acronis.com

Acronis Backup plugin for DirectAdmin

Integration with DirectAdmin

Integration Guide

REVISION: 7/5/2023

Table of contents

Solution overview

Acronis Cyber Protect Cloud integrates with the DirectAdmin hosting control panel, allowing administrators to back up the entire DirectAdmin server and restore individual web hosting accounts and associated data as well as recover the entire server in the event of a disaster.

This integration also provides self-service recovery options for end users, with the ability to set up different service levels, which is a great opportunity for web hosting providers to enhance their service offerings.

The integration includes a native plugin for seamless integration into the control panel's user interface, allowing administrators and end users to perform granular recovery or download of individual DirectAdmin accounts, files, folders, mailboxes, domains and databases.

System requirements and limitations

Supported DirectAdmin configurations

- DirectAdmin version 1.62.0 or later
- PHP version 7.4 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.

Supported operating systems

The integration has been tested on the following operating systems, supported by DirectAdmin:

- Almalinux 8
- Red Hat Enterprise Linux 7
- Red Hat Enterprise Linux 8
- RockyLinux 8
- Ubuntu 20.04 LTS

Note
The Debian operating system is currently not supported.

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 DirectAdmin application is supported only for Virtuozzo Hybrid Server 7.5 containers.
- To back up DirectAdmin 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 and updating the Acronis Backup plugin for DirectAdmin

You can install and update the Acronis Backup plugin for DirectAdmin on your server through either the command-line interface or the graphical user interface of DirectAdmin.

Once the installation process is complete, proceed with registering and configuring the plugin.

Installation and update via the DirectAdmin Plugin Manager

To install the plugin:

1. Log in to the DirectAdmin panel as an administrator.
2. Navigate to **Menu** > **Extra Features** > **Plugin Manager**.
3. Click **Add Plugin**.
4. Choose your preferred upload method: URL or File.
5. Depending on the choice in the previous step, either paste the URL or upload the plugin package file. The URL with the latest plugin version is https://download.acronis.com/ci/directadmin/stable/acronis-directadmin-stable/acronisbackup.tar.gz.
6. Select the **Install after upload** checkbox.
7. Enter your DirectAdmin password.
8. Click **Install**.

To update the plugin using the auto-update option:

1. Log in to the DirectAdmin panel as an administrator.
2. Navigate to **Menu** > **Extra Features** > **Plugin Manager**.
3. Find the Acronis Backup plugin in the list of installed plugins.
4. Click the **Update** button next to the plugin.
5. Enter your DirectAdmin password and click **Confirm**.

The DirectAdmin Plugin Manager will automatically download and install the latest stable version of the plugin.

To update the plugin using the manual update option:

You can also update the plugin manually by following the installation instructions listed above. The Plugin Manager will detect that the Acronis Backup plugin is already installed and will replace the old version with the new one.

Note

Replacing an already installed package with an earlier version is strongly discouraged, even though the DirectAdmin Plugin Manager allows it. Doing so may cause inconsistencies between the plugin code and the internal database, potentially leading to service disruptions.

Installation and update via the the command-line interface

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

1. Log in to the DirectAdmin server as a system administrator or root user.
2. Open the terminal on the server.
3. Copy and paste the following command into the terminal:

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

4. This command will download and run the installation script. The installation script will install the latest stable version of the plugin automatically.

This method is particularly useful for automation scenarios.

Early Access Program

The Early Access Program provides users with the opportunity to test new features and ensure their compatibility with their existing setup before the updates are made available to the entire production fleet.

For detailed information about the Early Access Program, please refer to https://kb.acronis.com/content/72508.

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 the following help pages:

- 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, refer to the Updating agents help page.

Uninstalling the agent and the plugin

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 protection plan and the backup chain will remain consistent.

To uninstall the Acronis Backup plugin for DirectAdmin:

1. Log in to the DirectAdmin panel as an administrator.
2. Navigate to **Menu** > **Extra Features** > **Plugin Manager**.
3. Use the **+** button next to Acronis Backup.
4. Click **Delete**.

If you need to uninstall the agent without removing the plugin, follow the next help pages:

- Uninstalling agents
- Unattended installation or uninstallation in Linux

Deployment in Virtuozzo Hybrid Server environment

The integration supports backup and recovery of DirectAdmin 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 DirectAdmin 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

Note

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
   ```

   Note

   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 DirectAdmin 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 DirectAdmin 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

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

- Installing and updating the Acronis Backup plugin for DirectAdmin
- 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 containers or all containers (if you do not specify the list explicitly) and register it in the Cyber Protect service.

Note

Please note that the DirectAdmin 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]
```

--username=LOGIN	Username for authentication with Acronis Cyber Protect Cloud. Only one of these is required: --username or --client-id.
--username=LOGIN	Username for authentication with Acronis Cyber Protect Cloud. Only one of these is required: --username or --client-id.

--client-id=API_CLIENT	Client ID for authentication with Acronis Cyber Protect Cloud. Only one of these is required: --username or --client-id.
--password-file=PASSWORD_FILE	File that contains the password. Only one of these is required: --password-file or --secret-file.
--secret-file=API_SECRET	File that contains the Client Secret. Only one of these is required: --password-file or --secret-file.
--container-id=CT1,CT2,CT3	[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 DirectAdmin 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 DirectAdmin panel:

1. Log in to the DirectAdmin panel as an administrator.
2. Navigate to **Menu** > **Extra Features** > **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.

Warning!

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 required ports 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 DirectAdmin 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/directadmin/stable/install_acronis_directadmin.sh
     || wget -O - https://download.acronis.com/ci/directadmin/stable/install_acronis_
     directadmin.sh)
     ```

   - If you have already installed the plugin, just skip this step.

3. Modify the configuration.ini file, located at:

   ```
   /usr/local/directadmin/plugins/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	OPTIONAL	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	OPTIONAL	Your API client ID
acronis_cyber_cloud_client_ secret	OPTIONAL	Your API client

Parameter name	Required	Value
		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: aes128 aes256 aes192
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

Parameter name	Required	Value
		when the backup will be started. If left empty, will be automatically set to 00.
backup_start_delay_window	OPTIONAL	String value, containing a single pair of integer and "m" or "h" suffix, e.g. 30m or 5h
reattempts	OPTIONAL	Integer. Specify number of times to re-execute the backup task in case of failure.
reattempt_period	OPTIONAL	String value. Specify time period between individual reattempts, 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.
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/directadmin/plugins/acronisbackup/python/lib/python3.8/sitepackages/
   acronis_backup_srv/bash_scripts/configurator.sh
   ```

   If your configuration file is located in another folder, use the following parameter to pass the patch 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.

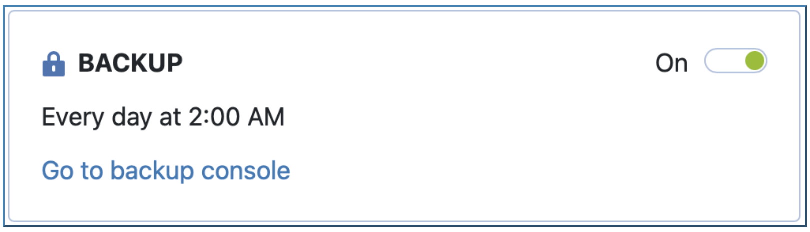
Enabling and disabling backup for the server

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 **Menu** > **Extra Features** > **Acronis Backup** > **Dashboard**.
2. Switch the **Backup** toggle button to **ON** or **OFF** mode.



BACKUP

Every day at 2:00 AM

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 1.2.0, 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 the Hosting control panel protection plan section. 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 recovery self-service for DirectAdmin users

The administrator enables self-service recovery per User Package together with other hosting settings like bandwidth, storage space, etc.

When enabling self-service recovery for a User Package, the administrator can limit recovery point exposure.

1. Log in to DirectAdmin as an administrator.
2. Navigate to the **Menu**.
3. Click **Account Manager**.
4. Click **Manage User Packages**.
5. Select the required package.
6. Select the **Acronis Backup** check box.
7. (Optional) Define the number of days for which available recovery points will be shown to end users in the DirectAdmin user interface.
8. (Optional) Use the **Acronis Backup Limit** field to set a limit on the exposed recovery points like number of days in the past.
9. Click **Save**.

As a result, end users with this package assigned will be able to access the Acronis Backup plugin from the DirectAdmin user interface. They will be able to browse through their own backed-up data and restore or download individual DirectAdmin objects such as the account, domains, databases, mailboxes, etc.

If the limit on the recovery points exposure has been set up, end users assigned with this package will be able to access backups for a limited number of past days defined in the plan.

The total number of recovery points available to the administrator or users with other packages will not be affected.

Recovery

The Acronis Backup plugin for DirectAdmin allows administrators and end users with self-service recovery enabled to restore and download individual DirectAdmin objects, including DirectAdmin user accounts, domains, databases, files, folders and mailboxes.

The administrator can access all users' data whereas end users' access is limited to their account only.

Additionally, the administrator is entitled to recover the entire server with all data in case of a disaster.

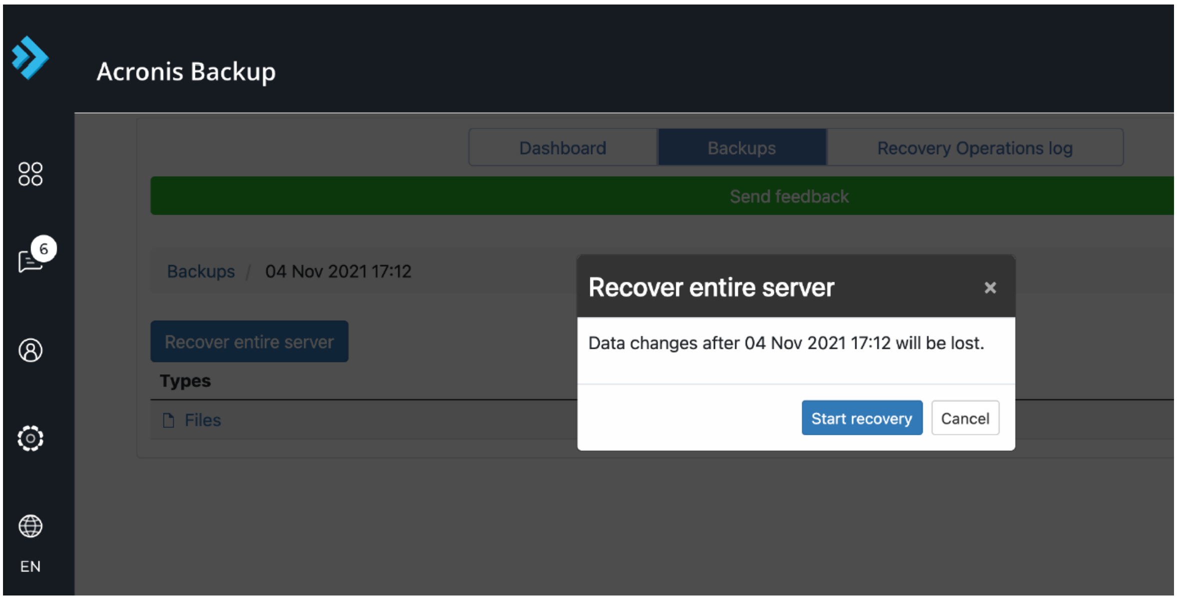
Notes for DirectAdmin server administrators

- When a user requests to download DirectAdmin objects, they are placed in the /usr/local/directadmin/plugins/acronisbackup/restored_data folder and are stored there for seven days by default.
- Download and recovery operations may require temporary local storage space to complete. The default location is the following folder : /usr/local/directadmin/plugins/acronisbackup/srv/tmp It can be changed by modifying the value of the tmp_path variable in the below file: /usr/local/directadmin/plugins/acronisbackup/srv/config.ini

Recover an entire server

This functionality is available to DirectAdmin administrators only.

1. Go to **Menu** > **Extra Features** > **Acronis Backup**.
2. Open the **Backups** tab.
3. Select a recovery point.
4. Click **Recover entire server** and confirm.



Data changes after 04 Nov 2021 17:12 will be lost.

The entire server will be then reverted to the selected recovery point. All changes made after the backup will be lost.

The progress of the operation can be tracked from the Acronis Cyber Protect Cloud console.

If DirectAdmin is not available as a result of the server failure, recover the server using the Acronis Cyber Protect console or Acronis bootable media.

Exporting and recovering accounts by the administrator

1. Log into the **DirectAdmin** panel.
2. Go to **Menu** > **Extra Features** > **Acronis Backup**.
3. Open the **Backups** tab.
4. Select a recovery point.
5. Click **Users.**
6. Select the accounts that need to be downloaded or recovered.
7. Click the corresponding action button: **Recover** or **Download**.
8. (Optional) Select **Skip export of databases** and **Skip export of home directory** check boxes.

In case of accounts download, a download link to the selected accounts will be available in the notification bar and in the **Operations log**.

In case of accounts recovery, the selected accounts will be restored to the state from the backup.

When recovering or downloading individual accounts from the admin interface, the following options can be configured:

- **Skip recovery/download of databases** - to omit the recovery of databases
- **Skip recovery/download of home directory** - to bypass the recovery of files in the user home directory.

Exporting and recovering the account by the end user

Exporting the account

Use the **Export Account** button to see the same selection of objects in the archive as available through the administrator user interface.

1. Log into the **DirectAdmin** panel.
2. Go to **Menu** > **Extra Features** > **Acronis Backup**.
3. Open the **Backups** tab.
4. Select a recovery point.
5. Click **Export the account**.
6. (Optional) Select the **Skip export of databases** and **Skip export of home directory** check boxes.
7. Once the archive is ready, download it using one of the following ways:
   - the link in the notification bar
   - the link in the **Operations log**

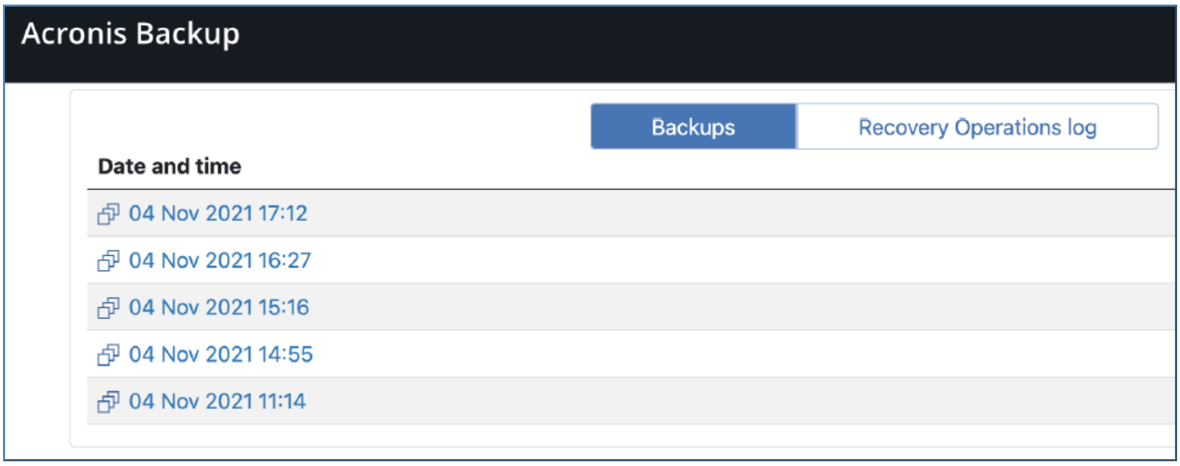
Recovering the account

1. Log into the **DirectAdmin** panel.
2. Go to **Menu** > **Extra Features** > **Acronis Backup**.
3. Open the **Backups** tab.
4. Select a recovery point.
5. Click **Recover the account**.
6. (Optional) Select the **Skip export of databases** and **Skip export of home directory** check boxes.

As a result, the entire account will be recovered to the state from the backup.

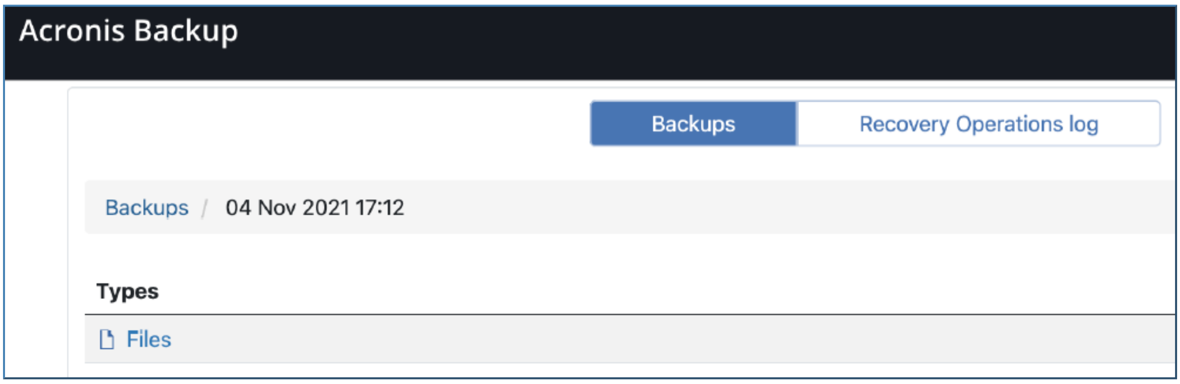
Downloading files

1. Go to **Menu** > **Extra Features**.
2. Click **Acronis Backup**.
3. Open the **Backups** tab.



Date and time
04 Nov 2021 17:12
04 Nov 2021 16:27
04 Nov 2021 15:16
04 Nov 2021 14:55
04 Nov 2021 11:14

4. Select a recovery point. Then the corresponding backup will be mounted to the server.

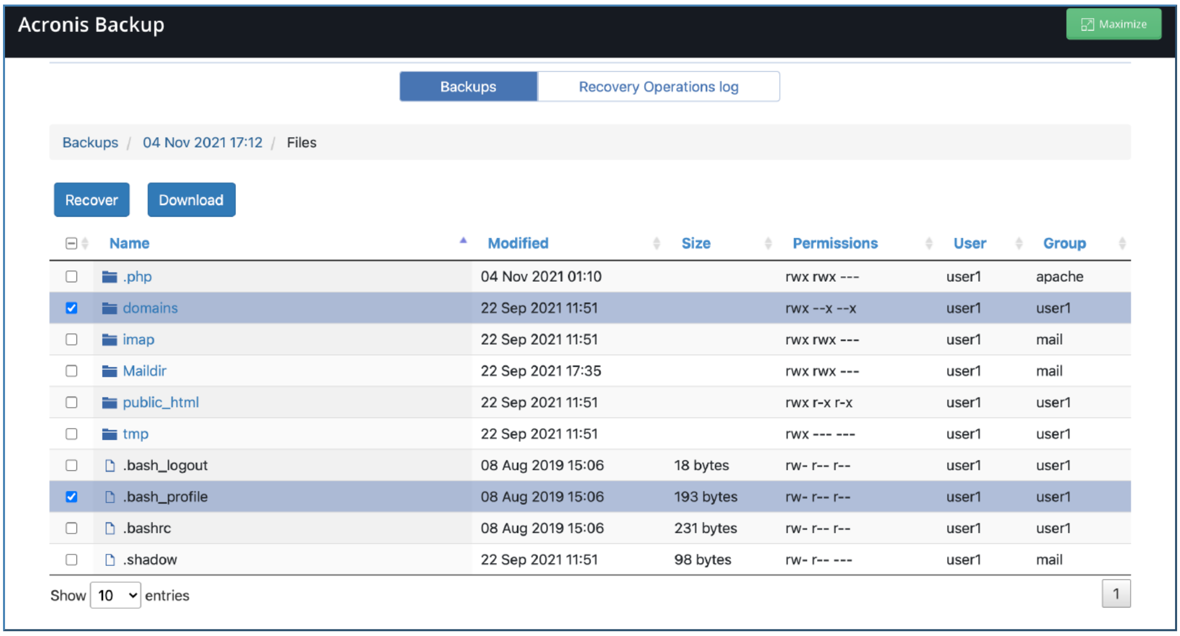


Types
Files

This process may take up to a few minutes.

5. Click **Files**.

6. Select the files and folders to download.



	Name	Modified	Size	Permissions	User	Group
☐	.php	04 Nov 2021 01:10		rwx rwx ---	user1	apache
☑	domains	22 Sep 2021 11:51		rwx --x --x	user1	user1
☐	imap	22 Sep 2021 11:51		rwx rwx ---	user1	mail
☐	Maildir	22 Sep 2021 17:35		rwx rwx ---	user1	mail
☐	public_html	22 Sep 2021 11:51		rwx r-x r-x	user1	user1
☐	tmp	22 Sep 2021 11:51		rwx --- ---	user1	user1
☐	.bash_logout	08 Aug 2019 15:06	18 bytes	rw- r-- r--	user1	user1
☑	.bash_profile	08 Aug 2019 15:06	193 bytes	rw- r-- r--	user1	user1
☐	.bashrc	08 Aug 2019 15:06	231 bytes	rw- r-- r--	user1	user1
☐	.shadow	22 Sep 2021 11:51	98 bytes	rw- r-- ---	user1	mail

7. Click **Download**.
   - The download of a single file will start immediately.
   - If you request to download several files, a .zip archive will be prepared and placed into your home folder. Once this archive is ready, download it by using the link in the notification bar or in the **Recovery Operations log**.

Recovering files to the original location

1. Go to **Menu** > **Extra Features**.
2. Click **Acronis Backup**.
3. Open the **Backups** tab.
4. Select a recovery point. The corresponding backup will be then mounted to the server. This process may take a few minutes.
5. Click **Files**.
6. Select files and folders to restore.
7. Click **Recover**.

If at least one folder is chosen, you can select **Delete any files** in the original location, created after the backup option. If this option is enabled, all files from selected folders will be deleted before the recovery.

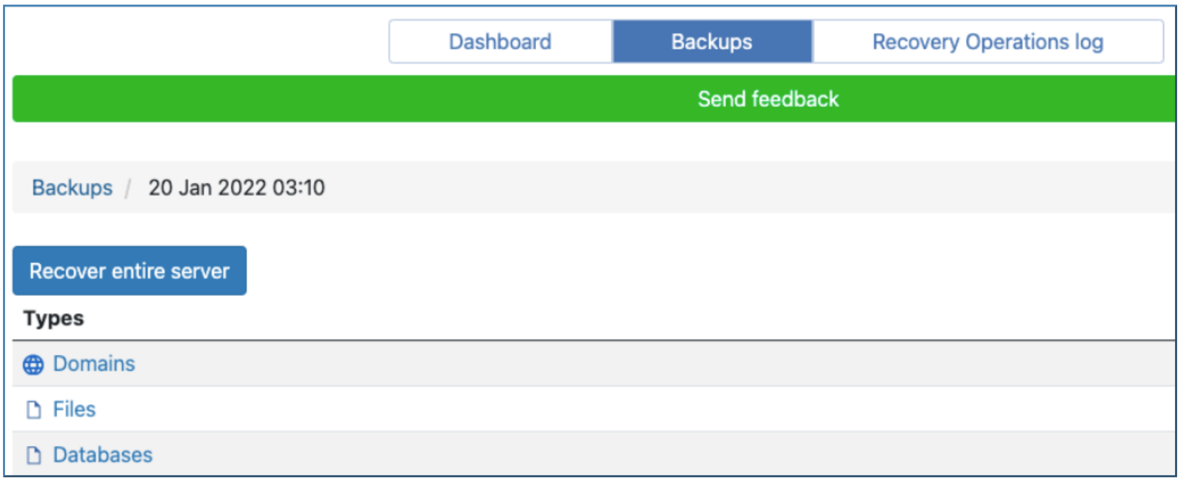
This option may be useful if your website was hacked, to ensure that all malicious files are deleted.

As a result, the files selected on the server will be replaced with their backup copies.

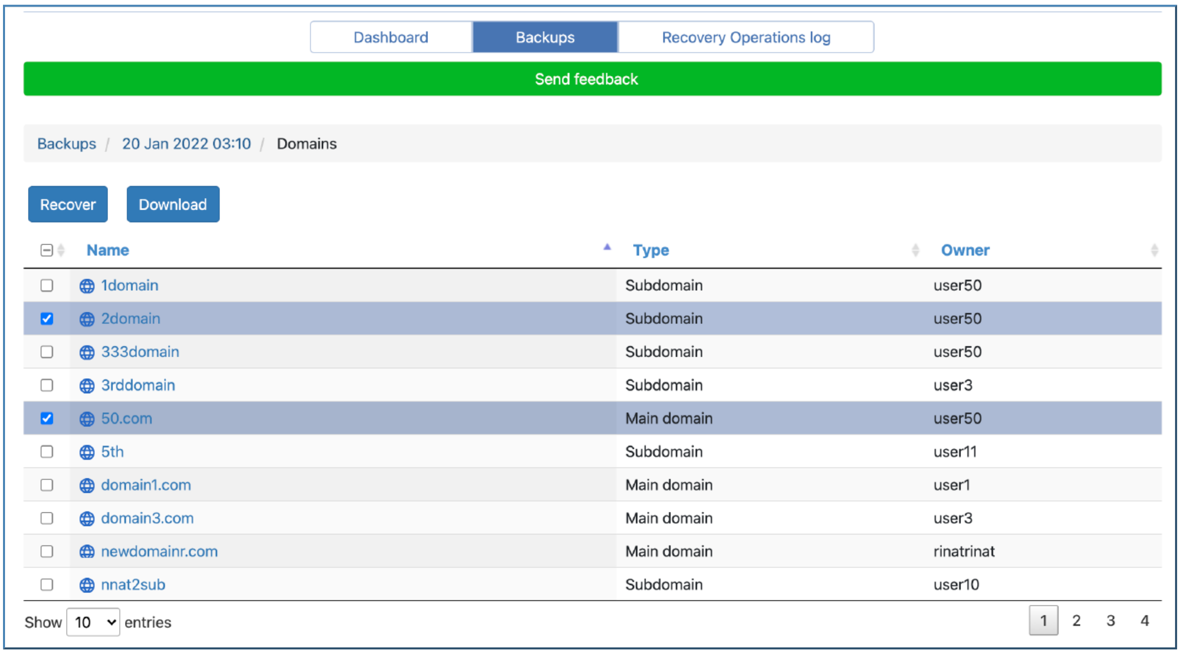
Downloading domains

This type of recovery stands for a collection of files associated with the specific domain and does not include databases.

1. Go to **Menu** > **Extra Features**.
2. Click **Acronis Backup**.
3. Open the **Backups** tab.
4. Select a recovery point. The corresponding backup will be then mounted to the server. This process may take a few minutes.
5. Click **Domains**.



6. Select the domains you would like to download.



⊟	Name	Type	Owner
☐	1domain	Subdomain	user50
☑	2domain	Subdomain	user50
☐	333domain	Subdomain	user50
☐	3rddomain	Subdomain	user3
☑	50.com	Main domain	user50
☐	5th	Subdomain	user11
☐	domain1.com	Main domain	user1
☐	domain3.com	Main domain	user3
☐	newdomainr.com	Main domain	rinatrinat
☐	nnat2sub	Subdomain	user10

7. Click **Download**.

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

Recovering domains to the original location

This type of recovery stands for a collection of files associated with the specific domain and does not include databases.

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

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

If a domain no longer exists, it will be automatically recreated.

Downloading database dumps

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

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

Recovering databases to the original location

1. Go to **Menu** > **Extra Features**.
2. Click **Acronis Backup**.
3. Open the **Backups** tab.
4. Select a recovery point.
5. Click **Databases**.
6. Select the databases to 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 will be recovered to the original location. The existing databases will be overwritten. If a database no longer exists, it will be recreated automatically.

Recovering databases as new ones

1. Go to **Menu** > **Extra Features**.
2. Click **Acronis Backup**.
3. Open the **Backups** tab.
4. Select a recovery point.
5. Click **Databases**.
6. Select the databases to recover.
7. Select the **Add suffix to the recovered database name** check box.
8. Click **Recover**.

As a result, new databases with the following name will be created: %original_name%%suffix%

The existing databases will not be affected.

Downloading mailboxes

To download mailbox(es) from one of the available archives/recovery points:

1. Log into the **DirectAdmin** panel.
2. Go to **Menu** > **Extra Features** > **Acronis Backup**.
3. Open the **Backups** tab.
4. Select a recovery point.
5. Click **Mailboxes**.
6. Select which mailbox(es) to download.
7. Click **Download**.
8. Once the archive is ready, download it by using one of the following ways:
   - the link in the notification bar
   - the link in the **Operations log**

Recovering mailboxes to the original location

The mailbox recovery operation presumes that the entire mailbox will be replaced with the one from the backup. New emails added after creating the backup will be permanently deleted.

To recover mailbox(es) from one of the available archives/recovery points:

1. Log into the **DirectAdmin** panel.
2. Go to **Menu** > **Extra Features** > **Acronis Backup**.
3. Open the **Backups** tab.
4. Select a recovery point.

5. Click **Mailboxes**.
6. Select which mailbox(es) to restore.
7. Click **Recover**.

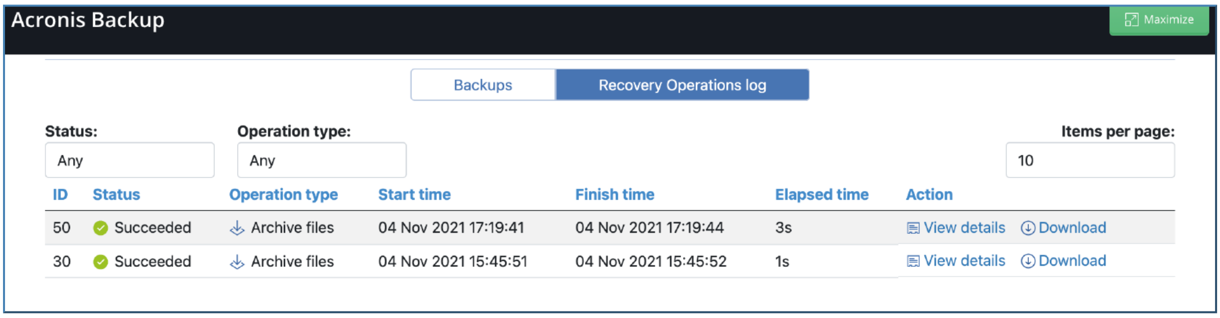
As a result, the selected mailboxes will be recovered to the original location. If the selected mailbox no longer exists on the server, it will be recreated automatically.

Note

You can choose to keep emails created after the backup. Otherwise, the entire mailbox will be overwritten, and all emails created after the backup will be lost as a result of the operation.

Tracking recovery progress

DirectAdmin users can view and monitor information about the recovery operations in the **Recovery Operations log**. This log can be filtered by operation status and type. It also contains download links for the download operations.



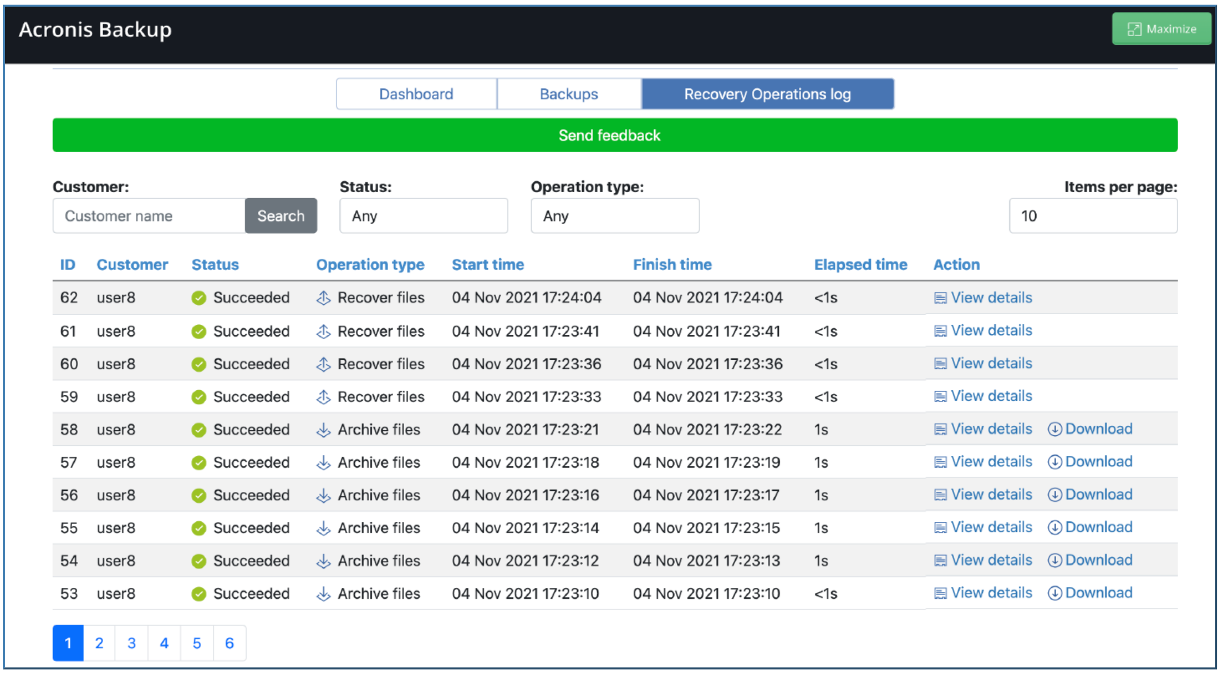
Status: Any

Operation type: Any

Items per page: 10

ID	Status	Operation type	Start time	Finish time	Elapsed time	Action
50	Succeeded	Archive files	04 Nov 2021 17:19:41	04 Nov 2021 17:19:44	3s	View details Download
30	Succeeded	Archive files	04 Nov 2021 15:45:51	04 Nov 2021 15:45:52	1s	View details Download

In the administrator user interface, you can see the same information across all users.



Customer: Customer name

Status: Any

Operation type: Any

Items per page: 10

ID	Customer	Status	Operation type	Start time	Finish time	Elapsed time	Action
62	user8	Succeeded	Recover files	04 Nov 2021 17:24:04	04 Nov 2021 17:24:04	<1s	View details
61	user8	Succeeded	Recover files	04 Nov 2021 17:23:41	04 Nov 2021 17:23:41	<1s	View details
60	user8	Succeeded	Recover files	04 Nov 2021 17:23:36	04 Nov 2021 17:23:36	<1s	View details
59	user8	Succeeded	Recover files	04 Nov 2021 17:23:33	04 Nov 2021 17:23:33	<1s	View details
58	user8	Succeeded	Archive files	04 Nov 2021 17:23:21	04 Nov 2021 17:23:22	1s	View details Download
57	user8	Succeeded	Archive files	04 Nov 2021 17:23:18	04 Nov 2021 17:23:19	1s	View details Download
56	user8	Succeeded	Archive files	04 Nov 2021 17:23:16	04 Nov 2021 17:23:17	1s	View details Download
55	user8	Succeeded	Archive files	04 Nov 2021 17:23:14	04 Nov 2021 17:23:15	1s	View details Download
54	user8	Succeeded	Archive files	04 Nov 2021 17:23:12	04 Nov 2021 17:23:13	1s	View details Download
53	user8	Succeeded	Archive files	04 Nov 2021 17:23:10	04 Nov 2021 17:23:10	<1s	View details Download

For operation failure details, click **View details**. From there you can send failure reports so that the plugin vendor can improve the plugin in future versions.

Recovery operations, performed from the DirectAdmin interface, do not appear in the Acronis Cyber Protect console.

Appendix

Installing the protection agent using a registration token

1. To obtain a registration token, log in to the Cyber Protection console with your credentials.
2. Go to **Devices** > **All devices** and click **Add**.
3. Scroll down to the **Registration token** section, then click **GENERATE**.
4. Specify the token lifetime.
5. Click **Generate token** > **Copy**.
6. Log on to the host as the root user.
7. Run the installation file, providing the generated token and datacenter address as the arguments. The datacenter address is the URL that you see once you log in to the Cyber Protection service.

   ```
   ./Backup_Agent_for_Linux_x86_64.bin --token=%generated token% --rain=%datacenter
   address%
   ```

8. Select the respective checkboxes of the agents you want to install. For example, Agent for Linux.
9. Complete the installation procedure.

The following file contains troubleshooting information:
/usr/lib/Acronis/BackupAndRecovery/HOWTO.INSTALL

Advanced plugin configuration

1. If you have configured a custom location for MySQL data on the server:
   a. Open the /usr/local/directadmin/plugins/acronisbackup/srv/config.ini file.
   b. Navigate to the [mysql] section.
   c. Locate and use the data_folder_ path parameter 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, the 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, the 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

Collecting logs

The Acronis Backup plugin for DirectAdmin log files are located in the following directories:

- /usr/local/directadmin/plugins/acronisbackup/log/*
- /usr/local/directadmin/plugins /acronisbackup/srv/log/*

A full set of the plugin logs will be included in the System report from the server together with the agent logs. Instructions on how to collect the system report are provided at https://kb.acronis.com/content/54608

Logs can also be collected using the plugin user interface:

1. Log into the DirectAdmin panel as an administrator.
2. Go to **Menu** > **Extra Features** > **Acronis Backup**.
3. On the **Dashboard** tab, scroll down to the bottom and click **Download log**.