

Acronis Backup plugin for cPanel & WHM

Table of contents

System requirements	4
Supported cPanel & WHM configurations	4
Supported database servers	4
Supported operating systems	4
Supported hypervisors	4
Installation, update and uninstallation	5
Installing the plugin	5
Updating the plugin	5
Installing and updating the protection agent	5
Uninstalling the plugin and the agent	6
Deployment in Virtuozzo Hybrid Server environment	6
Installing the protection agent on a Virtuozzo Hybrid Server host	7
Configuring the protection agent on a Virtuozzo Hybrid Server host	8
Installing and configuring the plugin	8
Configuration	10
Configuring in the plugin dashboard	10
Configuring in the Cyber Protect console	11
Unattended plugin configuration	11
Backup	15
Enabling and disabling backup for the server	15
Changing backup settings	16
Hosting control panel protection plan	16
Enabling self-service for cPanel accounts	18
Setting up different service levels for cPanel accounts	18
Enabling self-service for WHM Resellers	21
Recovery in the cPanel UI	22
Downloading domains	22
Recovering domains to the original location	24
Downloading files	24
Recovering files to the original location	24
Downloading database dumps	25
Recovering databases to the original location	25
Recovering databases as new ones	25
Downloading mailboxes	26
Recovering mailboxes to the original location	26

Downloading mail filters	26
Recovering mail filters to the original location	27
Downloading mail forwarders	27
Recovering mail forwarders to the original location	27
Exporting the entire account	27
Recovering from WHM interface	28
Reverting a running cPanel server to a previous state	28
Options for recovering individual accounts via WHM UI	29
Tracking recovery progress	30
Appendix	32
Installing the backup agent using a registration token	32
Unattended plugin configuration	32
Advanced plugin configuration	35
Specifying a custom MySQL location	35
Customizing database freeze before the snapshot	35
Forcing unmount of idle recovery points	36
Specifying a custom TMP directory	37
Forcing unmount of idle recovery points	37
Index	39

System requirements

Supported cPanel & WHM configurations

- cPanel & WHM version 11.102 or later
- PHP version 5.6 or later

Supported database servers

- MySQL 5.7 or later
- MariaDB 10.3.17 or later

Note

Backup and recovery of remote database servers is not supported.
Granular recovery of PostgreSQL databases is not supported.

Supported operating systems

The integration has been tested on the following operating systems supported by cPanel & WHM:

- AlmaLinux OS 8
- CentOS 7
- CloudLinux 6, 7 and 8
- Red Hat Enterprise Linux 7
- Ubuntu 20.04 LTS

For a full list of the operating systems, supported by the protection agent, refer to the [Acronis Cyber Protect Cloud documentation](#).

Supported hypervisors

- For a full list of virtualization platforms, supported by the protection agent, refer to the [Acronis Cyber Protect Cloud documentation](#).
- Agentless backup of the cPanel & WHM application is supported only for Virtuozzo Hybrid Server 7.5 containers.
- To back up cPanel & WHM running in a Virtuozzo container, both the Agent for Linux and the Agent for Virtuozzo must be installed on the host.

Installation, update and uninstallation

Installing the plugin

You can install or update the plugin on a cPanel server via the command-line interface by following these steps:

1. Log in to the cPanel server as a system administrator or root user.
2. Open the terminal on the server.
3. Execute the following command in the terminal:

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

This command will download and run the installation script. The installation script will install the latest stable version of the plugin automatically. Additionally, it will register the Stable plugin repository on the system for further plugin updates via **yum** or **apt** utilities.

If you want to participate in the Early Access Program (EAP) and install the latest version from the Current Update Channel, download the installation script from https://download.acronis.com/ci/cpanel/install_acronis_cpanel.sh and run it as follows:

```
sh install_acronis_cpanel.sh -c current
```

For detailed information about the Early Access Program, see <https://kb.acronis.com/content/72513>.

Updating the plugin

To update the Acronis Backup plugin for cPanel & WHM, run the following commands in the terminal:

RPM format

```
yum update acronis-backup-cpanel
```

DEB format

```
sudo apt update  
sudo apt upgrade acronis-backup-cpanel
```

Installing and updating the protection agent

The plugin requires the protection agent to be installed in order to perform backup and recovery operations.

In the mainstream scenario, the protection agent will be installed and registered as part of the [plugin configuration procedure](#). However, you have the option to manually install and register the protection agent or automate the procedure via the command-line interface.

For detailed instructions on alternative protection agent installation options, refer to:

- [Installing protection agents in Linux](#)
- [Unattended installation or uninstallation in Linux](#)

The protection agent can be updated either manually or automatically, depending on your preferences. It may have flexible configurations such as release channels and maintenance windows. For more details on updating and configuring the protection agent, see [Updating agents](#).

Uninstalling the plugin and the agent

Upon removal of the plugin, the protection agent will also be uninstalled from the server and unregistered from the Cyber Protect console. However, due to using the `--no-purge` key to call the protection agent uninstaller, the association between the server, its protection plan and the backup chain will be preserved.

Upon re-installation, the protection agent will be further protected with the same plan and the backup chain will remain consistent.

To uninstall the Acronis Backup plugin for cPanel & WHM, run the following command in the terminal:

RPM format

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

DEB format

```
sudo apt remove acronis-backup-cpanel
```

Check how to uninstall the agent without removing the plugin:

- [Uninstalling agents](#)
- [Unattended installation or uninstallation in Linux](#)

Deployment in Virtuozzo Hybrid Server environment

The integration supports backup and recovery of cPanel servers that reside on Virtuozzo Hybrid Server. If you are planning to deploy in this way, there are some specifics to keep in mind:

1. The protection agent must be installed on the Virtuozzo Hybrid Server host, not inside the container itself.
2. If you have a Virtuozzo cluster, the protection agent must be installed on each host, registered on the cluster.

3. To ensure proper integration, the plugin must be installed within each container that has the cPanel control panel installed, following the standard plugin installation procedure.
4. You can install the agent before or after installing the plugin, but you cannot do this from the plugin.
5. As an additional security measure, you will need to provide your Acronis account credentials in the plugin or using the `create_agent_client.py` script, explained further in this document.
6. If you plan to protect all or multiple containers with a single protection plan, you will need to create one in the Cyber Protect console or using RESTful API and assign this protection plan to each container. The plugin is only capable of creating individual protection plans.

Note

The plugin does not support two-factor (2FA) authentication at this time. If you have 2FA enabled, you can register the agent and the plugin using a [service account](#) or an [API Client](#). Alternatively, you can register the plugin using the `create_agent_client.py` script.

Installing the protection agent on a Virtuozzo Hybrid Server host

To install the protection agent in unattended mode, refer to [Unattended installation or uninstallation in Linux](#).

1. Log in to the host machine as a system administrator or root user.
2. Download the protection agent installation file to the host machine. See [Downloading protection agents](#).
3. Navigate to the installation file directory, make the file executable and then run it.

```
chmod +x ./Backup_Agent_for_Linux_x86_64.bin
./Backup_Agent_for_Linux_x86_64.bin --register-with-credentials
```

If two-factor authentication (2FA) is enabled for your account, use the following command instead:

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

To obtain a registration token, use the instructions from [Installing the protection agent using a registration token](#).

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

Note

Make sure to use the credentials of an account that belongs to a customer group, such as Customer administrator, Unit administrator or Protection User. Avoid using partner administrator credentials.

5. Select the checkboxes for the components to install:
 - Agent for Linux
 - Agent for Virtuozzo

6. Complete the installation procedure.

Configuring the protection agent on a Virtuozzo Hybrid Server host

After you install the protection agent on a Virtuozzo Hybrid Server host, make sure to update the `/etc/Acronis/BackupAndRecovery.config` file as described here. Otherwise, the plugin will not be able to connect to the agent.

- Set **EnableWebcp** to **Yes** to allow the agent to communicate with the plugin.
- [Optional] Set **EnableBackupForAll** to **Yes** if you want to allow cPanel administrators to enable and disable backup of a container from the plugin dashboard. Otherwise, the **Backup** toggle on the dashboard will be deactivated.
- [Optional] Set **RunBackupForAll** to **Yes** to allow cPanel administrators to run backups of a container on demand from the plugin dashboard. Otherwise, the **Backup now** button on the dashboard will be deactivated.

```
<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>
```

Installing and configuring the plugin

Use the standard installation and configuration flows to set up plugins on the per-container basis:

- [Installing and updating the Acronis Backup plugin for cPanel & WHM](#)
- [Configuring the plugin through the dashboard](#)

If you want to automate the registration of the plugin inside a container, you can use the [create_agent_client.py](#) script. This script will generate an agent client in the specified or all containers (if you do not specify the list explicitly) and register it in the Cyber Protect service.

Note

The cPanel control panel and the plugin must be installed in the containers for the operation to complete.

The script has the following syntax:

```
create_agent_client.py (--username=LOGIN|--client-id=API_CLIENT) (--password-
file=PASSWORD_FILE|--secret-file=API_SECRET) [--container-id=CT1,CT2,CT3]
```


<code>--username=LOGIN</code>	Username for authentication with Acronis Cyber Protect Cloud. Only one of these is required: <code>--username</code> or <code>--client-id</code> .
<code>--username=LOGIN</code>	Username for authentication with Acronis Cyber Protect Cloud. Only one of these is required: <code>--username</code> or <code>--client-id</code> .
<code>--client-id=API_CLIENT</code>	Client ID for authentication with Acronis Cyber Protect Cloud. Only one of these is required: <code>--username</code> or <code>--client-id</code> .
<code>--password-file=PASSWORD_FILE</code>	File that contains the password. Only one of these is required: <code>--password-file</code> or <code>--secret-file</code> .
<code>--secret-file=API_SECRET</code>	File that contains the Client Secret. Only one of these is required: <code>--password-file</code> or <code>{{ --secret-file }}</code> .
<code>--container-id=CT1,CT2,CT3</code>	[Optional] ID of the container to process. Multiple container IDs can be provided, separated by commas. If not defined, all containers will be processed.

The `create_agent_client.py` script supports two-factor authentication (2FA) in the interactive mode. Make sure to specify the same credentials that were used to install the protection agent.

Configuration

Once the plugin has been installed, you can proceed with its configuration and registration.

Even if you have already installed and registered the protection agent, you must still enter credentials to your Acronis account in the plugin as an additional security measure.

You can apply the default configuration by following the simple [configuration wizard](#) within the plugin.

For automation purposes and in order to apply a custom protection policy, you can use the [unattended configuration option](#).

Every time you configure the protection plan from within the plugin, the Cyber Protection service automatically creates an [individual protection plan](#) under your user account for each workload. This plan is associated with a specific workload and cannot be assigned to any other workloads. This approach ensures that each server has an isolated backup environment and prevents other workloads from being affected in the event of a compromise.

If you want a protection plan to protect multiple cPanel servers, create a regular protection plan in the Cyber Protection console and assign those workloads to it. However, any modifications to a protection plan shared by multiple servers can only be made in the Cyber Protection console.

Note

The plugin does not support two-factor (2FA) authentication at this time. If you have 2FA enabled, you can register the agent and the plugin using a [service account](#) or an [API Client](#).

Configuring in the plugin dashboard

Follow the steps below to configure the Acronis Backup plugin in the cPanel panel:

1. Log in to the WHM interface as an administrator.
2. Navigate to **Plugins > Acronis Backup**.
3. Specify the credentials of your Acronis Cyber Protect Cloud account, to which you want to assign the machine.

Note

Make sure to use the credentials of an account that belongs to a customer group, such as Customer administrator, Unit administrator, or Protection User. Avoid using partner administrator credentials.

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

Note

Once a backup plan is created and applied, you cannot modify the encryption settings. To use different encryption settings, you will need to create a new backup plan in the Acronis Cyber Protect Cloud console.

Note

If you lose or forget the encryption password, you won't be able to recover the encrypted backups.

5. Follow the installation wizard.
6. During the installation, the software checks if the ports required for communication with the cloud platform are open. If any of the ports are closed, the software will display their numbers and the corresponding host names, for which each port should be open. Open the required ports, close the wizard, and restart the installation.

After completing the above steps, the plugin will install and register the protection agent and create an [individual protection plan](#) with the default backup settings.

You can [modify the protection plan parameters in the Cyber Protection console](#) or use the [unattended configuration option](#) to make changes.

Configuring in the Cyber Protect console

The following procedure is only applicable to regular protection plans that are intended to be shared by multiple machines. Individual protection plans are created for specific resources via integration and cannot be assigned to other resources.

The procedure is as follows:

1. [Install a protection agent](#) on the machine.
2. Create a control panel-aware protection plan in the Cyber Protect console.
3. [Apply the newly created protection plan](#) to the machine.
4. Install and register the plugin.

Unattended plugin configuration

When configuring the plugin in unattended mode, the following tasks will be performed, depending on the current state of the plugin and the protection agent:

- Installing the protection agent or updating it to the latest version.
- Registering the protection agent and the plugin in the Cyber Protection console.
- Creating an [individual protection plan](#), based on the settings, provided in the corresponding configuration file as long as there is no control panel-aware protection plan, assigned to the machine.
- Running the first backup, if specified in the configuration file.

- Modifying the protection plan parameters, according to the settings in the respective configuration file.

Note

The plugin currently does not support two-factor (2FA) authentication. If you have 2FA enabled, you can register the agent and the plugin using a [service account](#) or an [API Client](#).

To configure the plugin in unattended mode, follow these steps:

1. Log in to the cPanel server as a system administrator or root user.
2. Depending on whether the plugin is installed:
 - If you have not installed the plugin yet, open the server terminal and run the below 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)
```

- If you have already installed the plugin, just skip this step.
3. Modify the configuration.ini file, located at:

```
/usr/local/cpanel/base/3rdparty/acronisbackup/python/lib/python3.8/site-packages/acronis_backup_srv/bash_scripts/configurator.ini
```

The following parameters are available:

PARAMETER NAME	REQUIRED	VALUE
acronis_cyber_cloud_url	NO	Acronis Cyber Protect 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: acronis_cyber_cloud_url = https://eu2-cloud.acronis.com
acronis_cyber_cloud_login	YES	User login
acronis_cyber_cloud_password	YES	User password
acronis_cyber_cloud_client_id	NO	Your API client ID
acronis_cyber_cloud_client_secret	NO	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.

PARAMETER NAME	REQUIRED	VALUE
encryption_type	NO	This parameter will be used to create an encrypted backup plan for your machine. Available values are: aes128 aes256 aes192
retention_number_of_backups	NO	Integer. Specify number of backups to keep.
retention_days	NO	Integer. Specify how long to keep backups, created by the backup plan.
retention_weeks	NO	Integer. Specify how long to keep backups, created by the backup plan.
retention_months	NO	Integer. Specify how long to keep backups, created by the backup plan.
backup_start_hours	NO	Integer. Specify when the backup will be started.
backup_start_minutes	NO	Integer. Specify when the backup will be started. If left empty, will be automatically set to 00.
backup_start_delay_window	NO	String value, containing a single pair of integer and "m" or "h" suffix, e.g. 30m or 5h
re-attempts	NO	Integer. Specify number of times to re-execute the backup task in case of failure.
re-attempt_period	NO	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	NO	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.
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

4. Run the script for unattended configuration located at:

```
/usr/local/cpanel/base/3rdparty/acronisbackup/python/lib/python3.8/site-packages/acronis_backup_srv/bash_scripts/configurator.ini
```

If your configuration file is located in another folder, use the following parameter to pass the path to the script:

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

For example:

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

Backup

Only the server administrator has permission to manage backups on the web hosting server. Resellers and end users can only access and restore their data if the self-service recovery feature is available for their accounts.

The protection plan, assigned to the web hosting server, defines its backup policy.

To perform a web hosting server backup, you need a [protection plan with a specific configuration](#). If you don't have the required protection plan, granular recovery in the control panel interface will not work.

For the same reasons, it is important not to apply web hosting server protection plans to other workload types because they will not work and will not be suitable for the task.

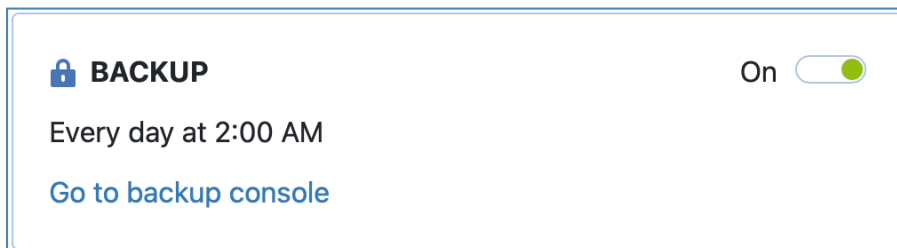
Enabling and disabling backup for the server

By default, an [individual protection plan](#) with predefined settings is automatically created and assigned when configuring the plugin through the control panel's user interface. Depending on the chosen configuration method, a customized protection plan can be assigned or this step can be entirely skipped.

While most operations related to protection plans are only available in the Cyber Protect console, the plugin's dashboard allows for a quick option to disable or enable backup for the server.

To change the backup status, follow these steps:

1. Navigate to **Plugins > Acronis Backup > Dashboard**.
2. Switch the **Backup** toggle button to **ON** or **OFF** mode.



When the toggle is turned OFF, the plugin will disable the execution of all hosting control panel protection plans currently assigned to this server. When the toggle is turned ON, the plugin will enable the execution of all hosting control panel plans currently assigned to the server.

If the server does not have any hosting control panel protection plans assigned to it, turning the toggle ON will create and assign an individual protection plan with the default settings.

Note

In plugin versions prior to 1.8.0, disabling the backup would cause the plan to be revoked from the server, whereas enabling backup would cause a randomly selected hosting control panel plan to apply to the server if several compatible plans were found.

Changing backup settings

By default, the protection plan created upon plugin configuration is set up to run a backup once every 24 hours at 2 AM local server time. However, you can modify this and other default settings using the Cyber Protect console, the unattended plugin configuration script, or the [RESTful public API](#).

For more information on how to change backup settings, refer to the following help pages:

- [Editing a protection plan](#)
- [Unattended plugin configuration](#)
- [Managing protection plans and policies](#)

Regardless of the approach you choose, ensure that you do not alter the parameters, described in [Hosting control panel protection plan](#). Doing so will prevent granular recovery in the control panel interface from working.

Hosting control panel protection plan

When creating or modifying a protection plan to back up a hosting control panel, make sure that it meets the requirements and recommendations outlined below. Otherwise, granular recovery of the control panel object will not work.

1. It must back up the entire server or all volumes that contain control panel data.
2. It must have Pre-post data capture commands, configured as follows:
 - 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**

3. Avoid configuring file or path exclusion rules. The mounting and recovery processes for such backups will slow down dramatically and might fail with a timeout error.

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**.

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. 19).

- 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. 32)).

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
```

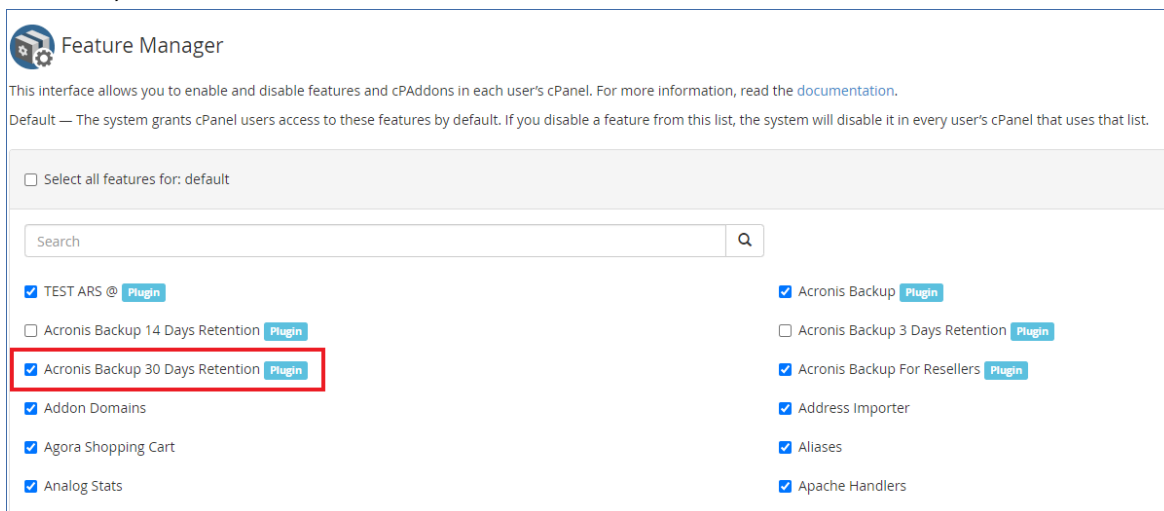
3. To create a feature without limitations (all available recovery points will be visible), run the following:

```
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 @ <small>Plugin</small>	<input checked="" type="checkbox"/> Acronis Backup <small>Plugin</small>
<input type="checkbox"/> Acronis Backup 14 Days Retention <small>Plugin</small>	<input type="checkbox"/> Acronis Backup 3 Days Retention <small>Plugin</small>
<input checked="" type="checkbox"/> Acronis Backup 30 Days Retention <small>Plugin</small>	<input checked="" type="checkbox"/> Acronis Backup For Resellers <small>Plugin</small>
<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.

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. 21) 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.

Recovery in the cPanel UI

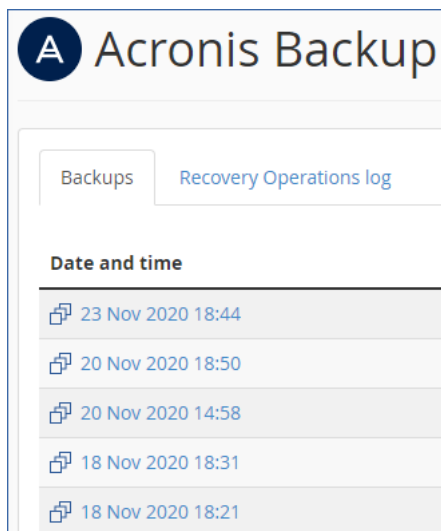
Accounts with the Acronis WHM and cPanel privilege enabled can browse backups in their cPanel interface and download or recover domains, files, folders, databases, mailboxes, mail filters and forwarders as well as entire accounts.

Note

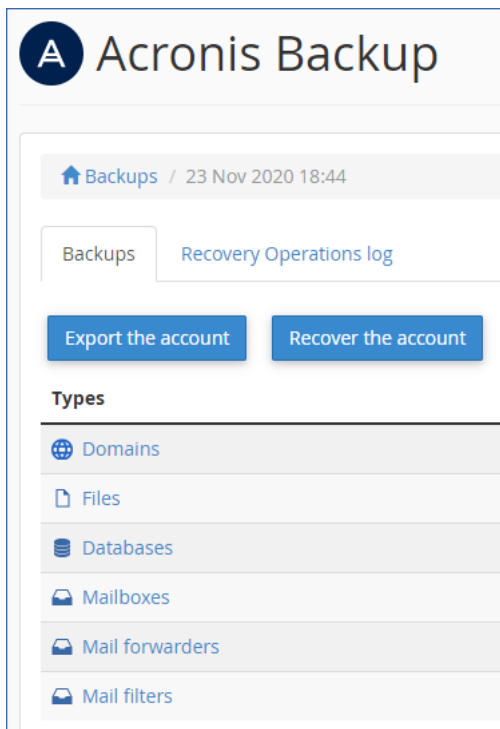
Custom DNS records, associated with the hosting service domains, are not retained after account recovery.

Downloading domains

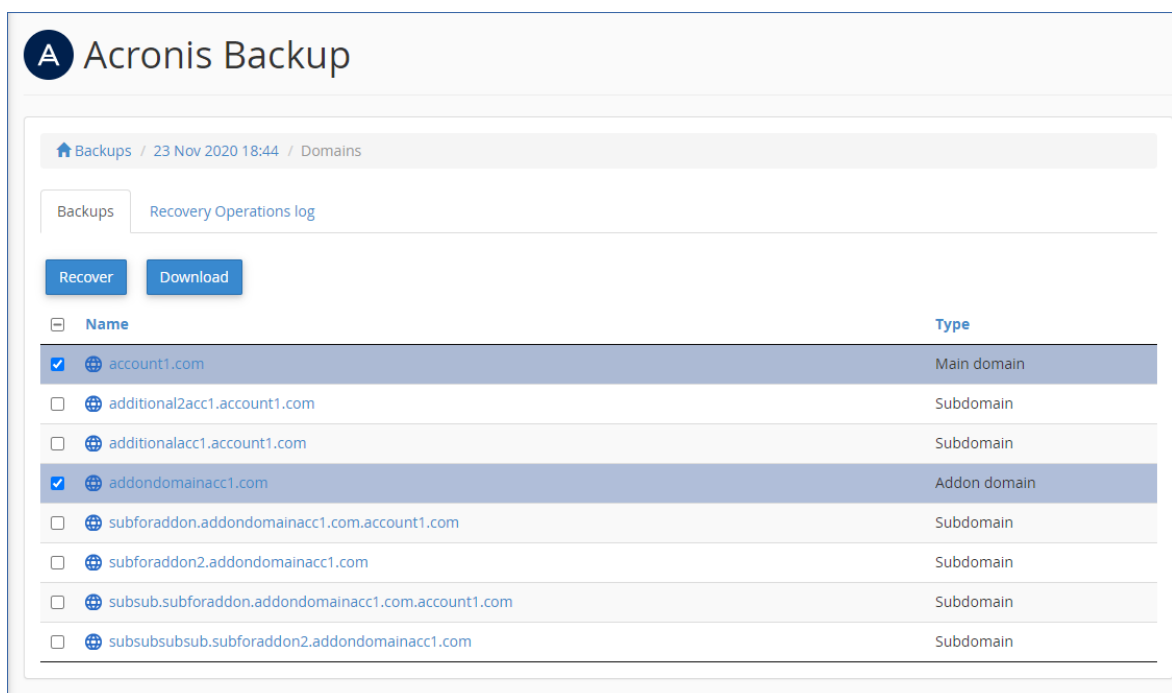
1. Click **Acronis Backup**.
2. Open the **Backups** tab.



3. Select a recovery point.
The corresponding backup is then mounted to the cPanel server. This 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.

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, the selected domains are recovered to their original location. All existing files are overwritten.

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

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**.

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.

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.

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. Make sure that the **Add suffix to the recovered database name** check box is cleared.
7. [Optional] Select to restore database users.
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.

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.

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.

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.

Note

When recovering a maildir mailbox, you can choose to either keep or delete emails created after the backup. For mbox mailboxes, it is only possible to overwrite the entire mailbox, and all emails created after the backup will be lost as a result of the operation.

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**.

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.

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**.

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.

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.

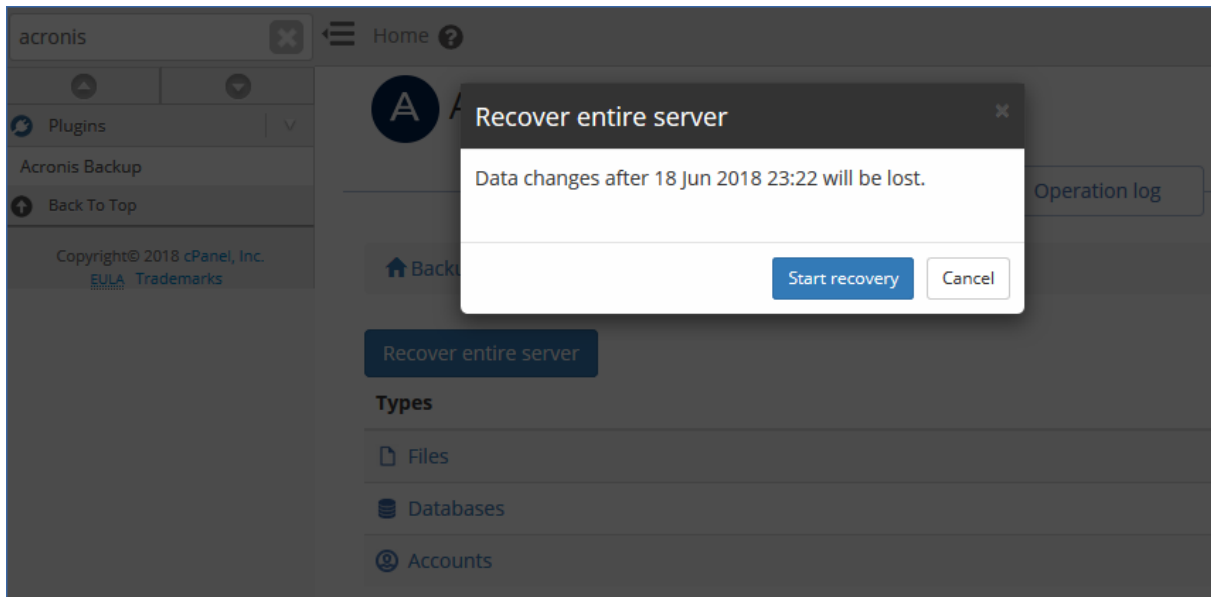
Recovering from WHM interface

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.

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.

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.

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.

A

Acronis Backup

Backups

Recovery Operations log

Status:

Any

Operation type:

Any

Items per page:

10

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.

A

Acronis Backup

Dashboard

Backups

Recovery Operations log

Customer:

Customer name

Search

Status:




















Any

Operation type:

Any

Items per page:

10

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.

Appendix

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
```

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: acronis_cyber_cloud_url = https://eu2-cloud.acronis.com

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. 34).

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. 18) 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`)

Advanced plugin configuration

Specifying a custom MySQL location

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%
```

Customizing database freeze before the snapshot

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.

Forcing unmount of idle recovery points

Every time users access a recovery point inside a backup archive, this point gets mounted to the system. Then recovery points may fail to unmount automatically due to specifics of how the WHM and cPanel internal tools interact with the mount points.

On a system where a lot of users access recovery points frequently, such issue may cause significant resource consumption.

You can configure the plugin to forcibly unmount idle recovery points at certain intervals of time.

1. Locate and open the following file:

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

2. Navigate to the [app] section.

3. Add the below parameter:

```
[app]
...
clean_idle_devices=true
```

4. For the changes to take effect, restart the python service with the following command:

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

This setting will instruct the plugin to scan mount points every 5 minutes and forcibly unmount the recovery points that haven't been addressed for the past 30 minutes.

Additionally, you can fine-tune the setting to change the check interval to more than 5 minutes (which must be a multiple of 5 minutes, e.g., 5, 10, 15 minutes, etc.) as well as the idle time before unmounting.

All values are defined in seconds.

```
[app]
...
clean_idle_devices = true
clean_idle_devices_interval = 600
purge_mounts_idle_timeout = 3600
```

Specifying a custom TMP directory

The plugin needs temporary storage space on the local drive to accomplish recovery operations. By default, the temporary directory is a folder inside the plugin's installation directory.

You can define a custom location for the temporary directory by modifying the value of the `tmp_path` parameter in the `/usr/local/cpanel/base/3rdparty/acronisbackup/srv/config.ini` file.

In addition to that, you can change the default location for the backup archive mount points by modifying the value of `mms_mountpoint_path` in the `/usr/local/cpanel/base/3rdparty/acronisbackup/srv/config.ini` file.

Note

For the sake of unification, the values above override the values of the `ACRONIS_MOUNT_DIR` and `ACRONIS_MOUNT_TMP_DIR` parameters in the `/usr/lib/Acronis/system_libs/config` file. The change applies automatically upon the restart of the plugin service.

Important

If you have enabled a jailed shell environment for users to connect to a server via SSH, make sure that they do **not** have read and write access to the temporary directory.

Forcing unmount of idle recovery points

Every time users access a recovery point inside a backup archive, this point gets mounted to the system. Then recovery points may fail to unmount automatically due to specifics of how the WHM and cPanel internal tools interact with the mount points.

On a system where a lot of users access recovery points frequently, such issue may cause significant resource consumption.

You can configure the plugin to forcibly unmount idle recovery points at certain intervals of time.

1. Locate and open the following file:

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

2. Navigate to the `[app]` section.
3. Add the below parameter:

```
[app]
...
clean_idle_devices=true
```

4. For the changes to take effect, restart the python service with the following command:

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

This setting will instruct the plugin to scan mount points every 5 minutes and forcibly unmount the recovery points that haven't been addressed for the past 30 minutes.

Additionally, you can fine-tune the setting to change the check interval to more than 5 minutes (which must be a multiple of 5 minutes, e.g., 5, 10, 15 minutes, etc.) as well as the idle time before unmounting.

All values are defined in seconds.

```
[app]
...
clean_idle_devices = true
clean_idle_devices_interval = 600
purge_mounts_idle_timeout = 3600
```

Index

A

Advanced plugin configuration 35

Appendix 32

B

Backup 15

C

Changing backup settings 16

Configuration 10

Configuring in the Cyber Protect console 11

Configuring in the plugin dashboard 10

Configuring the protection agent on a Virtuozzo
Hybrid Server host 8

Customizing database freeze before the
snapshot 35

D

Deployment in Virtuozzo Hybrid Server
environment 6

Downloading database dumps 25

Downloading domains 22

Downloading files 24

Downloading mail filters 26

Downloading mail forwarders 27

Downloading mailboxes 26

E

Enabling and disabling backup for the
server 15

Enabling self-service for cPanel accounts 18

Enabling self-service for WHM Resellers 21

Exporting the entire account 27

F

Forcing unmount of idle recovery points 36-37

H

Hosting control panel protection plan 16

I

Installation, update and uninstallation 5

Installing and configuring the plugin 8

Installing and updating the protection agent 5

Installing the backup agent using a registration
token 32

Installing the plugin 5

Installing the protection agent on a Virtuozzo
Hybrid Server host 7

O

Options for recovering individual accounts via
WHM UI 29

R

Recovering databases as new ones 25

Recovering databases to the original
location 25

Recovering domains to the original location 24

Recovering files to the original location 24

Recovering from WHM interface 28

Recovering mail filters to the original
location 27

Recovering mail forwarders to the original location 27

Recovering mailboxes to the original location 26

Recovery in the cPanel UI 22

Reverting a running cPanel server to a previous state 28

S

Setting up different service levels for cPanel accounts 18

Specifying a custom MySQL location 35

Specifying a custom TMP directory 37

Supported cPanel & WHM configurations 4

Supported database servers 4

Supported hypervisors 4

Supported operating systems 4

System requirements 4

T

Tracking recovery progress 30

U

Unattended plugin configuration 11, 32

Uninstalling the plugin and the agent 6

Updating the plugin 5