Recovering mailboxes to the original location	15
9.10 Downloading mail filters	15
9.11 Recovering mail filters to the original location	15
9.12 Downloading mail forwarders	16
9.13 Recovering mail forwarders to the original location	16
9.14 Exporting the entire account	16
10 Recovering from WHM interface	16
10.1 Reverting a running cPanel server to a previous state	17
10.2 Options for recovering individual accounts via WHM UI	18
11 Tracking recovery progress	18
12 Appendix	19
12.1 Installing the backup agent on a Virtuozzo host	19
12.2 Configuring a backup plan for a cPanel server	21
12.3 Installing the backup agent using a registration token	22

12.4 Unattended plugin configuration	23
12.5 Advanced plugin configuration	26
Index	27

1 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.

2 Obtaining the Acronis product

An Acronis Cyber Cloud or Acronis WHM and cPanel 12.5 subscription is required to use the plugin.

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

To purchase an Acronis WHM and cPanel 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.

3 Installing the plugin

To install the Acronis WHM and cPanel 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.

4 Installing the backup agent

Note

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](#) section.

To install the backup agent:

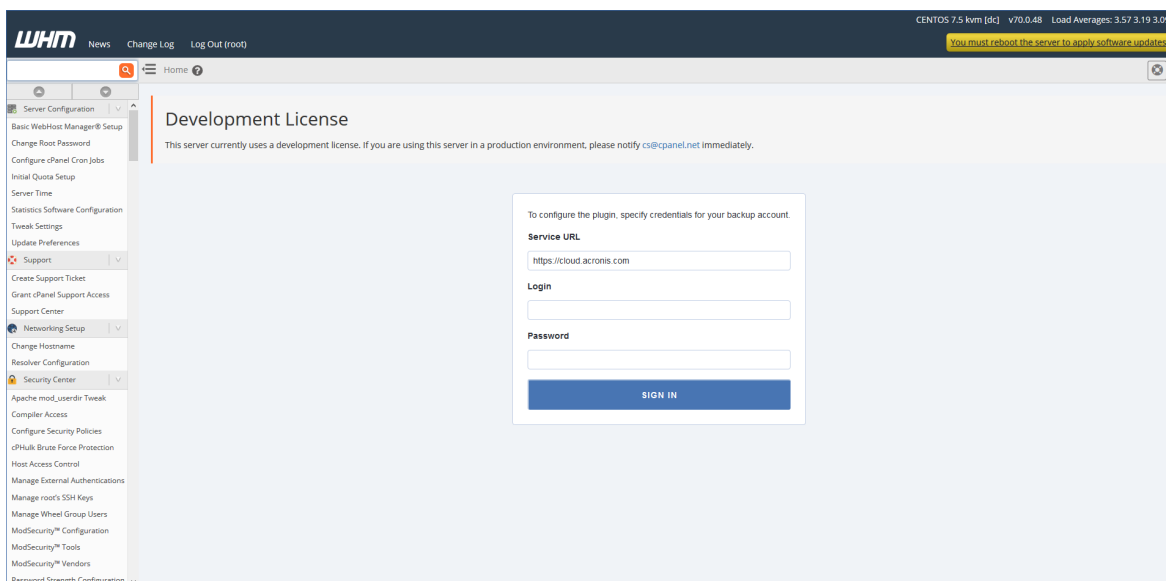
1. Log in to WHM UI.
2. Click **Plugins > Acronis WHM and cPanel** .

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

Note

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](#) 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.

Warning!

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.

Note

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.

Note

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>

5 Uninstalling the plugin

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

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

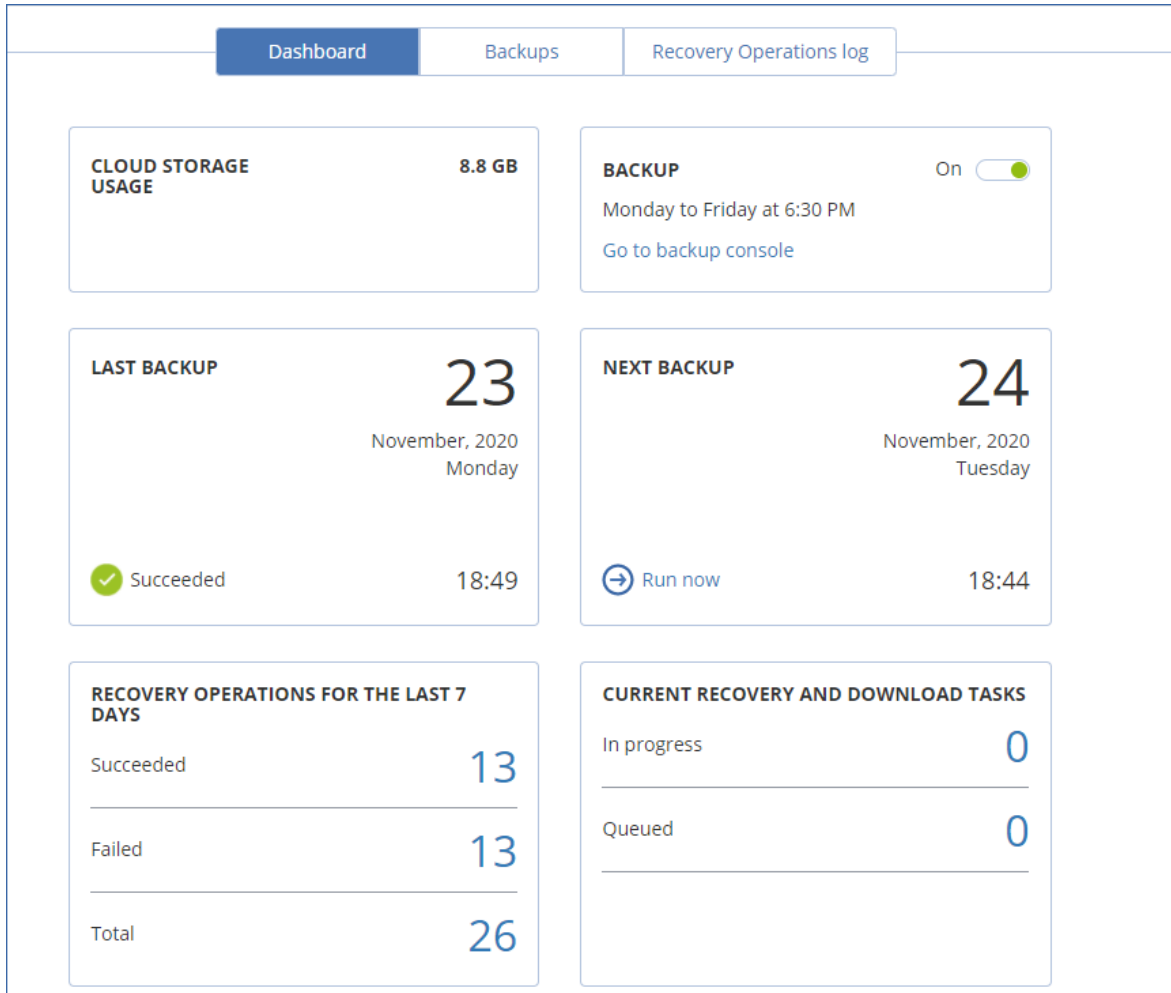
Removing the extension will also uninstall the backup agent from the cPanel server. The backup accounts you created and the backed-up data will be left intact.

6 Backup

The following operations are available in WHM UI.

6.1 Enabling backup for a server

1. Click **Plugins > Acronis WHM and cPanel** .
2. Enable the backup switch.



The screenshot displays the Acronis WHM and cPanel backup management interface. At the top, there is a navigation bar with three tabs: "Dashboard" (selected), "Backups", and "Recovery Operations log". Below the navigation bar, the interface is organized into several sections:

- CLOUD STORAGE USAGE:** Shows 8.8 GB usage.
- BACKUP:** Shows the backup status as "On" (indicated by a green toggle switch). The backup schedule is "Monday to Friday at 6:30 PM". A link "Go to backup console" is provided.
- LAST BACKUP:** Shows the last backup was on "23 November, 2020 Monday" at "18:49". The status is "Succeeded" (indicated by a green checkmark).
- NEXT BACKUP:** Shows the next backup is on "24 November, 2020 Tuesday" at "18:44". A "Run now" button (indicated by a blue arrow icon) is available.
- RECOVERY OPERATIONS FOR THE LAST 7 DAYS:** Shows a summary of recovery operations: Succeeded (13), Failed (13), and Total (26).
- CURRENT RECOVERY AND DOWNLOAD TASKS:** Shows the current status of recovery and download tasks: In progress (0) and Queued (0).

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

- Avoid configuring file or path exclusion rules in protection plans for entire machine backups. The mounting and recovery processes for such backups will be dramatically slow and might fail with a timeout error.
- Do not change the parameters described in "[Configuring a backup plan for a cPanel server](#)". 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.

6.2 Running a backup on demand

1. Click **Plugins > Acronis WHM and cPanel** .
2. Click **Run now**.

6.3 Accessing the backup console

1. Click **Plugins > Acronis WHM and cPanel** .
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.

7 Enabling self-service for cPanel accounts

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

7.1 Setting up different service levels for cPanel accounts

To enable different service levels for cPanel accounts, the WHM administrator needs to create plugin *features* to define the number of days, for which available recovery points will be shown in the cPanel user interface.

Note

For example, suppose that you have 3 cPanel accounts: **Account1**, **Account2**, **Account3**. You can create 3 features:

1. **Feature1**: to show recovery points created for the last day
2. **Feature2**: to show recovery points created for the last 14 days
3. **Feature3**: to show recovery points created for the last 30 days

If you assign **Feature1** to **Account1** in the WHM Feature manager, the corresponding cPanel account will see only recovery points created for the last day in its plugin UI. **Account2** with **Feature2** will be able to access recovery points created for the last 14 days, **Account3** with **Feature3** - recovery points created for the last 30 days.

There are two options to create plugin features:

1. Create all the features automatically during plugin configuration

Note

This option works only for the initial plugin installation and configuration. If the plugin is already installed and configured, use the second option - "Create WHM features manually" (p. 9).

- a. Log on to the host as a root user, then open:

```
/usr/local/cpanel/base/3rdparty/acronisbackup/srv/config.ini
```

- b. Add `enable_retention_service_plans = 1`

Note

If this option is enabled (`enable_retention_service_plans = 1`), but no features are created or set, recovery points will not be shown to any cPanel accounts on this server.

- c. Under the `[retention_service_plans]` section, add features like shown below:

```
acronisbackup_1 = 1
acronisbackup_14 = 14
acronisbackup_30 = 30
```

- d. Restart python service:

```
/usr/local/cpanel/base/3rdparty/acronisbackup/scripts/acronis-backup-srv.sh restart
```

- e. Perform plugin configuration as usual (refer to "Unattended plugin configuration" (p. 23)).

Note

The naming structure is obligatory: `acronisbackup_NUMBER = NUMBER`. Entering it in a different way will result in an error.

2. Create WHM features manually

- a. Log on to the host as a root user
- b. Run the following command:

```
vim /usr/local/cpanel/whostmgr/addonfeatures/acronisbackup_1
```

where **acronisbackup_1** is a file name for the feature.

- c. Add content as shown in the below example:

```
acronisbackup_1: Acronis Backup 1 Days Retention
```

The second part is a human readable name of the feature that the WHM admin will see in the Feature manager.

d. Open

```
/usr/local/cpanel/base/3rdparty/acronisbackup/srv/config.ini
```

e. Add `enable_retention_service_plans = 1`

f. Restart python service:

```
/usr/local/cpanel/base/3rdparty/acronisbackup/scripts/acronis-backup-srv.sh restart
```

3. To create a feature without limitations (all available recovery points will be visible), run the following:

```
vim /usr/local/cpanel/whostmgr/addonfeatures/acronisbackup_0
```

a. Add content as shown in the below example:

```
acronisbackup_0: Acronis Backup Unlimited
```

To assign created features to cPanel accounts:

1. In the WHM UI, click **Feature Manager**.
2. Select a feature list and click **Edit**.
3. Select a check box with the required feature name (for example - *Acronis Backup 30 Days Retention*).

Feature Manager

This interface allows you to enable and disable features and cPAddons in each user's cPanel. For more information, read the [documentation](#).

Default — The system grants cPanel users access to these features by default. If you disable a feature from this list, the system will disable it in every user's cPanel that uses that list.

Select all features for: default

Search

<input checked="" type="checkbox"/> TEST ARS @ Plugin	<input checked="" type="checkbox"/> Acronis Backup Plugin
<input type="checkbox"/> Acronis Backup 14 Days Retention Plugin	<input type="checkbox"/> Acronis Backup 3 Days Retention Plugin
<input checked="" type="checkbox"/> Acronis Backup 30 Days Retention Plugin	<input checked="" type="checkbox"/> Acronis Backup For Resellers Plugin
<input checked="" type="checkbox"/> Addon Domains	<input checked="" type="checkbox"/> Address Importer
<input checked="" type="checkbox"/> Agora Shopping Cart	<input checked="" type="checkbox"/> Aliases
<input checked="" type="checkbox"/> Analog Stats	<input checked="" type="checkbox"/> Apache Handlers

4. Click **Save**.

In case the plugin is uninstalled, all features will be removed automatically.

8 Enabling self-service for WHM Resellers

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

As a result, WHM Resellers with the selected feature list assigned, will be able to browse, download and recover all the objects belonging to cPanel accounts under them.

Note

By default this option is not enabled. After plugin upgrade to version 1.6, WHM Resellers will not be able to access its functionality until the corresponding feature is enabled for the required feature lists.

Features for different service levels, described in "Enabling self-service for WHM Resellers" (p. 10) can be also assigned to WHM Reseller accounts.

Note

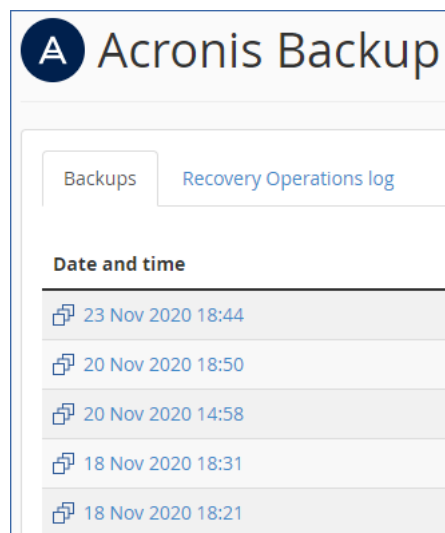
Features assigned to WHM Reseller accounts don't affect the service levels of its cPanel accounts. Only features assigned to cPanel accounts directly affect their service level.

9 Recovery in the cPanel UI

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

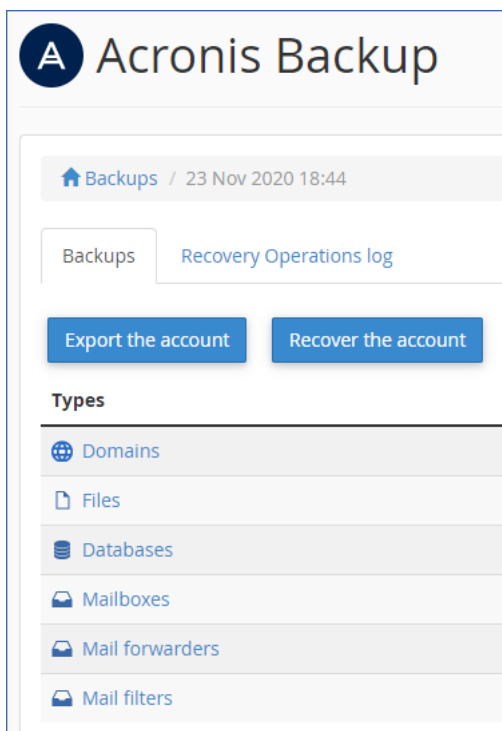
9.1 Downloading domains

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

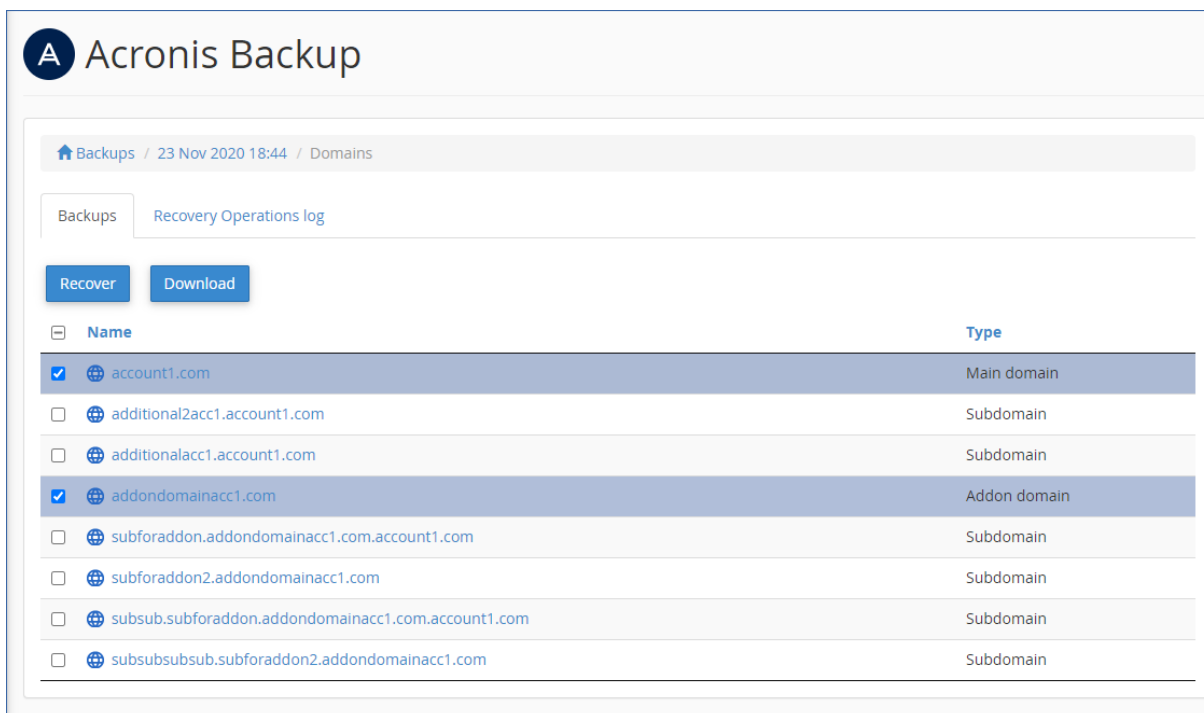


3. Select a recovery point.

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



4. Click **Domains**.
5. Select the domains to download.



6. Click **Download**.

As a result, a .zip archive with the selected domains content is prepared and placed into your home folder.

9.2 Recovering domains to the original location

1. Click **Acronis Backup**.
2. Open the **Backups** tab.
3. Select a recovery point.
4. Click **Domains**.
5. Select the domains to recover.
6. Click **Recover**.

As a result, selected domains are recovered to the original location. All existing files are overwritten.

If a domain no longer exists, it is recreated automatically.

9.3 Downloading files

1. Click **Acronis WHM and cPanel**.
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**.

9.4 Recovering files to the original location

1. Click **Acronis WHM and cPanel**.
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.

9.5 Downloading database dumps

1. Click **Acronis WHM and cPanel**.
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.

9.6 Recovering databases to the original location

1. Click **Acronis WHM and cPanel**.
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.

9.7 Recovering databases as new ones

1. Click **Acronis WHM and cPanel**.
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.

9.8 Downloading mailboxes

1. Click **Acronis WHM and cPanel**.
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.

9.9 Recovering mailboxes to the original location

1. Click **Acronis WHM and cPanel**.
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.

9.10 Downloading mail filters

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

9.11 Recovering mail filters to the original location

1. Click **Acronis WHM and cPanel**.
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.

9.12 Downloading mail forwarders

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

9.13 Recovering mail forwarders to the original location

1. Click **Acronis WHM and cPanel**.
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.

9.14 Exporting the entire account

1. Click **Acronis WHM and cPanel**.
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

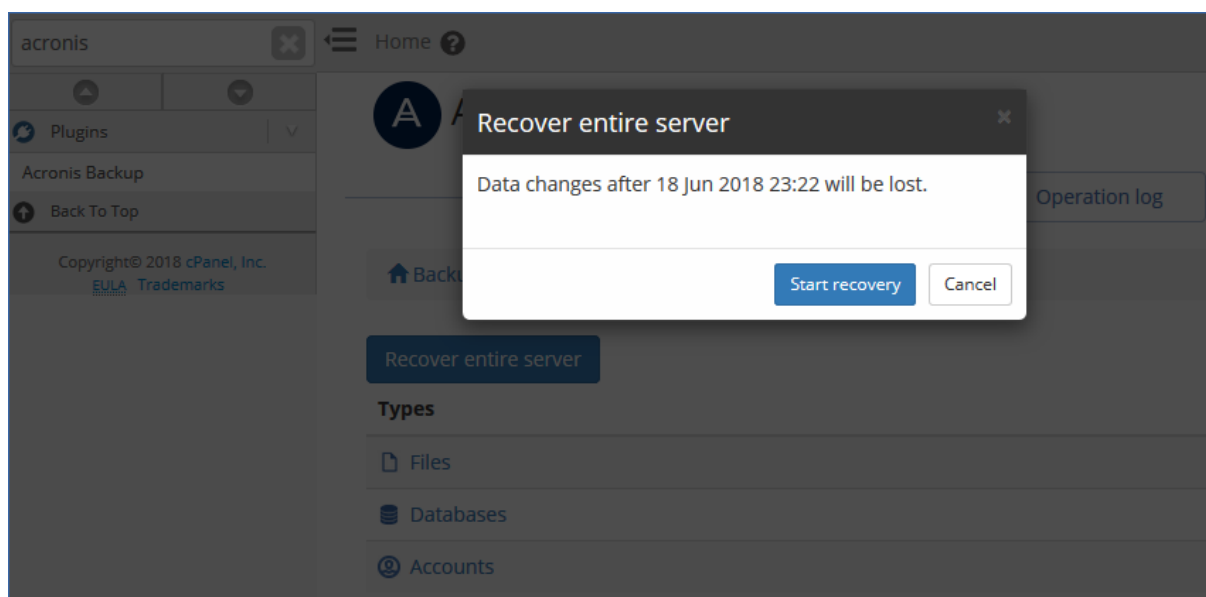
The recovery is similar to what is described in [Recovery in the cPanel UI](#). The differences are as follows:

- 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](#).
- WHM Resellers can access their own files as well as files of cPanel accounts belonging to them. They cannot recover the entire server or change any settings, which require root privileges on the server.

10.1 Reverting a running cPanel server to a previous state

1. Click **Plugins > Acronis WHM and cPanel**.
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.

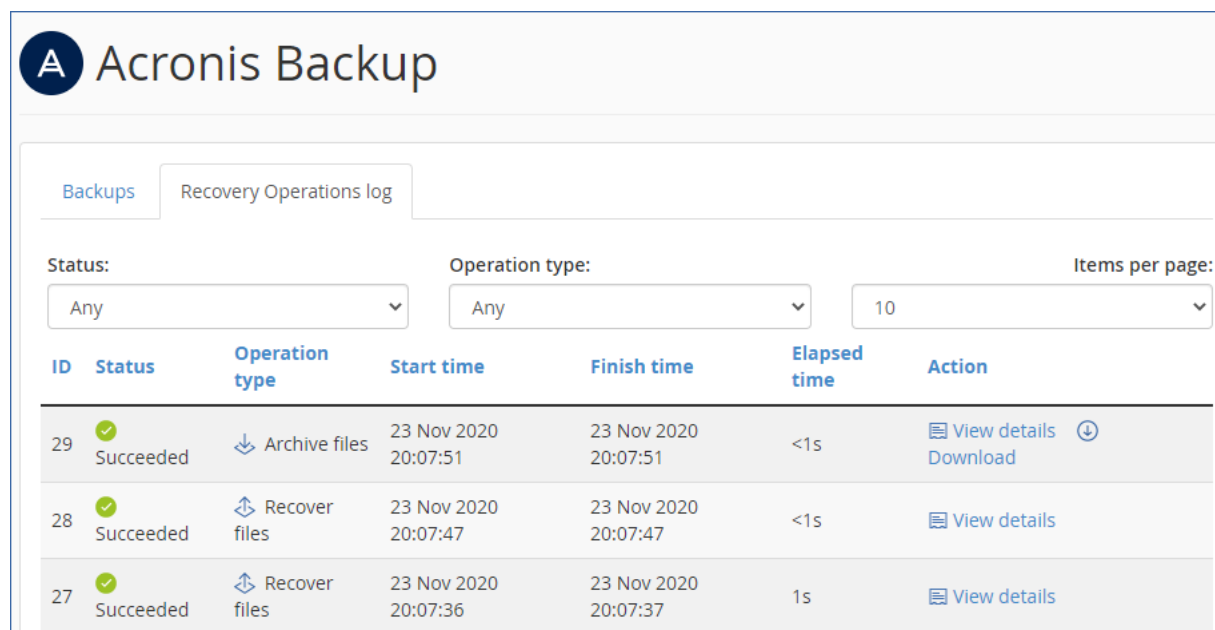
10.2 Options for recovering individual accounts via WHM UI

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 **Recovery Operations log**. The log can be filtered by operation status and type. The log also contains download links for the download operations.



The screenshot shows the Acronis Backup interface with the 'Recovery Operations log' tab selected. It features a table with columns for ID, Status, Operation type, Start time, Finish time, Elapsed time, and Action. The table contains three rows of log entries, all with a 'Succeeded' status. The first row (ID 29) shows an 'Archive files' operation with a download link. The second (ID 28) and third (ID 27) rows show 'Recover files' operations.

ID	Status	Operation type	Start time	Finish time	Elapsed time	Action
29	Succeeded	Archive files	23 Nov 2020 20:07:51	23 Nov 2020 20:07:51	<1s	View details Download
28	Succeeded	Recover files	23 Nov 2020 20:07:47	23 Nov 2020 20:07:47	<1s	View details
27	Succeeded	Recover files	23 Nov 2020 20:07:36	23 Nov 2020 20:07:37	1s	View details

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

ID	Customer	Status	Operation type	Start time	Finish time	Elapsed time	Action
29	account1	✔ Succeeded	↓ Archive files	23 Nov 2020 20:07:51	23 Nov 2020 20:07:51	<1s	View details Download
28	account1	✔ Succeeded	↕ Recover files	23 Nov 2020 20:07:47	23 Nov 2020 20:07:47	<1s	View details
27	account1	✔ Succeeded	↕ Recover files	23 Nov 2020 20:07:36	23 Nov 2020 20:07:37	1s	View details
26	root	✔ Succeeded	↕ Recover accounts	23 Nov 2020 19:58:23	23 Nov 2020 19:59:38	1m 15s	View details
25	root	✔ Succeeded	↕ Recover accounts	23 Nov 2020 18:17:48	23 Nov 2020 18:18:45	57s	View details
24	root	✘ Failed	↕ Recover accounts	23 Nov 2020 18:12:37	23 Nov 2020 18:13:45	1m 8s	View details

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
```

Note

If you have enabled two-factor authentication (2FA) for your Acronis Cyber Cloud account, use the following command instead:

```
./Backup_Agent_for_Linux_x86_64.bin --token=%generated token%
```

To obtain a registration token, use the instruction provided in the [Installing the backup agent using a registration token](#) 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 VirtuozzoAgent 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](#) 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

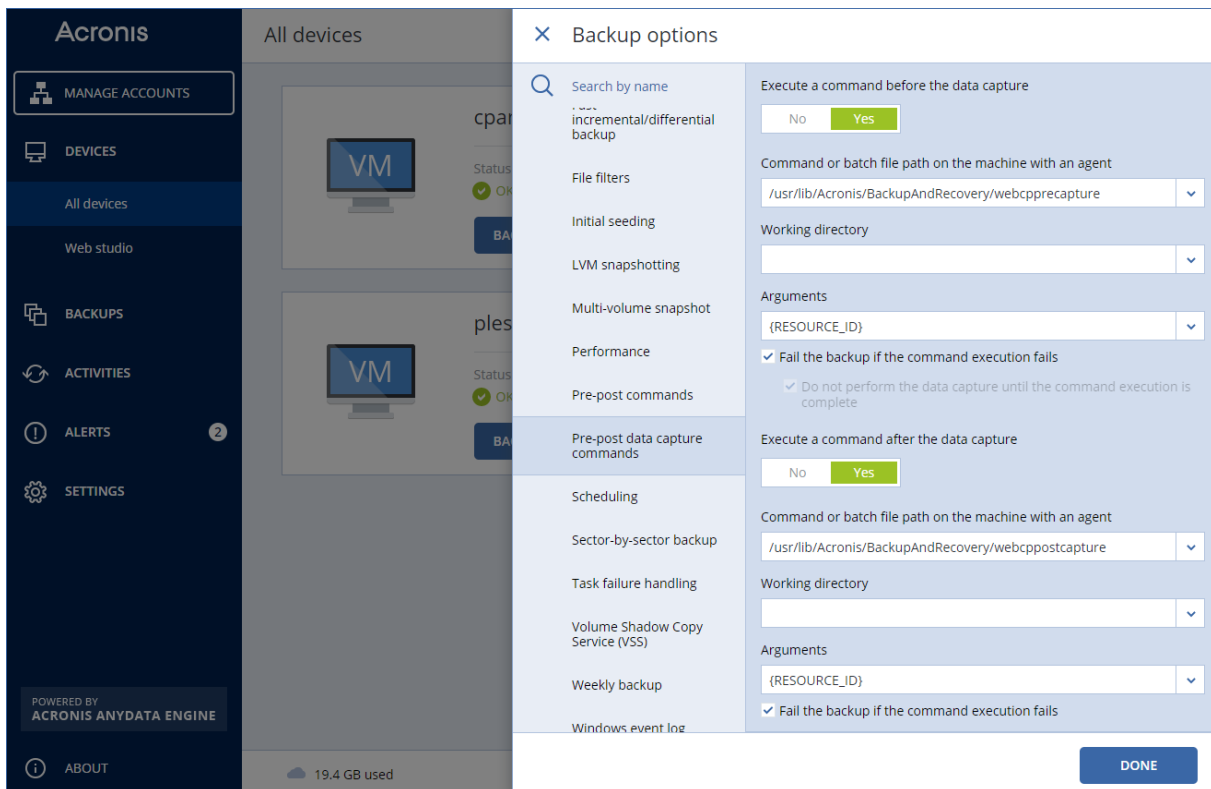
You can change parameters of the default backup plan or create a new plan for your cPanel server.

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](#).

Note

If you are setting up a new plan from the backup console or adjusting any parameters of an existing one, then such plan cannot be recalled or modified by a plugin anymore. It doesn't affect backups execution or restoration process for administrator as well as end user accounts.



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/lib/python3.8/site-packages/acronis_backup_srv/bash_scripts/configurator.ini
```

Parameter name	Required	Value
acronis_cyber_cloud_url	OPTIONAL	Acronis Cyber Cloud DC address, used together with Client ID and Client secret. You don't need to provide it in case you are using tenant login and password. Example: <code>acronis_cyber_cloud_url = https://eu2-cloud.acronis.com</code>
acronis_cyber_cloud_login	YES	Tenant login name
acronis_cyber_cloud_password	YES	Tenant password
acronis_cyber_cloud_client_id	OPTIONAL	Your API client ID
acronis_cyber_cloud_client_secret	OPTIONAL	Your API client secret
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
enable_backup	YES	1 – assign and enable backup plan, 0 – do not assign backup plan
run_backup	YES	1 - run backup, 0 – do not run backup
retention_number_of_backups	OPTIONAL	Integer. Specify number of backups to keep.

retention_days	OPTIONAL	Integer. Specify how long to keep backups created by the backup plan.
retention_weeks	OPTIONAL	Integer. Specify how long to keep backups created by the backup plan.
retention_months	OPTIONAL	Integer. Specify how long to keep backups created by the backup plan.
backup_start_hours	OPTIONAL	Integer. Specify when the backup will be started.
backup_start_minutes	OPTIONAL	Integer. Specify when the backup will be started. If left empty, will be automatically set to 00.
backup_start_delay_window	OPTIONAL	String value containing single pair of integer and suffix "m" or "h", e.g. 30m or 5h
re-attempts	OPTIONAL	Integer. Specify number of times to re-execute the backup task in case of failure.
re-attempt_period	OPTIONAL	String value. Specify time period between individual re-attempts, indicated by a single pair of integer values and 'h' or 'm' suffix, e.g. 43m or 3h.
alert_period	OPTIONAL	Integer. Specify number of days without a single successful backup, after which the "No successful backups for a specified number of consecutive days" alert will be triggered.

Note

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

4. If you would like to enable different service levels for cPanel accounts, open the following file:

```
/usr/local/cpanel/base/3rdparty/acronisbackup/srv/config.ini
```

- a. Add `enable_retention_service_plans = 1`

Otherwise just skip this step and follow the instructions under the next "Run a script for unattended configuration:" (p. 25).

Note

If this option is enabled (`enable_retention_service_plans = 1`), but no features are created or set, recovery points will not be shown to any cPanel accounts on this server.

- b. Under the `[retention_service_plans]` section, add features as shown below:

```
acronisbackup_1 = 1
acronisbackup_14 = 14
acronisbackup_30 = 30
```

Note

You can specify a desired number of days here, but note that the naming structure is obligatory: `acronisbackup_NUMBER = NUMBER`. Entering it in a different way will result in an error.

- c. Restart python service:

```
/usr/local/cpanel/base/3rdparty/acronisbackup/scripts/acronis-backup-srv.sh restart
```

Note

If you want to add new features after the plugin has been installed and configured, refer to the instructions provided in the "Setting up different service levels for cPanel accounts" (p. 8) section.

5. Run a script for unattended configuration:

```
/usr/local/cpanel/base/3rdparty/acronisbackup/python/lib/python3.8/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.inifile`) 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

1. In case you have configured custom location for MySQL data on the server, use the `data_folder_path` parameter under the `[mysql]` section in `/usr/local/cpanel/base/3rdparty/acronisbackup/srv/config.ini` to specify it:

```
[mysql]
data_folder_path = %path%
```

2. 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.

Index

A

- Accessing the backup console 8
- Advanced plugin configuration 26
- Appendix 19

B

- Backup 6

C

- Configuring a backup plan for a cPanel server 21

D

- Downloading database dumps 14
- Downloading files 13
- Downloading mail filters 15
- Downloading mail forwarders 16
- Downloading mailboxes 15

E

- Enabling backup for a server 7
- Enabling self-service for cPanel accounts 8
- Exporting the entire account 16

I

- Installing the backup agent 4
- Installing the backup agent on a Virtuozzo host 19
- Installing the backup agent using a registration token 22
- Installing the plugin 4

O

- Obtaining the Acronis product 4
- Options for recovering individual accounts via WHM UI 18

R

- Recovering databases as new ones 14
- Recovering databases to the original location 14
- Recovering files to the original location 13
- Recovering from WHM interface 16
- Recovering mail filters to the original location 15
- Recovering mail forwarders to the original location 16
- Recovering mailboxes to the original location 15
- Recovery in the cPanel UI 11
- Reverting a running cPanel server to a previous state 17

- Running a backup on demand 8

S

- System requirements 4

T

- To install the backup agent 4
- Tracking recovery progress 18

U

- Unattended plugin configuration 23

Uninstalling the plugin 6