USER GUIDE

HYCU Data Protection as a Service for AWS

November 2022

Legal notices

Copyright notice

Trademarks

Disclaimer

The details and descriptions contained in this document are believed to have been accurate and up to date at the time the document was written. The information contained in this document is subject to change without notice.

HYCU provides this material "as is" and makes no warranty of any kind, expressed or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. HYCU shall not be liable for errors and omissions contained herein. In no event shall HYCU be liable for any direct, indirect, consequential, punitive, special or incidental damages, including, without limitation, damages for loss and profits, loss of anticipated savings, business interruption, or loss of information arising out of the use or inability to use this document, or any action taken based on the information contained herein, even if it has been advised of the possibility of such damages, whether based on warranty, contract, or any other legal theory.

The only warranties for HYCU products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty.

Notice

This document is provided in connection with HYCU products. HYCU may have copyright, patents, patent applications, trademark, or other intellectual property rights covering the subject matter of this document.

Except as expressly provided in any written license agreement from HYCU, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property on HYCU products. Use of underlying HYCU product(s) is governed by their respective Software License and Support Terms.

Important: Please read Software License and Support Terms before using the accompanying software product(s).

HYCU
www.hycu.com

Contents

Chapter 1

About HYCU for AWS

HYCU Data Protection as a Service for AWS (HYCU for AWS) is a fully managed backup and recovery service for Amazon Web Services (AWS) that is specifically designed to make data protection as simple and cost-effective as possible, to improve your business agility, and to bring unified security, reliability, performance, and user experience.

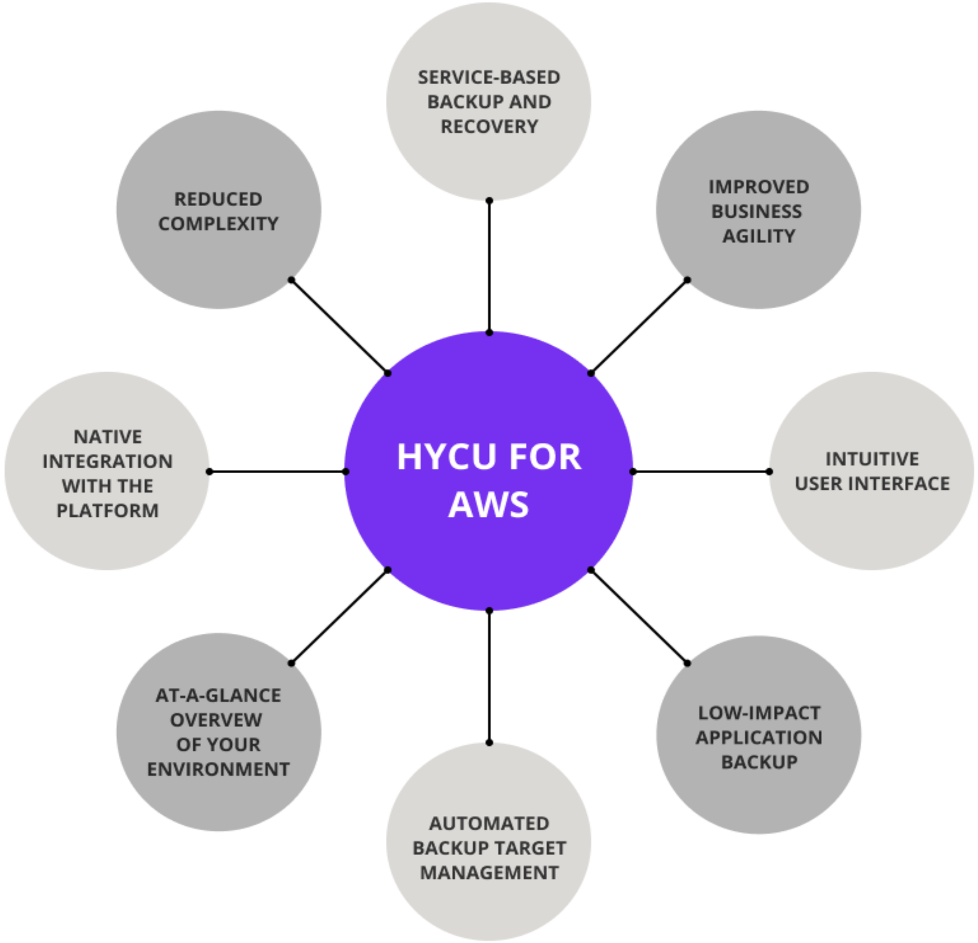

SERVICE-BASED BACKUP AND RECOVERY
REDUCED COMPLEXITY
IMPROVED BUSINESS AGILITY
NATIVE INTEGRATION WITH THE PLATFORM
HYCU FOR AWS
INTUITIVE USER INTERFACE
AT-A-GLANCE OVERVEW OF YOUR ENVIRONMENT
LOW-IMPACT APPLICATION BACKUP
AUTOMATED BACKUP TARGET MANAGEMENT

Figure 1–1: Introduction to HYCU for AWS

Key features and benefits

The following features make HYCU for AWS a solution that can transform your business—achieving complete compliance and data protection:

- **Protection against data loss**

  Delivers native data protection for Amazon EC2 instances and Amazon S3 buckets, ensuring data consistency and easy recoverability.

- **Data protection in a few minutes**

  Data protection can be enabled in a few minutes after you subscribe to HYCU for AWS, with no deployment and configuration concerns.

- **Predefined policies and options for policy customization**

  Simplifies implementation of data protection by providing predefined policies and includes options for policy customization that can address your special data protection needs.

- **Scheduled backups**

  Automatic backup scheduling provides data protection based on your recovery point objectives (RPOs).

- **Centralized data protection management and monitoring**

  You can join AWS accounts into protection sets to establish centralized data protection management and monitoring.

- **Low impact on the environment**

  Agentless architecture reduces backup load on production instances. In addition, backup windows enable you to completely avoid the impact of backup activity on your production environment during peak hours.

- **Use of data archives**

  When you create an archive of data, you ensure your data is isolated from your current activity and safely stored for future reference.

- **Restore of individual files**

  A possibility to restore one or more files is an alternative to restoring the entire instance.

- **At-a-glance overview of the data protection environment**

  The HYCU for AWS dashboard helps you to identify potential problems and bottlenecks to improve the performance of your data protection environment.

- **Optimized consumption of storage space**

  The HYCU changed block tracking feature slows down the growth of backup data on targets, resulting in significant space savings and consequently reduced storage cost.

- **Integration with the AWS billing system**

  Cost of data protection is billed by AWS through existing management accounts, without requiring you to provide additional billing information.

Data protection environment overview

Before you start protecting data with HYCU for AWS, make yourself familiar with the following terms related to the data protection environment:

Term	Description
HYCU for AWS web user interface	An interface for protecting Amazon EC2 instances and Amazon S3 buckets.
Protection sets	Groups that join together AWS accounts that you have successfully added to HYCU for AWS as a source.
Instances	Instances to which you can assign policies and for which you therefore provide data protection. Data is always protected at a granular level, allowing you to restore either the entire instances, individual volumes, or individual files.
Buckets	Containers in Amazon S3 holding your data to which you can assign a policy and for which you therefore provide data protection. Buckets can also be added to HYCU for AWS as targets for storing backup data.
Targets	S3 buckets that HYCU for AWS uses for storing backup data. Backup data can also be stored as snapshots.

HYCU for AWS data protection

With the HYCU for AWS data protection solution, you can be confident that your business data is protected, which means that it is backed up in a consistent state, stored to a target, and can be restored.

The AWS accounts that you add as sources define the scope of data protection.

HYCU for AWS enables you to protect instances and data in buckets. After you establish your data protection environment, you can enable data protection. After the first backup is successfully completed, you can restore the data if it becomes damaged or corrupted.

Chapter 2

Starting with HYCU for AWS

You can start protecting data after you perform the following tasks:

Task	Instructions
Getting familiar with HYCU for AWS pricing concepts	"Service pricing" below
Subscribing to HYCU for AWS	"Subscribing to the service" on page 13
Signing in to the HYCU for AWS web user interface	"Signing in to HYCU for AWS" on page 14

Service pricing

Because HYCU for AWS utilizes AWS for its service needs, when you enable data protection, you are charged for the backup service, data retention, and the resources that are required for the backup and recovery services.

The total data protection cost is the sum of the following costs:

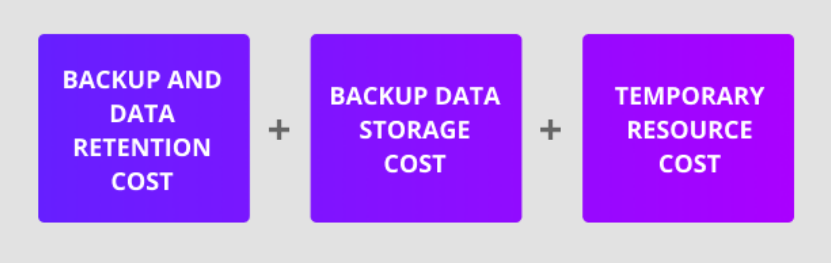


Figure 2–1: Data protection cost

Cost	Details
Backup and data retention	Cost of backing up data and data retention. For details, see "Backup and data retention pricing" on the next page.
Backup data storage	Cost of storing backup data. The following factors are considered: • Target type (a snapshot or a bucket)

Cost	Details
	• Backup frequency • Size of backup data • Backup retention period If you use a bucket as a target, the following is also considered: • Use of copies of backup data • Use of data archives, configured archive tiers and their retention periods • Enabled restore of individual files or folders
Temporary resources	Cost of temporary resources that HYCU for AWS creates in AWS when performing the following tasks: • Instance rediscovery after assigning a credential group • Instance rediscovery after selecting the Enable restore of individual files option • Backup of instances • Backup of buckets • Restore of instances or entire instance volumes • Restore of individual files or folders • Restore of buckets

A HYCU for AWS subscription includes a 14-day free trial period. During this time, HYCU does not charge you for the backup and data retention cost. The cost of backup data storage and temporary resources is charged by Amazon as usual.

For more details on pricing, see AWS Marketplace.

Backup and data retention pricing

The HYCU for AWS backup and data retention pricing model provides you with the simplicity and transparency of consumption-based pricing. At the end of your 14-day free trial period, you are billed according to the subscription plan that you select when subscribing to HYCU for AWS. For details on the subscription plans, see "HYCU for AWS subscription plans" on the next page.

Pricing for data protection is based on the following (within a monthly billing cycle):

- Capacity of all volumes belonging to protected instances
- Size of protected buckets
- Pricing tiers to which protected instances and buckets belong

A pricing tier to which a protected instance or bucket belongs is determined when you assign a policy to the instance or bucket. HYCU for AWS automatically associates the instance or bucket with one of the pricing tiers based on the value of the Backup every option in the policy that defines how frequently data is backed up. For details on policies, see "Defining your backup strategy" on page 20.

Depending on how frequently your data is backed up, each protected instance or bucket belongs to one of the following pricing tiers:

Pricing tier	Data backup frequency (in hours)
platinum	1-3 hours
gold	4-11 hours
silver	12-23 hours
bronze	24 hours or more

Considerations

- If an instance or a bucket is deleted from AWS, but it still has at least one valid restore point available, it is considered protected (its status is PROTECTED_DELETED) and HYCU automatically associates such an entity with the bronze pricing tier. It charges you for protecting only the included volumes.
- If you unassign a policy from an instance or a bucket that still has at least one valid restore point available, such an entity is considered protected and HYCU automatically associates it with the bronze pricing tier. It charges you for protecting only the included volumes.

HYCU for AWS subscription plans

HYCU for AWS offers you the pay-as-you-go plan. With this plan, you pay only for what you use for data protection each month.

For details on the pay-as-you-go subscription plan, see AWS Marketplace.

Subscribing to the service

You subscribe to HYCU for AWS online from the AWS Marketplace. This is usually done by one user for an entire organization.

Prerequisites

- You have access to an AWS account.
- Your user account has the AWSMarketplaceManageSubscriptions predefined role attached (`arn:aws:iam::aws:policy/AWSMarketplaceManageSubscriptions`).

For details, see AWS documentation.

Consideration

If you violate the terms of use of HYCU for AWS, HYCU may temporarily suspend the service for your subscription. Your complete data protection environment is retained for the duration of suspension, but you cannot use the service until the violation is resolved.

Procedure

1. Open a web browser and go to the HYCU | AWS Market webpage.
2. Read the solution description, and then click **View purchase options**.
3. On the Configure your contract page, check the displayed contract information, and click **Create contract**. If required, you can modify the contract information.
4. Verify the contract summary, and then click **Pay now**.
5. Click **Setup your account** to complete the registration.
6. On the HYCU Data Protection as a Service for AWS sign-in webpage, enter the required information and click **Submit**.
7. When HYCU Data Protection as a Service for AWS is deployed, click **Go to application**.

HYCU automatically creates a user account for the HYCU Customer Support portal for your subscription and sends you an email notification about it. You can use this account for submitting requests to HYCU Customer Support.

Signing in to HYCU for AWS

After successfully subscribing to HYCU for AWS, you can sign in to the HYCU for AWS web user interface.

Prerequisite

You are using a supported web browser. For a list of supported web browsers, see the *HYCU for AWS Compatibility Matrix*.

Procedure

1. Open a web browser and go to the HYCU Data Protection as a Service for AWS webpage, by using the link you received when you subscribed to HYCU for AWS.

   Alternatively, open the HYCU Data Protection as a Service for AWS webpage and enter the HYCU account ID you received when you subscribed to HYCU for AWS.

   > Tip You can set a sign-in alias for your HYCU account. For details, see "Viewing subscription information" on page 84.

2. Click **Next**.
3. On the sign-in webpage, depending on how you want to sign-in to HYCU for AWS, do one of the following:
   - *By using dedicated sign-in credentials for HYCU*. Enter your sign-in name and password.

- *By using an identity provider.* Click the preferred identity provider, and then, if required, enter your credentials.

  For details on how to integrate HYCU for AWS with identity providers, see "Managing identity providers" on page 87.

After you sign in to the HYCU for AWS web user interface, the Dashboard panel appears and you can start establishing your data protection environment and protecting data.

> ⚠ Important You are automatically signed out of the HYCU for AWS web user interface after 15 minutes of inactivity and any unsaved changes are lost.

To sign out manually, click 👤 ***<EmailAddress>*** to open the Session menu, and then click **Sign Out**.

Chapter 3

Establishing a data protection environment

After you sign in to HYCU for AWS, you must establish a data protection environment in which data will be effectively protected.

Consideration

Keep in mind that the role you have assigned determines what kind of actions you can perform. For details on roles, see “Managing roles” on page 90.

If you have the Administrator role assigned, you can switch between the Subscription and Protection set contexts. Depending on the scope of the tasks that you want to perform, click ⌄ next to the name of the currently selected context to switch to another one. The Subscription context enables you to perform administration tasks related to the selected subscription such as adding identity providers, adding or removing users, and changing roles, whereas the Protection set context enables you to perform data protection tasks related to the selected protection set. See “Managing identity and access” on page 87 and “Managing protection sets” on page 91 for details.

Tasks

Establishing a data protection environment involves the following tasks:

Task	Instructions
1. Add AWS accounts to HYCU for AWS.	“Managing sources” on page 94
2. *Only if you plan to use multiple protection sets.* Configure a protection set and select it.	“Managing protection sets” on page 91 and “Selecting a HYCU for AWS protection set” on the next page
3. *Only if you plan to use manually created targets.* Add Amazon S3 buckets to HYCU for AWS as targets.	“Setting up targets” on page 18
4. Decide for predefined policies or create custom ones.	“Defining your backup strategy” on page 20
5. *Required only in special data protection scenarios.*	“Enabling access to data” on

Task	Instructions
Configure credential groups and assign them to instances.	page 29

After the data protection environment is established, data protection can be accomplished in several ways to fulfill your particular business needs.

Switching the user interface context

In the HYCU for AWS user interface, the scope of tasks you can perform depends on the context you select. You can choose between a subscription context that is used for administration tasks and a protection set context:

- Subscription

  In Subscription context, only the IAM panel is active. Use this context to perform administration tasks related to your subscription, such as adding identity providers, adding or removing users, or changing roles. See “Managing identity and access” on page 87.

- Protection set

  In the protection set context, you select the scope of data protection by selecting a specific protection set.

  The HYCU for AWS web user interface switches the context to the selected scope of data protection. See “Managing protection sets” on page 91.

Procedure

1. On the toolbar, click ⌄ next to the name of the selected protection set or subscription. The Context Picker dialog box opens.
2. In the Context Picker dialog box, select the context.
3. Click **Save**.

   The HYCU for AWS web user interface switches the context. The context that you select is remembered for the next time you sign in.

Selecting a HYCU for AWS protection set

An environment for which HYCU for AWS provides data protection consists of one or more protection sets that join together AWS accounts. When you subscribe to HYCU for AWS, a default protection set is created automatically (represented by the 🔖 icon).

Depending on your business needs, you can create additional protection sets and distribute your accounts among them, having in mind that you must implement data protection for each protection set individually. For details on managing protection sets, see “Managing protection sets” on page 91.

If no multiple protection sets are available in your data protection environment, your data protection scope is always the same and you can safely skip the procedure described in this section.

Consideration

Only if multiple protection sets are available in your data protection environment. The currently selected protection set has the ✓ icon next to it.

Procedure

1. On the toolbar, click ⌄ next to the name of the selected protection set.
2. In the Context Picker dialog box, from the list of available protection sets, select the scope of your data protection by selecting the preferred protection set.

   > Tip You can also search for a protection set by entering its name or the ID of an included account and then pressing **Enter** in the Protection set search field.

3. Click **Select**.

The HYCU for AWS web user interface switches the context to the selected scope of data protection. The protection set that you selected last is remembered for the next time you sign in.

Setting up targets

Targets are locations where backup data is stored. HYCU for AWS allows you to define either a bucket or a snapshot as a location for storing your data.

Target	Description
Bucket	Backup data is stored in Amazon S3 buckets that you create yourself or HYCU for AWS creates for you automatically: • Manually created targets You can create your own buckets in Amazon S3 and add them to HYCU for AWS as targets. For instructions, see "Adding a bucket to HYCU for AWS as a target" on the next page. • Automatically created targets *Applicable only if you are protecting instances.* HYCU for AWS creates Amazon S3 buckets automatically while backing up data and uses them as targets. For increasing restore speed and minimizing costs, these targets are created in the same AWS account and at the same location as the instances you are backing up. The same target is used for storing the backup data of multiple instances where possible. You can use these targets also for storing your data (for example, for individual files that you restore).

Target	Description
	For the target naming conventions, see “Objects created by the service” on page 101. Caution Never delete any targets used by HYCU for AWS because this may result in data loss. Additionally, within targets, ensure that the `hycu/backups/` folders are always kept intact.
Snapshot	*Available only if you are protecting instances.* Backup data is stored as a snapshot in an AWS account that contains the instances you want to protect. Note If snapshots created by HYCU for AWS are deleted from AWS, you will not be able to restore backup data from this location. However, you can still restore your data from targets if copies of backup data or data archives exist. For the snapshot naming conventions, see “Objects created by the service” on page 101.

Adding a bucket to HYCU for AWS as a target

Prerequisites

- The AWS account where the bucket resides must be added to HYCU for AWS as a source. For instructions on how to add accounts as sources, see “Managing sources” on page 94.
- *For adding a bucket with Object Lock (WORM) enabled:* The Object Lock option must be enabled for the bucket. For details on how to configure buckets, see AWS documentation.

Limitations

- Publicly available buckets cannot be added as targets.
- *Only if you are adding a bucket with the S3 Glacier Flexible Retrieval or S3 Glacier Deep Archive storage tier.* Only copies of backup data can be stored to this type of target. Keep in mind that AWS can charge you additionally for premature removal of data if the retention period specified in your policy is shorter than the recommended (minimum) retention period in AWS.

Consideration

You can set up the same target in multiple protection sets.

Accessing the Targets panel

To access the Targets panel, in the navigation pane, click **Targets**. Alternatively, in the Dashboard panel, click the **Targets** widget title.

Procedure

1. In the Targets panel, click + **Add**. The Add Target dialog box opens.
2. In the Target field, enter the name of the bucket that you want to add to HYCU for AWS as a target.
3. In the Size field, specify the amount of storage space that should be used for storing backup data (in MiB, GiB, or TiB).

   > ⚠ Important The specified amount represents a soft limit, therefore actual usage may exceed it.

4. In the Account ID field, enter the AWS account ID.
5. From the Storage class drop-down, select the storage class of the objects that are uploaded during backup or copy.
6. Click **Save**.

The target is added to the list of targets in the Targets panel. For details on managing targets, see "Managing targets" on page 77.

Defining your backup strategy

HYCU for AWS enables you to schedule automatic backups to achieve the optimum level of data protection based on your recovery point objective (RPO) and backup retention requirements. Backups can be scheduled to start each time the specific number of minutes, hours, days, weeks, or months has passed.

When defining your backup strategy, consider the specific needs of your environment and the RPO that represents the maximum period of time for which data loss is considered acceptable. For example, setting the RPO to 24 hours means that your business can tolerate losing only data from the last 24 hours.

Decide which of the following policy approaches best suits the needs of your environment:

Policy approach	Description
Applying a predefined policy	You can use any of the predefined policies to simplify the data protection implementation. For details, see "Taking advantage of predefined policies" on the next page.
Creating a custom policy	If none of the predefined policies meets the needs of your environment, you can create a new policy and tailor it to your needs. For details, see "Creating custom policies" on the next page.

If you consider one of the predefined or custom policies satisfies all data protection goals of your environment, you can set such a policy as default. For details, see "Setting default policies" on page 28.

Taking advantage of predefined policies

When establishing a data protection environment, you can take advantage of the predefined policies that provide a fast and convenient way of enabling data protection, and cover the most common data protection scenarios.

HYCU for AWS comes with the following predefined policies:

Predefined policy name	Back up data every...	Keep snapshots for...	Keep copies of backup data for...
platinum	2 hours	1 day	1 week
gold	4 hours	1 day	1 week
silver	12 hours	1 day	1 week
bronze	24 hours	2 days	1 week

If you want to exclude instances or buckets from backups, you can use the exclude policy.

Consideration

Predefined policies use automatically created targets for storing backup data. For details on targets, see "Setting up targets" on page 18.

Creating custom policies

If the needs of your data protection environment are not covered with any of the predefined policies, you can create a new policy and tailor it to your needs. In this case, besides setting the desired RPO, the retention period for the backup data, and the target, you can also enable one or more additional policy options for optimal policy implementation.

You can also enable one or more of the following policy options:

Policy option	Allows you to...
Backup Window	Start all backup tasks within specified time frames to improve effectiveness and avoid an overload of your environment. For details, see "Creating backup windows" on page 24.
Copy	Create a copy of backup data.
Archiving	Preserve your data for future reference. For details, see "Creating data archives" on page 26.
Labels	Set up automatic policy assignment based on the labels or tags added to the instances in Amazon EC2, or the buckets in Amazon S3.

Prerequisites

- *Only if you plan to select a manually created target.* A bucket must be added to HYCU for AWS as a target. For instructions, see "Setting up targets" on page 18.
- *Only if you plan to enable the Backup Window policy option.* A backup window must exist for the selected HYCU for AWS protection set. For instructions, see "Creating backup windows" on page 24.
- *Only if you plan to enable the Archiving policy option.* A data archive must exist for the selected HYCU for AWS protection set. For instructions, see "Creating data archives" on page 26.
- *Only if you plan to enable the Labels policy option.*
  - The labels that you plan to specify in HYCU for AWS must be added to instances in Amazon EC2 as labels (preferred) or to buckets in Amazon S3 as bucket labels.

    For instructions on how to do this, see AWS documentation.

Considerations

- HYCU for AWS automatically associates the resource with one of the pricing tiers based on the value of the Backup every option that you set in the policy. However, if you are storing data as a snapshot and have enabled the Archiving option, the pricing tier is automatically set to bronze regardless of the specified RPO.
- If you want that your data to be stored as a snapshot and on a target, make sure to select the Snapshot backup target type and also enable the Copy policy option.
- *Only if you plan to enable the Labels policy option.*
  - Labels that you specify in policies in HYCU for AWS must be unique within the selected protection set.
  - When matched, the `hycu-policy` custom tag takes precedence over other labels or tags that might be added to the same instance in Amazon EC2 or to the same bucket in Amazon S3. For more information on the `hycu-policy` tag, see "Setting up automatic policy assignment" on page 28.
- *Only if you plan to store backup data on a target.* Backup and restore speed depends on the region of the chosen target and the regions of the instances . The optimum speed is achieved when the target and the instances reside in the same region.

> ### Accessing the Policies panel
>
> To access the Policies panel, in the navigation pane, click 🛡 **Policies**. Alternatively, in the Dashboard panel, click the **Policies** widget title.

Procedure

1. In the Policies panel, click + **New**. The New Policy dialog box opens.
2. Enter a name for your policy and, optionally, its description.
3. Enable the required policy options by clicking them (the Backup policy option is

mandatory and therefore enabled by default). The following policy options are available:

- **Backup Window**
- **Copy**
- **Archiving**
- **Labels**

4. In the Backup section, do the following:

   a. In the Backup every fields, set the RPO (in months, weeks, days, hours, or minutes).

   > Note You can set the RPO to 30 minutes in the following cases:
   >
   > - If you are storing data only as a snapshot.
   > - If you are storing data as a snapshot and have enabled the Archiving option.
   >
   > For all other cases, the minimum RPO is one hour.

   b. In the Retention fields, set a retention period (in months, weeks, or days) for the backup data.

   c. Select one of the following backup target types:

   - **Snapshot**
   - **Target**

     From the Target drop-down menu, select the target that you want to use for storing data.

     If you select the **Automatically selected** option, HYCU for AWS creates a bucket in the region of the instance and uses it as a target for storing the data. If an automatically created bucket already exists, it is used instead.

     > ⚠ Important Automatically created targets can be selected only if you plan to protect instance data (and not bucket data).

5. Depending on which policy options you have enabled, do the following:

Policy option	Instructions
Backup Window	In the Backup Window section, from the Backup window drop-down menu, select a backup window for backup tasks. If you do not select a backup window, the Always value is shown, which means that your backups are allowed to run at any time.
Copy	In the Copy section, do the following: a. Set a retention period (in months, weeks, or days) for the copy of backup data. b. From the Target drop-down menu, select a target that you

Policy option	Instructions
	want to use for storing data. If you want the target to be selected automatically, make sure the **Automatically selected** option is selected. In this case, HYCU for AWS creates a bucket in the region of the instance and uses it as a target for storing the data. If an automatically created bucket already exists, it is used instead. If you want to select a manually created target, make sure that this target is different from the one you selected for the backup.
Archiving	In the Archiving section, from the Data archive drop-down menu, select a data archive.
Labels	In the Labels section, enter a label key and value, and then click **Add**. If required, repeat the action as appropriate. For details on automatic policy assignment, see "Setting up automatic policy assignment" on page 28.

6. Click **Save**.

The policy is created and added to the list of policies. For details on managing policies, see "Managing policies" on page 80.

Creating backup windows

HYCU for AWS enables you to define time frames when backup tasks are allowed to start. If you use a backup window, the backup tasks are started only within the hours you specify, which improves effectiveness and prevents overloading your data protection environment. For example, you can schedule your backup tasks to run on non-production hours to reduce the load during peak hours.

You can use backup windows with both predefined policies and custom policies.

> ⚠ Important When defining a backup window, make sure that the RPO specified in the affected policy can be achieved within this backup window. If the RPO is shorter than any time frame during which backups are not allowed to start, this will result in your instances and buckets not being compliant with backup requirements.

Accessing the Policies panel

To access the Policies panel, in the navigation pane, click 🛡 **Policies**. Alternatively, in the Dashboard panel, click the **Policies** widget title.

Procedure

1. In the Policies panel, click **Backup Window**. The Backup Window dialog box opens.
2. Click + **New**.
3. Enter a name for your backup window and, optionally, its description.
4. From the Time zone drop-down menu, select the time zone for the backup window.

   > Note If the time zone that you selected supports daylight saving time, it is enabled by default.

5. Select the days and hours during which backups are allowed to run.

   > Tip If you click a day label or an hour label, you allow backups to run that whole day or that hourly period for all days of the week. You can also click and drag to quickly select a time frame that includes your preferred days and hours.

   The selected time frames are displayed in the Time frames field. If you want to delete any of the selected time frames, pause on it, and then click ✕ .
6. Click **Save**.
7. Click **Close**.

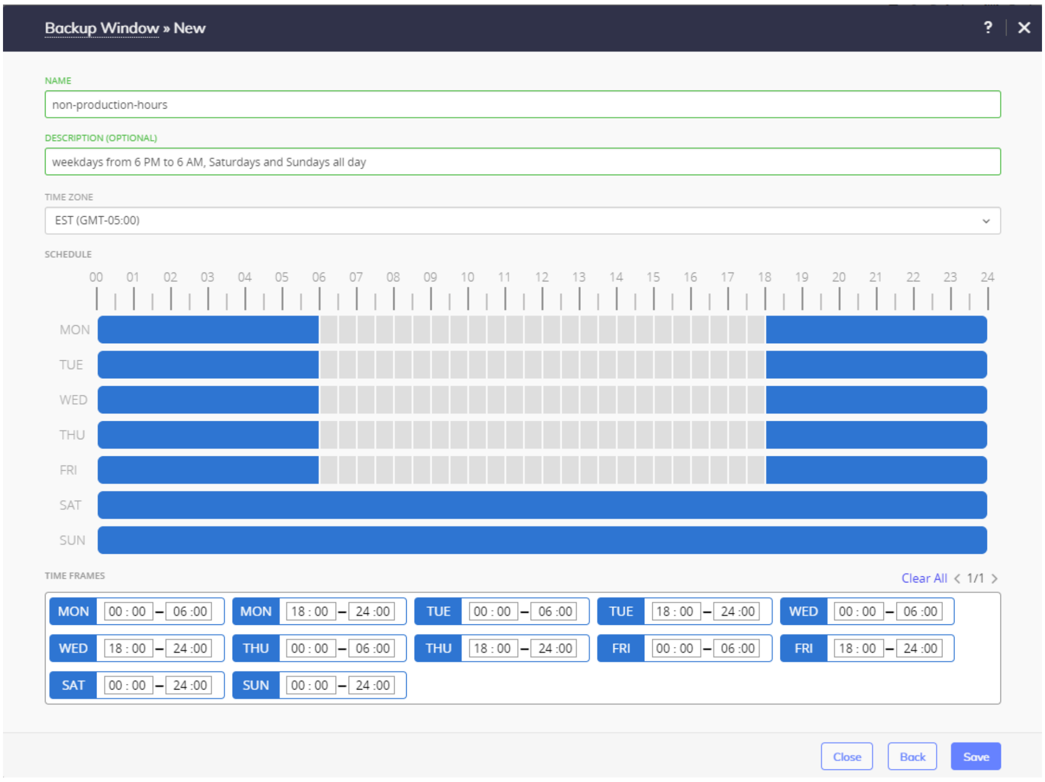
You can later edit any of the existing backup windows (click ✎ **Edit** and make the required modifications) or delete the ones that you do not need anymore (click 🗑 **Delete**).

After you create a backup window, you can do the following:

- Specify the backup window when creating a new policy. For details, see "Creating custom policies" on page 21.
- Assign the backup window to an existing policy. To do so, select the policy, click ✎ **Edit**, and then make the required modifications.

Example

You have selected the bronze policy and allowed new backup tasks to run on weekdays from 6 PM to 6 AM (Eastern Time), and on Saturday and Sunday all day long.



NAME
non-production-hours

DESCRIPTION (OPTIONAL)
weekdays from 6 PM to 6 AM, Saturdays and Sundays all day

TIME ZONE
EST (GMT-05:00)

TIME FRAMES

MON 00 : 00 – 06 :00	MON 18 : 00 – 24 :00	TUE 00 : 00 – 06 :00	TUE 18 : 00 – 24 :00	WED 00 : 00 – 06 :00
WED 18 : 00 – 24 :00	THU 00 : 00 – 06 :00	THU 18 : 00 – 24 :00	FRI 00 : 00 – 06 :00	FRI 18 : 00 – 24 :00
SAT 00 : 00 – 24 :00	SUN 00 : 00 – 24 :00			

In this case, the backup tasks can be run every 24 hours at any point of time within the specified time frames.

Creating data archives

HYCU for AWS enables you to create archives of your protected data and keep them for a longer period of time. By archiving data, the data is stored for future reference on a daily, weekly, monthly, or yearly basis. Your data is isolated from current activity and safely stored in a secure cloud archive location.

Prerequisite

Only if you plan to select a manually created target for the data archive. You have created a bucket and added it to targets of the selected protection set in HYCU for AWS.

Accessing the Policies panel

To access the Policies panel, in the navigation pane, click 🛡 **Policies**. Alternatively, in the Dashboard panel, click the **Policies** widget title.

Procedure

1. In the Policies panel, click **Archiving**. The Archiving dialog box opens.
2. Click + **New**.
3. Enter a name for your data archive and, optionally, its description.
4. Add any of the following archiving options to the list of the enabled options by clicking it:

Daily	Allows you to create a daily archive of data.
Weekly	Allows you to create a weekly archive of data.
Monthly	Allows you to create a monthly archive of data.
Yearly	Allows you to create a yearly archive of data.

5. In the Start at fields, specify the hour and the minute when the archiving task should start.
6. From the Time zone drop-down menu, specify the appropriate time zone.
7. *Only if you have enabled the Weekly, Monthly, and/or Yearly archiving option.* Specify when to archive data.
8. For each enabled archiving option, do the following:
   a. In the Retention box, set the retention period to be used.

      > Note Make sure that the retention period is longer than the RPO to prevent the data archive from expiring before a new backup is performed.

   b. From the Target drop-down menu, select a target that you want to use for storing the data archive.

      If you select the **Automatically selected** option, HYCU for AWS creates a bucket in the region of the instance and uses it as a target for storing the data. If an automatically created bucket already exists, it is used instead.

   c. From the Storage class drop-down menu, select the storage class that you want to use for storing the data archive.

      If you select the **Automatically selected** option, a storage class is automatically selected depending on the specified retention.

      For details on storage classes, see AWS documentation.
9. Click **Save**.

You can later edit any of the existing data archives (click **Edit** and make the required modifications) or delete the ones that you do not need anymore (click **Delete**). Keep in mind that you cannot modify a target if an archiving task is in progress on that target.

After you create a data archive, you can do the following:

- Specify a data archive when creating a new policy. For details, see "Creating custom policies" on page 21.
- Include the data archive into an existing policy. To do so, select the policy, click ✎ **Edit**, and then make the required modifications.

Setting default policies

You can select one of the predefined or custom policies to be the default policy for your data protection environment. When you set the default policy, depending on your choice, the default policy will be assigned to one of the following:

- Only newly discovered resources.
- Both newly discovered resources and all existing resources that do not have an assigned policy yet.

Consideration

Setting a default policy is overridden by assigning policies automatically. For more information, see "Setting up automatic policy assignment" below.

> Accessing the Policies panel
>
> To access the Policies panel, in the navigation pane, click **Policies**. Alternatively, in the Dashboard panel, click the **Policies** widget title.

Procedure

1. In the Policies panel, select the policy that you want to set as the default one, and then click 🔖 **Set Default**. The Set Default Policy dialog box opens.
2. Depending on the resources to which you want the default policy to be assigned, select one or more check boxes:
   - **Instances**
   - **Buckets**

   The default policy will be assigned to all newly discovered resources.
3. Enable the **Assign to resources without policy** switch if you want the default policy to be assigned also to all selected resources that do not have an assigned policy yet.
4. Click **Save**.

The default policy is represented by the 🔖 icon. If you later decide not to use this policy as the default one, click **Clear Default**. Keep in mind that by doing so, you do not unassign this policy from the resources to which it was assigned.

Setting up automatic policy assignment

You can set up automatic assignment of policies to instances or buckets by using one of the following methods:

Resources	Method 1	Method 2
Instances	By first adding custom tags to instances in Amazon EC2, and then specifying the corresponding label names and values in HYCU for AWS policies. For details, see "Creating custom policies" on page 21.	By adding the `hycu-policy` tag to instances in Amazon EC2 or buckets in Amazon S3. Use the following name/value pair: Name: `hycu-policy` Value: <*PolicyName*> In this case, <*PolicyName*> is the name of a HYCU for AWS policy (for example, Gold).
Buckets	By first adding bucket labels to buckets in Amazon S3, and then specifying the corresponding label names and values in HYCU for AWS policies. For details, see "Creating custom policies" on page 21.	

The corresponding policies are automatically assigned to the instances or buckets during the next instance or bucket synchronization in HYCU for AWS.

Prerequisite

All relevant prerequisites that apply also for manual policy assignment are fulfilled. For details, see "Backing up instances" on page 36.

Considerations

- Assigning policies automatically takes precedence over assigning policies manually or setting a default policy. This means that the label or the tag added to the preferred instance or bucket defines which policy is assigned to it, even if the same instance or bucket already has an assigned policy.
- If you want to assign a new policy to an instance or a bucket for which automatic policy assignment has been set up, do one of the following:
  - Define new tags or labels as described in this section.
  - Assign the policy to the instance or the bucket as described in "Backing up instances" on page 36 or "Backing up buckets" on page 55. In this case, the manually assigned policy will not be overridden by the automatically assigned one again.

Enabling access to data

You must manually enable access to the instances by assigning credential groups to them in HYCU for AWS:

Guest OS	Data protection scenario
any	• You plan to restore individual files using a user account that you specify. • You plan to use a specified user account for the restore, either to reuse

	an already existing user account or to comply with policies that impose restrictions on the utilized user names and passwords.
Linux	• You plan to use pre-snapshot or post-snapshot scripts and run them with a user account that you specify. • The SSH server is configured to use a non-default TCP port. • The SSH server is configured to use public key authentication.
Windows	• You plan to use pre-snapshot or post-snapshot scripts. • The WinRM server is configured to use the HTTP transport protocol or a non-default TCP port.

Configuring and assigning credential groups manually

Prerequisites

- A user account with sufficient privileges is configured within each instance. For details on how to do this, see AWS documentation.
- *For Linux instances:*
    - Ensure the following within the instance:
        - The specified user account is a member of the `sudo` user group.
        - The following line is included in the `/etc/sudoers` file:

          ```
          <UserName> ALL=(ALL) NOPASSWD: /bin/lsblk, /bin/ls, /bin/mkdir,
          /bin/mv, /bin/umount, /bin/cp, /bin/rm, /bin/mount
          ```
    - *Only if you want HYCU for AWS to access the instance by using a specific user account with password authentication.* The SSH server is configured to allow password authentication for signing-in on to the instance.
    - *For Ubuntu 22.04 instances that have RSA key-based authentication configured:*

      You must add the `PubkeyAcceptedKeyTypes=+ssh-rsa` parameter to the `/etc/ssh/sshd_config` file, and then restart the SSH service by running the `systemctl restart ssh.service` command.

Limitation

Only if you use the SSH protocol with public key authentication. If keys are generated with PuttyKeyGen or ssh-keygen using the legacy PEM format, only DSA and RSA keys are supported.

> Accessing the Instances panel
>
> To access the Instances panel, in the navigation pane, click **Instances**. Alternatively, in the Dashboard panel, click the **Instances** widget.

Procedure

1. In the Instances panel, select the instance to which you want to assign a credential group.
2. Click 🔑 **Credentials**. The Credential Groups dialog box opens.
3. Click + **New**.
4. In the Credential group name field, enter a name for the credential group.
5. From the Protocol drop-down menu, select one the following protocol options:

<table>
<tr><th>Protocol option</th><th>Instructions</th></tr>
<tr><td><b>Automatic</b></td><td>Select this option if you want HYCU for AWS to automatically select a protocol for accessing the instance—the SSH protocol (TCP port 22) or the WinRM protocol (TCP port 5985, HTTP transport)—, and then enter the user name and password of a user account that has required permissions to access the instance.
Use the following format for the user name:<ul><li>Linux: <code><i>&lt;LocalOrDomainUserName&gt;</i></code></li><li>Windows: <code><i>&lt;LocalUserName&gt;</i></code>, <code><i>&lt;Domain&gt;</i>\<i>&lt;DomainUserName&gt;</i></code>, <code><i>&lt;DomainUserName&gt;</i>@<i>&lt;Domain&gt;</i></code></li></ul></td></tr>
<tr><td><b>SSH</b></td><td>Select this option if you want to use the SSH protocol for accessing the instance, and then do the following:<ol type="a"><li>In the Port field, enter the SSH server port number.</li><li>From the Authentication drop-down menu, select the type of authentication you want to be used, and then provide the required information:<table><tr><td><b>Password authentication</b></td><td>Enter the user name (in the <code><i>&lt;LocalOrDomainUserName&gt;</i></code> format) and password of a user account that has required permissions to access the instance.</td></tr><tr><td><b>Public key authentication</b></td><td>Do the following:<ol type="i"><li>Enter the user name (in the <code><i>&lt;LocalOrDomainUserName&gt;</i></code> format) and password of a user account that has required permissions to access the instance.</li><li>Click <b>Browse</b>. Browse for and then</li></ol></td></tr></table></li></ol></td></tr>
</table>

Protocol option	Instructions
	select the file with the private key, and click **Open**. For information on how to obtain the private key, see AWS documentation. iii. *Only if the private key is encrypted.* Enter the private key passphrase.
WinRM	Select this option to use the WinRM protocol for instance access and to enable the credential group adjustment for the actual WinRM server configuration. a. From the Transport drop-down menu, select the transport protocol of the WinRM server in the instance. b. In the Port field, enter the WinRM server port number. c. Enter the user name (in the `<localuser>`, `<domain>\<user>`, or `<user>@<domain>` format) and password of a user account that has required permissions to access the instance.

6. Click **Save**.
7. Click **Assign**.

The name of the assigned credential group appears in the Credential group column of the Instances panel. HYCU for AWS performs instance discovery after you assign the credentials to the instance and the Discovery status in the Instances panel is updated accordingly.

> 💡 Tip If several instances share the same user name and password, you can use multiple selection to assign the same credential group to them.

To unassign a credential group from an instance, in the Instances panel, select the instance, click 🔑 **Credentials**, and then click **Unassign**.

You can also edit any of the existing credential groups (select a credential group, click ✎ **Edit** , and then make the required modifications) or delete the ones that you do not need anymore (select a credential group, and then click 🗑 **Delete**).

Chapter 4

Protecting instances

HYCU for AWS enables you to protect your instance data with fast and reliable backup and restore operations.

Prerequisites

- To protect instances in Virtual Private Clouds (VPC) without public IPs or in subnets without public IPs, you must create the following VPC endpoints:
  - Interface endpoints: Amazon EC2 (`ec2`), AWS Security Token Service (`sts`), Amazon SQS (`sqs`), and Amazon SNS (`sns`)
  - Gateway endpoint for Amazon S3

  For details on how to enable AWS VPC endpoints, see AWS documentation.
- The security group that the instance belongs to must have an inbound firewall rule for port 443 (HTTPS), source IP 0.0.0.0/0 and an outbound firewall rule for port 443 (HTTPS), destination IP 0.0.0.0/0.

  For instructions on how to configure and apply the network firewall rule, see AWS documentation.

Limitations

- Instance memory is not protected.
- Crash consistency of backup data is guaranteed only for each volume individually.

Considerations

- Keep in mind that the role you have assigned determines what kind of actions you can perform. For details on roles, see "Managing roles" on page 90.
- Data in instance backup images, copies of backup images, and data archives that HYCU for AWS creates is crash-consistent, but it may not always be application-consistent. If pre-snapshot scripts are not provided, the application consistency of backup data is limited to applications that store their data on a single volume, and instances and applications that comply with the prerequisites for creating a Windows Volume Shadow Copy Service (VSS) snapshot. For more information about Windows VSS snapshot prerequisites, see "Backing up instances" on page 36.

For details on how to efficiently protect instance data, see the following sections:

- "Configuring instance backup options" below
- "Backing up instances" on page 36
- "Restoring instances" on page 38
- "Restoring individual files or folders" on page 46

Configuring instance backup options

Before you start protecting instances, you can adjust instance protection to the needs of your data protection environment by configuring backup options.

Backup option	Description
Running pre/post scripts	You can use the pre-snapshot and post-snapshot scripts to perform necessary actions before and after the snapshot of an instance is created. For example, if the instance hosts a database management system, you may want to put the database offline before the snapshot is created to ensure an application-consistent backup and bring the database back online when the snapshot creation completes.
Excluding volumes from the backup	You can specify any volume to be excluded from the instance backup.
Allowing the restore of individual files	You can allow the restore of individual files if your data protection needs require that only individual files are restored, and not the entire instance. As an alternative to allowing the restore of individual files by using the Configuration option described in this procedure, you can also tag an instance in AWS, and by doing so, instruct HYCU for AWS to allow it automatically. For details, see "Allowing the restore of files by tagging the instance in AWS" on page 36.

Prerequisites

Only if you plan to use pre-snapshot and post-snapshot scripts.

- Access to the instance file system must be enabled. For instructions, see "Enabling access to data" on page 29.
- A script must be available in an accessible folder.
- The user account must have permissions to run a script on the instance with the assigned credentials.

Considerations

- *Only if you plan to use pre-snapshot and post-snapshot scripts.* The scripts are run from the home directory of the user account that HYCU for AWS uses for running the scripts.

The following account is used: the user account that is assigned to the instance in HYCU for AWS through a credential group.

- *Only if you plan to exclude the boot volume from the backup.* When restoring the instance whose boot volume was excluded from the backup, the Restore Instance and Clone Instance options are not available.

Accessing the Instances panel

To access the Instances panel, in the navigation pane, click **Instances**. Alternatively, in the Dashboard panel, click the **Instances** widget.

Procedure

1. In the Instances panel, select the instance for which you want to configure backup options.

   > Tip To configure the same backup options for multiple instances at once, select the preferred instances.
   >
   > Keep in mind that you cannot configure volume exclusion from backup for multiple instances at the same time. You can edit other backup options only if they currently have the same settings for all selected instances.

2. Click **Configuration**. The Instance Configuration dialog box opens.
3. Depending on what you want to do, perform the required action:
   - Run the pre-snapshot and post-snapshot scripts:

     On the Pre/post scripts tab, do the following:

     - In the Pre-snapshot script field, enter the script that HYCU for AWS runs before it creates a snapshot of the instance. The following are examples of the scripts:
       - GNU/Linux: `bash /home/<UserName>/freeze_db.sh`
       - Microsoft Windows: `%USERPROFILE%\quiesce_db.bat`
     - In the Post-snapshot script field, enter the script that HYCU for AWS runs after it creates a snapshot of the instance. The following are examples of the scripts:
       - GNU/Linux: `bash /home/<UserName>/thaw_db.sh`
       - Microsoft Windows: `%USERPROFILE%\resume_db.bat`
   - Exclude volumes from the backup:

     On the Exclude from backup tab, select the volumes that you want to exclude from the backup.
   - Allow the restore of individual files or folders:

     On the Restore individual files tab, enable the **Enable restore of individual files** switch.
4. Click **Save**.

Allowing the restore of files by tagging the instance in AWS

As an alternative to allowing the restore of individual instance files in HYCU for AWS, you can add the `hycu-enable-flr` tag as the label or the custom tag to the instance in AWS, and by doing so, instruct HYCU for AWS to allow it automatically.

Procedure

In AWS, use the following name/value pair for the instance:

Name	Value
`hycu-enable-flr`	True[a]

[a] By setting the value to `False`, you disallow the restore of individual files for the specific instance.

If the instance has credentials assigned, HYCU for AWS automatically allows the restore of its individual files. Otherwise, you must assign the credentials to the instance. For details on how to do this, see "Enabling access to data" on page 29.

Backing up instances

With HYCU for AWS, you can back up your instances in a fast and efficient way.

Prerequisite

For instances running Microsoft Windows: If you want HYCU for AWS to create a Windows VSS snapshot for the instance to ensure application consistency of backup data, you must create an IAM role for VSS-enabled snapshots and attach it to the instance as described in AWS documentation.

> Note You can check if VSS snapshots were successfully configured for the instance in the backup task summary and report.

Prerequisites when planning to restore individual files or folders

- The security group that the instance belongs to must have an inbound rule for the following ports:
  - WinRM: TCP port 5986 (or a different port if configured for SSH communication)
  - GNU/Linux: TCP port 22 (or a different port if configured for SSH communication)

  For instructions on how to configure and apply the network firewall rule, see AWS documentation.
- On the instances that you plan to protect, WinRM is configured to use a TCP port (by default, 5986) for HTTPS or HTTP communication. The firewall is configured to enable inbound network traffic through this port.
- The restore of individual files or folders is enabled for the instance. For instructions on

how to enable the restore of individual files or folders, see “Configuring instance backup options” on page 34.

- The correct credential group is assigned to the original instance, and the corresponding credentials belong to a user account with sufficient privileges. For instructions on how to assign access credentials, see “Enabling access to data” on page 29.

Prerequisites when planning to use pre-snapshot or post-snapshot scripts

- The security group that the instance belongs to must have an inbound rule for the following ports:
  - WinRM: TCP port 5986 (or a different port if configured for SSH communication)
  - GNU/Linux: TCP port 22 (or a different port if configured for SSH communication)

  For instructions on how to configure and apply the network firewall rule, see AWS documentation.
- *For instances running GNU/Linux:* On the instances that you plan to protect, an SSH server is installed and configured to use a TCP port (by default, 22) for SSH communication. The firewall is configured to enable inbound network traffic through this port.
- *For instances running Microsoft Windows:* On the instances that you plan to protect, WinRM is configured to use a TCP port (by default, 5986) for HTTPS or HTTP communication. The firewall is configured to enable inbound network traffic through this port.
- *For instances running Microsoft Windows, and for instances running GNU/Linux with non-default configuration of SSH server or if you want to use custom user accounts for running the script:* The correct credential group is assigned to the instance and the corresponding credentials belong to a user account with sufficient privileges. For instructions on how to assign access credentials, see “Enabling access to data” on page 29.

> ### Accessing the Instances panel
>
> To access the Instances panel, in the navigation pane, click **Instances**. Alternatively, in the Dashboard panel, click the **Instances** widget.

Procedure

1. Select the instances that you want to back up. You can update the instance list by clicking **Synchronize**. In a protection set with a large number of accounts, the update may take a while.

   To narrow down the list of displayed instances, use the filtering options as described in “Filtering and sorting data in panels” on page 72.
2. Click **Policies**. The Policies dialog box opens.
3. From the list of available policies, select the desired policy.
4. Click **Assign** to assign the policy to the selected instances.

When you assign a policy to an instance, a backup task starts immediately. Subsequent backups are scheduled according to the values defined in the policy.

> Note The first backup task may be delayed if a backup image of the instance already exists.

You can also perform a manual backup of individual instances at any time. For details, see "Performing manual backups" on page 82.

Restoring instances

HYCU for AWS enables you to restore an entire instance or its individual volumes to a specific point in time.

Consideration

Only one restore task can run at the same time for the instance.

When you restore an instance or its volumes, you can select among the following restore options:

Restore option	Description	Instructions
Restore Instance	Enables you to restore an instance and its volumes to the original location with the same settings.	"Restoring an instance" below
Clone Instance	Enables you to restore an instance and its volumes by creating a clone of the instance.	"Cloning an instance" on the next page
Restore Volumes	Enables you to restore instance volumes and attach them to the same instance.	"Restoring volumes" on page 43
Clone Volumes	Enables you to restore instance volumes by creating their clones and attaching them to the same or a different instance.	"Cloning volumes" on page 43
Export Volumes	Enables you to restore instance volumes to the same or a different account or zone without attaching them to an instance.	"Exporting volumes" on page 45

Accessing the Instances panel

To access the Instances panel, in the navigation pane, click **Instances**. Alternatively, in the Dashboard panel, click the **Instances** widget.

Restoring an instance

You can restore an instance and its volumes to the original location with the same settings. In this case, you replace the original instance with the restored one.

Consideration

Any data changes after the last successful backup are not protected and therefore cannot be restored.

Procedure

1. In the Instances panel, click the instance that you want to restore to open the Details section.

   > Note The Details section appears only if you click an instance. Selecting the check box before the name of the instance does not open the Details section.

2. In the Details section that appears at the bottom of the screen, select the desired restore point.
3. Click **Restore Instance**. The Restore Options dialog box opens.
4. Select **Restore Instance**, and then click **Next**.
5. From the Restore from drop-down menu, select which tier you want to use for the restore. Your restore point can contain one or more tiers among which you can select:
   - **Automatic**: This option ensures the fastest and most cost-effective restore.
   - **Backup (Snapshot)**
   - **Backup (Target)**
   - **Copy**
   - **Archive — (daily, weekly, monthly, yearly)**
6. From the Volumes drop-down menu, select the instance volumes that you want to restore.

   > Note All volumes of the instance are preselected for the restore. With such selection, the entire instance is restored. The boot volume is restored even if you do not select it.

7. Click **Restore**.

Cloning an instance

You can clone an instance by restoring it to its original or a new location with custom settings. In this case, you create a new instance containing the restored data alongside the original instance. When cloning an instance, you can change the following properties: the selection of the backed up volumes, the destination account, region, and zone, and the instance network configuration.

Limitation

You cannot restore instances that belong to a deleted AWS account. Such instances are not listed in the Instances panel of the HYCU for AWS web user interface.

Procedure

1. In the Instances panel, click the instance that you want to restore to open the Details section.

   > Note The Details section appears only if you click an instance. Selecting the check box before the name of the instance will not open the Details section.

2. In the Details section that appears at the bottom of the screen, select the desired restore point.
3. Click **Restore Instance**. The Restore Options dialog box opens.
4. Select **Clone Instance**, and then click **Next**.
5. In the New instance name field, specify a new name for the instance.
6. From the Restore from drop-down menu, select which tier you want to use for the restore. Your restore point can contain one or more tiers among which you can select:
   - **Automatic**: This option ensures the fastest and most cost-effective restore.
   - **Backup (Snapshot)**
   - **Backup (Target)**
   - **Copy**
   - **Archive — (daily, weekly, monthly, yearly)**
7. *Only if the original operating system image was not found.* From the Image drop-down menu, select the operating system image you want to use.

   To use a custom image, enable the **Use custom image** switch and enter the image AMI ID.

8. From the Destination account ID drop-down menu, select the account ID to which you want to restore the instance. The original account ID of the instance is preselected. You can choose from account IDs that belong to the currently selected protection set and that your user account can access.
9. From the Destination region and Destination zone drop-down menus, select the AWS region and zone to which you want to restore the instance. The original region and zone of the instance are preselected.
10. Under Volume name, do the following:

    a. Select the instance volumes that you want to restore.

    > Note All volumes of the instance are preselected for the restore. With such selection, the entire instance is restored. The boot volume is restored even if you do not select it.

    b. Edit the volumes as required. For each selected volumes, do the following:

    i. Click **Edit Volume**.

    ii. *Only if you do not want HYCU for AWS to automatically generate a name for the restored volume device or volume.* Do the following:

i. In the New device name field, enter a name for the restored volume device.

ii. In the New volume name, enter a name for the restored volume.

iii. If you want to change the volume type, from the Volume type drop-down menu, select one of the available volume types for the restored volume. By default, the original volume type is selected.

The list shows only the volume types that match the required volume size and can include the following volume types: General Purpose SSD, Previous Generation Volume, and/or Provisioned IOPS SSD.

If you selected Provisioned IOPS SSD or General Purpose SSD, enter the IOPS number.

iv. If you want to add labels to the restored volume, click **Add Tags**, enter a key and a value, and then click **Add** for each label that you want to add.

> Note If the selected volume already has one or more labels added, they are listed under Labels. If you want to delete any of the added labels, click ✕ next to it.

v. Click **Save**.

11. Under Network interfaces, review the list of networks that the original instance was configured in at the time of backup. The list shows the following for each such network:

- VPC ID
- Subnet ID

For each configured network interface, you can separately adjust its public and private IP address types. By default, the public IP address configuration of the original instance is kept.

Modifying network settings

If you want to modify network settings, you can add an additional network interface, edit an existing network interface, or delete a network interface:

- Click **Add network interface** to add a network interface or click ✎ **Edit** next to the network interface that you want to edit, and then follow these steps:

a. From the Subnet network drop-down menu, select the subnet.

b. From the Security group drop-down menu, select the security group.

c. In the Public address type field, select the public IP address for the network interface. You can select among the following options:

Option	Description
None	The network interface does not use a public IP address. This option is preselected if the network interface of the original instance did not use a public IP address.

Auto-assign	The network interface uses an automatically allocated public IP address. This option is preselected if the network interface of the original instance used a public IP address. Note Auto-assign will not work if the Auto-assign public IPv4 address on a subnet option is set to `No` or if more than one network interface is specified.
Elastic IP (Reserved)	The network interface uses an elastic public IP address that was reserved in Amazon EC2 in advance.
Elastic IP (New)	The network interface uses a new elastic public IP address. Note Allocation of the IP address in Amazon EC2 is performed at the very beginning of the restore. If the allocation fails, the restore task is terminated without being logged.

d. In the Private address type field, select the private IP address for the network interface. You can select between the following options:

Option	Description
Auto-assign	The network interface uses an automatically allocated private IP address. This option is selected by default.
Custom	The network interface uses a private IP address that is defined by you. ⚠ Important Use of this option might result in IP address conflicts.

e. Click **Add** or **Save**.

- Click 🗑 **Delete** next to the network interface that you want to delete. Keep in mind that you cannot restore the instance without a network interface.

12. If you want to add tags to the restored instance, click **Add Tags** and then for each that you want to add enter a key and a value, and then click **Add**.

> Note If the selected instance already has one or more tags added, they are listed under Custom metadata. If you want to delete any of the added tags, click × next to it.

13. Click **Validate** to validate the restore specification.

14. Click **Restore**.

Restoring volumes

You can restore instance volumes and attach them to the same instance. In this case, you replace the original volumes with the restored ones.

Procedure

1. In the Instances panel, click the instance whose volumes you want to restore to open the Details section.

   > Note The Details section appears only if you click an instance. Selecting the check box before the name of the instance will not open the Details section.

2. In the Details section that appears at the bottom of the screen, select the desired restore point.
3. Click **Restore Instance**. The Restore Options dialog box opens.
4. Select **Restore Volumes**, and then click **Next**.
5. From the list of volumes that are available for the restore, select the ones that you want to restore, and then click **Next**.

   > Note If you select the boot volume, the instance will be shut down and restarted when the
   >
   > a. Click **Validate** to validate the restore specification.
   >
   > volumes are restored.

6. From the Restore from drop-down menu, select which tier you want to use for the restore. Your restore point can contain one or more tiers among which you can select:
   - **Automatic**: This option ensures the fastest and most cost-effective restore.
   - **Backup (Snapshot)**
   - **Backup (Target)**
   - **Copy**
   - **Archive — (daily, weekly, monthly, yearly)**
7. Click **Validate** to validate the restore specification.
8. Click **Restore**.

Cloning volumes

You can create clones of instance volumes by restoring them and attaching them to the same or a different instance. In this case, the original volumes will not be overwritten.

Limitation

You can attach the restored volumes only to an instance that is running the same operating system as the original instance and that belongs to the same protection set as the original instance.

Consideration

For details on how the restored volumes are named, see "Objects created by the service" on page 101.

Procedure

1. In the Instances panel, click the instance whose volumes you want to restore to open the Details section.

   > Note The Details section appears only if you click an instance. Selecting the check box before the name of the instance will not open the Details section.

2. In the Details section that appears at the bottom of the screen, select the desired restore point.
3. Click **Restore Instance**. The Restore Options dialog box opens.
4. Select **Clone Volumes**, and then click **Next**.
5. From the list of volumes that are available for the restore, select the ones that you want to restore, and then click **Next**.
6. From the Restore from drop-down menu, select which tier you want to use for the restore. Your restore point can contain one or more tiers among which you can select:
   - **Automatic**: This option ensures the fastest and most cost-effective restore.
   - **Backup (Snapshot)**
   - **Backup (Target)**
   - **Copy**
   - **Archive — (daily, weekly, monthly, yearly)**
7. Select the account and the zone that contain the instance to which you want to attach the restored volumes, and then select the instance to which you want to attach the restored volumes.
8. Edit the volumes as required. For each selected volumes, do the following:

   a. Click **Edit Volume**.

   b. *Only if you do not want HYCU for AWS to automatically generate a name for the restored volume device or volume.* Do the following:

      i. In the New device name field, enter a name for the restored volume device.

      ii. In the New volume name, enter a name for the restored volume.

   c. If you want to change the volume type, from the Volume type drop-down menu, select one of the available volume types for the restored volume. By default, the original volume type is selected.

      The list shows only the volume types that match the required volume size and can include the following volume types: General Purpose SSD, Previous Generation Volume, and/or Provisioned IOPS SSD.

If you selected Provisioned IOPS SSD or General Purpose SSD, enter the IOPS number.

d. If you want to add labels to the restored volume, click **Add Tags**, enter a key and a value, and then click **Add** for each label that you want to add.

> Note If the selected volume already has one or more labels added, they are listed under Labels. If you want to delete any of the added labels, click ✕ next to it.

e. Click **Save**.

9. Click **Validate** to validate the restore specification.
10. Click **Restore**.

Exporting volumes

You can export instance volumes by restoring them to the same or a different account or zone. In this case, the volumes will not be attached to any instance.

Prerequisite

Only if you plan to restore volumes to a different account. The default network must be set for the account to which you plan to restore volumes, or the account to which you plan to restore volumes must have the same network as the instance whose volumes you plan to restore.

Consideration

For details on how the restored volumes are named, see "Objects created by the service" on page 101.

Procedure

1. In the Instances panel, click the instance whose volumes you want to restore to open the Details section.

   > Note The Details section appears only if you click an instance. Selecting the check box before the name of the instance will not open the Details section.

2. In the Details section that appears at the bottom of the screen, select the desired restore point.
3. Click **Restore Instance**. The Restore Options dialog box opens.
4. Select **Export Volumes**, and then click **Next**.
5. From the list of volumes that are available for the restore, select the ones that you want to restore, and then click **Next**.
6. From the Restore from drop-down menu, select which tier you want to use for the restore. Your restore point can contain one or more tiers among which you can select:

- **Automatic**: This option ensures the fastest and most cost-effective restore.
- **Backup (Snapshot)**
- **Backup (Target)**
- **Copy**
- **Archive — (daily, weekly, monthly, yearly)**

7. From the Target account ID drop-down menu, select the account to which you want to restore the volumes. You can choose from the accounts that belong to the currently selected protection set.
8. From the Target region and Target zone drop-down menus, select the AWS region and zone to which you want to restore the volumes.
9. Edit the volumes as required. For each selected volumes, do the following:
   a. Click ✎ **Edit Volume**.
   b. *Only if you do not want HYCU for AWS to automatically generate a name for the restored volume device or volume.* Do the following:
      i. In the New device name field, enter a name for the restored volume device.
      ii. In the New volume name, enter a name for the restored volume.
   c. If you want to change the volume type, from the Volume type drop-down menu, select one of the available volume types for the restored volume. By default, the original volume type is selected.

      The list shows only the volume types that match the required volume size and can include the following volume types: General Purpose SSD, Previous Generation Volume, and/or Provisioned IOPS SSD.

      If you selected Provisioned IOPS SSD or General Purpose SSD, enter the IOPS number.
   d. If you want to add labels to the restored volume, click **Add Tags**, enter a key and a value, and then click **Add** for each label that you want to add.

      > Note If the selected volume already has one or more labels added, they are listed under Labels. If you want to delete any of the added labels, click × next to it.
   e. Click **Save**.
10. Click **Validate** to validate the restore specification.
11. Click **Restore**.

Restoring individual files or folders

You can restore one or more individual files or folders to an instance or to a target.

Depending on where you want to restore individual files or folders, see one of the following sections:

- “Restoring files or folders to an instance” below
- “Restoring files or folders to a target” on page 51

> Accessing the Instances panel
>
> To access the Instances panel, in the navigation pane, click 🖥 **Instances**. Alternatively, in the Dashboard panel, click the **Instances** widget.

Restoring files or folders to an instance

You can restore one or more individual files or folders to the same or a new location on the original instance, or to a custom location on a different instance.

Prerequisites

- The instance to which you are restoring data is up and running.
- The target volume uses one of the supported file systems. For details, see the *HYCU for AWS Compatibility Matrix*.
- The security group that the instance belongs to must have an inbound rule for the following ports:
  - WinRM: TCP port 5986 (or a different port if configured for SSH communication)
  - GNU/Linux: TCP port 22 (or a different port if configured for SSH communication)

  For instructions on how to configure and apply the network firewall rule, see AWS documentation.
- *For Linux instances:*
  - On the original instance, an SSH server is installed and configured to use a TCP port (by default, 22) for SSH communication. The firewall is configured to enable inbound network traffic through this port.
  - *Only if the SSH server is configured to use a non-default TCP port or public key authentication, or OS Login is enabled on the instance in* Amazon EC2. An appropriate credential group is assigned to the original instance.
- *For Windows instances:*
  - On the original instance, WinRM is configured to use a TCP port (by default, 5986) for HTTPS or HTTP communication. The firewall is configured to enable inbound network traffic through this port.
  - An appropriate credential group is assigned to the original instance, and the supplied credentials belong to a user account with sufficient privileges. Credential group assignment is performed automatically by HYCU for AWS. For instructions on how to manually assign credential groups, see “Enabling access to data” on page 29.
  - *Only if you plan to restore individual files or folders to a different instance.* The discovery status of the instance to which you want to restore the individual files or folders is ✓.

Limitations

- You cannot restore individual files or folders located on an extended Master Boot Record (MBR) partition to their original location.
- *For restoring files or folders to a different instance:*
  - You can restore individual files or folders only to an instance that is running the same operating system as the original instance and that belongs to the same protection set as the original instance.
  - *Only if you plan to enable the Restore ACL option.* An LDAP directory service or any similar directory information service is configured.

Considerations

- HYCU for AWS considers folders as containers of the file system objects. This means that in a restore task:
  - Folders are never renamed.
  - Folder access control lists (ACLs) are never restored and the original folder ACLs are kept on the file system.
- For details on how the restored individual files or folders are named, see "Objects created by the service" on page 101.

Restoring files or folders to the original instance

Procedure

1. In the Instances panel, click the instance that contains the files or folders that you want to restore. The Details section appears at the bottom of the screen.

   > Note The Details section appears only if you click an instance. Selecting the check box before the name of the instance does not open the Details section.

2. In the Details section, select the desired restore point, and then click **Restore Files**.

   If needed, click < or > to move between the pages, or enter a page number to go directly to that page. You can also adjust the number of items shown in a page.

3. In the File Restore Options dialog box, select **Restore to original instance**, and then click **Next**.
4. In the Restore Settings dialog box, do the following:

   a. From the Restore from drop-down menu, select which tier you want to use for the restore. Your restore point can contain one or more tiers among which you can select:

      - **Automatic**: This option ensures the fastest and most cost-effective restore.
      - **Backup (Snapshot)**
      - **Backup (Target)**

      - **Copy**
      - **Archive — (daily, weekly, monthly, yearly)**

   b. In the Volumes drop-down menu, make sure only the volumes with the files or folders that you want to restore are selected.

   c. Click **Next**.

5. In the Choose Files and Folders dialog box, from the list of available files and folders, select the ones that you want to restore, and then click **Next**.

   If needed, click < or > to move between the pages, or enter a page number to go directly to that page. You can also adjust the number of items shown in a page.

   > Tip You can also search for a file or a folder by entering its name in the Search field and then pressing **Enter**.

6. In the Restore to Instance dialog box, do the following:

   a. Select the location on the instance where you want to restore the files or folders, and provide the required information:

      - **Original location**

        Select how the restore should save the files when there is a file with the same name at the original location (overwrite the file, rename the original file, or rename the restored file).

        For naming conventions, see "Objects created by the service" on page 101.

      - **Alternate location**

        Specify the path to an alternate location on the instance in the following format:

        - Linux:

          ```
          /<Path>/<FolderName>
          ```

        - Windows:

          ```
          <DriveLetter>:\<Path>\<FolderName>
          ```

        The restored file overwrites the file with the same name that might exist at the alternate location.

   b. Use the **Restore ACL** switch if you want to restore the original access control list. If enabled, HYCU for AWS preserves original ACLs. If disabled, HYCU for AWS applies inherited ACLs on the restored files (according to the file system ACL inheritance rules).

7. Click **Restore**.

Restoring files or folders to a different instance

Procedure

1. In the Instances panel, click the instance that contains the files or folders that you want to restore. The Details section appears at the bottom of the screen.

   > Note The Details section appears only if you click an instance. Selecting the check box before the name of the instance does not open the Details section.

2. In the Details section, select the desired restore point, and then click **Restore Files**.

   If needed, click ‹ or › to move between the pages, or enter a page number to go directly to that page. You can also adjust the number of items shown in a page.

3. In the File Restore Options dialog box, select **Restore to different instance**, and then click **Next**.

4. In the Restore Settings dialog box, do the following:

   a. From the Restore from drop-down menu, select which tier you want to use for the restore. Your restore point can contain one or more tiers among which you can select:
      - **Automatic**: This option ensures the fastest and most cost-effective restore.
      - **Backup (Snapshot)**
      - **Backup (Target)**
      - **Copy**
      - **Archive — (daily, weekly, monthly, yearly)**

   b. From the Zone drop-down menu, select the zone to which the instance to which you want to restore data belongs.

   c. From the Instances drop-down menu, select the instance to which you want to restore data.

   d. Click **Next**.

5. In the Choose Files and Folders dialog box, from the list of available files and folders, select the ones that you want to restore, and then click **Next**.

   If needed, click ‹ or › to move between the pages, or enter a page number to go directly to that page. You can also adjust the number of items shown in a page.

   > Tip You can also search for a file or a folder by entering its name in the Search field and then pressing **Enter**.

6. In the Restore to Different Instance dialog box, do the following:

   a. Specify the path to a custom location on the instance to which you want to restore data in the following format:
      - Linux:

```
/<Path>/<FolderName>
```

  - Windows:

    ```
    <DriveLetter>:\<Path>\<FolderName>
    ```

  The restored file overwrites the file with the same name that might exist at the custom location on the instance to which you want to restore data.

  b. Use the **Restore ACL** switch if you want to restore the original access control list. If enabled, HYCU for AWS preserves original ACLs. If disabled, HYCU for AWS applies inherited ACLs on the restored files (according to the file system ACL inheritance rules).

7. Click **Restore**.

Restoring files or folders to a target

Prerequisite

At least one target is set up in the protection set that includes the account of the original instance. For information on how to add manually created targets, see “Adding a bucket to HYCU for AWS as a target” on page 19.

Consideration

For details on how the restored individual files or folders are named, see “Objects created by the service” on page 101.

Procedure

1. In the Instances panel, click the instance that contains the files or folders that you want to restore. The Details section appears at the bottom of the screen.

   > Note The Details section appears only if you click an instance. Selecting the check box before the name of the instance does not open the Details section.

2. In the Details section, select the desired restore point, and then click **Restore Files**.

   If needed, click < or > to move between the pages, or enter a page number to go directly to that page. You can also adjust the number of items shown in a page.

3. In the File Restore Options dialog box, select **Restore to target**, and then click **Next**.

4. In the Restore Settings dialog box, do the following:

   a. From the Restore from drop-down menu, select which tier you want to use for the restore. Your restore point can contain one or more tiers among which you can select:

      - **Automatic**: This option ensures the fastest and most cost-effective restore.
      - **Backup (Snapshot)**
      - **Backup (Target)**
      - **Copy**
      - **Archive — (daily, weekly, monthly, yearly)**

   b. In the Volumes drop-down menu, make sure only the volumes with the files or folders that you want to restore are selected.

   c. Click **Next**.

5. In the Choose Files and Folders dialog box, from the list of available files and folders, select the ones that you want to restore, and then click **Next**.

   If needed, click < or > to move between the pages, or enter a page number to go directly to that page. You can also adjust the number of items shown in a page.

   > Tip You can also search for a file or a folder by entering its name in the Search field and then pressing **Enter**.

6. From the Target name drop-down menu, select a target to which you want to restore data.

7. Click **Restore**.

Chapter 5

Protecting buckets

HYCU for AWS enables you to protect your data in buckets with fast and reliable backup and restore operations. After you optionally configure bucket backup options and back up the bucket, you can choose to restore one or more individual files or folders inside the bucket.

Limitation

Bucket data (backup data, copies of backup data, and data archives) can be stored only to manually created targets, and not to automatically created targets or as a snapshot. For instructions on how to add a bucket to HYCU for AWS as a target, see "Adding a bucket to HYCU for AWS as a target" on page 19.

Consideration

Keep in mind that the role you have assigned determines what kind of actions you can perform. For details on roles, see "Managing roles" on page 90.

For details on how to protect bucket data efficiently, see the following sections:

- "Configuring bucket backup options" below
- "Backing up buckets" on page 55
- "Restoring buckets" on page 55

Configuring bucket backup options

Before you start protecting data in buckets, you can adjust bucket protection to the needs of your data protection environment by using bucket backup options.

Backup option	Description
Specifying the temporary instance location and subnet	You can specify the location and the subnet where you want HYCU for AWS to create a temporary instance during the backup. By default, the temporary instance is created in the original account of the bucket.
Running pre/post scripts	You can specify the pre-backup and post-backup scripts to perform necessary actions before and after the backup of the bucket is performed.

Prerequisite

Only if you plan to specify pre-backup and post-backup scripts. The `#!/usr/bin/env python3` header must be specified in the script.

Limitations

Only if you plan to specify pre-backup and post-backup scripts.

- Currently only Python scripts are supported.
- The pre-backup and post-backup scripts must be located in the same account and in the same region as the bucket.

Consideration

Only when specifying the location or the subnet for a temporary instance. If not specified otherwise, the temporary instance will be created in the same region as the bucket (for example, US-EAST-1).

> ### Accessing the Buckets panel
>
> To access the Buckets panel, in the navigation pane, click **Buckets**.

Procedure

1. In the Buckets panel, select the bucket for which you want to configure backup options.
2. Click **Configuration**. The Bucket Configuration dialog box opens.
3. Depending on what you want to do, provide the required information:
   - Specify the region and the subnet where you want HYCU for AWS to create a temporary instance:
     a. From the Region drop-down menu, select the preferred region.

        > Note It is recommended that you select the same region as the one where the bucket resides. Otherwise, you will be charged for outbound data transfer. For details, see Amazon S3 pricing.

     b. From the Subnet drop-down menu, select the preferred subnet. By default, the temporary instance is created in the default subnet of the preferred region and zone.

        > Important A policy cannot be assigned to a bucket on which HYCU for AWS could not detect the subnet.

   - Specify the scripts to perform necessary actions before and/or after the backup of the bucket is performed:
     - In the Pre-backup script field, enter the path to the script that HYCU for AWS will run just before it performs the backup of the bucket.
     - In the Post-backup script field, enter the path to the script that HYCU for AWS will run immediately after it performs the backup of the bucket.

> ⚠ Important When entering the path to the script, make sure to enter it correctly, including lowercase and uppercase letters, as the path is case sensitive. You must specify the path in the following format:
>
> ```
> s3://bucket-name/script.py parameter1 parameter2 ...
> ```

4. Click **Save**.

Backing up buckets

With HYCU for AWS, you can back up data that is stored in Amazon S3 buckets in a fast and efficient way.

Consideration

The information on the bucket size becomes available in the Detail view after you assign a policy to the bucket. Keep in mind that this size is always rounded up to the full unit, the minimum being 1 GiB.

> Accessing the Buckets panel
>
> To access the Buckets panel, in the navigation pane, click **Buckets**.

Procedure

1. In the Buckets panel, select the buckets that you want to back up. You can update the bucket list by clicking **Synchronize**.

   > Tip To narrow down the list of displayed buckets, you can use the filtering options as described in "Filtering and sorting data in panels" on page 72.

2. Click **Policies**. The Policies dialog box opens.
3. From the list of available policies, select the desired policy.
4. Click **Assign** to assign the policy to the selected buckets.

After you assign a policy to a bucket, a backup task starts immediately. Subsequent backups are scheduled according to the values defined in the policy.

> Note If required, you can also perform a manual backup of any bucket at any time. For details, see "Performing manual backups" on page 82.

Restoring buckets

HYCU for AWS enables you to restore one or more individual files or folders inside an Amazon S3 bucket to the original or a different bucket.

Consideration

For details on how the restored individual files or folders are named, see "Objects created by the service" on page 101.

Procedure

1. In the Buckets panel, click the bucket that contains the files or folders that you want to restore. The Details section appears at the bottom of the screen.

   > Note The Details section appears only if you click a bucket. Selecting the check box before the name of the bucket does not open the Details section.

2. In the Details section, select the desired restore point, and then click ↻ **Restore Files**.

   If needed, click < or > to move between the pages, or enter a page number to go directly to that page. You can also adjust the number of items shown in a page.

3. From the Restore from drop-down menu, select which tier you want to use for the restore. Your restore point can contain one or more tiers among which you can select:
   - **Automatic**: This option ensures the fastest and most cost-effective restore.
   - **Backup (Target)**
   - **Copy**
   - **Archive — (daily, weekly, monthly, yearly)**

4. In the Choose Files and Folders dialog box, from the list of available files and folders, select the ones that you want to restore, and then click **Next**.

   If needed, click < or > to move between the pages, or enter a page number to go directly to that page. You can also adjust the number of items shown in a page.

   > Tip You can also search for a file or a folder by entering its name in the Search field and then pressing **Enter**.

5. Depending on where you want to restore data, select the desired restore option, and then follow the instructions:

Restore option	Instructions
Restore to original bucket	a. Select the location on the bucket where you want to restore the files or folders, and provide the required information: • **Original location** Specify which action should be performed during the restore operation if a file with the same name already exists in the selected location (overwrite the file, rename the original file, or rename the restored file). • **Alternate location** Specify the path to an alternate location on the bucket. The restored file overwrites the file with the same name that might exist in the alternate location. b. If you want to add custom metadata tags to the restored bucket objects, click **Add Tags**, enter a key and value, and then click

Restore option	Instructions
	Add for each custom metadata tag that you want to add. Note If you want to delete any of the added custom metadata tags, click × next to it.
Restore to different bucket	a. From the Account ID drop-down menu, select the account that contains the bucket to which you want to restore data. Note You can select only among the accounts inside the selected protection set. b. From the Bucket name drop-down menu, select the name of the bucket to which you want to restore data, and then click **Next**. c. Select the location on the bucket where you want to restore the files or folders, and provide the required information: • **Original location** Specify which action should be performed during the restore operation if a file with the same name already exists in the selected location (overwrite the file, rename the original file, or rename the restored file). • **Alternate location** Specify the path to an alternate location on the bucket. The restored file overwrites the file with the same name that might exist in the alternate location. d. If you want to add custom metadata tags to the restored bucket objects, click **Add Tags**, enter a key and value, and then click **Add** for each custom metadata tag that you want to add. Note If you want to delete any of the added custom metadata tags, click × next to it.

6. Click **Restore**.

Chapter 6

Performing daily tasks

To ensure your data protection environment is in the optimal state in terms of security, reliability, and efficiency, HYCU for AWS provides various mechanisms to support your daily activities.

Consideration

Keep in mind that the role you have assigned determines what kind of actions you can perform. For details on roles, see "Managing roles" on page 90.

I want to ...	Instructions
Get an at-a-glance overview of the data protection environment state, identify eventual bottlenecks, and inspect different areas of the data protection environment.	"Using the HYCU for AWS dashboard" on the next page
Track tasks that are running in the data protection environment and get an insight into the status of a specific task.	"Checking task statuses" on page 60
View all events that occurred in my data protection environment.	"Viewing events" on page 60
View instance and bucket details.	"Viewing instance and bucket details" on page 69
Narrow down the list of displayed items by applying filters and sort the items in panels.	"Filtering and sorting data in panels" on page 72
View target information, activate or deactivate a target, and edit or remove a target.	"Managing targets" on page 77
View policy information, edit a policy, or delete a policy.	"Managing policies" on page 80
Back up data manually.	"Performing manual backups" on page 82
Mark a restore point as expired.	"Expiring backups manually" on page 82

I want to ...	Instructions
Export data that I can view in a table in any of the panels to a JSON or CSV file.	"Exporting the contents of the panel" on page 64

Using the HYCU for AWS dashboard

The HYCU for AWS dashboard provides you with an at-a-glance overview of the data protection status in your environment. This intuitive dashboard enables you to monitor all data protection activity and to quickly identify the areas that need your attention. You can use this dashboard as a starting point for your everyday tasks because it enables you to easily access the area of interest by simply clicking the corresponding widget.

Accessing the Dashboard panel

To access the Dashboard panel, in the navigation pane, click **Dashboard**.

The following table describes what kind of information you can find within each widget.

Widget	Description
Instances	Percentage of protected instances, and the exact number of protected and unprotected instances in the protection set. An instance is considered protected if it has a policy assigned and at least one valid backup within the retention period specified in the policy. Instances that have the exclude policy assigned are omitted from the figures depicted in this widget. For details about instances, see "Protecting instances" on page 33.
Backups	Backup success rate for the last seven days.
Targets	Number of targets in the protection set, and the information about how much space is used and available for storing backup data. For details, see "Setting up targets" on page 18.
Policies	Percentage of policies that are compliant, and the number of compliant and non-compliant policies in the protection set. A policy is considered compliant if all instances or buckets to which this policy is assigned are compliant with the policy settings. For details on policies, see "Defining your backup strategy" on page 20.
Tasks	Total number of tasks in the protection set, and the number of tasks according to their status (Success, Warning, Failed, In progress) in the last 48 hours. For details on tasks, see "Checking task statuses" on the next page.
Events	Total number of events in the protection set, and the number of events according to their severity level in the last 48 hours. For details on events, see "Viewing events" on the next page.

Tip By clicking icons that denote different statuses within a widget, you are

> automatically taken to the corresponding panel with the data already filtered accordingly.

Checking task statuses

In the Tasks panel, you can do the following:

- Check the overall status of the tasks in your data protection environment.
- Check the status of tasks that are currently running.
- Check the status of completed and stopped tasks.
- Check more details about a specific task.

  The information is presented in the Details section that appears at the bottom of the screen after you select the task.

  > Tip To minimize the Details section, click ▼ **Minimize** or press the Spacebar. To return it to its original size, click ▲ **Maximize** or press the Spacebar.

- Generate a report about a specific task.

  To generate the report, select a task, and then click **View Report**. To copy the report to the clipboard, in the Task Report dialog box that opens, click **Copy to clipboard**.

- Cancel any currently running task by selecting it, and then clicking **Abort Task**. Keep in mind that you cannot abort tasks related to retention maintenance.

Accessing the Tasks panel

To access the Tasks panel, in the navigation pane, click **Tasks**. Alternatively, in the Dashboard panel, click the **Tasks** widget title.

Task information	Description
Description	Summary of the task (for example, running a backup, performing a restore, restoring individual files or folders).
Status	Current status of a task (for example, Ready, a progress bar indicating the Running status, Done, Done with errors, Failed, or Aborted).
Started	The task's start date and time.
Finished	The task's finish date and time.

Viewing events

In the Events panel, you can do the following:

- View all events that occurred in your data protection environment.
- Check more details about a specific event in the Details section that appears at the

bottom of the screen after you select the event.

> 💡 Tip If you click the related task link in the Details section, you are directed to the Tasks panel where you can view more details about the related task.

- List the events that match the specified filter.
- Configure HYCU for AWS to send notifications when new events occur in your data protection environment. For details, see "Configuring event notifications" below.

Accessing the Events panel

To access the Events panel, in the navigation pane, click 📋 **Events**. Alternatively, in the Dashboard panel, click the **Events** widget title.

The following information is available for each event:

Severity	Severity level of the event: • ✓ (Info): Events representing regular service operation. • ! (Warning): Potentially harmful situations that do not represent an immediate threat to service operation. • ✗ (Error): Errors that immediately affect service operation.
Message	Description of the event.
Category	Functional area of HYCU for AWS to which the event belongs (for example, Targets, Credentials, Policies, System for an internal event, and so on).
Timestamp	Event creation date and time.

Configuring event notifications

You can configure HYCU for AWS to send notifications when new events occur in your data protection environment. This allows you to monitor and manage your data protection environment more efficiently, and to immediately respond to the events if required. You can set up emails or webhooks as a notification channel.

> ⚠ Important Make sure to configure event notifications for each protection set separately.

Accessing the Notifications dialog box

To access the Notifications dialog box, click 📋 **Events** in the navigation pane, and then click 🔔 **Notifications** in the toolbar.

Depending on which notification channel you want to use, see one of the following sections:

- "Creating email notifications" on the next page
- "Creating webhook notifications" on the next page

Creating email notifications

Procedure

1. In the Notifications dialog box, click the **Email** tab, and then click + **New**.
2. In the Subject field, enter a subject for the email notification.
3. From the Category drop-down menu, select one or more categories. To include all categories, click **Select All**. For a description of categories, see "Viewing events" on page 60.
4. From the Status drop-down menu, select one or more statuses. To include all statuses, click **Select All**. For a description of statuses, see "Viewing events" on page 60.
5. In the Email address field, enter the recipient's email address. If you are entering more than one email address, make sure to press the Spacebar after entering each one.
6. Click **Save**.

Your changes take effect immediately and email notifications are sent to any email address that you specified in the notification settings.

You can later edit settings for existing email notifications (click ✎ **Edit** and make the required modifications) or delete the ones that you do not need anymore (click 🗑 **Delete**).

Creating webhook notifications

Procedure

1. In the Notifications dialog box, click the **Webhooks** tab, and then click + **New**.
2. Enter a name for the webhook notification and, optionally, its description.
3. From the Category drop-down menu, select one or more categories. To include all categories, click **Select All**.
4. From the Status drop-down menu, select one or more statuses. To include all statuses, click **Select All**.
5. In the Post URL field, enter the URL of the endpoint the webhook notifications should be sent to in one of the following formats:

   ```
   https://<Host>
   https://<Host>/<Path>
   ```

6. *Only if the receiving endpoint requires sender's identification.* From the Authentication type drop-down menu, select one of the following authentication types:
   - **Authentication by secret**, and then enter the secret to connect to your webhook endpoint.
   - **Basic authentication**, and then enter the user name and password associated with your webhook endpoint.

7. Click **Next**.
8. *Optional.* Customize the body of the request that is sent by HYCU for AWS. You can click the appropriate fields in the HYCU fields list to easily insert event variables into the body.

   > ⚠ Important Make sure the format you define in the body is supported by the platform to which webhook notifications will be sent.

   For details on the format of the data that HYCU for AWS sends to the specified URL, see "Webhook data format" below.
9. Click **Save**.

Your changes take effect immediately and webhook notifications are sent to any URL that you specified in the notification settings.

You can later edit settings for existing webhook notifications (click ✎ **Edit** and make the required modifications) or delete the ones that you do not need anymore (click 🗑 **Delete**).

Webhook data format

The webhook data format is defined by:

- HTTP request header sent by HYCU for AWS
- HTTP request body sent by HYCU for AWS
- HTTP response code sent by the webhook endpoint and received by HYCU for AWS

HTTP request headers

The request headers are sent in the following format:

```
content-type = application/json
x-hycu-signature = base64(hmac(body, secret, 'sha256'))
```

> Note The `x-hycu-signature` request header is sent only if the webhook secret is specified.

HTTP request body

The request body is sent in the following format:

```
{
"severity": "<severity-value>",
"created": "<created-value>",
"details": "<details-value>",
"category": "<category-value>",
"message": "<message-value>",
"user": "<user-value>",
"taskId": "<taskId-value>"
}
```

> Note Null values are ignored.

HTTP response code

Your webhook URL should return a response with HTTP status code `204`.

Exporting the contents of the panel

Data that you can view in a table in any of the panels can be exported to a file in JSON or CSV format.

Consideration

If you want to export only specific data, click **Filters**, select your filter criteria based on what kind of data you want to export to a file, and then click **Apply Filters**. You can also use the Search box on the left side of the main panel to filter the data.

Procedure

1. Navigate to the panel whose data you want to export.
2. Click **Export**, and then, from the drop-down menu, select one of the following options:

Option	Description
Export to JSON (Current)	Exports the current table page to a JSON file.
Export to JSON (All)	Exports all table data to a JSON file.
Export to CSV (Current)	Exports the current table page to a CSV file.
Export to CSV (All)	Exports all table data to a CSV file.

Using HYCU for AWS reports

HYCU for AWS reports provide you with a visual presentation of data protection environment resources within the currently selected protection set. This comprehensive and precise presentation allows you to have an optimum view for analyzing data so that you can make the best decisions when it comes to protecting your data. Report data can be presented as a table or as a chart.

> ⚠ Important Reports reflect the state of your data protection environment with an up to 60-minute latency period.

After you get familiar with the reports as described in "Getting started with reporting" on the next page, you can continue as follows:

- View reports. For details, see "Viewing reports" on page 66.
- Generate reports. For details, see "Generating reports" on page 67.
- Schedule reports. For details, see "Scheduling reports" on page 68.

  > Note When scheduling the reports, you can also choose to send them by

> email.

- Export and import reports. For details, see “Exporting and importing reports” on page 68.

Accessing the Reports panel

To access the Reports panel, in the navigation pane, click 📋 **Reports**.

> Tip To minimize the Details section, click ▼ **Minimize** or press the Spacebar. To return it to its original size, click ▲ **Maximize** or press the Spacebar.

Getting started with reporting

You can take advantage of predefined reports or create additional reports to better understand your data protection environment, identify potential problems, and improve performance.

For a list of predefined reports, see “Predefined reports” below. For instructions on how to create reports, see “Creating reports” on the next page.

Predefined reports

Predefined reports, represented by the 🔖 icon, provide you with information on the key aspects of your data protection environment, such as the size of instance volumes and the total size of instance backup data. These reports cannot be edited or deleted.

Name	Description
backup-tasks-for-last-24-hours	List of backup tasks for the last 24 hours.
protected-data-on-targets-per-vm	Amount of protected data on targets for each protected instance.
protected-data-on-targets-per-policy	Amount of protected data on targets for each policy.
protected-data-on-targets-per-storage-class	Amount of protected data on targets for each storage class.
protected-vm-disk-capacity-per-policy	Amount of protected instance volume capacity for each policy.
total-vm-disk-capacity-trend	Total amount of instance volume capacity through time.
total-protected-data-on-targets-trend	Total amount of protected data on targets through time.
transferred-data-per-vm-for-previous-month	Amount of transferred data for each protected instance (per backup tier) for

Name	Description
	the previous month.
unprotected-vms	List of unprotected instances.
vm-compliance-status	List of instances, their compliance statuses, assigned policies, and the corresponding policy tiers.

Creating reports

If none of the predefined reports meets your reporting requirements, you can create a new report and tailor it to your needs.

Depending on whether you want to create a new report from scratch or edit an existing report and save it as a new report, do the following:

I want to...	Procedure
Create a new report from scratch.	1. Click + **New**. The Report Configuration dialog box opens. 2. Enter a report name and, optionally, its description. 3. Select the type of report (a table or a chart). 4. Specify the time range for the report. 5. Select the aggregation value that you want to use to perform a calculation on a set of collected data. 6. Distribute the report tags for the collected data that you want to include in your report between x-axis and y-axis to determine how the collected data will be presented in the report. 7. Click **Save**.
Edit an existing report and save it as a new report.	1. From the list of reports, select the one that you want to edit and save as a new report, and then click ✎ **Edit**. The Report Configuration dialog box opens. 2. Enter a new name for the report, and then make the required modifications. 3. Click **Save as**.

Viewing reports

You can view the reports on the current state of your data protection environment or the saved report versions that were generated either manually or automatically.

I want to...	Procedure
View a report on the current state of my data protection environment.	From the list of reports, select the desired report, and then double-click it or click 👁 **Preview**.
View a saved report version.	1. From the list of reports, select the desired report. 2. In the Details section that appears at the bottom of the screen, select the desired report version, and then double-click it or click 📋 **View Report**. For instructions on how to generate report versions manually or automatically, see "Generating reports" below or "Scheduling reports" on the next page.

In the dialog box that opens, besides viewing the report data, you can also download and export the report in the PDF, PNG, or CSV format. To do so, click ⤓ **Download**, and then select one of the available formats.

Generating reports

When you generate a report, you save a copy of the current version of the selected report (a report version) for future reference.

Procedure

1. From the list of reports, select the one that you want to generate.

   > Note If none of the available reports meets your reporting requirements, you can create a new report. For details, see "Creating reports" on the previous page.

2. In the Details section that appears at the bottom of the screen, click + **Generate**. The Generate Report Version dialog box opens.
3. *Optional.* Enter a description for the report version.
4. Click **Generate**.

> Tip You can save a version of the selected report also by clicking 👁 **Preview** followed by **Generate**.

The generated report version is added to the list of report versions in the Details section that appears at the bottom of the screen when you select a corresponding report.

You can later do the following:

- View the saved report versions. For details, see "Viewing reports" on the previous page.
- Delete the saved report versions that you do not need anymore. To do so, select the desired report version, and then click 🗑 **Delete**.

Scheduling reports

You can use scheduling to generate report versions automatically at a particular time each day, week, or month. You can view these report versions in the web browser or schedule them by email.

Procedure

1. From the list of reports, select the one that you want to be generated on a regular basis, and then click **Scheduler**. The Report Scheduler dialog box opens.

   > Note If none of the available reports meets your reporting requirements, you can create a new report. For details, see "Creating reports" on page 66.

2. In the Schedule date box, specify the date and the time of day when you want the report generation to begin.
3. From the Interval drop-down menu, select how often you want the report versions to be generated (daily, weekly, or monthly).
4. Use the **Send** switch if you want to schedule the automatic delivery of the reports to email recipients, and then do the following:
   a. From the Report format drop-down menu, select a file format for your report (PDF, PNG, or CSV).
   b. In the Email address field, enter one or more email recipients that should receive the reports. If you are entering more than one email address, make sure to press the Spacebar after entering each one.
5. Click **Save**.

> Tip The reports that are generated automatically are marked by the ✓ icon in the Scheduled column of the Reports panel .

You can later do the following:

- Edit scheduling options of any of the scheduled reports. To do so, select the report, click **Scheduler**, make the required modification, and then click **Schedule**.
- Unschedule any of the reports if you do not want them to be generated automatically anymore. To do so, select the report, click **Scheduler**, and then click **Unschedule**.

Exporting and importing reports

HYCU for AWS enables you to share user-created reports among different HYCU for AWS subscriptions by exporting the reports to a JSON file and then importing the reports from the JSON file.

Exporting reports

Procedure

From the list of all reports, select the one that you want to export, and then click **Export**.

The selected report will be exported to a JSON file and saved to the download location on your system.

Importing reports

Procedure

1. Click **Import**. The Import Report dialog box opens.
2. Browse your file system for a report that you want to import.
3. Enter a name for the report and, optionally, its description.

   > Note If the JSON file name and description are already defined in the file itself, the Name and Description fields will be populated automatically. You can, however, use another name and description.

4. Click **Import**.

A new report will be added to the list of the reports.

Viewing instance and bucket details

You can view the details about each instance or bucket in the Detail view section of the Instances or Buckets panel.

> Note The Details section appears only if you click an instance or a bucket. Selecting the check box before its name will not open the Details section.

The following details are available:

Instance or bucket information	Description
Summary	Shows detailed information about the selected instance or bucket.
Restore point	Shows the following information for the restore point: • Creation date and time. • Available tiers from which you can restore data: ○ *For instances:* ▪ SNAP or S : Snapshot. Displayed if a snapshot of the instance exists. Snapshots allow faster completion of restore tasks. ▪ BCKP or B : Backup data on a target. Displayed if backup data is stored on a target. ▪ COPY or C : Copy of a backup image. Displayed if a copy of a backup image (snapshot or backup data on a

	target) exists on another target. ■ ARCH-D or D : Data archive—daily. Displayed if a daily data archive exists on a target. ■ ARCH-W or W : Data archive—weekly. Displayed if a weekly data archive exists on a target. ■ ARCH-M or M : Data archive—monthly. Displayed if a monthly data archive exists on a target. ■ ARCH-Y or Y : Data archive—yearly. Displayed if a yearly data archive exists on a target. ■ CTLG or C : Catalog. Displayed if a restore of individual files or folders is available. Note A restore point may or may not include backup data of the entire instance. This depends on the volumes included in the corresponding backup. Visual labels of the tiers may be specially marked to denote different statuses. For more information, see "Tier statuses" on page 72. ○ *For buckets:* ■ BCKP or B : Backup data on a target. ■ COPY or C : Copy of backup data. Displayed if a copy of a backup data exists on another target. ■ ARCH-D or D : Data archive—daily. Displayed if a daily data archive exists on a target. ■ ARCH-W or W : Data archive—weekly. Displayed if a weekly data archive exists on a target. ■ ARCH-M or M : Data archive—monthly. Displayed if a monthly data archive exists on a target. ■ ARCH-Y or Y : Data archive—yearly. Displayed if a yearly data archive exists on a target.
Compliance	Shows the compliance status of the backup (and the resulting restore point): • The ✓ icon: The backup is compliant (the RPO setting in the policy assigned to the instance or the bucket was met). • The ✗ icon: The backup is not compliant (the RPO setting in the policy assigned to the instance or the bucket was not met). • The ? icon: The backup compliance status is undefined (the backup is still running).

	By pausing on a compliance status icon, additional information about the backup is available. You can see backup frequency, the elapsed time since the last successful backup, and the expiration time for each available tier.
Backup status	Shows the backup status of your instance or bucket. For more information, see "Viewing the backup status of instances and buckets" below.
Restore status	Shows a progress bar indicating the progress of the instance or bucket restore. Tip If you double-click a progress bar, you are directed to the Tasks panel where you can check details about the related task.

> Tip To minimize the Details section, click ▼ **Minimize** or press the Spacebar. To return it to its original size, click ▲ **Maximize** or press the Spacebar.

Viewing the backup status of instances and buckets

The backup status of your instance or bucket determines whether it is possible to restore it.

Backup status	Restore an instance or volumes?	Restore files?	Restore a bucket?
(Done)	✓	✓ [a]	✓
(Done with warnings)	✓	✓ [a]	✓
(Done with errors)	✓ [b]	? [c]	✓ [d]
(Failed)	×	×	×
Aborted	×	×	×
(Expired / Inaccessible on Source / Deleted from Source)	×	×	×

[a] All instance volumes were backed up successfully, but the disk catalog creation task might have failed. In this case, you will not be able to restore individual files or folders.

[b] This backup status may indicate one of the following:

- Not all instance volumes were backed up successfully, therefore the instance can be restored only partially. If backing up a boot disk of an instance failed, you may not be able to start the instance after the restore.

- Creating a copy of backup data or a data archive failed. However, the instance can still be fully restored from the backup.
- The backup is not application-consistent.
- *Applicable only if you are using the pre-backup and post-backup scripts.* Some actions specified by the scripts might not be performed.

[c] This backup status may indicate one of the following:

- Not all instance volumes were backed up successfully and the disk catalog creation task might have failed. In this case, you will not be able to restore individual files or folders.
- Not all instance volumes were backed up successfully, therefore only the files that belong to the volumes displayed in the Restore Settings dialog box can be restored.

[d] *Applicable only if you are using the pre-backup and post-backup scripts.* Some actions specified by the scripts might not be performed.

> Note By pausing on a backup status icon, additional information about the restore point is shown. You can see the backup duration and ID.

Tier statuses

Tier labels may be visually marked to represent backup statuses of individual tiers. These statuses define whether it is possible to restore an instance or a bucket. The following is an example of possible marks:

Tier status	Restore an instance or a bucket?
BCKP or B (Done)	✓
BCKP● or B● (Done with warnings or Done with errors)	✓ For details on what data can be restored if one of these backup statuses is shown, see "Viewing the backup status of instances and buckets" on the previous page.
BCKP● or B● (Failed)	×
BCKP● or B● (Aborted)	×
BCKP or B (Expired)	×
BCKP● or B● (Inaccessible on source)	×
BCKP● or B● (Deleted from source)	×

Filtering and sorting data in panels

HYCU for AWS enables you to filter data in the panels so you can easily find what you need. Each panel contains different filtering options and it can display only the entries that meet the specified filter criteria. For example, filtering the data in the Instances panel helps you to focus only on the instances that you are interested in. In addition, you can sort displayed items in ascending or descending order based on an alphabetical value or a label. For example, sorting data in the Policies panel by the Compliance label helps you easily track non-compliant policies.

> Tip After selecting a set of items in the filtered view, you can easily clear the list of selected items by clicking the ✕ icon next to the number of displayed items.

Filtering data in panels

Procedure

1. Go to the web user interface panel of interest.
2. *Optional.* On the left side of the main pane, in the Search field, enter your main filter keyword. Which property can be used as the main filter keyword depends on the panel you are in.
3. To filter the data set (when no main filter keyword is specified) or filter the resulting data set further, follow the steps:
   a. On the right side of the main pane, click **Filters**. The Filters side pane opens.
   b. In the Filters pane, specify your filtering options.
   c. Click **Apply Filters**.

Depending on the panel the contents of which you want to filter, see one of the following sections for information on the available filtering options:

- “Filtering options in the Instances panel” below
- “Filtering options in the Buckets panel” on the next page
- “Filtering options in the Policies panel” on page 75
- “Filtering options in the Targets panel” on page 75
- “Filtering options in the Tasks panel” on page 75
- “Filtering options in the Events panel” on page 76
- “Filtering options in the IAM panel” on page 77

Filtering options in the Instances panel

You can enter an instance name (or a part of it) as the main filter keyword.

In the Filters side panel, you can select one or more filtering options:

Filtering option	Action
Account ID	From the drop-down menu, select the AWS accounts of interest.
Policy	From the drop-down menu, select the policies that are assigned to the instances.

Filtering option	Action
Credential group	From the drop-down menu, select the credential groups that are assigned to the instances.
Zone	From the drop-down menu, select the Amazon EC2 instance zones.
Compliance	Select one or more options to filter by the compliance status: • **Success**: The instance is compliant. • **Failure**: The instance is not compliant. • **Undefined**: The exclude policy is assigned to the instance, or the instance does not have a policy assigned.
Protection	Select one or more options to filter by the protection status: • **Yes**: The instance is protected. • **No**: The instance is not protected. • **Deleted**: The instance no longer exists, but at least one of its backup images does.
Discovery	Select one or more options to filter by the instance discovery status: • **Success**: Connection to the instance was established (as part of checking the connectivity after assigning a credential group to the instance, selecting the Enable restore of individual files option, or specifying the pre-snapshot or post-snapshot scripts). • **Failure**: The instance could not be connected to. • **Warning**: The account has moved to another protection set. • **Undefined**: Connectivity to the instance has not been checked.

Filtering options in the Buckets panel

You can enter a bucket name (or a part of it) as the main filter keyword.

In the Filters side panel, you can select one or more filtering options:

Account ID	From the drop-down menu, select the AWS accounts to which the buckets that you want to filter belong.
Policy	From the drop-down menu, select the policies that are assigned to the buckets.
Location	From the drop-down menu, select the Amazon S3 location of the buckets.
Compliance	Select one or more options to filter by the compliance status: • **Success**: The bucket is compliant. • **Failure**: The bucket is not compliant. • **Undefined**: The exclude policy is assigned to the bucket or the bucket does not have a policy assigned.

Protection	Select one or more options to filter by the protection status: • **Yes**: The bucket is protected. • **No**: The bucket is not protected. • **Deleted**: The bucket is deleted or the status of the bucket is PROTECTED_DELETED.

Filtering options in the Policies panel

You can enter a policy name (or a part of it) as the main filter keyword.

In the Filters side panel, you can select one or more filtering options:

Filtering option	Action
Compliance	Select one or more options to filter by the compliance status: • **Success**: All instances or buckets to which the policy is assigned are compliant. • **Failure**: Not all instances or buckets to which the policy is assigned are compliant. • **Undefined**: The policy is not assigned to any instance or bucket, or this is the exclude policy.

Filtering options in the Targets panel

You can enter a target name (or a part of it) as the main filter keyword.

In the Filters side panel, you can select one or more filtering options:

Filtering option	Action
Storage class	Select one or more options to filter by the AWS S3 storage class: • **S3 Standard** • **S3 Intelligent-Tiering** • **S3 Standard-IA** • **S3 One Zone-IA** • **S3 Glacier Instant Retrieval** • **S3 Glacier Flexible Retrieval** • **S3 Glacier Deep Archive**
Health	Select one or more options to filter by the status of the target: • **Ok** • **Warning** • **Error** • **Undefined**

Filtering options in the Tasks panel

You can enter a task description (or a part of it) or a task ID as the main filter keyword.

In the Filters side panel, you can select one or more filtering options:

Filtering option	Action
Account ID	From the drop-down menu, select the AWS accounts of interest.
Username	From the drop-down menu, select items to filter the list to include only the tasks started by any of the selected user accounts.
Type	From the drop-down menu, select one or more items to filter the list to include only the selected task types.
Status	Select one or more options to filter by the status of the task: • **Ready** • **Running** • **Aborting** • **Aborted** • **Done** • **Failed** • **Done with errors** • **Done with warnings** • **Skipped**
Time range	Specify a time range to limit your search for tasks. You can select one of the predefined time ranges (Last 1 hour, Last 24 hours, or Last week), or use the calendar to select a start date and hour and an end date and hour of the time range for tasks to be displayed.

Filtering options in the Events panel

You can enter a text string as the main filter keyword.

In the Filters side panel, you can select one or more filtering options:

Filtering option	Action
Account ID	From the drop-down menu, select the AWS accounts of interest.
Category	From the drop-down menu, select items to filter the list to include only the selected event categories.
Username	From the drop-down menu, select items to filter the list to include only the events resulting from the selected user account actions.
Severity	Select one or more options to filter by the event severity: • **Success** • **Warning** • **Failed**
Time range	Specify a time range to limit your search for events. You can select

Filtering option	Action
	one of the predefined time ranges (Last 1 hour, Last 24 hours, or Last week), or use the calendar to select a start date and hour and an end date and hour of the time range for events to be displayed.

Filtering options in the IAM panel

In the Filters side panel, you can select one or more filtering options:

Filtering option	Action
Type	Select one or more options to filter by the type: • **User** • **Service account**.
Status	Select one or more option to filter by status: • **Active** • **Deactivated**

Sorting data in panels

Procedure

1. Go to the web user interface panel of interest.
2. Click the table column heading of the property that you want to sort the data in table rows by.

   The ⌃ icon appears in the heading cell, indicating that the column data is sorted in ascending order.
3. Click the column heading again to toggle the sort order.

   The ⌄ icon appears in the heading cell, indicating that the column data is sorted in descending order.

Managing targets

You can view target information, edit a target, deactivate or activate a target, or remove a target if you do not want to use it for storing backup data anymore.

Consideration

Only Amazon S3 buckets that were added to HYCU for AWS as targets either automatically or manually are listed in the Targets panel. Snapshots are not included in this list.

> Accessing the Targets panel
>
> To access the Targets panel, in the navigation pane, click ⊙ **Targets**. Alternatively, in the

> Dashboard panel, click the **Targets** widget title.

Viewing target information

You can view information about each target in the list of targets in the Targets panel. This allows you to have an overview of the general status of the targets. The following information is available for each target:

Property name	Description
Name	Target name (globally unique). A target that has Object Lock (WORM) enabled is represented by the 🔒 icon in the list of targets. For information on how automatically created targets are named, see "Objects created by the service" on page 101. Tip You can click the target name to open the target details page of the AWS Management Console in your web browser.
Location	Name of the Amazon S3 region in which the target resides.
Storage Class	Default object storage class of the target in the Amazon S3 service: S3 Standard, S3 Intelligent-Tiering, S3 Standard-IA, S3 One Zone-IA, S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval, or S3 Glacier Deep Archive.
State	Status of the target: • Active: You can use the target for backing up data, creating data archives, and restoring data. • Inactive: The target has been deactivated within HYCU for AWS. As long as it is not activated you can use it only for restoring data. • Inaccessible on source: Insufficient permissions are set on the target in the Amazon S3 service. HYCU for AWS cannot access the target. • Deleted from source: The target no longer exists in Amazon S3. For instructions on how to change the status of active or inactive targets, see "Deactivating and activating targets" on the next page.
Size Limit	Maximum amount of the target storage space (expressed in MiB, GiB, or TiB) that is allowed to be used by backup data created by HYCU for AWS. The amount represents a soft limit, therefore actual usage may exceed it.
Health	Health status of the target: • The ? icon: Indicates one of the following:

Property name	Description
	◦ The target health has not been determined yet. ◦ The target is inactive. • The ✅ icon: The target is in a healthy state. Utilization of storage space for backup data in the target is less than 90 percent of the configured size limit. • The ❗ icon: Utilization of storage space for backup data in the target is over 90 percent and under 100 percent of the configured size limit, or the target is publicly accessible in AWS. • The ❌ icon: Indicates one of the following: ◦ Target storage space occupied by backup data exceeds the configured size limit. ◦ The target is not accessible due to an I/O error, insufficient permissions, or some other reason.
Utilization	Ratio (expressed in percentage) between the target storage space occupied by backup data and the configured size limit.
Automatic	Indicator of whether the target was created automatically by HYCU for AWS (✓) or not (✕).

To open the Details section where you can find more details about the target, click the desired target.

> Tip To minimize the Details section, click ▼ **Minimize** or press the Spacebar. To return it to its original size, click ▲ **Maximize** or press the Spacebar.

Editing targets

Procedure

1. In the Targets panel, select the target that you want to edit, and then click ✎ **Edit**. The Edit Target dialog box appears.
2. Edit the selected target as required.
3. Click **Save**.

Deactivating and activating targets

Deactivation of a target makes the target unavailable for backup operations in HYCU for AWS. The target remains registered with HYCU for AWS with all the contained backup data intact. Restore of data from the target is still possible.

> Note You cannot deactivate targets that were created automatically by HYCU for

> AWS.

Prerequisite

For target deactivation: The target is not specified in the Target option of any policy or data archive.

Consideration

After deactivating a target, the target cannot be selected for the Target option of a policy until it is activated again.

Procedure

1. In the Targets panel, select the target that you want to deactivate or activate.
2. Change the status of the selected target: click 🔒 **Deactivate** or 🔓 **Activate**.
3. *Only for deactivation.* Click **Yes** to confirm that you want to deactivate the selected target.

Removing targets

Removal of a target deregisters the target from HYCU for AWS. After deregistration, the target and its contained data other than backup data continue to be available in your AWS account.

Prerequisites

- The target contains no backup data.
- The target is not specified in the Target option of any policy or data archive.

Considerations

- After removing a target, no backup operations that include this target are possible anymore.
- You cannot remove targets that were created automatically by HYCU for AWS unless they have been deleted from AWS.

Procedure

1. In the Targets panel, select the target that you want to remove, and then click 🗑 **Remove**.
2. Click **Yes** to confirm that you want to remove the selected target.

Managing policies

You can view policy information, edit policy properties, or delete a policy if you do not want to use it for protecting data anymore.

Consideration

You cannot view information about the exclude policy, edit it, or delete it.

Accessing the Policies panel

To access the Policies panel, in the navigation pane, click 🛡 **Policies**. Alternatively, in the Dashboard panel, click the **Policies** widget title.

Viewing policy information

You can view information about each policy in the list of policies in the Policies panel.

Property name	Description
Name	Policy name.
Compliance	Compliance status of the policy: • The ✓ icon: The policy is compliant. • The ✗ icon: The policy is non-compliant. • The ? icon: Policy compliance is undefined. The policy is not assigned to any instance or bucket, or this is the exclude policy.
Instance Count	Number of the instances that have the policy assigned to them.
Bucket Count	Number of the buckets that have the policy assigned to them.
Description	Description of the policy.

> Note To open the Details section where you can find more details about the policy, click the desired policy.

> Tip To minimize the Details section, click ▼ **Minimize** or press the Spacebar. To return it to its original size, click ▲ **Maximize** or press the Spacebar.

Creating a policy

See "Creating custom policies" on page 21.

Editing a policy

Procedure

1. In the Policies panel, select the policy that you want to edit, and then click ✎ **Edit**. The Edit Policy dialog box appears.
2. Edit the selected policy as required. For details about policy properties, see "Creating custom policies" on page 21.
3. Click **Save**.

Deleting a policy

Procedure

1. In the Policies panel, select the policy that you want to delete, and then click 🗑 **Delete**.
2. Click **Yes** to confirm that you want to delete the selected policy.

Performing manual backups

HYCU for AWS backs up your data automatically after you assign a policy to the selected instances or buckets. However, you can also back up your data manually at any time, for example, for testing purposes or if an automatic backup fails.

Prerequisite

A policy other than the exclude policy is assigned to the instance or the bucket.

Consideration

When the assigned policy uses a backup window, manual backups may prevent the scheduled backup from starting within the defined time frame. This may result in data not being protected until the next backup window or the next manual backup.

Procedure

1. In the Instances or Buckets panel, select which instances or buckets you want to back up.
2. Click ⟲ **Backup** to perform the backup of the selected instances or buckets.
3. Click **Yes** to confirm that you want to start the manual backup.

> 💡 Tip In the navigation pane, click 📋 **Tasks** to check the overall progress of the backup.

Expiring backups manually

HYCU for AWS expires backups automatically according to the retention period that is set for the backup data in the policy. However, if there is a restore point that you do not want to use for restoring data anymore, you can at any time expire it manually. You can do this also for restore points whose backup status is Failed or Aborted if you want to free storage space.

A restore point represents data that was backed up at a specified point in time. Your restore point can contain one or more tiers—Backup, Copy, Archive—that can be marked as expired also individually. Keep in mind that the Catalog tier cannot be marked as expired.

The selected restore point can contain one or more tiers that you can mark as expired:

- *For instances:* Snapshot, Backup, Copy, and/or Archive
- *For buckets:* Backup, Copy, and/or Archive

You can mark as expired one of the following:

- Entire restore point

  Make sure that all tiers are marked for expiration.
- One or more tiers:

  Make sure that only the tiers that you want to expire are marked for expiration.

  > Note You cannot manually expire tiers on targets with Object Lock (WORM) enabled.

> ⚠ Important Marking a restore point or its tiers as expired cannot be undone.

To expire old backups for an instance or a bucket, access the following panels:

- Accessing the Instances panel

  To access the Instances panel, in the navigation pane, click **Instances**.
- Accessing the Buckets panel

  To access the Buckets panel, in the navigation pane, click **Buckets**.

Procedure

1. In the Instances or Buckets panel, click the instance or the bucket for which you want to expire a backup. The Details section appears at the bottom of the screen.

   > Note The Details section appears only if you click an instance or a bucket. Selecting the check box before its name does not open the Details section.
2. In the Details section, select the restore point that you want to mark as expired.
3. Click **Expire**. The Expire dialog box opens
4. *Only if marking a restore point as expired and its backup status is not Failed or Aborted.* Select the tiers that you want to mark as expired:
   - Backup (Snapshot): *Available only for instances.*
   - Backup (Target)
   - Copy
   - Archive - daily
   - Archive - weekly
   - Archive - monthly
   - Archive - yearly

   The tiers that are available for expiration are based on the options that you set in your policy. By selecting all the tiers, you mark the entire restore point as expired.
5. Click **Yes** to confirm that you want the selected tiers to be marked as expired.

The first next retention maintenance task in HYCU for AWS removes the corresponding data from Amazon EC2 (snaphosts) or Amazon S3 (other tiers).

Viewing subscription information

This section describes the HYCU for AWS subscription information that is provided in the HYCU for AWS web user interface. You can check the information about the current subscription.

> ### Accessing the Subscription Information dialog box
>
> To access the Subscription Information dialog box, click **?** in the toolbar, and then select **Subscription Information**.

The following information is displayed in the Subscription Information dialog box for the HYCU for AWS subscription:

Subscriber	
First name	Information about the person who subscribed to HYCU for AWS.
Last name	
Company	
Notification email recipients	A list of recipients to whom notifications related to the selected HYCU for AWS subscription will be sent. If this field is empty, all important notifications related to the HYCU for AWS subscription, such as support and upgrade information, are by default sent to all users that are using the service. It is recommended that you verify these email addresses and, if required, update the list of email addresses to which the notifications are sent.
Subscription details	
Subscription ID	An identification that is automatically assigned to the subscription by AWS.
Subscription plan	The plan that your HYCU for AWS subscription is using. Subscriptions that are not based on a quote are using the Basic plan (also called the Pay-as-You-Go plan). For more information, see "Backup and data retention pricing" on page 12.
Subscribed on	The date of subscribing to HYCU for AWS.
HYCU account	
Account ID	Information about your HYCU account.
Login Url	The login URL for the HYCU account.

Alias	An alias for your HYCU account that you can use to sign-in to HYCU for AWS.

Chapter 7

Customizing HYCU for AWS

After you subscribe to HYCU for AWS, you can perform various tasks to customize HYCU for AWS for your data protection environment.

Consideration

Keep in mind that the role you have assigned determines what kind of actions you can perform. For details on roles, see "Managing roles" on page 90.

If you have the Administrator role assigned, the scope of tasks you can perform depends on the user interface context you select. You can switch between the following two contexts:

- Subscription

  In the subscription context, only the IAM panel is active. Use this context to perform administration tasks related to your subscription, such as adding identity providers, adding or removing users, or changing roles

- Protection set

  In the protection set context, you select the scope of data protection by selecting a specific protection set.

Switching the user interface context

1. On the toolbar, click ⌄ next to the name of the selected protection set or subscription. The Context Picker dialog box opens.
2. In the Context Picker dialog box, select the context.
3. Click **Save**.

   The HYCU for AWS web user interface switches the context. The context that you select is remembered for the next time you sign in.

Tasks

Task	Instructions
Manage identity providers, add or remove users and add or remove roles.	"Managing identity and access" on the next page
Manage HYCU for AWS protection sets.	"Managing protection sets" on page 91

Task	Instructions
Add, edit, or remove an AWS account from sources.	"Managing sources" on page 94
Hide instances from HYCU for AWS.	"Excluding instances from synchronization by tagging the instance in AWS" on page 96
Stop protecting individual accounts.	"Stopping protection for individual accounts" on page 95

Managing identity and access

You can use the Identity and access management panel (IAM) to manage identity providers, users, and user roles in HYCU for AWS.

The scope of tasks you can perform depends on roles assigned to you and the selected context:

- **Subscription**:

Task	Instructions
Add, edit, or remove identity providers from HYCU for AWS	"Managing identity providers" below
Add, deactivate, or remove users	"Managing users" on page 89
Add or remove user roles	"Managing roles" on page 90

- **Protection set**:

Task	Instructions
Add users	"Managing users" on page 89
Assign or unassign user roles	"Managing roles" on page 90

Accessing the IAM panel

To access the IAM panel, in the navigation pane, click **IAM**.

Managing identity providers

You can integrate HYCU with identity providers that support the OpenID Connect authentication protocol, such as Google, Microsoft, and Okta, to give users the possibility to securely sign in to HYCU for AWS by using these identity providers, without the need to maintain dedicated credentials for HYCU for AWS.

Accessing the Identity Providers dialog box

> To access the Identity Providers dialog box, in the Subscription context, in the IAM panel, click **Identity Providers**.

Adding an identity provider to HYCU

Procedure

1. In the Identity Providers dialog box, click + **New**.
2. Enter a name for the identity provider.
3. From the Type drop-down menu, select one of the following types of identity providers, and then follow the instructions:

Identity provider type	Instructions
Google	a. In the Client ID field, enter the application ID that is generated by the identity provider. b. In the Client secret field, enter the application secret that is associated with the client ID and generated by the identity provider.
Microsoft	a. In the Client ID field, enter the application ID that is generated by the identity provider. b. In the Client secret field, enter the application secret that is associated with the client ID and generated by the identity provider. c. In the Issuer field, enter the URL of the issuer of the identity provider.
Okta	
OIDC	
Cognito	

4. Click ⧉ **Copy to clipboard** to copy the redirect URL that you need to input when you create the application integration with HYCU for AWS.
5. Click **Save**.
6. Configure your identity provider and enter the redirect URL that you copied. For details on the required format, see the identity provider documentation.

You can later do the following:

- Edit information about any of the existing identity providers by clicking ✎ **Edit** and making the required modifications.
- Delete any of the existing identity providers by clicking 🗑 **Delete**.

Managing users

The HYCU for AWS user management system provides security mechanisms to help prevent unauthorized users from accessing protected data. Only users that are given specific rights have access to the data protection environment. These users can be authenticated either by HYCU or any of the supported identity providers. For details on identity providers, see "Managing identity providers" on page 87.

Consideration

The scope of tasks you can perform depends on the UI context. In the Protection set context, you can only add users but cannot deactivate or remove them.

Adding a user

1. In the IAM panel, click **+New User**.
2. In the New User dialog box, enter the email address of the user that you want to add.
3. *Optional, if the user will log on using an identity provider.* Select **Generate password** to automatically generate a password. The user must change the generated password during the first log on.

   > ⚠ Important If the user has no identity provider configured and you do not generate a password, the user will not able to log on to HYCU for AWS.

4. Select one of the following options:
   - **Assign to subscription**

     Assign the user to the subscription.
   - **Assign to protection set**

     From the list of protection sets, select the one to which you assign the user.

     > Tip You can search for a protection set by entering its name in the Protection set search field and then pressing **Enter**. By selecting the Name check box, you select all protection sets at once.

5. From the Role drop-down menu, select the role for the user.

   You can select more than one role if needed. For more information about user roles, see "HYCU for AWS roles" on the next page.
6. Click **Save**.

Deactivating a user

Consideration

When you deactivate a user, the user can no longer perform any actions. However, the inactive account is preserved in AWS, including all of the data that the user has backed up.

Procedure

1. In the IAM panel, from the list of available users, select the user that you want to deactivate.

2. Click **Deactivate**. The Deactivate dialog box opens.
3. Click **Deactivate** to confirm the deactivation of the user.

Deleting a user

Considerations

- You cannot delete yourself from HYCU for AWS.
- Any upcoming data protection tasks related to the user that you delete will be automatically assigned to you.

Procedure

1. In the IAM panel, from the list of available users, select the one that you want to delete.

   > Tip You can also search for a user by entering their name in the Search field.

2. Click 🗑 **Remove**. The Remove dialog box opens.
3. Click **Remove** to confirm that you want the selected user to be deleted from HYCU for AWS.

Managing roles

A role determines the scope of actions that can be performed in the HYCU for AWS data protection environment by a specific user. This means that access to data and information within the data protection environment is limited based on the assigned role. As an administrator, you can manage these roles and define what actions can be performed by each user.

Considerations

- At least one user with the Administrator role assigned must exist in the data protection environment for each subscription, at the subscription level.
- User roles are inherited from the subscription level to all protection sets under one subscription. User roles set in a protection set are local to that protection set.

HYCU for AWS roles

A user can be assigned one or more of the following roles:

Role	Allowed actions
Viewer	Acquire information about instances, buckets, policies, targets, tasks, events, and protection sets in the data protection environment.
Backup Operator	Acquire the same information as Viewer, define backup strategies, and back up instances and buckets.
Restore Operator	Acquire the same information as Viewer and restore instances and

Role	Allowed actions
	buckets.
Administrator	Perform all actions in the data protection environment.

Assigning or unassigning roles

Consideration

If you plan to remove your own Administrator role, keep in mind the following:

- At least one user with the Administrator role assigned must exist in the data protection environment for each subscription.
- You will not be able to change your role back to Administrator yourself.

Procedure

1. In the IAM panel, from the list of available users, select the user for whom you want to change the roles and then click ✎ **Edit**.
2. In the Edit Role dialog box, from the drop-down list, select the roles that you want to assign or unassign. You can select or deselect roles individually or you can click **Select all** to select all roles at once.
3. Click **Save** to save the selected roles.

Managing protection sets

By default, a predefined protection set is created automatically (named default-protection-set and represented by the 🔖 icon) and accounts are added to it when they are added to sources. You can adjust the default setup to better suit your needs by creating additional protection sets and distributing your accounts among them.

You can perform the following tasks related to protection sets:

Task	Instructions
Create a protection set and include preferred accounts in it.	"Creating protection sets" on the next page
Edit an existing protection set.	"Editing protection sets" on the next page
Exclude an account from a protection set.	"Excluding accounts from protection sets" on page 93
Delete a protection set that you no longer need.	"Deleting protection sets" on page 93

Accessing the Protection Sets dialog box

To access the Protection Sets dialog box, click ⚙ **Administration** in the toolbar, and then select **Protection Sets**.

Creating protection sets

If you have the required permissions granted, you can create additional protection sets that allow you to have different data protection setup for different groups of AWS accounts.

Considerations

If you move an account to a different protection set, consider the following:

- Policies will be automatically unassigned from the instances and the buckets in the accounts.
- Credential groups that were manually assigned to instances in the accounts will be automatically unassigned from those instances.

Procedure

1. In the Protection Sets dialog box, click + **New**. The New Protection Set dialog box opens.
2. Enter a name for your protection set and, optionally, its description.
3. From the list of available accounts, select one or more accounts that you want to include in the protection set.

   > Tip You can search for an account by entering its name in the Account ID search field and then pressing **Enter**. By selecting the Account ID check box, you select all accounts at once.

4. Click **Save**.

The protection set is created and added to the list of protection sets.

Editing protection sets

If you have the required permissions granted, you can change the name of a protection set, and include or exclude accounts from the protection set. You can exclude the accounts from the protection set also directly by following the procedure described in "Excluding accounts from protection sets" on the next page.

Consideration

If you move an account to a different protection set, consider the following:

- Policies will be automatically unassigned from the instances and the buckets in the accounts.
- Credential groups that were manually assigned to instances in the accounts will be automatically unassigned from those instances.

Procedure

1. In the Protection Sets dialog box, from the list of protection sets, select the one that you want to edit, and then click ✎ **Edit**.
2. Edit the selected protection set as required.
3. Click **Save**.

Excluding accounts from protection sets

If you have the required permissions granted, you can exclude an account from a protection set. When you exclude the account from the protection set other than the default one, it is automatically moved to the default protection set. If you want to completely remove the account from HYCU for AWS and to stop protecting its resources, you must exclude the account from the default protection set.

Procedure

1. *Only if the account belongs to a protection set other than the default one.* Do the following:
   a. Click › next to the protection set with the account that you want to exclude. The list of all included accounts is displayed.
   b. Select the account that you want to exclude from the protection set, and then click 🗑 **Remove**.
   c. Click **Yes** to confirm that you want to exclude the selected *account*.

   The excluded account is added to the default protection set.
2. *Only if you want to exclude the account from the default protection set.* Do the following:
   a. Click › next to the default protection set. The list of all included accounts is displayed.
   b. Select the *account* that you want to exclude from the default protection set, and then click 🗑 **Remove**.
   c. Click **Yes** to confirm that you want to exclude the selected *account*.

   The account is no longer included in any protection set and HYCU for AWS no longer retrieves the account information from AWS.

Deleting protection sets

You can at any time delete protection sets that you no longer need.

Prerequisites

- The protection set that you want to delete is empty with no included accounts.
- The current data protection scope is set to a protection set other than the protection set that you want to delete.

Consideration

The default protection set created by HYCU for AWS cannot be deleted (represented by the 🔖 icon).

Procedure

1. In the Protection Sets dialog box, from the list of protection sets, select the one that you want to delete from HYCU for AWS, and then click 🗑 **Delete**.
2. Click **Yes** to confirm that you want to delete the selected protection set.

Managing sources

An AWS subscription for which HYCU for AWS provides data protection consists of one or more AWS accounts that you add to HYCU for AWS as sources.

You can perform the following tasks related to sources:

Task	Instructions
Add an AWS account.	"Adding accounts" below
Edit an existing AWS account.	"Editing accounts" on the next page
Remove an AWS account that you no longer need.	"Removing accounts" on the next page

> ### Accessing the Sources dialog box
>
> To access the Sources dialog box, click ⚙ **Administration** in the toolbar, and then select **Sources**.

Adding accounts

If you have the required permissions granted, you can add accounts.

Procedure

1. In the Sources dialog box, click + **New**.
2. Enter the account ID, and optionally a display name.

   Click **Add**.
3. Click **Create IAM Role**. The AWS Management Console opens.

   > ⚠ Important You must be logged on to AWS Management Console with the account that you are adding to HYCU for AWS. If you are already logged in to AWS Management Console with a different account when you create the IAM roles, the creation fails.
4. In the AWS Management Console, on the Quick create stack page, confirm the

capabilities required by HYCU for AWS by clicking **I acknowledge that AWS CloudFormation might create IAM resources with custom names** and then click **Create stack**.

5. Return to the HYCU for AWS web user interface and click **Save**.

   The account is added to the list of sources.

Editing accounts

Procedure

1. In the Sources dialog box, from the list of account IDs, select the one that you want to edit, and then click ✎ **Edit**.
2. Edit the display name and click **Save**.

Removing accounts

You can at any time remove sources that you no longer need.

Consideration

Removing the account from HYCU for AWS does not delete any IAM resources that were created in the AWS account.

Procedure

1. In the Sources dialog box, from the list of account IDs, select the one that you want to remove from HYCU for AWS, and then click 🗑 **Remove**.
2. Click **Yes** to confirm that you want to remove the selected account.

Stopping protection for individual accounts

This section provides instructions that you must follow to stop protecting individual accounts in HYCU for AWS.

> Note If you want to stop using HYCU for AWS completely, see “Unsubscribing from HYCU for AWS” on page 98.

Procedure

1. In HYCU for AWS, unassign policies from all protected instances and buckets in the account. For instructions, see “Stopping service charges” on page 98.
2. In HYCU for AWS, manually mark restore points of all instances and buckets in the account as expired. For instructions, see “Expiring backups manually” on page 82.
3. Exclude the account from any protection set. For instructions, see “Excluding accounts from protection sets” on page 93.

When an account is no longer protected, irrelevant notifications are prevented, and the unneeded associated charges are avoided.

Excluding instances from synchronization by tagging the instance in AWS

This section provides information on how to make selected instances invisible to HYCU for AWS. The needs of your environment may require that some instances are not protected by HYCU for AWS. To leave some instances unprotected, you can exclude them from synchronization so that they are not visible to HYCU for AWS. The invisible instances cannot be assigned policies in any way.

Procedure

1. In the AWS Management Console, choose an AWS account to which the instances that you want to leave unprotected belong.
2. Within the AWS account, choose an instance and add it the `hycu-instance-sync` tag in Amazon EC2. Use the following data:

Key	Value
hycu-instance-sync	false

   Custom tags can be added from the Amazon EC2 console. For instructions, see AWS documentation.
3. Repeat step 2 for each additional instance that you want to make invisible to HYCU for AWS.
4. Sign in to the HYCU for AWS web user interface.
5. Select the protection set that includes the same AWS account as you selected in step 1 of the procedure. For instructions on selecting protection sets in HYCU for AWS, see "Selecting a HYCU for AWS protection set" on page 17.
6. In the navigation pane, click **Instances**.
7. Click **Synchronize** or wait until the next instance synchronization cycle.

   In the Instances panel, the names of the instances that you excluded from synchronization are not present.

Chapter 8

Troubleshooting

If you encounter a problem while using HYCU for AWS, use the following approach to troubleshoot it:

1. You first need to identify the cause of the problem, collect and analyze all available information about it, and then solve the problem. Answering the following questions may help you to solve your problem:

   a. Did you fulfill all the prerequisites and are you aware of all the limitations that come with HYCU for AWS?

   b. Do you receive any errors?

      You can view all events that occurred in your environment in the Events panel. In addition, you can track tasks that are running in your data protection environment and get an insight into the specific task status. For this purpose, use the Tasks panel. For detailed information on events and tasks, see "Viewing events" on page 60 and "Checking task statuses" on page 60.

   c. Is your problem related to any third-party hardware or software?

      In this case, contact the respective vendor for support.

2. If the problem still persists, contact HYCU Customer Support. It is recommended that you collect and send the following information to HYCU Customer Support:

   - Description of your data protection environment
   - Description of your problem
   - Results of any testing you have done (if available)

Chapter 9

Unsubscribing from HYCU for AWS

If for whatever reason you decide that you no longer want to use HYCU for AWS for protecting your data, you can easily unsubscribe from the service.

Unsubscribing from HYCU for AWS includes the following tasks:

Task	Instructions
1. Stop being charged for using HYCU for AWS.	"Stopping service charges" below
2. Prevent HYCU for AWS to access your AWS account.	"Preventing account access" on the next page
3. Cancel your HYCU for AWS subscription in AWS.	"Canceling your HYCU for AWS subscription" on page 100

Stopping service charges

To avoid unnecessary charges for the backup and recovery service, perform the following tasks:

Task	Instructions
1. Stop charges for backup and recovery.	In HYCU for AWS, unassign policies from all protected instances and buckets: • To unassign policies from instances: 1. In the navigation pane, click **Instances**. 2. Select all instances with assigned policies, and then click **Policies**. 3. Click **Unassign**, and then click **Yes** to confirm that you want to unassign the policies from the selected instances. • To unassign policies from buckets: 1. In the navigation pane, click **Buckets**.

	2. Select all buckets with assigned policies, and then click 🛡 **Policies**. 3. Click **Unassign**, and then click **Yes** to confirm that you want to unassign the policies from the selected buckets. ⚠ Important *Only if multiple protection sets are available in your data protection environment.* Make sure to follow these steps for each protection set separately.
2. Stop charges for backup data storage.	1. Manually mark restore points of all instances and buckets as expired. For instructions, see "Expiring backups manually" on page 82. ⚠ Important *Only if multiple protection sets are available in your data protection environment.* Make sure to do this for each protection set separately. 2. Remove all backup data created by HYCU for AWS from AWS (delete all automatically or manually created targets that contain only backup data, and delete all backup data that is stored on automatically or manually created targets that contain also other kind of data). For the target naming conventions, see "Objects created by the service" on page 101. For instructions on how to delete targets and remove backup data from targets, see AWS documentation. 3. Remove all snapshots created by HYCU for AWS from AWS. For the snapshot naming conventions, see "Objects created by the service" on page 101. For instructions on how to remove snapshots, see AWS documentation.

Preventing account access

When you added an account as a source to HYCU for AWS, you assigned HYCU for AWS IAM roles to your AWS account. After you stop using the solution, you must remove the roles.

Procedure

1. Open a web browser, go to the Sign in page of the AWS Management Console and sign in.
2. Open the AWS CloudFormation console and in the navigation pane, choose **Stacks**.
3. In the list of stacks, select `CreateHycuRole` and delete it. When prompted, confirm the deletion.

> Note *Only if multiple sources are available in your data protection environment.* Make

> sure to follow these steps for each source.

For details on removing AWS stacks, see AWS documentation.

Canceling your HYCU for AWS subscription

Prerequisite

Your user account has the `AWSMarketplaceManageSubscriptions` predefined role assigned.

Procedure

1. Open a web browser and go to the AWS Marketplace webpage.
2. Search for "HYCU Data Protection as a Service for AWS" to find your subscription.
3. On the Manage Subscription page, cancel the subscription. For details on how to cancel an AWS subscription, see AWS documentation.

After you cancel your HYCU for AWS subscription, your data is kept for 14 days before it is permanently deleted. If during this period you change your mind and you want to continue using HYCU for AWS, subscribe from the same account.

Appendix A

Objects created by the service

During data protection tasks, HYCU for AWS creates temporary and persistent HYCU objects in your AWS accounts. Temporary HYCU objects exist only for the duration of a task, and persistent HYCU objects are preserved after tasks are completed.

> Caution With the exception of the restored files and unless specifically instructed to do so, never rename or delete any HYCU objects.

Names or location path templates of persistent HYCU objects created during backup tasks

- Snapshot:
  - If all volumes on the instance are backed up:

    `HYCU-<InstanceID>-snapshot`
  - If any volume is excluded:

    `HYCU-<VolumeID>-snapshot`
- Automatically created target:

  `hycu-<CloudStorageRegionName>-<UUID>`
- Target folder with a backup, a backup copy, or a data archive:

  `hycu/backups/<AccountID>/<Region>/<InstanceID>/disks/<VolumeID>/<StorageClass>/`
- Target folder with a disk catalog:

  `hycu/backups/<AccountID>/<Region>/<InstanceID>/tasks/<TaskID>/<VolumeID>/`

Names or location path templates of persistent HYCU objects created during restore tasks

- Renamed original file (at the original location on an instance):

  `<OriginalFileName>.hycu.orig[.<OriginalFileExtension>]`
- Renamed restored file (at the original location on an instance):

  `<OriginalFileName>[.<OriginalFileExtension>].<TimeStamp>.restored`
- Target folder with restored files or folders:

`hycu/restores/<AccountID>/<InstanceID>/<TaskUUID>/<Path>`

- Restored file:

  `<FileName>.<FileExtension>.<TimeStamp>.restored`

- Cloned volume:

  `<OriginalVolumeName>`

- Exported volume:

  `hycu-export-<VolumeID>`

Name templates of temporary HYCU objects created during backup and restore tasks

- Temporary volume:

  `hycu-temporary-<SnapshotID>`

Appendix B

Deploying a HYCU backup controller

If you are employing HYCU Protégé, you can use the HYCU for AWS web user interface to deploy a HYCU backup controller instance to AWS in the event of a disaster in the on-premises data protection environment.

For details on the supported on-premises infrastructures and how to employ HYCU Protégé, see HYCU for Enterprise Clouds documentation.

Prerequisites

- You must own the HYCU and HYCU Protégé licenses. For details on how to obtain these licenses, see HYCU for Enterprise Clouds documentation.
- You must have the Administrator role assigned.

Considerations

- The recommended requirements for the HYCU backup controller are 4 vCPU cores and 8 GiB of memory.
- Each HYCU backup controller is by default deployed with the system disk size of 10 GiB and the data disk size of 32 GiB.

> ### Accessing the HYCU Controller Deployment dialog box
>
> To access the HYCU Controller Deployment dialog box, click ⚙ **Administration** on the toolbar, and then select **HYCU Controller Deployment**.

Procedure

1. From the AWS account drop-down menu, select the AWS account to which you want to deploy the HYCU backup controller.
2. From the Region drop-down menu, select the geographic region for the HYCU backup controller.

   > ⚠ Important Make sure that at least one virtual network is configured in the selected region.

3. From the Zone drop-down box, select the zone for the HYCU backup controller.
4. Click **Next**.

5. In the Instance name field, enter a name for the HYCU backup controller.
6. In the vCPU cores field, enter the number of virtual CPUs to be assigned to the HYCU backup controller multiplied by the number of cores per virtual CPU. The value that you specify must be a whole number and cannot be higher than 128.
7. In the Memory field, enter the amount of memory (in GiB) to be assigned to the HYCU backup controller. The value that you specify must be a whole number and cannot be higher than 24576.
8. From the Available versions drop-down menu, select the version of the HYCU backup controller. By default, the latest version is selected.
9. From the Instance type drop-down menu, select the instance type.

   > Note The list of available instance types is based on the number of virtual CPU cores and the amount of memory that you specified. If no instance type exactly corresponds to the specified values, the list is empty and you need to adjust the values in the vCPU and Memory fields.

10. Under Network interfaces, you can view the network interface that will be added to the HYCU backup controller. By default, this is the first network interface from the region/zone that you selected for the HYCU backup controller.

    If you want to modify network settings, you can add an additional network interface, edit an existing network interface, or delete a network interface:

    Modifying network settings

    To modify a network interface:

    - Click **Add Network Interface** to add a network interface or click ✎ **Edit** next to the network interface that you want to edit, and then follow these steps:
      a. From the Subnet drop-down menu, select the subnet.
      b. From the Security groups drop-down menu, select one or more security groups.
      c. In the Public address type field, select the public IP address for the network interface. You can select among the following options:

Option	Description
None	The network interface does not use a public IP address. This option is preselected if the network interface of the original instance did not use a public IP address.
Auto-assign	The network interface uses an automatically allocated public IP address. This option is preselected if the network interface of the original instance used a public IP address.

	Note Auto-assign will not work if the Auto-assign public IPv4 address on a subnet option is set to `No` or if more than one network interface is specified.
Elastic IP (Reserved)	The network interface uses an elastic public IP address that was reserved in Amazon EC2 in advance.
Elastic IP (New)	The network interface uses a new elastic public IP address. Note Allocation of the IP address in Amazon EC2 is performed at the very beginning of the deployment. If the allocation fails, the deployment task is terminated without being logged.

d. In the Private address type field, select the private IP address for the network interface. You can select between the following options:

Option	Description
Auto-assign	The network interface uses an automatically allocated private IP address. This option is selected by default.
Custom	The network interface uses a private IP address that is defined by you. ⚠ Important Use of this option might result in IP address conflicts.

e. Click **Add** or **Save**.

- Click 🗑 **Delete** next to the network interface that you want to delete. Keep in mind that you cannot deploy the HYCU backup controller without a network interface.

11. Click **Deploy**.

Accessing the HYCU web user interface

After you deploy the HYCU backup controller, you must configure a port in AWS to be able to access the HYCU web user interface.

Procedure

Add rules to the security groups to allow inbound traffic. Specify the following settings:

- Source port ranges: 0.0.0.0/0 (to allow any source port)
- Destination port ranges: 8443

For instructions, see AWS documentation.

You can access the HYCU web user interface by entering the following URL:

```
https://<HYCUBackupControllerPublicIPAddress>:8443
```

On the logon page, enter your logon name and password. You can use the default user name and password for initial access:

User name:	**admin**
Password:	**admin**

> ⚠ Important For security purposes, it is highly recommended that you change the default password.

Appendix C

Least-privilege permissions used by HYCU for AWS

By default, HYCU for AWS automatically creates an IAM role with a predefined set of permissions that are required to perform different tasks such as discovery, backing up, or restoring. If you need to create a custom role with the least-privilege permissions needed to access your environment, you can use a role template with a predefined set of permissions.

Using a template with a predefined least-privilege set of permissions

Prerequisite

You have the HYCU account ID of your subscription. To get the HYCU account ID, click **?** in the toolbar, and then click **Subscription information** to display the Subscription information dialog box. The account ID is listed under the section HYCU Account.

Consideration

Make sure that the account for which you are creating the role is not already added as a source in HYCU for AWS, otherwise the creation of the least-permissions role will fail and the role with default permissions will stay in place. If you already added the account as a source, delete its role or the AWS CloudFormation stack with which you created the original role before you start the process or use a different account.

Procedure

To add the role template to your AWS account, perform the following:

1. Open the following URL in your browser:

   https://us-east-2.console.aws.amazon.com/cloudformation/home?region=us-east-2#/stacks/quickcreate?templateUrl=https%3A%2F%2Fhycu-resources.s3.amazonaws.com%2Fcloudformation%2F08082022-HycuRoleTemplate-AWSLeastPermissions.json&stackName=HycuStack&param_ExternalId=<*HycuAccountId*>

   where <*HycuAccountId*> at the end of the URL is the account ID of your subscription.

> ⚠ Important You must be logged on to the AWS Management Console with the account for which you are creating roles. If you are already logged in to the AWS Management Console with a different account when you create the IAM roles, the creation fails.

2. In the AWS Management Console, on the Quick create stack page, confirm the capabilities required by HYCU for AWS by clicking **I acknowledge that AWS CloudFormation might create IAM resources** and then click **Create stack**.

Permissions required by HYCU for AWS

The following is a list of permissions required by HYCU for AWS:

Service	Permissions
S3	ListAllMyBuckets, ListBucket, GetBucketLocation, GetBucketLogging, GetBucketObjectLockConfiguration, GetBucketTagging, GetBucketVersioning, GetObject, GetObjectTagging, DeleteJobTagging, DeleteObjectTagging, DeleteObjectVersionTagging, DeleteStorageLensConfigurationTagging, PutBucketTagging, PutJobTagging, PutObjectTagging, PutObjectVersionTagging, PutStorageLensConfigurationTagging, ReplicateTags, CreateBucket, PutObject
STS	AssumeRole
SQS	GetQueueUrl, ListQueues, ReceiveMessage, CreateQueue, DeleteMessage, DeleteQueue, SendMessage
IAM	GetAccountSummary, PassRole
EC2	DescribeAddresses, DescribeAvailabilityZones, DescribeInstances, DescribeInstanceStatus, DescribeInstanceTypes, DescribeRegions, DescribeSecurityGroups, DescribeSnapshots, DescribeSubnets, DescribeVolumes, GetConsoleOutput, CreateTags, AllocateAddress, AssociateAddress, AttachVolume, CopyFpgaImage, CopyImage, CopySnapshot, CreateNetworkInterface, CreateSnapshot, CreateSnapshots, CreateVolume, DeleteSnapshot, DeleteVolume, DeregisterImage, DetachVolume, ImportImage, ImportInstance,

	ImportKeyPair, ImportSnapshot, ImportVolume, RegisterImage, RunInstances, StartInstances, StopInstances, TerminateInstances
Elastic Block	Store CompleteSnapshot, StartSnapshot, GetSnapshotBlock, ListChangedBlocks, ListSnapshotBlocks, PutSnapshotBlock
SNS	ListSubscriptions, ListSubscriptionsByTopic, ListTopics, GetSubscriptionAttributes, GetTopicAttributes, ListTagsForResource, TagResource, UnTagResource, ConfirmSubscription, CreateTopic, DeleteTopic, Publish, SetSubscriptionAttributes, SetTopicAttributes, Subscribe, Unsubscribe
S3 Object Lambda	ListBucket, ListBucketMultipartUploads, ListBucketVersions, ListMultipartUploadParts, GetObject, GetObjectRetention, PutObject, PutObjectLegalHold, PutObjectRetention, RestoreObject, WriteGetObjectResponse

Provide feedback

For any suggestions and comments regarding this product or its documentation, send us an e-mail to:

info@hycu.com

We will be glad to hear from you!

www.hycu.com

HYCU®