

USER GUIDE

HYCU Data Protection as a Service for Azure

February 2023



Legal notices

Copyright notice

© 2023 HYCU. All rights reserved.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, distributed, transmitted, stored in a retrieval system, modified or translated to another language in any form by any means, without the prior written consent of HYCU.

Trademarks

HYCU logos, names, trademarks and/or service marks and combinations thereof are the property of HYCU or its affiliates. Other product names are the property of their respective trademark or service mark holders and are hereby acknowledged.

Azure®, Microsoft®, Microsoft Edge™, and Windows® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Google Chrome™ is a trademark of Google LLC.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Mozilla and Firefox are trademarks of the Mozilla Foundation in the U.S. and other countries.

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

1 About HYCU for Azure	7
Key features and benefits	8
Data protection environment overview	9
HYCU for Azure data protection	10
2 Starting with HYCU for Azure	11
Service pricing	11
Backup and data retention pricing	12
Subscribing to HYCU for Azure	14
Adjusting firewall configuration	15
Signing in to HYCU for Azure	16
3 Establishing a data protection environment	18
Determining the scope of data protection	20
Setting up targets	20
Adding a storage account to HYCU for Azure	21
Defining your backup strategy	22
Taking advantage of predefined policies	23
Creating a custom policy	24
Creating a backup window	26
Creating a data archive	28
Setting a default policy	30
Setting up automatic policy assignment	30
Configuring backup options	31
Enabling the restore of files by tagging the virtual machine in Azure	35
Enabling access to virtual machines	35
4 Protecting virtual machines	39
Backing up virtual machines	39
Restoring virtual machines	40
Restoring a virtual machine	41

Cloning a virtual machine	43
Restoring virtual machine disks	45
Cloning virtual machine disks	46
Exporting virtual machine disks	48
Restoring individual files	49
5 Performing daily tasks	52
Using the HYCU for Azure dashboard	53
Checking the status of tasks	54
Viewing events	54
Configuring event notifications	55
Creating email notifications	56
Creating webhook notifications	56
Using HYCU for Azure reports	58
Getting started with reporting	58
Viewing reports	60
Generating reports	60
Scheduling reports	61
Exporting and importing reports	62
Viewing virtual machine details	62
Viewing the backup status of virtual machines	64
Tier statuses	64
Filtering data	65
Applying the main filter	65
Applying the detail filter	66
Filtering options in the Virtual Machines panel	66
Filtering options in the Policies panel	67
Filtering options in the Targets panel	67
Filtering options in the Tasks panel	68
Filtering options in the Events panel	69
Managing targets	69
Viewing target information	70

Editing a target	71
Activating or deactivating a target	71
Removing a target	72
Managing policies	72
Viewing policy information	72
Editing a policy	73
Deleting a policy	73
Performing a manual backup	73
Expiring backups manually	74
6 Customizing HYCU for Azure	76
Managing roles	76
Changing a role	77
Changing the default role	78
Deleting a user	78
Configuring service principals	78
Adding a service principal	79
Setting the active service principal	79
Editing a service principal	80
Deleting a service principal	80
Managing protection sets	80
Creating a protection set	81
Editing a protection set	81
Adding a resource group to a protection set by using a tag	82
Excluding a resource group from a protection set	82
Deleting a protection set	83
Managing HYCU for Azure subscriptions	83
7 Canceling your HYCU for Azure subscription	85
8 Troubleshooting	87
A Deploying a HYCU backup controller	88
Accessing the HYCU web user interface	90

Chapter 1

About HYCU for Azure

HYCU Data Protection as a Service for Azure (HYCU for Azure) is a fully managed backup and recovery service for Microsoft Azure 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.

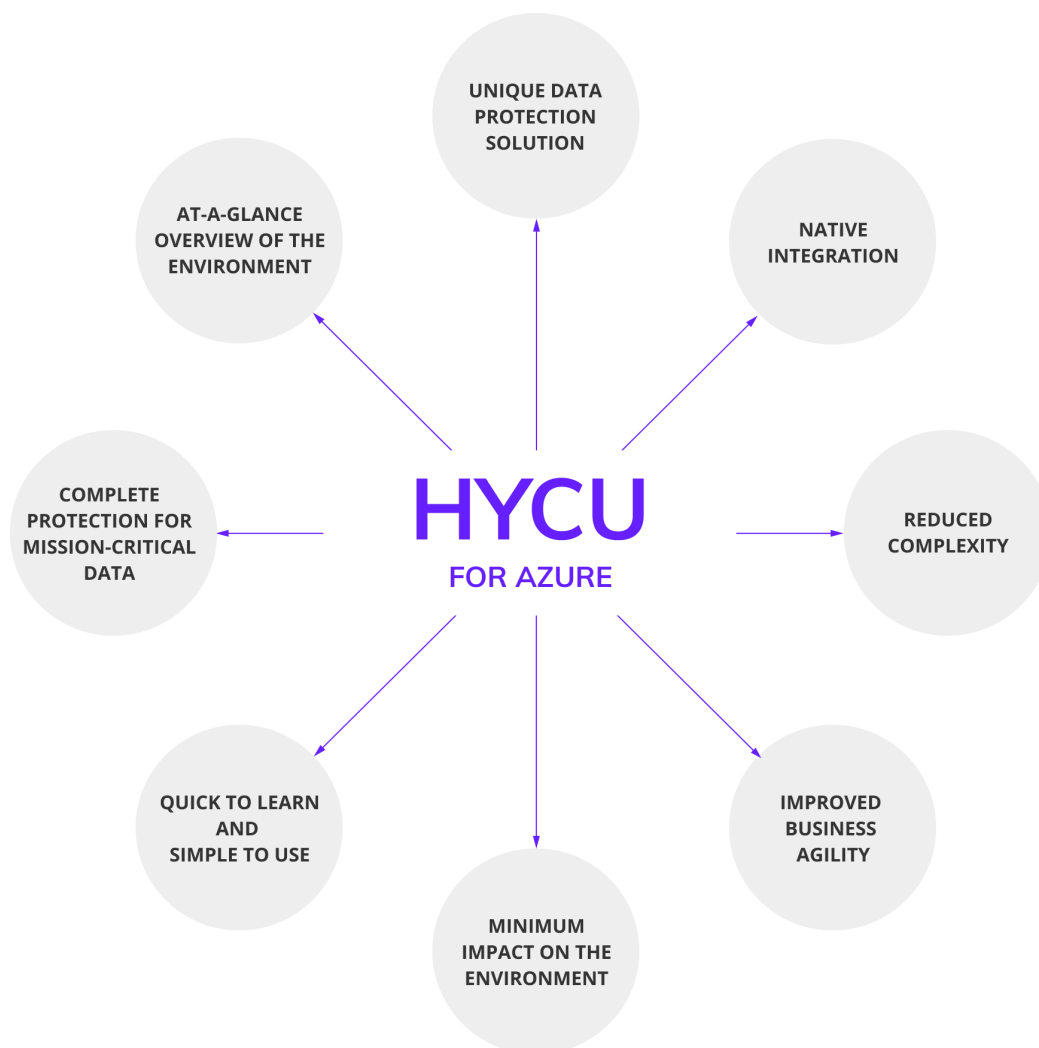


Figure 1-1: Introduction to HYCU for Azure

Key features and benefits

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

- **Protection against data loss**

Delivers native data protection for Azure virtual machines and ensures data consistency and easy recoverability.

- **Data protection in a few minutes**

Data protection for virtual machines can be enabled in a few minutes after you subscribe to HYCU for Azure, 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).

- **Low impact on the environment**

Agentless architecture reduces backup load on production virtual machines. 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.

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

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

- **Restore of individual files**

A possibility to restore one or more files to the original or a different location on the virtual machine, or to a target is an alternative to restoring the entire virtual machine.

- **Integration with the Azure billing system**

Cost of data protection is billed by Microsoft through existing subscriptions, without requiring you to provide additional billing information.

- **Business continuity of your data protection environment across different infrastructures**

HYCU Protégé ensures data resilience by using the SpinUp functionality to migrate protected data between the on-premises and Azure infrastructures. In the event of a disaster in your on-premises environment, HYCU Protégé provides disaster recovery of

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

Data protection environment overview

The data protection environment consists of the following components:

HYCU for Azure web user interface	An interface for protecting virtual machines and managing the data protection environment.
Resource groups	Containers that include resources managed as a group—virtual machines, targets, and temporary resources.
Targets	Storage accounts that HYCU for Azure uses for storing backup data. Backup data can also be stored as snapshots.
Virtual machines	Resources to which you can assign a policy and for which you therefore provide data protection. Data is always protected at a granular level, allowing you to restore either the entire virtual machines, individual disks, or individual files.
Temporary resources	Virtual machines and disks that HYCU for Azure creates automatically for data protection purposes.

The following figure shows the data protection environment and its components:

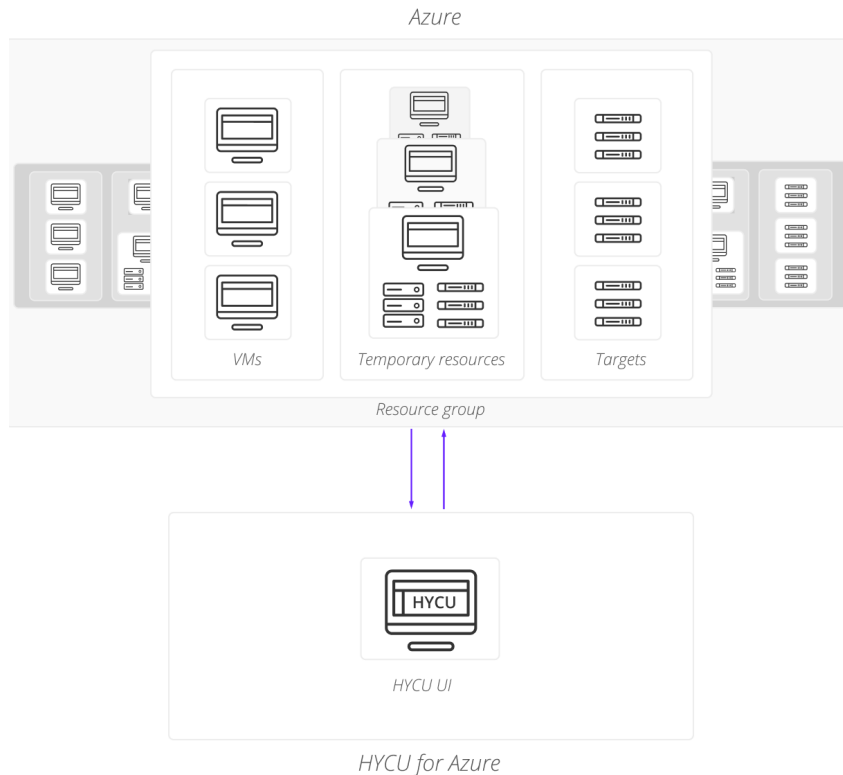


Figure 1–2: HYCU for Azure architecture

HYCU for Azure data protection

With the HYCU for Azure 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.

HYCU for Azure enables you to protect virtual machines. After you establish your data protection environment, you can enable data protection by selecting the virtual machines that you want to protect and assigning policies to them. After the backup is completed, you can restore data from such a backup.

Chapter 2

Starting with HYCU for Azure

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

Task	Instructions
Getting familiar with HYCU for Azure pricing concepts	"Service pricing" below
Subscribing to HYCU for Azure	"Subscribing to HYCU for Azure" on page 14
<i>Only if Azure Firewall is configured.</i> Adjusting firewall configuration	"Adjusting firewall configuration" on page 15
Signing in to the HYCU for Azure web user interface	"Signing in to HYCU for Azure" on page 16

Service pricing

Because HYCU for Azure utilizes the Azure platform 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:

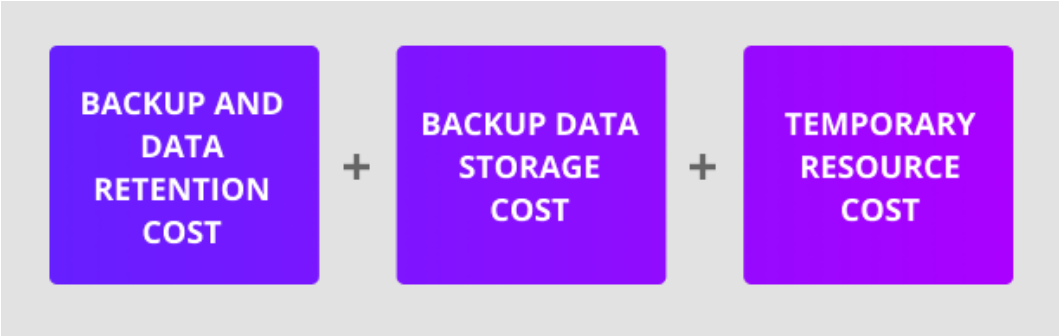




Figure 2-1: Data protection cost

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.

Cost	Details
Backup data storage	<p>Cost of storing backup data. The following factors are considered:</p> <ul style="list-style-type: none"> Target type (a snapshot or a storage account) <p> Note If backup data is stored in an Azure storage account, the cost may vary depending on whether you are using a manually created storage account or an automatically created one (StorageV2 by default).</p> <ul style="list-style-type: none"> Access tier (hot, cool, or archive) Size of backup data Backup retention period Backup frequency <p>If you use a storage account as a target, the use of copies of backup data and/or data archives is also considered.</p>
Temporary resources	<p>Cost of temporary virtual machines and disks that HYCU for Azure creates in Azure when performing the following tasks:</p> <ul style="list-style-type: none"> Backing up virtual machines Restoring virtual machines or virtual machine disks Restoring individual files Performing maintenance operations <p> Important The names of the temporary resources that HYCU for Azure creates for data protection purposes start with the hycuazure or hycu-azure prefix. Make sure not to rename or delete any of them unless specifically instructed to do so.</p>

A HYCU for Azure 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 Microsoft as usual.

For more details on pricing, see [Azure Marketplace](#).

Backup and data retention pricing

HYCU for Azure 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 software plan that you select when subscribing to HYCU for Azure. For details on the software plans, see [“HYCU for Azure software plans” on the next page](#).

Pricing for data protection is based on the capacity of all disks belonging to protected virtual machines and pricing tiers to which these virtual machines belong, within a monthly billing cycle. A pricing tier to which a protected virtual machine belongs is determined when you assign a policy to the virtual machine. HYCU for Azure automatically associates the virtual machine 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 22](#).

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

Virtual machine pricing tier	Data backup frequency (in hours)
Platinum	1–3
Gold	4–11
Silver	12–23
Bronze	Greater than or equal to 24

Considerations

- If a virtual machine is deleted from Azure, but it still has at least one valid restore point available, it is considered protected (its status is PROTECTED_DELETED). HYCU automatically associates such a virtual machine with the Bronze pricing tier and charges you for protecting only the included disks.
- If you unassign a policy from a virtual machine that still has at least one valid restore point available, it is considered protected. HYCU automatically associates such a virtual machine with the Bronze pricing tier and charges you for protecting only the included disks.

HYCU for Azure software plans

HYCU for Azure offers you the following software plans:

- **Pay-as-you-go plan**
Select this plan if you want to pay only for what you use for data protection each month.
For details on the pay-as-you-go software plan, see [Azure Marketplace](#).
- **Token-based plan**
Select this plan if you want to pay a fixed subscription fee. In this case, you pay for the number of HYCU tokens that you plan to consume for data protection each month.
For details on the token-based software plan, contact your HYCU sales representative.

Subscribing to HYCU for Azure

You subscribe to HYCU for Azure online from Azure Marketplace and HYCU then automatically activates the service for you. This is usually done by one user for an entire organization.

Prerequisites

- You have an Azure account.
- You have the Contributor role assigned at the subscription level. This applies to all Azure subscriptions that you plan to connect with HYCU for Azure.


For details on Azure accounts and subscriptions, see Azure documentation.

Consideration


If you violate the terms of use of HYCU for Azure, 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. In the Azure portal, click **Marketplace**, and then in the Search the Marketplace field, type **HYCU for Azure** and press **Enter**.
2. Click the service entry, and then do the following:
 - a. From the Select a software plan drop-down menu, select the HYCU for Azure software plan that best suits your business needs. For details on the software plans, see ["HYCU for Azure software plans" on the previous page](#).
 - b. Click **Create**.
3. On the Subscribe to plan page, provide the following information:
 - a. Enter a name for your service.
 - b. From the Subscription drop-down menu, select the Azure subscription that will be connected with HYCU for Azure.

 **Important** You will be able to protect only the virtual machines within the selected subscription.
 - c. Review the HYCU for Azure software plan and change it, if required.
 - d. Accept the terms of use by selecting the check box, and then provide the preferred email address and phone number as contact information.
 - e. Click **Subscribe**.
4. Navigate to the Software as a Service (SaaS) page, and then, from the list of all services, select the one to which you are subscribing.
5. Activate and configure your HYCU for Azure subscription. To do so, follow these steps:

- a. Click **Configure Account**. The HYCU Data Protection as a Service for Azure webpage opens.

 **Tip** An email notifying you that you must configure your HYCU for Azure subscription is also sent to you. It contains a link to the HYCU Data Protection as a Service for Azure webpage, and you can follow this link to perform the required action.

- b. Click **Sign up with Azure**.
- c. Specify the same Azure account as you used to initiate the process of subscribing to HYCU for Azure.
- d. Provide the required information, taking into account that you must specify the same subscription as you specified when subscribing to the service in the Azure portal, and then click **Submit**.

You will receive an email confirming that you have successfully subscribed to HYCU for Azure.

6. Navigate to **Subscriptions** and grant access to resources at the subscription scope by assigning a role to the HYCU for Azure application:
 - a. Select the same subscription as you selected when subscribing to HYCU for Azure.
 - b. Click **Access control (IAM)**, and then click **Add > Add role assignment**.
 - c. In the Add role assignment pane, do the following:
 - i. From the Role drop-down menu, select **Contributor**.
 - ii. From the Assign access to drop-down menu, select **Azure AD user, group, or service principal**.
 - iii. In the Select field, enter **HYCU for Azure**.
 - iv. Click **Save**.

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 to submit requests to HYCU Customer Support.


Adjusting firewall configuration

Consideration

You can associate a custom application security group (ASG) or a custom network security group (NSG) with the temporary virtual machine that HYCU for Azure creates for data protection purposes. For instructions on how to do this, contact HYCU Customer Support.


Procedure

If you have Azure Firewall configured, you must adjust the firewall rules and open the required ports for HYCU for Azure to operate properly and protect your data:

Purpose	Protocol	Destination	Port
Access to Azure Service Bus	TCP	hycu-dpaas-sb-prod.servicebus.windows.net	5671
Authorization	TCP	login.microsoftonline.com	443
Compute/networking	TCP	management.azure.com	443
Access to storage accounts ^a	TCP	<StorageAccountName> .blob.core.windows.net <div>  Important Using the Azure Storage service tag is recommended. </div>	443

^a If you are not using the Storage service tag, keep in mind the following:

- You must open access to all storage accounts that you use when backing up data, creating copies of backup data, and archiving data.
- Restoring individual files cannot be performed because a temporary storage account is created during the restore.
- You must open access to the HYCU log storage account. To obtain the storage account name that is used for HYCU logs, contact HYCU Customer Support.

 **Important** Only if a custom firewall rule is applied. Traffic to the *.azure.com, *.core.windows.net, *.servicebus.windows.net, and *.microsoftonline.com endpoints must be allowed.

If you employ HYCU Protégé in your environment, make sure to additionally adjust firewall configuration as follows:

Purpose	Protocol	Source	Destination	Port
HYCU Protégé ^a	TCP	HYCU backup controller IP address or host name	Firewall IP address	443
		Firewall IP address	HYCU backup controller IP address or host name	

^a The HYCU backup controller must have access to all storage accounts that are used when migrating data to and from Azure.

Signing in to HYCU for Azure


Prerequisites

- You have the Contributor role assigned at the resource group or subscription level.
- You are using a supported web browser. For a list of supported web browsers, see the *HYCU for Azure Compatibility Matrix*.


Procedure

1. Open a web browser and go to the [HYCU Data Protection as a Service for Azure](#) webpage.
2. On the sign-in webpage, click **Sign in with Microsoft**.
3. *Only if your HYCU for Azure subscription has multiple tenants.* In the Select Tenant dialog box, from the Tenant drop-down menu, select the Azure tenant you want to sign in with.
4. Specify or select the email address of your Azure account. If you are not signed in with this account yet, enter the password, and then click **Next**.
5. Review the permissions that will be granted to HYCU for Azure. If you consent to allow HYCU for Azure to access data on your behalf, click **Accept**.

HYCU for Azure requires these permissions to perform actions such as creating temporary resources for backup and restore purposes, accessing Azure virtual machines and their disks during the backup and restore processes, and creating and/or accessing Azure storage accounts to store backup data. Keep in mind that the permission for sending you notifications related to your subscription by email is implied.

 **Note** You can at any time revoke the consent for HYCU for Azure by removing it from the list of applications in Azure. For details on how to do this, see Azure documentation.

After you sign in to the HYCU for Azure 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 Azure web user interface after 15 minutes of inactivity and any unsaved changes are lost.

Chapter 3

Establishing a data protection environment

After you sign in to HYCU for Azure, 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 76](#).

Establishing the data protection environment involves the following tasks:

Task	Instructions
1. <i>Recommended.</i> Configure service principals.	“Configuring service principals” on page 78
2. Determine the scope of data protection.	“Determining the scope of data protection” on page 20
3. <i>Only if you plan to use manually created storage accounts.</i> Add an Azure storage account to HYCU for Azure as a target.	“Setting up targets” on page 20
4. Decide for predefined policies or create custom ones.	“Defining your backup strategy” on page 22
5. <i>Only if you plan to run the pre-snapshot and post-snapshot scripts, to exclude individual disks from the backup, or to restore individual files.</i> Configure virtual machine backup options.	“Configuring backup options” on page 31
6. <i>Only if you plan to run the pre-snapshot and post-snapshot scripts, or to restore individual files.</i> Assign credential groups to virtual machines.	“Enabling access to virtual machines” on page 35

The following flowchart shows the tasks that you need to perform to establish your data protection environment:

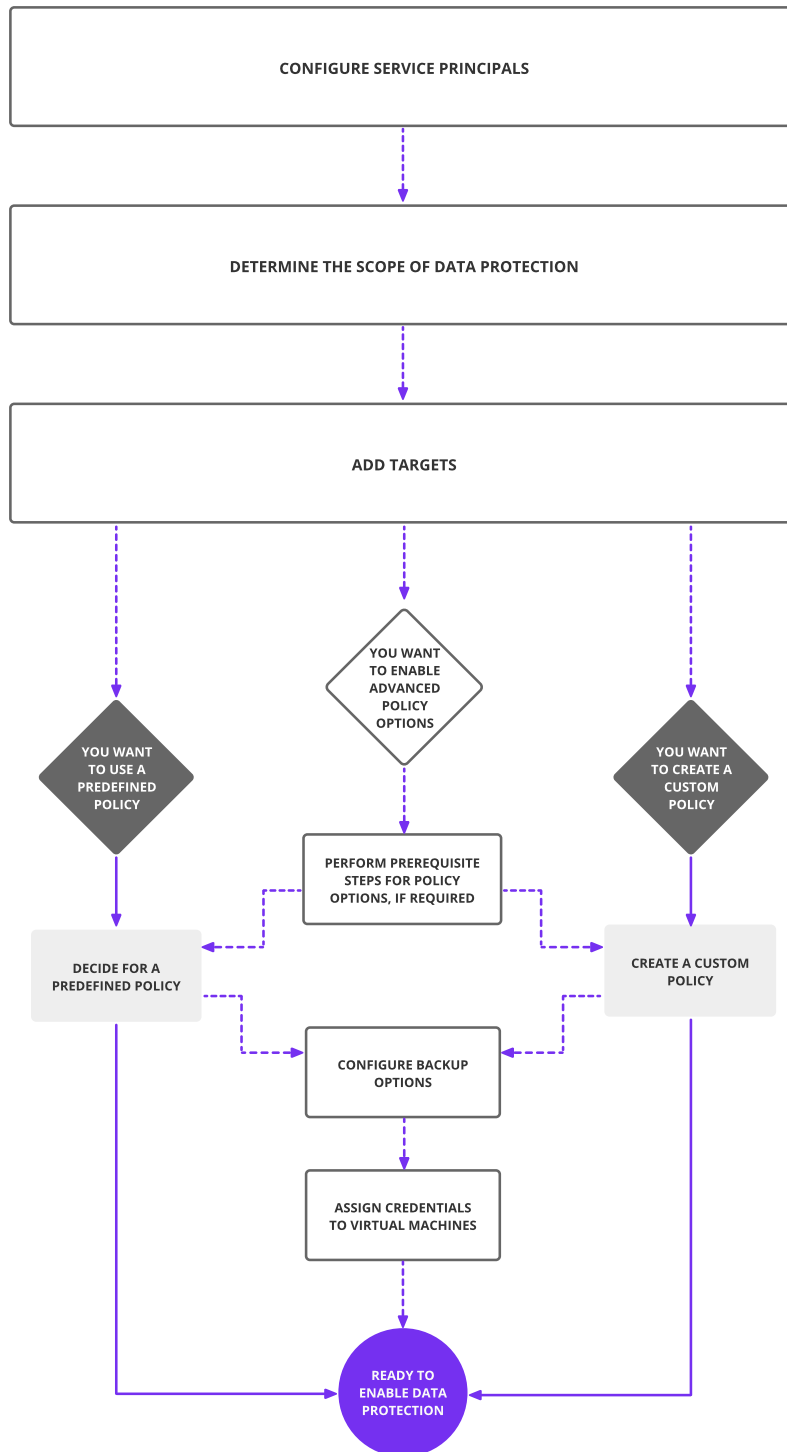



Figure 3-1: Establishing a data protection environment



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

Determining the scope of data protection


An environment for which HYCU for Azure provides data protection consists of one or more protection sets that join together Azure resource groups for which you have access permissions within a subscription.

When you subscribe to HYCU for Azure, a default protection set is created automatically (represented by the  icon) and all the resource groups for which you have the required permissions are included in it. Depending on your business needs, you can create additional protection sets, having in mind that you must implement data protection for each of them individually. For details on managing protection sets, see [“Managing protection sets” on page 80](#).

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.

 **Note** 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 Protection Sets dialog box, from the Subscription drop-down menu, select the HYCU for Azure subscription that contains the protection set for which you want to perform data protection tasks.
3. From the list of available protection sets, select the scope of your data protection by selecting the desired protection set.
4. Click **Select**.

The HYCU for Azure 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 Azure allows you to define either a snapshot or a storage account as a location for storing your backup data.

Target	Description
Snapshot	<p>Backup data is stored as a snapshot in an Azure resource group that contains the virtual machine that you want to protect.</p> <p> Note If snapshots created by HYCU for Azure are deleted from Azure, you will not be able to restore backup data from this location. However, you can still restore your data from targets if</p>

Target	Description
	<p>copies of backup data or data archives exist.</p>
Storage account	<p>Backup data is stored in an Azure storage account that you create yourself or HYCU for Azure creates for you automatically:</p> <ul style="list-style-type: none"> Manually created storage account: You can create your own storage account in Azure and add it to HYCU for Azure as a target. For instructions, see “Adding a storage account to HYCU for Azure” below. Automatically created storage account: HYCU for Azure creates an Azure storage account automatically while backing up data and uses it as a target: <ul style="list-style-type: none"> The size of the automatically created targets is 50 TiB and you can change it if required. For details on how to do this, see “Editing a target” on page 71. For increasing restore speed and minimizing costs, these targets are created in the same region as the virtual machines you are backing up. The same target is used for storing the backup data of multiple virtual machines where possible. <p> Important Automatically created storage accounts are reserved for storing the backup data. Make sure not to store any other kind of data to them.</p> <p>You can view all storage accounts added to HYCU for Azure as targets in the Targets panel. The ones that are created automatically start with the hycuazure prefix. You can use also these targets for storing your backup data.</p>

Adding a storage account to HYCU for Azure

Prerequisite

You have the Contributor role assigned at the storage account level. This applies to all Azure storage accounts that you plan to add to HYCU for Azure as targets.


Limitations

- HYCU for Azure does not support storing data to premium file share and premium page blob storage accounts.
- Adding a storage account for which public access is allowed in Azure is not supported.
- Storing data to a storage account that has a hierarchical namespace enabled is not supported.

Considerations


- When adding a storage account to HYCU for Azure as a target, you can choose to add the storage account that belongs to the subscription associated with your current HYCU for Azure session or a different Azure subscription to which you have access.
- Storing data to a target whose container has an immutable storage policy (WORM) configured is supported.
- You can add the same target to multiple protection sets. In this case, keep in mind that the status, health, and utilization of such a target might differ for each protection set (depending on the data protection needs).
- If the amount of storage space required for storing backup data exceeds the value that you specify when adding a storage account, HYCU for Azure automatically creates a new storage account and uses it as a target.
- *Only if the storage account connectivity method is not set to Public endpoint (all networks).* The virtual machine that you plan to protect must be in the same Azure Virtual Network (VNet) as the storage account that you want to use as a target.

Accessing the Targets panel

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

Procedure

1. In the Targets panel, click **+ Add**.
2. In the Size field, specify the amount of storage space that should be used for storing backup data (in MiB, GiB, or TiB).
3. From the Select target list, select one or more storage accounts that you want to add to HYCU for Azure as targets. You can also search for a storage account by entering its name in the Search targets field.

 **Important** Storage accounts that belong to a subscription other than the one associated with your current HYCU for Azure session are not listed under Select target. If you want to add a storage account that belongs to a different subscription, in the Search targets field, enter its name.

4. 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 69](#).

Defining your backup strategy

HYCU for Azure 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” below.
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 a custom policy” 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 a default policy”](#) on page 30.

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.

Consideration

Predefined policies use targets that HYCU for Azure creates automatically for storing backup data. For details on targets, see [“Setting up targets”](#) on page 20.

HYCU for Azure 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 virtual machines from backups, you can use the Exclude policy.

Creating a custom policy

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.

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 a backup window” on page 26 .
Copy	Create a copy of backup data.
Archiving	Preserve your data for future reference. For details, see “Creating a data archive” on page 28 .
Tags	Set up automatic assignment of policies to virtual machines based on tags that are added to virtual machines in Azure. For details, see “Setting up automatic policy assignment” on page 30 .

Prerequisites


- *Only if you plan to select a manually created storage account.* A storage account is added to HYCU for Azure as a target. For instructions, see [“Adding a storage account to HYCU for Azure” on page 21](#).
- *Only if you plan to enable the Backup Window policy option.* A backup window exists. For instructions, see [“Creating a backup window” on page 26](#).
- *Only if you plan to enable the Archiving policy option.* A data archive exists. For instructions, see [“Creating a data archive” on page 28](#).
- *Only if you plan to enable the Tags policy option.* The virtual machine is tagged in Azure. For details on how to do this, see Azure documentation.

Considerations

- HYCU for Azure 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.
- *Only if you plan to select a manually created storage account for storing backup data.* If there is insufficient space on the selected target, an automatically created one will be used instead.
- If you want your data to be stored as a snapshot and on a target, make sure to select the Snapshot target and also enable the Copy policy option.


- *Only if you plan to enable the Tags policy option.*
 - Tags that you specify in a HYCU for Azure policy must be unique within the selected protection set. Using the same tag (both its name and value) in another policy in the same protection set is not possible.
 - The `hycu-policy` tag takes precedence over any other tag that might be added to the virtual machine in Azure. For more information on the `hycu-policy` tag, see [“Setting up automatic policy assignment” on page 30](#).

Accessing the Policies panel

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

Procedure



1. In the Policies panel, click **+ New**.
2. Enter a name for your policy and, optionally, its description.
3. Add any of the following policy options to the list of the enabled options by clicking it:
 - **Backup** (*mandatory and enabled by default*)
 - **Backup Window**
 - **Copy**
 - **Archiving**
 - **Tags**
4. In the Backup section, do the following:
 - a. In the Backup every field, 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 field, set a retention period (in months, weeks, or days) for the backup data.
 - c. From the Target drop-down menu, select a location for storing your backup data.
If you select the **Automatically selected** option, HYCU for Azure creates a storage account in the region of the virtual machine and uses it as a target for storing the backup data. If an automatically created storage account already exists, it is used instead.
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.

Policy option	Instructions
	If you do not select any backup window, the Always option is shown, which means that your backups are allowed to run at any time.
Copy	<p>In the Copy section, do the following:</p> <ol style="list-style-type: none"> Set a retention period (in months, weeks, or days) for the copy of backup data. From the Target drop-down menu, select a location that you want to use for storing the backup data. If you select a manually created storage account, make sure it is different from the one you selected for the backup. <p>If you select the Automatically selected option, HYCU for Azure creates a storage account in the region of the virtual machine and uses it as a target for storing the copy of backup data. If an automatically created storage account already exists, it is used instead.</p>
Archiving	In the Archiving section, from the Data archive drop-down menu, select a data archive.
Tags	<p>In the Tags section, enter a tag name and value, and then click Add.</p> <p>During the next virtual machine synchronization, the policy is automatically assigned to all the virtual machines with the corresponding tags in Azure.</p> <p> Note HYCU for Azure performs automatic synchronization of virtual machines every five minutes. However, you can at any time update the list of virtual machines also manually by clicking  Synchronize in the Virtual Machines panel.</p>


6. Click **Save**.

The policy is created and added to the list of policies. For details on managing policies, see [“Managing policies” on page 72](#).


Creating a backup window

HYCU for Azure 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 virtual machine not being compliant with backup requirements.


Accessing the Policies panel

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



Procedure

1. In the Policies panel, click  **Backup Window**.
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.
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 a custom policy” on page 24](#).
- Assign the backup window to an existing policy. To do so, select the policy, click  **Edit**, and 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.

The screenshot shows the 'Backup Window > New' configuration window. It includes the following fields and sections:

- NAME:** non-production-hours
- DESCRIPTION (OPTIONAL):** weekdays from 6 PM to 6 AM, Saturdays and Sundays all day
- TIME ZONE:** EST (GMT-05:00)
- SCHEDULE:** A 24-hour grid showing backup windows. Blue bars indicate active backup periods:
 - Monday through Friday: 00:00 to 06:00 and 18:00 to 24:00.
 - Saturday and Sunday: 00:00 to 24:00.
- TIME FRAMES:** A section with buttons for each day and time range. The active frames are:
 - MON: 00:00 - 06:00 and 18:00 - 24:00
 - TUE: 00:00 - 06:00 and 18:00 - 24:00
 - WED: 00:00 - 06:00 and 18:00 - 24:00
 - THU: 00:00 - 06:00 and 18:00 - 24:00
 - FRI: 00:00 - 06:00 and 18:00 - 24:00
 - SAT: 00:00 - 24:00
 - SUN: 00:00 - 24:00
- Buttons:** Close, Back, Save.

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

Creating a data archive

HYCU for Azure enables you to create an archive of your data and keep it 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 storage account. A storage account is added to HYCU for Azure as a target. For instructions, see ["Adding a storage account to HYCU for Azure" on page 21](#).

Accessing the Policies panel

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

Procedure


1. In the Policies panel, click **Archiving**.
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 field, 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 field, 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 Azure creates a storage account in the region of the virtual machine and uses it as a target for storing the archive data. If an automatically created storage account already exists, it is used instead.


- c. From the Access tier drop-down menu, select the access tier that you want to use for storing the data archive.

If you select the **Automatically selected** option, an access tier is automatically selected depending on the specified retention.

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 an archive target if an archiving task is in progress on that target.

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


- Specify the data archive when creating a new policy. For details, see [“Creating a custom policy” on page 24](#).
- Include the data archive into an existing policy. To do so, select the policy, click  **Edit**, and then make the required modifications.

Setting a default policy


You can select one of the predefined or custom policies to be the default policy for your data protection environment. After you set a default policy, it is assigned to one of the following:



- All existing virtual machines that do not have an assigned policy and all newly discovered virtual machines.
- All newly discovered virtual machines.

Accessing the Policies panel

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

Procedure

1. In the Policies panel, select the policy that you want to set as default, and then click  **Set Default**.
2. In the Set Default Policy dialog box, do one of the following:
 - Click **Yes** to assign the default policy to all virtual machines that do not have an assigned policy and all newly discovered virtual machines.
 - Click **No** to assign the default policy only to newly discovered virtual machines.

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 virtual machines to which it was assigned.

Setting up automatic policy assignment

You can set up automatic assignment of policies to virtual machines in one of the following ways:

- By first adding tags to virtual machines in Azure and then specifying the corresponding tag names and values in HYCU for Azure policies. If the comparison of these values shows that the specified values match, the corresponding policies are automatically assigned to the virtual machines during the next virtual machine synchronization in HYCU for Azure.
- By adding the `hycu-policy` tag to virtual machines in Azure. Use the following name-value pair:

Name	Value
<code>hycu-policy</code>	<code><PolicyName>^a</code>

^a The name of a HYCU for Azure policy (for example, Gold).

The corresponding policy is automatically assigned to the virtual machines during the next virtual machine synchronization in HYCU for Azure.

Considerations

- Assigning policies automatically takes precedence over assigning policies manually (see [“Backing up virtual machines” on page 39](#)) or setting a default policy (see [“Setting a default policy” on the previous page](#)). This means that the tag added to the virtual machine defines which policy is assigned to it, even if the virtual machine already has an assigned policy.
- If tags added to a virtual machine in Azure match tags specified in several HYCU for Azure policies, the policy with the lowest RPO is assigned to the virtual machine.

Configuring backup options

Before you start protecting virtual machines, you can adjust virtual machine 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 a virtual machine is created. For example, if the virtual machine 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 disks from the backup	You can specify any disk to be excluded from the virtual machine backup.
Enabling the restore of individual files	<p>You can enable the restore of individual files if your data protection needs require that only individual files are restored, and not the entire virtual machine. By enabling the restore of individual files, you prepare the files for the restore. For instructions on how to restore individual files, see “Restoring individual files” on page 49.</p> <p>As an alternative to enabling the restore of individual files by using the Configuration option described in this procedure, you can also tag a virtual machine in Azure, and by doing so, instruct HYCU for Azure to enable it automatically. For details, see “Enabling the restore of files by tagging the virtual machine in Azure” on page 35.</p>

Prerequisite

Only if you plan to run pre/post scripts or enable the restore of individual files. Virtual machine discovery must be successful. If you select multiple virtual machines, discovery must be successful for all the selected virtual machines.


Limitations

- *For virtual machines with unmanaged disks:* Restoring individual files is not supported.
- *For virtual machines with encrypted managed disks:* Restoring individual files is supported only for virtual machines that have managed disks encrypted with SSE with PMK. For a list of data protection operations that are supported based on how the managed disks are encrypted, see the *HYCU for Azure Compatibility Matrix*.

Consideration


Only if you are running pre/post scripts. A snapshot is created even if the pre-snapshot script fails. The post-snapshot script is run even if the pre-snapshot script, snapshot creation, or both actions fail. When a pre-snapshot or post-snapshot script returns an error, the backup status of the virtual machine is set to Done with errors.


Accessing the Virtual Machines panel



To access the Virtual Machines panel, in the navigation pane, click  **Virtual Machines**.




Procedure


1. In the Virtual Machines panel, select one or more virtual machines for which you want to configure backup options.

 **Important** If you select multiple virtual machines, you will be able only to run pre/post scripts or enable the restore of individual files.


2. Click  **Configuration**.
3. *Only if you want to run the pre-snapshot and post-snapshot scripts.* Depending on whether you are running the scripts for one virtual machine or multiple virtual machines, on the Pre/post scripts tab, do one of the following:

I want to run pre/post scripts for...	Instructions
One virtual machine	<ul style="list-style-type: none"> • If you want to run a pre-snapshot script, do the following: <ol style="list-style-type: none"> a. In the Pre-snapshot script path field, specify the path to the script. <p> Note If no script is set for the selected virtual machine, None is shown.</p> b. Click Save. • If you want to run a post-snapshot script, do the following: <ol style="list-style-type: none"> a. In the Post-snapshot script path field, specify the path to the script. <p> Note If no script is set for the selected virtual</p>

I want to run pre/post scripts for...	Instructions
	<p>machine, None is shown.</p> <p>b. Click Save.</p>
Multiple virtual machines	<ul style="list-style-type: none"> If you want to run a pre-snapshot script, do the following: <ol style="list-style-type: none"> From the Pre-snapshot script path drop-down menu, select the path to the script. <p> Note If no script is set for the selected virtual machines, None is shown. If the selected virtual machines already have different scripts set (including the virtual machines without the scripts), Mixed is shown.</p> <p>If no path to the script exists, or you want to add and set a different script from the ones already available, follow these steps before selecting the script:</p> <ol style="list-style-type: none"> From the Pre-snapshot script path drop-down menu, select + Add new. The Add Pre-Snapshot Script dialog box opens. Specify the path to the script, and then click Save. <p> Note If you want to delete any of the added pre-snapshot scripts, click × next to it.</p> <ol style="list-style-type: none"> <i>Only if some of the selected virtual machines already have a pre-snapshot script set.</i> Select the Override virtual machines with pre-snapshot script already set check box if you want the script selected in the previous step to be used instead of the already existing script. Click Save. If you want to run a post-snapshot script, do the following: <ol style="list-style-type: none"> From the Post-snapshot script path drop-down menu, select the path to the script. <p> Note If no script is set for the selected virtual machines, None is shown. If the selected virtual machines already have different scripts set (including the virtual machines without the scripts), Mixed is shown.</p> <p>If no path to the script exists, or you want to add and set a</p>

I want to run pre/post scripts for...	Instructions
	<p>different script from the ones already available, follow these steps before selecting the script:</p> <ol style="list-style-type: none"> From the Post-snapshot script path drop-down menu, select + Add new. The Add Post-Snapshot Script dialog box opens. Specify the path to the script, and then click Save. <p> Note If you want to delete any of the added post-snapshot scripts, click × next to it.</p> <ol style="list-style-type: none"> <i>Only if some of the selected virtual machines already have a post-snapshot script set.</i> Select the Override virtual machines with post-snapshot script already set check box if you want the script selected in the previous step to be used instead of the already existing script. Click Save.

4. *Only if you want to exclude disks from the backup.* On the Exclude from backup tab, select the disks that you want to exclude from the backup, and then click **Save**.

 **Important** *Only if you plan to exclude the boot disk from the backup.* Restoring the entire virtual machine is not possible if the boot disk is excluded from the backup.

5. *Only if you want to enable the restore of individual files.* Depending on whether you want to enable the restore of individual files for one virtual machine or multiple virtual machines, on the Restore individual files tab, do one of the following:

I want to enable the restore of files for...	Instructions
One virtual machine	Use the Enable restore of individual files switch, and then click Save .
Multiple virtual machines	Select the Enable for all option, and then click Save .

You can at any time disable the restore of individual files for each virtual machine individually by disabling the **Enable restore of individual files** switch or for a group of virtual machines by selecting the **Disable for all** option.

Enabling the restore of files by tagging the virtual machine in Azure

As an alternative to enabling the restore of individual virtual machine files in HYCU for Azure, you can add the `hycu-enable-flr` tag to the virtual machine in Azure, and by doing so, instruct HYCU for Azure to enable it automatically. Use the following name-value pair:

Name	Value
<code>hycu-enable-flr</code>	<code>True^a</code>

^a By setting the value to `False`, you disable the restore of individual files for the specific virtual machine.

If the virtual machine has credentials assigned, HYCU for Azure automatically enables the restore of its individual files. Otherwise, you must assign the credentials to the virtual machine. For details on how to do this, see [“Enabling access to virtual machines”](#) below.

Enabling access to virtual machines

If you plan to run the pre-snapshot and post-snapshot scripts, or to restore individual files, you must enable HYCU for Azure to access these virtual machines by assigning credentials to them.

Prerequisites

- *For Windows virtual machines:*
 - A user account with the admin privileges must be configured on the virtual machine.
 - WinRM must be enabled and configured on the virtual machine.
 - A firewall must be configured to allow inbound network traffic through the required TCP port for WinRM.
- *For Linux virtual machines:*
 - A user account with the `sudo` privileges must be configured on the virtual machine.
 - *Only if using password authentication.* The `sudoers` file must be configured to allow a user that has permissions to access the virtual machine to run `sudo` commands without being asked for the password (the `NOPASSWD` tag must be added to the `sudoers` file).
 - A firewall must be configured to allow inbound network traffic through the required TCP port for SSH.
 - *For Ubuntu 22.04 virtual machines 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

If you use the SSH protocol with private key authentication, only the RSA key type is supported.



Consideration


If a virtual machine is deleted from Azure, but still has at least one valid restore point available, keep in mind that you can unassign credentials from such a virtual machine, but cannot assign them.

Accessing the Virtual Machines panel


To access the Virtual Machines panel, in the navigation pane, click  **Virtual Machines**.

Procedure

1. In the Virtual Machines panel, select the virtual machine to which you want to assign a credential group.
2. Click  **Credentials**.
3. Click  **New**.
4. Enter a name for the credential group.
5. From the Protocol drop-down menu, select one of the following protocol options:


Protocol option	Instructions
Automatic	<p>Select this option if you want HYCU for Azure to automatically select a protocol for accessing the virtual machine: 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 virtual machine.</p> <p> Note <i>For Linux virtual machines:</i> Password authentication is used by default. If you want to use public key authentication, select the SSH protocol option and make the required modifications.</p>
SSH	<p>Select this option if you want to use the SSH protocol, and then make the following:</p> <ol style="list-style-type: none"> a. In the Port field, enter the SSH server port number. b. From the Authentication drop-down menu, select the type of authentication you want to be used, and then provide the required information:


Protocol option	Instructions	
	Password authentication	Enter the user name and password of a user account that has required permissions to access the virtual machine.
	Public key authentication	Enter the user name of a user account that has required permissions to access the virtual machine.
	Private key authentication	Do the following: <ul style="list-style-type: none"> i. Enter the user name of a user account that has required permissions to access the virtual machine. ii. Choose a private key. iii. <i>Only if the private key is encrypted.</i> Enter the private key passphrase.
WinRM	Select this option if you want to use the WinRM protocol, and then do the following: <ul style="list-style-type: none"> a. In the Port field, enter the WinRM server port number. b. From the Transport drop-down menu, select one of the following transport protocol options: <ul style="list-style-type: none"> • HTTPS • HTTP c. Enter the user name and password of a user account that has required permissions to access the virtual machine. 	



6. Click **Save**.
7. *Only if using the public key authentication type.* Download a public SSH key in HYCU for Azure and reset it in Azure. To do so, follow these steps:
 - a. In HYCU for Azure, select the required credential group, click  **Download Key**, and then copy the public SSH key.
 - b. In Azure, reset the public SSH key for the selected virtual machine and, as a new public SSH key, specify the one you copied from HYCU for Azure. For details on how to do this, see Azure documentation.
8. Click **Assign**.

The name of the assigned credential group appears in the Credential group column of the Virtual Machines panel. HYCU for Azure performs virtual machine discovery after you

assign the credentials to the virtual machines and the Discovery status in the Virtual Machines panel is updated accordingly.

 **Tip** If several virtual machines 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 a virtual machine, in the Virtual Machines panel, select the virtual machine, 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 virtual machines

HYCU for Azure enables you to protect your virtual machine data with fast and reliable backup and restore operations. After you back up a virtual machine, you can choose to restore either the entire virtual machine, individual disks, or individual files.

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 76](#).
- If private endpoints are configured in Azure, backing up and restoring data is always performed over the Azure backbone network. For details on how to configure private endpoints, see Azure documentation.

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

- [“Backing up virtual machines” below](#)
- [“Restoring virtual machines” on the next page](#)
- [“Restoring individual files” on page 49](#)

Backing up virtual machines

With HYCU for Azure, you can back up your virtual machines in a fast and efficient way.

Prerequisite

Only if a custom firewall rule is applied. Traffic to the *.azure.com, *.core.windows.net, *.servicebus.windows.net, and *.microsoftonline.com endpoints must be allowed.

Limitations


- Ultra disks are not protected.
- Azure temporary storage disks are not protected.
- Virtual machine memory is not protected.
- Backing up virtual machines that have shared disks attached is not supported.
- Backing up virtual machines with unmanaged disks is supported only if the unmanaged disks are in the same resource group as the virtual machine.
- Backing up virtual machines that have managed disks encrypted with SSE with PMK &

ADE is not supported. For a list of data protection operations that are supported based on how the managed disks are encrypted, see the *HYCU for Azure Compatibility Matrix*.

Considerations




- To optimize the use of storage space in the Azure storage accounts, HYCU for Azure employs the HYCU changed block tracking (CBT) technique on the backup data before storing it. This technique is applied to all backup data, including copies of backup data and data archives.
- Only one backup task can run at the same time for the virtual machine.
- *Only if you plan to run the pre-snapshot and post-snapshot scripts.* Make sure that the credential group is assigned to the virtual machine and virtual machine discovery is successful. For instructions on how to enable access to the virtual machine, see [“Enabling access to virtual machines” on page 35](#).
- *Only if you plan to restore individual files.*
 - Make sure that the restore of individual files is enabled for the virtual machine. For details on how to do this, see [“Configuring backup options” on page 31](#).
 - *For Windows virtual machines:* Make sure that the credential group is assigned to the virtual machine. For instructions on how to enable access to the virtual machine, see [“Enabling access to virtual machines” on page 35](#).

Accessing the Virtual Machines panel

To access the Virtual Machines panel, in the navigation pane, click  **Virtual Machines**.

Procedure

1. In the Virtual Machines panel, select the virtual machines that you want to back up.

 **Note** You can update the list of virtual machines by clicking  **Synchronize**. To narrow down the list of displayed virtual machines, you can use the filtering options as described in [“Filtering data” on page 65](#).
2. Click  **Policies**.
3. From the list of available policies, select the desired policy.
4. Click **Assign** to assign the policy to the selected virtual machines.

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

If required, you can also perform a manual backup of virtual machines at any time. For details, see [“Performing a manual backup” on page 73](#).

Restoring virtual machines

HYCU for Azure enables you to restore an entire virtual machine or individual virtual machine disks to a specific point in time.

Prerequisite

Only if a custom firewall rule is applied. Traffic to the *.azure.com, *.core.windows.net, *.servicebus.windows.net, and *.microsoftonline.com endpoints must be allowed.

Considerations


- Only one restore task can run at the same time for the virtual machine.
- When restoring data archives, HYCU for Azure performs data rehydration during which an archived blob is copied to the online hot tier (on a temporary container). Keep in mind that this can take a few hours to complete.

Restore options

You can select among the following restore options:

Restore option	Description	Instructions
Restore VM	Enables you to restore a virtual machine to its original location with the same configuration settings.	“Restoring a virtual machine” below
Clone VM	Enables you to restore a virtual machine by creating a virtual machine clone in its original or a new location with different configuration settings.	“Cloning a virtual machine” on page 43
Restore Disks	Enables you to restore virtual machine disks with the same configuration settings.	“Restoring virtual machine disks” on page 45
Clone Disks	Enables you to restore virtual machine disks by creating disk clones with different configuration settings.	“Cloning virtual machine disks” on page 46
Export Disks	Enables you to restore virtual machine disks to the same or a different Azure region.	“Exporting virtual machine disks” on page 48

Accessing the Virtual Machines panel

To access the Virtual Machines panel, in the navigation pane, click  **Virtual Machines**.

Restoring a virtual machine

You can restore an entire virtual machine to its original location with the same settings.

Prerequisites


- *Only if you plan to restore an entire virtual machine.* You have deleted the original virtual machine and all its disks from Azure.
- *Only if you plan to restore individual disks other than the boot disk.* You have deleted only the individual disks (not the entire virtual machine) from Azure.
- *Only if you plan to restore the boot disk.* You have deleted the entire virtual machine and the boot disk from Azure.


Consideration


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

Procedure


1. In the Virtual Machines panel, click the virtual machine 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 virtual machine. Selecting the check box before the name of the virtual machine will not open the Details section.

2. In the Details section, select the desired restore point, and then click  **Restore VM**.
3. Select **Restore VM**, and then click **Next**.
4. 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**
 - **Archive - weekly**
 - **Archive - monthly**
 - **Archive - yearly**

 **Important** *Only if the virtual machine that you are restoring has trusted launch enabled and you want to keep this security type also after the restore.* Make sure to select the **Backup (Snapshot)** tier. Otherwise, the security type of the restored virtual machine will be changed to Standard.

5. From the Disks drop-down menu, select the disks that you want to restore.


 **Note** By default, all the disks are selected. This means that the entire virtual machine will be restored if you did not exclude the individual disks from the backup as described in [“Configuring backup options” on page 31](#).

6. Click **Validate** to verify if the restore task can be run successfully.
7. Click **Restore**.

Cloning a virtual machine

You can restore a virtual machine to its original or a new location with custom settings. In this case, you create a new virtual machine containing the restored data alongside the original virtual machine. For the new virtual machine, you can specify a different resource group, geographic region, and/or virtual network.

Prerequisite



Only if you plan to restore multiple virtual machine disks. You have updated the list of virtual machines. To update the list of virtual machines, in the Virtual Machines panel, click  **Synchronize**.


Limitation


Restoring virtual machines with unmanaged disks to a different resource group is not supported.

Procedure


1. In the Virtual Machines panel, click the virtual machine 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 virtual machine. Selecting the check box before the name of the virtual machine will not open the Details section.
2. In the Details section, select the desired restore point, and then click  **Restore VM**.
3. Select **Clone VM**, and then click **Next**.
4. In the New virtual machine name field, enter a name for the virtual machine.
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**
 - **Archive - weekly**
 - **Archive - monthly**
 - **Archive - yearly**


 **Important** *Only if the virtual machine that you are restoring has trusted launch enabled and you want to keep this security type also after the restore. Make sure to select the **Backup (Snapshot)** tier. Otherwise, the security type of the restored virtual machine will be changed to Standard.*
6. From the Disks drop-down menu, select the disks that you want to restore.

 **Note** By default, all the disks are selected. This means that a new virtual machine containing the restored data will be created alongside the original virtual machine. The new virtual machine will include all the disks if you did not exclude individual disks from the backup as described in [“Configuring backup options” on page 31](#).

7. From the Resource group drop-down menu, select the resource group for the restored virtual machine.
8. From the Location drop-down menu, select the geographic region for the restored virtual machine.

 **Important** If you select a region other than the original one for the restored virtual machine, you will be charged for outbound data transfer. For details, see [Azure pricing](#).


9. From the Availability Zone drop-down menu, select the zone for the restored virtual machine.


 **Note** Keep in mind the following:



- The selected geographic region and the size of the virtual machine determine to which zones you can restore data. If you do not want to restore data to any zone, select **None**.
 - If you select a zone, only static public IP addresses can be assigned to the network interface on the restored virtual machine. For more information about public IP addresses, see [Azure documentation](#).
10. Under Network interfaces, you can view the network interface that will be added to the restored virtual machine. By default, this is the first network interface from the resource group that you selected for the restored virtual machine. If required, you can also modify network settings.

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. *Only if you are adding a network interface.* From the Virtual network drop-down menu, select the virtual network for the network interface.


 **Note** The list of available virtual networks includes only the ones within the region you selected for the restored virtual machine.
 - b. Select the subnet to which the network interface should be assigned.
 - c. In the Public IP address type field, select the public IP address for the network interface. You can select among the following options:

Option	Description
None	No public IP address will be assigned to the network interface on the restored virtual machine.
Dynamic	A dynamic public IP address will be assigned to the network interface on the restored virtual machine.  Note This option is not available if you previously selected a zone for your restored virtual machine.
Static	A static public IP address will be assigned to the network interface on the restored virtual machine.
Existing	A preferred public IP address that you have created in Azure will be assigned to the network interface on the restored virtual machine.  Note Because the restored virtual machine can only be assigned a Regional Tier public IP address, only such addresses are available from the drop-down list.

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

Option	Description
Dynamic	A dynamic private IP address will be assigned to the network interface on the restored virtual machine.
Static	A static private IP address will be assigned to the network interface on the restored virtual machine.

- 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 virtual machine without a network interface.

11. Click **Validate** to verify if the restore task can be run successfully.

12. Click **Restore**.

Restoring virtual machine disks



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


Limitation

Restoring unmanaged disks is not supported.

Procedure

1. In the Virtual Machines panel, click the virtual machine whose disks you want to restore. The Details section appears at the bottom of the screen.

 **Note** The Details section appears only if you click a virtual machine. Selecting the check box before the name of the virtual machine will not open the Details section.
2. In the Details section, select the desired restore point, and then click  **Restore VM**.
3. Select **Restore Disks**, and then click **Next**.
4. From the list of disks that are available for the restore, select the ones that you want to restore, and then click **Next**.

 **Note** If you select the boot disk, the virtual machine will be restarted after the disks are restored.
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**
 - **Archive - weekly**
 - **Archive - monthly**
 - **Archive - yearly**
6. Click **Validate** to verify if the restore task can be run successfully.
7. Click **Restore**.

Cloning virtual machine disks

You can create clones of virtual machine disks by restoring the disks and attaching them to the same or a different virtual machine. In this case, the disks will be attached to the preferred virtual machine.

Limitations



- Cloning unmanaged disks is not supported.
- You can attach the cloned disks only to a virtual machine that is running the same operating system as the original virtual machine and that belongs to the same protection set as the original virtual machine.



Considerations



- The name format of the cloned disk is `hycu-disk-<UUID>-<DiskName>`.
- *Only if you are cloning disks to the same virtual machine.* After cloning the disks, make sure to change their UUIDs to be able to perform further tasks on the virtual machine.

Procedure

1. In the Virtual Machines panel, click the virtual machine whose disks you want to restore. The Details section appears at the bottom of the screen.

 **Note** The Details section appears only if you click a virtual machine. Selecting the check box before the name of the virtual machine will not open the Details section.
2. In the Details section, select the desired restore point, and then click  **Restore VM**.
3. Select **Clone Disks**, and then click **Next**.
4. From the list of disks that are available for the restore, select the ones that you want to restore, 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**
 - **Archive - weekly**
 - **Archive - monthly**
 - **Archive - yearly**
6. From the Subscription drop-down menu, select the subscription that contains the virtual machine to which you want to attach the cloned disks.
7. From the Resource group drop-down menu, select the resource group of the virtual machine to which you want to attach the cloned disks.
8. From the Location drop-down menu, select the geographic region of the virtual machine to which you want to attach the cloned disks.

 **Important** If you select a region other than the original one, you will be charged for outbound data transfer. For details, see Azure pricing.
9. From the Virtual machine drop-down menu, select the virtual machine to which you want to attach the cloned disks.
10. *Only if you want to change the cloned disk name.* Under Disk name, for each disk whose name you want to change, do the following:
 - a. Click  **Edit Disk** next to the name of the disk.
 - b. In the New disk name field, enter a new name for the cloned disk.
 - c. Click **Save**.

 **Note** You can always change the name of the disk back to the original one by clicking  **Undo New Disk Name** next to the name of the disk whose name you changed.

11. Click **Validate** to verify if the restore task can be run successfully.
12. Click **Restore**.

Exporting virtual machine disks

You can export disks by restoring them to the same or a different Azure region. In this case, the disks will not be attached to any virtual machine.

Limitation



Exporting unmanaged disks is not supported.

Consideration


The name format of the exported disk is `hycu-disk-<UUID>-<DiskName>`.


Procedure



1. In the Virtual Machines panel, click the virtual machine whose disks you want to export. The Details section appears at the bottom of the screen.

 **Note** The Details section appears only if you click a virtual machine. Selecting the check box before the name of the virtual machine will not open the Details section.
2. In the Details section, select the desired restore point, and then click  **Restore VM**.
3. Select **Export Disks**, and then click **Next**.
4. From the list of disks that are available for the restore, select the ones that you want to restore, 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**
 - **Archive - weekly**
 - **Archive - monthly**
 - **Archive - yearly**
6. From the Subscription drop-down menu, select the subscription to which you want to export the disks.
7. From the Resource group drop-down menu, select the resource group to which you want to export the disks.
8. From the Location drop-down menu, select the geographic region to which you want to export the disks.

9. From the Availability Zone drop-down menu, select the zone to which you want to export the disks.

 **Note** The selected geographic region determines to which zones you can restore data. If you do not want to restore data to any zone, select **None**.

10. *Only if you want to change the exported disk name.* Under Disk name, for each disk whose name you want to change, do the following:
 - a. Click  **Edit Disk** next to the name of the disk.
 - b. In the New disk name field, enter a new name for the exported disk.
 - c. Click **Save**.

 **Note** You can always change the name of the disk back to the original one by clicking  **Undo New Disk Name** next to the name of the disk whose name you changed.

11. Click **Validate** to verify if the restore task can be run successfully.
12. Click **Restore**.

Restoring individual files

You can restore one or more files to the same or a different location on the original virtual machine, or to a target.

Prerequisites

- The restore of individual files must be enabled for the virtual machine. For details on how to do this, see [“Configuring backup options” on page 31](#).
- The credential group must be assigned to the virtual machine and virtual machine discovery must be successful. For instructions on how to enable access to the virtual machine, see [“Enabling access to virtual machines” on page 35](#).
- *Only if you plan to restore individual files to a target.* A storage account to which you want to restore data must be added to HYCU for Azure as a target and it must be reserved only for restored data. For details on targets, see [“Setting up targets” on page 20](#).
- *Only if a custom firewall rule is applied.* Traffic to the *.azure.com, *.core.windows.net, *.servicebus.windows.net, and *.microsoftonline.com endpoints must be allowed.

Considerations

Only if restoring files to the virtual machine:


- If the virtual machine is not accessible, the restore operation fails. The virtual machine may not be accessible if it is stopped or if it no longer exists.
- *Only if you plan to restore the original access control lists (ACLs):*


- Because restoring ACLs is not supported on FAT file system types, the status of the restore task for such files will be Done with errors. This means that the files have been restored, but because the files in the FAT file system do not have ACLs, the ACLs have not been set for the files.
- The ACL information is not restored during the cross-file system restore.

Accessing the Virtual Machines panel

To access the Virtual Machines panel, in the navigation pane, click  **Virtual Machines**.

Procedure

1. In the Virtual Machines panel, click the virtual machine that contains the files that you want to restore. The Details section appears at the bottom of the screen.
2. In the Details section, select the desired restore point, and then click  **Restore Files**.
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 (Snapshot)**
 - **Backup (Target)**
 - **Copy**
 - **Archive - daily**
 - **Archive - weekly**
 - **Archive - monthly**
 - **Archive - yearly**
4. In the Disks drop-down menu, make sure only the disks with the files that you want to restore are selected, and then click **Next**. By default, all the disks are selected.
5. From the list of available files, select the ones that you want to restore, and then click **Next**.

 **Important** You can select only individual files or folders for the restore, not whole disks or entire partitions.

6. Select whether you want to restore the files to the virtual machine or to a target, and then perform the required steps:

Restore files to...	Instructions
Virtual machine	<ol style="list-style-type: none"> a. Select Restore to virtual machine, and then click Next. b. Select the location on the virtual machine to which you want to restore the files, and then provide the required information:

Restore files to...	Instructions
	<ul style="list-style-type: none"> • Original location Select how the restore should save the files when there is a file with the same name and location on the virtual machine (overwrite the file, rename the original file, or rename the restored file). • Alternate location Specify the path to an alternate location on the virtual machine in the following format: <ul style="list-style-type: none"> ◦ Windows: <pre data-bbox="687 831 1185 864"><DriveLetter>:\<Path>\<FolderName></pre> ◦ Linux: <pre data-bbox="692 958 981 992">/<Path>/<FolderName></pre> <p>The restored files overwrite the files with the same name that might exist at the alternate location.</p> c. Use the Restore ACL switch if you want to restore the original access control list. If enabled, HYCU for Azure preserves original ACLs. If disabled, HYCU for Azure applies inherited ACLs on the restored files (according to the file system ACL inheritance rules).
Target	<ol style="list-style-type: none"> Select Restore to target, and then click Next. From the Target drop-down menu, select the target to which you want to restore the files.

7. Click **Restore**.

Chapter 5

Performing daily tasks

To ensure your data protection environment is in the optimal state in terms of security, reliability, and efficiency, HYCU for Azure 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 76](#).


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 Azure 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 the status of tasks” on page 54
View all events that occurred in the data protection environment.	“Viewing events” on page 54
Configure HYCU for Azure to send notifications when new events occur in your data protection environment.	“Configuring event notifications” on page 55
Obtain reports on different aspects of the data protection environment.	“Using HYCU for Azure reports” on page 58
View virtual machine details.	“Viewing virtual machine details” on page 62
Narrow down the list of displayed items by applying filters.	“Filtering data” on page 65
View target information, edit a target, or remove a target.	“Managing targets” on page 69
View policy information, edit a policy, or	“Managing policies” on page 72

I want to...	Instructions
delete a policy.	
Back up data manually.	"Performing a manual backup" on page 73
Mark a restore point as expired.	"Expiring backups manually" on page 74

Using the HYCU for Azure dashboard


The HYCU for Azure 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**.



You can find the following information within each widget:

Dashboard widget	Information
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 virtual machines to which this policy is assigned are compliant with the policy settings. For details on policies, see "Defining your backup strategy" on page 22 .
Virtual Machines	Percentage of virtual machines that are protected, and the number of protected and unprotected virtual machines in the protection set. A virtual machine is considered protected if it has an assigned policy and at least one valid backup within the retention period specified in the policy. For details on protecting virtual machines, see "Protecting virtual machines" on page 39 .
Backups	Backup success rate for the last seven days.
Targets	Number of storage accounts in the protection set, and the information on how much space is used and available for storing backup data. For details on targets, see "Setting up targets" 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 the status of tasks" on the next page .


Dashboard widget	Information
Events	<p>Total number of events and the number of events according to their severity level (Success, Warning, Failed) in the last 48 hours. For details on events, see “Viewing events” below.</p> <p> Note <i>Only if multiple protection sets are available in your data protection environment. HYCU for Azure shows the events for all protection sets and not only for the currently selected one.</i></p>

Checking the status of tasks

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 the tasks that are currently running.
- Check the completed and stopped tasks.
- List the tasks that match the specified filter.
- Check more details about a specific task in the Details section that appears at the bottom of the screen after you select the task.
- Generate a report about a specific task by selecting it, and then clicking  **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**.

Task information	Description
Description	Summary of the task (for example, running a backup, performing a restore, restoring individual files, and so on).
Status	Current status of the task (for example, Done, Ready, a progress bar indicating the Running status, Failed, Done with errors, and so on).
Started	Date and time the task started running.
Finished	Date and time the task finished.

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 Azure to send notifications when new events occur in your data protection environment. For details, see [“Configuring event notifications” below](#).

Consideration

Only if multiple protection sets are available in your data protection environment. HYCU for Azure shows the events for all protection sets and not only for the currently selected one.


Accessing the Events panel

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



Event information	Description
Severity	Severity level of the event (Info, Warning, Error).
Message	Description of the event.
Category	Functional area of HYCU for Azure to which the event belongs (for example, Targets, Credentials, Policies, System for an internal event, and so on).
Timestamp	Date and time the event was created.

Configuring event notifications

You can configure HYCU for Azure 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” below](#)
- [“Creating webhook notifications” below](#)

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 event categories. To include all categories, click **Select All**.
4. From the Severity drop-down menu, select one or more severity levels of events. To include all severity levels, click **Select All**.
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. In the Name field, enter a name for the webhook notification and, optionally, its description.
3. From the Category drop-down menu, select one or more event categories. To include all categories, click **Select All**.
4. From the Severity drop-down menu, select one or more severity levels of events. To include all severity levels, 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.* In the Secret field, enter a secret for authentication.
7. Click **Next**.



8. *Optional.* Customize the body of the request that is sent by HYCU for Azure. 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 webhook data format that HYCU for Azure 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 Azure
- HTTP request body sent by HYCU for Azure

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>",
  "authorityIdentifier": "<authorityIdentifier-value>",
  "created": "<created-value>",
  "details": "<details-value>",
  "category": "<category-value>",
  "message": "<message-value>",
  "taskUUID": "<taskUUID-value>"
}
```

 **Note** Null values are set to N/A.


Using HYCU for Azure reports

HYCU for Azure 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 10 minute latency period.


After you get familiar with reports as described in [“Getting started with reporting” below](#), you can continue as follows:


- View reports. For details, see [“Viewing reports” on page 60](#).
- Generate reports. For details, see [“Generating reports” on page 60](#).
- Schedule reports. For details, see [“Scheduling reports” on page 61](#).

 **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 62](#).

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 **Spacebar**. To return it to its original size, click ▲ **Maximize** or press **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 total size of virtual machine backup data and the size of virtual machine disks. These reports cannot be edited or deleted.

Name	Description
Protected data on targets – per	Amount of protected data on targets per access tier.


Name	Description
access tier	
Protected data on targets – per policy	Amount of protected data on targets per policy.
Protected data on targets – per virtual machine	Amount of protected data on targets per virtual machine.
Protected virtual machine disk capacity – per policy	Amount of protected virtual machine disk capacity per policy.
Total protected data on targets (trend)	Total amount of protected data on targets through time.
Total virtual machine disk capacity (trend)	Total amount of virtual machine disk capacity through time.
Virtual machine compliance status	List of virtual machines, 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.	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 1. From the list of reports, select the one that you want to


I want to...	Procedure
and save it as a new report.	<p>edit and save as a new report, and then click  Edit. The Report Configuration dialog box opens.</p> <ol style="list-style-type: none"> Enter a new name for the report, and then make the required modifications. Click Save as.

Viewing reports

You can view the reports on the current state of your data protection environment or the saved reports 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.	<ol style="list-style-type: none"> From the list of reports, select the desired report. 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. <p>For instructions on how to generate reports manually or automatically, see “Generating reports” below or “Scheduling reports” on the next page.</p>

In the dialog box that opens, besides viewing the report data, you can also do the following:


- Switch between the reports.
- 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.
- If you view a report on the current state of the data protection environment, you can save this version of the report by clicking **Generate**. The saved report is added to the list of report versions.

Generating reports


When you generate a report, you are saving 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 page 59](#).

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 reports. For details, see [“Viewing reports” on the previous page](#).
- Delete the saved reports 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 reports automatically at a particular time each day, week, or month. You can view these reports in the web browser or schedule them to be delivered 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 59](#).



2. In the Schedule date field, specify the date and the time of the day when you want the report generation to begin.
3. From the Interval drop-down menu, select how often you want the reports 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 **Schedule**.

 **Tip** The reports that are generated automatically are marked by  in the Scheduled column of the Reports panel and have Auto-generated in their description.

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 Azure enables you to share reports among different HYCU for Azure 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 the 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 reports.

Viewing virtual machine details


You can view detailed information about virtual machines in the Details section of the Virtual Machines panel.










Accessing the Virtual Machines panel


To access the Virtual Machines panel, in the navigation pane, click  **Virtual Machines**.

Procedure

In the Virtual Machines panel, click the virtual machine whose details you want to view. The Details section appears at the bottom of the screen.







 **Note** The Details section appears only if you click a virtual machine. Selecting the check box before the name of the virtual machine will not open the Details section.

VM information	Description
Details	Detailed information about the selected virtual machine such as its UUID, type, operating system, and so on.
Restore point	<p>Detailed information about the restore point:</p> <ul style="list-style-type: none"> • Date and time the restore point was created. • Available tiers from which you can restore data: <ul style="list-style-type: none"> ◦  SNAP Snapshot: Available if a virtual machine snapshot exists, enabling a faster restore. ◦  BCKP Backup: Available if backup data is stored on a target. ◦  COPY Copy: Available if a copy of backup data was created. ◦  ARCH Data archive: Available if a data archive was created. ◦  CTLG Catalog: Available if the restore of individual files was enabled. <p> Note <i>Only if you excluded individual disks from the backup.</i> The restore point does not include the backup data of the entire virtual machine.</p>
Compliance	<p>Compliance status of the backup:</p> <ul style="list-style-type: none"> •  Success. The backup is compliant (the RPO setting in the policy assigned to the virtual machine was met). •  Failure: The backup is not compliant (the RPO setting in the policy assigned to the virtual machine was not met). •  Undefined: Backup compliance is undefined. <p>By pausing on the compliance status indicated by an icon, additional information about the backup is available. You can see backup frequency and the elapsed time since the last successful backup.</p>

Backup status	Backup status of the virtual machine. For details, see “Viewing the backup status of virtual machines” below.
Restore status	Progress bar indicating the progress of the virtual machine restore.  Note By double-clicking a progress bar, you are directed to the Tasks panel where you can check details about the related task.


Viewing the backup status of virtual machines

The backup status of your virtual machine determines whether it is possible to restore it.

Backup status	Restore a VM or disks?	Restore files?
 Done	✓	✓
 Done with warnings	✓ ^a	✓
 Done with errors	✓ ^a	×
 Failed	×	×
 Aborted	×	×
 (Expired / Inaccessible on Azure / Deleted from Azure)	×	×


^a This backup status may indicate the following:






- Not all virtual machine disks were backed up successfully, therefore the virtual machine can be restored only partially. If backing up a boot disk failed, you may not be able to start the virtual machine after the restore.
- Creating a copy of backup data failed. However, the virtual machine can still be fully restored from the backup or the data archive (if it exists).

 **Note** By pausing on the backup status indicated by an icon, additional information about the backup is available. You can see the backup type, the duration and size of the backup, which target was used, and the backup 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 a virtual machine. The following is an example of possible marks:

Tier status	Restore a virtual machine?
 (Done)	✓

Tier status	Restore a virtual machine?
 (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 virtual machines” on the previous page.
 (Failed)	×
 (Aborted)	×
 (Expired)	×
 (Inaccessible on Azure / Deleted from Azure)	×

Filtering data

HYCU for Azure provides you with two types of filters that you can apply—the main filter and the detail filter. After you apply any of the filters, only data that matches the filter criteria is displayed and you can easily find what you need.


 **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.

Applying the main filter

Apply the main filter when you want to focus on certain aspects of your data protection environment. For example, filtering data in the Virtual Machines panel helps you to focus only on the virtual machines that you are interested in.

Procedure

In the Search field of the selected panel, enter a search term to filter data. If required, narrow down the search scope by using more specific filtering options:

1. Click  **Main Filter**. The Filters - Main view side panel opens.
2. Specify your filter criteria.
3. Click **Apply Filters**.

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

- [“Filtering options in the Virtual Machines panel” on the next page](#)
- [“Filtering options in the Policies panel” on page 67](#)
- [“Filtering options in the Targets panel” on page 67](#)


- [“Filtering options in the Tasks panel” on page 68](#)
- [“Filtering options in the Events panel” on page 69](#)

Applying the detail filter

Apply the detail filter when you want to focus on the information about the restore and backup data of the selected item.

 **Note** The detail filter is available in the Virtual Machines panel.

Procedure

1. From the list of all virtual machines in the Virtual Machines panel, select the virtual machine that you want to filter by restore and backup data.
2. In the Detail view that appears at the bottom of the screen, click  **Detail Filter**. The Filters - Detail view side panel opens.
3. Specify your filter criteria.
4. Click **Apply Filters**.

For the information on the available filtering options, see [“Filtering options in the Virtual Machines panel” below](#).

Filtering options in the Virtual Machines panel

In the Filters - Main view side panel, select one or more filtering options:

Filtering option	Action
Resource groups	From the drop-down menu, select the resource groups to which the virtual machines belong.
Policies	From the drop-down menu, select the policies that are assigned to the virtual machines.
Credential groups	From the drop-down menu, select the credential groups that are assigned to the virtual machines.
Compliance	Select one or more options to filter by the compliance status (a virtual machine is considered compliant if the time since the last successful backup is lower than the RPO policy setting): <ul style="list-style-type: none"> • Success • Failure • Undefined
Protection	Select one or more options to filter by the virtual machine protection status: <ul style="list-style-type: none"> • Yes

Filtering option	Action
	<ul style="list-style-type: none"> • No • Deleted
Discovery	Select one or more options to filter by the virtual machine discovery status: <ul style="list-style-type: none"> • Success • Failure • Warning • Undefined

In the Filters - Detail view side panel, select one or more filtering options:

Filtering option	Action
Tiers	From the drop-down menu, select one or more tiers.
Restore point date	Select the time to filter by when the restore points were created.
Status	Select one or more check boxes to filter by status.
Compliance	Select one or more check boxes to filter by the compliance status.

Filtering options in the Policies panel

In the Filters - Main view side panel, select one or more filtering options:

Filtering option	Action
Compliance	Select one or more options to filter by the compliance status (a policy is considered compliant if all virtual machines to which this policy is assigned are compliant with the policy settings): <ul style="list-style-type: none"> • Success • Failure • Undefined

Filtering options in the Targets panel

In the Filters - Main view side panel, select one or more filtering options:

Filtering option	Action
Kind	<p>Select one or more check boxes to filter by the Azure storage account kind:</p> <ul style="list-style-type: none"> • Storage • StorageV2 • BlockBlobStorage
Health	<p>Select one or more check boxes to filter by the health of the target:</p> <ul style="list-style-type: none"> • Ok • Warning • Error • Undefined

Filtering options in the Tasks panel

In the Filters - Main view side panel, select one or more filtering options:

Filtering option	Action
Resource groups	From the drop-down menu, select the resource groups of interest.
Authority	From the drop-down menu, select the items to filter the list to include only the tasks that are the results of the selected authority's actions (users or service principals).
Type	From the drop-down menu, select the items to filter the list to include only the tasks according to their type (for example, running a backup, performing a restore, restoring individual files, and so on).
Status	<p>Select one or more options to filter by the status of the task:</p> <ul style="list-style-type: none"> • Ready • Running • Pausing • Paused • Aborting • Aborted • Done • Failed • Done with errors • 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

Filtering option	Action
	week), or use the calendar to select the start date and hour and the end date and hour of the time range for tasks to be displayed.

Filtering options in the Events panel

In the Filters - Main view side panel, select one or more filtering options:

Filtering option	Action
Resource groups	From the drop-down menu, select the resource groups of interest.
Category	From the drop-down menu, select the items to filter the list to include only the selected event categories.
Authority	From the drop-down menu, select the items to filter the list to include only the events that are the results of the selected authority's actions (users or service principals).
Severity	Select one or more options to filter by the severity level of the event: <ul style="list-style-type: none"> • Info • Warning • Error
Time range	Specify a time range to limit your search for events. You can select one of the predefined time ranges (Last 1 hour, Last 24 hours, or Last week), or use the calendar to select the start date and hour and the end date and hour of the time range for events to be displayed.


Managing targets

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

Consideration






Only Azure storage accounts that were added to HYCU for Azure 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**.

Viewing target information

You can view the information about each target in the list of targets in the Targets panel.

Target information	Description
Name	<p>Name of the target.</p> <p> Tip If you click a target name, you are directed to the Azure portal where you can view more details about the related target.</p>
Region	Azure region where the target resides.
Kind	Storage account kind of the target in Azure: Storage (general purpose v1), StorageV2 (general purpose v2), or BlockBlobStorage.
Status	<p>Shows the status of the target:</p> <ul style="list-style-type: none"> • Active: You can use the target for backup and restore operations. • Inactive: The target has been deactivated in HYCU for Azure and you can use it only for restore operations. • Inaccessible on Azure: Insufficient permissions are set on the target in Azure and HYCU for Azure cannot access the target. • Deleted from Azure: The target no longer exists in HYCU for Azure. <p>For instructions on how to change the status of active or inactive targets, see “Activating or deactivating a target” on the next page.</p>
Size limit	Amount of storage space for storing backup data.
Health	<p>Health status of the target:</p> <ul style="list-style-type: none"> •  The target is in a healthy state. The utilization of storage space for backup data is less than 90 percent of the specified size limit. •  The utilization of storage space for backup data is over 90 percent of the specified size limit or the target is publicly accessible in Azure. •  The utilization of storage space for backup data is over the specified size limit, the target has been deleted from Azure, or the target is not accessible due to an I/O error, insufficient permissions, or some other reason. •  The target health has not been checked yet.
Utilization	Ratio (in percentage) of storage space used for backup data to free

Target information	Description
	storage space according to the specified size limit.
Automatic	Shows whether the target was created automatically by HYCU for Azure (✓) or not (✕).


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

Editing a target

Limitation

You cannot edit targets whose status is Inaccessible on Azure or Deleted from Azure.

Procedure

1. In the Targets panel, select the target that you want to edit, and then click  **Edit**.
2. Edit the selected target as required. For details on target properties, see [“Adding a storage account to HYCU for Azure” on page 21](#).
3. Click **Save**.

Activating or deactivating a target



Prerequisite

For target deactivation: The target is not specified as the location for storing data in any of the policies.

Limitations

- You cannot deactivate targets that were created automatically by HYCU for Azure.
- You cannot activate or deactivate targets whose status is Inaccessible on Azure or Deleted from Azure.

Procedure

1. In the Targets panel, select the target that you want to activate or deactivate.
2. Change the status of the selected target by clicking  **Activate** or  **Deactivate**.
3. *Only if you are deactivating a target.* Click **Yes** to confirm that you want to deactivate the selected target.

If you deactivate a target, this target will not be used for backup and restore operations anymore.

You can check the status of each target in the list of targets in the Targets panel.

Removing a target

If you do not want to use a target for storing backup data anymore, you can remove it from HYCU for Azure.


Prerequisites

- No backup data is stored on the target.
- The target is not specified as the location for storing data in any of the policies.

Consideration

Removing the target from HYCU for Azure does not remove the corresponding storage account from Azure, but only deletes the backup data from it.

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 a policy, 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**.

Viewing policy information

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


Policy information	Description
Name	Name of the policy.
Compliance	Compliance status of the policy: <ul style="list-style-type: none"> •  The policy is compliant. •  The policy is non-compliant. •  Policy compliance is undefined. The policy is not assigned to any virtual machine or this is the Exclude policy.
Virtual machine	Number of the virtual machines that have the policy assigned to

Policy information	Description
count	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.


Editing a policy

Procedure

1. In the Policies panel, select the policy that you want to edit, and then click  **Edit**.
2. Edit the selected policy as required. For details on policy properties, see [“Creating a custom policy” on page 24](#).
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 a manual backup

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


Consideration

When the assigned policy uses a backup window, manual backups may prevent the scheduled backup for the virtual machine from starting within the defined time frame. If this happens, the virtual machine becomes non-compliant with the policy settings until the next backup window or the next manual backup.

Accessing the Virtual Machines panel

To access the Virtual Machines panel, in the navigation pane, click  **Virtual Machines**.

Procedure


1. In the Virtual Machines panel, select the virtual machines that you want to back up.
2. Click  **Backup** to perform the backup of the selected virtual machines.
3. Click **Yes** to confirm that you want the manual backup to start.

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

Expiring backups manually


HYCU for Azure 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.


 **Tip** By pausing on the tier indicated by an icon in the Details section of the Virtual Machines panel, you can check the backup, copy, and/or archive expiration time.

You can mark as expired one of the following:

- Whole restore point
Make sure that all tiers are marked for expiration.
- One or more tiers
Make sure that only tiers that you want to expire are marked for expiration.


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


Accessing the Virtual Machines panel

To access the Virtual Machines panel, in the navigation pane, click  **Virtual Machines**.

Procedure

1. In the Virtual Machines panel, click the virtual machine 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 a virtual machine. Selecting the check box before the name of the virtual machine will not open the Details section.

2. In the Details section, select the restore point that you want to mark as expired.
3. Click  **Expire**.
4. Make sure the tiers that you want to mark as expired are selected:
 - Backup (Snapshot)
 - 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.

HYCU for Azure automatically removes the expired backup during the next retention maintenance task.

Chapter 6

Customizing HYCU for Azure

After you subscribe to HYCU for Azure, as an administrator, you can perform various tasks to customize HYCU for Azure for your data protection environment.

Task	Instructions
Change roles, set the default role for users and service principals, and delete users.	“Managing roles” below
Add, edit, and delete service principals, as well as change the default service principal.	“Configuring service principals” on page 78
Create, edit, and remove protection sets, as well as add resource groups to protection sets by using a tag.	“Managing protection sets” on page 80
View and manage HYCU for Azure subscriptions.	“Managing HYCU for Azure subscriptions” on page 83

Managing roles

A role determines the scope of actions that can be performed in the HYCU for Azure data protection environment by a specific user or service principal. 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 authority.

Considerations

- Each user that signs in to HYCU for Azure or each configured service principal has by default the Administrator role assigned unless set otherwise. For details on changing the default role, see [“Changing the default role” on page 78](#).
- At least one user and one service principal that have the Administrator role assigned must exist in the data protection environment.
- If multiple protection sets are available in your data protection environment, a user or a service principal has the same role in all protection sets within the same subscription.

- If a user or a service principal has access to multiple subscriptions, they can have different roles assigned in different subscriptions. The user can also switch among these subscriptions while being signed in to HYCU for Azure.

Accessing the Roles dialog box

To access the Roles dialog box, click  on the toolbar, and then select **Roles**.

HYCU for Azure roles

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

Role	Allowed actions
Viewer	Acquire information about virtual machines, policies, targets, tasks, events, reports, service principals, and protection sets in the data protection environment.
Backup Operator	Acquire the same information as Viewer, define backup strategies, and back up virtual machines.
Restore Operator	Acquire the same information as Viewer and restore virtual machines.
Protégé Operator	<i>Reserved for service principals.</i> Migrate protected data from the on-premises environment to Azure and the other way round by using the HYCU SpinUp functionality. For details on how to employ HYCU Protégé, see HYCU documentation.
Administrator	Perform all actions in the data protection environment.

Changing a role

Consideration


If you plan to change your own role, keep in mind that you will not be able to change it back to Administrator yourself.


Procedure

1. In the Roles dialog box, from the list of available authorities (users and service principals), select the one to which you want to assign a different role.



Tip You can also search for an authority by entering its name in the Search field.


2. Click  **Change Role**. The Role Change dialog box opens.
3. From the Role drop-down menu, select the role that you want to assign to the user or the service principal.

 **Note** You can assign multiple roles to the same user or service principal if the needs of your data protection environment require it.

Changing the default role

You can at any time change the default role for users and service principals. This means that all new users that sign in to HYCU for Azure and all newly configured service principals will automatically acquire the new default role.

Procedure



1. Click  **Change Role** next to Default Role at the upper right of the Roles dialog box. The Default Role Change dialog box opens.
2. From the Role drop-down menu, select which role you want to be the default one.
3. Click **Save**.

Deleting a user

Considerations

- Deleting a user from HYCU for Azure does not remove it from Azure.
- You cannot delete yourself from HYCU for Azure.
- Any upcoming data protection tasks related to the user that you delete will be automatically assigned to you.



Procedure

1. In the Roles dialog box, 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 **Yes** to confirm that you want the selected user to be deleted from HYCU for Azure.

Configuring service principals

For security reasons, a service principal is used instead of a user identity to run automated tasks in HYCU for Azure. The service principal is a service account that has access to a predefined set of Azure resources and is always used to run automated tasks instead of your own account.


You can define as many service principals as your business requires. Take into account that HYCU for Azure automatically creates a service principal for you in Azure, adds it to HYCU for Azure as the default service principal, and sets it as the active service principal.

The default service principal is represented by the  icon and the active service principal is represented by the  icon.

Prerequisites

- *Only if you plan to use a service principal other than the default one.* You have created a service principal in Azure.
- The service principal—the default one or the one you have created yourself—must have the Contributor role assigned at the subscription level. For instructions on how to assign a role to a service principal, see Azure documentation.


Accessing the Service Principals dialog box

To access the Service Principals dialog box, click  on the toolbar, and then select **Service Principals**.

Adding a service principal

Procedure

1. In the Service Principals dialog box, click **+ Add**.
2. In the Name field, enter a name for your service principal.


 **Note** It is recommended that you enter the same name for the service principal as the one that you used when registering the application and creating the service principal.
3. In the Tenant ID field, enter your tenant ID.
4. In the Application ID field, enter the ID of the application's registration in your Azure Active Directory.
5. In the Application secret field, enter the secret that is associated with the application ID.
6. Click **Save**.


Setting the active service principal

Consideration

The default service principal is the one that is used to run automated tasks unless you set another service principal as the active service principal.


Procedure

1. In the Service Principals dialog box, select the service principal that you want to set as the active service principal.
2. Click  **Set Active**.

The  icon appears next to the service principal indicating that you have successfully set it as the active service principal.

Editing a service principal

Procedure

1. In the Service Principals dialog box, select the service principal that you want to edit, and then click  **Edit**.
2. Edit the selected service principal as required.
3. Click **Save**.


Deleting a service principal

You can at any time delete a service principal that you no longer need from HYCU for Azure. Deleting the service principal from HYCU for Azure does not remove it from Azure.

Considerations

- The default service principal that is automatically created and added to HYCU for Azure cannot be deleted.
- *Only if a service principal other than the default one is set as the active service principal. If you delete the active service principal, the default service principal is automatically set as the active service principal.*

Procedure

1. In the Service Principals dialog box, select the service principal that you want to delete, and then click  **Delete**.
2. Click **Yes** to confirm that you want to delete the selected service principal.


Managing protection sets

If you have the required permissions granted, you can perform the following protection set-related tasks:

Task	Instructions
Create a protection set and include preferred resource groups in it.	“Creating a protection set” on the next page
Edit an existing protection set.	“Editing a protection set” on the next page
Add a resource group to a protection set by using a tag.	“Adding a resource group to a protection set by using a tag” on page 82
Exclude a resource group from a protection set.	“Excluding a resource group from a protection set” on page 82
Delete a protection set that you no longer need.	“Deleting a protection set” on page 83

For details on protection sets, see [“Determining the scope of data protection” on page 20](#).


Accessing the Protection Sets dialog box

To access the Protection Sets dialog box, click  on the toolbar, and then select **Protection Sets**.

Creating a protection set

Procedure

1. In the Protection Sets dialog box, from the Subscription drop-down menu, select the HYCU for Azure subscription for which you want to create a new protection set.
2. Click **+ New**.
3. Enter a name for your protection set.
4. From the list of available resource groups, select one or more resource groups that you want to include in the protection set.

 **Tip** You can search for a resource group by entering its name in the Search field and then pressing **Enter**. By selecting the Resource group check box, you select all resource groups at once.


5. Click **Save**.

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


Editing a protection set

You can modify the name of a protection set, and include or exclude resource groups from the protection set. You can exclude the resource groups from the protection set also directly by following the procedure described in [“Excluding a resource group from a protection set” on the next page](#).

Consideration

You cannot edit the default protection set created by HYCU for Azure (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 edit, and then click  **Edit**.
2. Edit the selected protection set as required.
3. Click **Save**.

Adding a resource group to a protection set by using a tag

As an alternative to adding a resource group to a protection set by using the HYCU for Azure web user interface, you can also add a resource group to a protection set by applying the `hycu-protection-set` tag to the resource group in Azure.

Prerequisite

The protection set to which you want to add the resource group must be created in HYCU for Azure.

Procedure

In Azure, apply the tag to the resource group as the following key-value pair:

Name	Value
<code>hycu-protection-set</code>	<p><code><ProtectionSetName></code></p> <p>In this case, <code><ProtectionSetName></code> is the name of the protection set to which you want to add the resource group.</p>


The resource group is automatically added to the preferred protection set during the next virtual machine synchronization in HYCU for Azure.

For detailed instructions on how to create and manage tags, see Azure documentation.



Excluding a resource group from a protection set

By excluding a resource group from a protection set, you do not remove the selected resource group from HYCU for Azure, but move it to the default protection set.

Consideration

You cannot exclude resource groups from the default protection set created by HYCU for Azure (represented by the  icon).


Procedure

1. In the Protection Sets dialog box, from the list of protection sets, click  before the name of the protection set that contains resource groups that you want to exclude. The list of all included resource groups is displayed.
2. Select the resource group that you want to exclude from the protection set, and then click  **Remove**.
3. Click **Yes** to confirm that you want to remove the selected resource group.


Deleting a protection set

By deleting a protection set, you do not remove its resource groups from HYCU for Azure, but move them to the default protection set.

Consideration

You cannot delete the default protection set created by HYCU for Azure (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 Azure, and then click  **Delete**.
2. Click **Yes** to confirm that you want to delete the selected protection set.


Managing HYCU for Azure subscriptions

In the SaaS Subscription Information dialog box, you can view and manage your HYCU for Azure subscriptions. The following information is available for each subscription:

- Subscriber's name and company
- Notification email recipients

 **Note** If this field is empty, all important notifications related to the HYCU for Azure subscription, such as support and upgrade information, are by default sent to the email address that was provided when subscribing to HYCU for Azure. It is recommended that you verify this email address and, if required, update the list of email addresses to which the notifications are sent.


- HYCU for Azure subscription ID, activation status, and software plan

 **Note** If you determine that another software plan would be more suitable for your data protection environment, you can change it directly from this dialog box.

- Azure subscription name and ID
- List of all resource groups within the selected subscription

You can also unsubscribe from HYCU for Azure from this dialog box. For details on how to cancel your HYCU for Azure subscription, see [“Canceling your HYCU for Azure subscription” on page 85](#).

Accessing the SaaS Subscription Information dialog box

To access the SaaS Subscription Information dialog box, click  on the toolbar, and then select **SaaS Subscription Information**.

Prerequisite

Only if you plan to change the software plan. You have signed in to HYCU for Azure with the same user account that you used for subscribing to the service.

Procedure

1. In the SaaS Subscription Information dialog box, from the SaaS subscription drop-down menu, select the HYCU for Azure subscription that you want to view or customize.
2. *Only if you plan to specify email addresses for notifications.* In the Notification email recipients field, enter one or more email addresses to which the notifications related to the selected HYCU for Azure subscription will be sent.
3. *Only if you plan to change the HYCU for Azure software plan.* From the Software plan drop-down menu, select the HYCU for Azure software plan that is best suitable for your data protection environment.
4. Click **Update**, and then click **Yes** to confirm the changes.
5. Click **Close**.

Chapter 7




Canceling your HYCU for Azure subscription

If for whatever reason you decide that you no longer want to use HYCU for Azure for protecting your data, you can easily cancel your HYCU for Azure subscription.

Prerequisite

You have signed in to HYCU for Azure with the same user account that you used for subscribing to the service.

Procedure

Task	Instructions
1. Stop charges for backup and recovery.	<p>In HYCU for Azure, unassign policies from all virtual machines:</p> <ol style="list-style-type: none">1. In the navigation pane, click  Virtual Machines.2. Select all the virtual machines, and then click  Policies.3. Click Unassign, and then click Yes to confirm that you want to unassign the policies from the selected virtual machines. <p> Important Only if multiple protection sets are available in your data protection environment. Make sure to follow these steps for each protection set separately.</p>
2. Stop charges for backup data storage.	<p>In Azure, do the following:</p> <ul style="list-style-type: none">• Delete all automatically created storage accounts and all backup data that is stored in manually created storage accounts.• Delete all snapshots created by HYCU for Azure. <p>For instructions, see Azure documentation.</p>
3. Unsubscribe from HYCU for Azure.	<p>In HYCU for Azure, do the following:</p>

Task	Instructions
	<ol style="list-style-type: none"> 1. Navigate to the SaaS Subscription Information dialog box by clicking ? on the toolbar, and then selecting SaaS Subscription Information. 2. From the SaaS subscription drop-down menu, select the HYCU for Azure subscription that you want to cancel. 3. Click Unsubscribe. 4. Click Yes to confirm that you want to unsubscribe from the selected HYCU for Azure subscription.
4. Prevent HYCU for Azure from accessing data on your behalf.	In Azure, revoke the consent for HYCU for Azure by removing it from the list of app registrations. For details on how to do this, see Azure documentation.
5. Delete HYCU for Azure as a SaaS application from Azure.	In Azure, delete HYCU for Azure from the list of SaaS applications. For details on how to do this, see Azure documentation.

After you cancel your HYCU for Azure 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 Azure, contact HYCU Customer Support.

Chapter 8

Troubleshooting

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

1. Try to solve the problem on your own. When doing so, 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 Azure?
- 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 54](#) and [“Checking the status of tasks” on page 54](#).

- 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)

Appendix A

Deploying a HYCU backup controller

If you are employing HYCU Protégé, you can use the HYCU for Azure web user interface to deploy a HYCU backup controller virtual machine to Azure 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 own the HYCU and HYCU Protégé licenses. For details on how to obtain these licenses, see HYCU for Enterprise Clouds documentation.
- You have the Administrator role assigned.

Consideration

Minimum requirements for the HYCU backup controller are 4 vCPU cores and 4 GiB of memory.

Accessing the HYCU Controller Deployment dialog box

To access the HYCU Controller Deployment dialog box, click  on the toolbar, and then select **HYCU Controller Deployment**.

Procedure

1. From the Resource group drop-down menu, select the resource group to which you want to deploy the HYCU backup controller.
2. From the Location 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 resource group location.


3. From the Availability Zone drop-down menu, select the zone for the HYCU backup controller.



Note Keep in mind the following:

- The selected geographic region determines to which zones you can deploy the HYCU backup controller. If you do not want to deploy the HYCU backup controller to any zone, select **None**.
- If you select a zone, only static public IP addresses can be assigned to the network interface of your HYCU backup controller. For more information about public IP addresses, see Azure documentation.


4. Click **Next**.
5. In the VM 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 1024.
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 4096.
8. From the Virtual machine type drop-down menu, select the virtual machine type.


 **Note** The list of available virtual machine types is based on the number of virtual CPU cores and the amount of memory that you specified. If no virtual machine type exactly corresponds to the specified values, the closest matches are shown.



9. 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 resource group that you selected for the HYCU backup controller. If required, you can also modify network settings.

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. *Only if you are adding a network interface.* From the Virtual network drop-down menu, select the virtual network for the network interface.


 **Note** The list of available virtual networks includes only the ones within the region you selected for the HYCU backup controller.
 - b. Select the subnet to which the network interface should be assigned.
 - c. In the Public IP address type field, select the public IP address for the network interface. You can select among the following options:

Option	Description
None	No public IP address will be assigned to the network interface on the HYCU backup controller.
Dynamic	A dynamic public IP address will be assigned to the network interface on the HYCU backup controller.  Note This option is not available if you previously selected a zone for your HYCU backup controller.
Static	A static public IP address will be assigned to the network interface on the HYCU backup controller.
Existing	A preferred public IP address that you have created in Azure will be assigned to the network interface on the HYCU backup controller.  Note Because the HYCU backup controller can only be assigned a Regional Tier public IP address, only such addresses are available from the drop-down list.

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

Option	Description
Dynamic	A dynamic private IP address will be assigned to the network interface on the HYCU backup controller.
Static	A static private IP address will be assigned to the network interface on the HYCU backup controller.

- 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.

10. Click **Deploy**.

Accessing the HYCU web user interface

After you deploy the HYCU backup controller, you must perform the following tasks in Azure to be able to access the HYCU web user interface:

Task	Instructions
1. Configure a port.	Create an inbound security rule to allow traffic. Specify the following settings:

Task	Instructions
	<ul style="list-style-type: none"> Source port ranges: * (to allow any source port) Destination port ranges: 8443 For instructions, see Azure documentation.
2. Create a public IP address.	For instructions on how to create a public IP address, see Azure documentation.

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

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

You can also access the HYCU web user interface by providing a host name instead of a public IP address. In this case, you must configure an alias record to refer to the public IP address. For instructions on how to do this, see Azure documentation.

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**

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

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!

