Acronis Cyber Infrastructure
5.0

Backup Gateway Quick Start Guide for Microsoft Azure

REVISION: 3/3/2022
Table of contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Important requirements and restrictions</td>
<td>4</td>
</tr>
<tr>
<td>Creating Acronis Cyber Infrastructure virtual machine</td>
<td>5</td>
</tr>
<tr>
<td>Adding space to Acronis Cyber Infrastructure</td>
<td>10</td>
</tr>
<tr>
<td>Performing additional tasks</td>
<td>12</td>
</tr>
</tbody>
</table>

© Acronis International GmbH, 2003-2022
Introduction

This guide explains how to set up Backup Gateway on Microsoft Azure to store backups in the Azure cloud.

Typically, you will only need to create a virtual machine (VM) with Acronis Cyber Infrastructure on Azure, specifying the required details like VM user name and password, credentials for a partner account in Acronis Cyber Protect Cloud, and such. Once the virtual machine is running, you should be able to store backups in the Azure cloud, without having to log in to Acronis Cyber Infrastructure. However, if necessary, you can log in to the admin panel at the VM hostname and port 8888. For example, https://backupgateway.azure.com:8888/.

Backups are cold data with a specific access pattern: the data is not accessed frequently but is expected to be available immediately when accessed. For this use case, it is cost-efficient to choose storage classes intended for long-term storage with infrequently accessed data. The recommended storage class for Microsoft Azure is Cool Blob Storage. Archive storage classes like Azure Archive Blob cannot be used for backup because they do not provide instant access to data. High access latency (several hours) makes it technically impossible to browse archives, restore data fast, and create incremental backups. Even though the archive storage is usually very cost-efficient, keep in mind that there are a number of different cost factors. In fact, the total cost of public cloud storage consists of payments for storing data, operations, traffic, data retrieval, early deletion, and so on. For example, an archive storage service can charge six months’ storage payment for just one data recall operation. If the storage data is expected to be accessed more frequently, the added costs increase significantly the total cost of data storage. In order to avoid the low data retrieval rate and to cut expenses, we recommend using Acronis Cyber Cloud for storing backup data.
Important requirements and restrictions

- When working with public clouds, Backup Gateway uses the local storage as the staging area as well as to keep service information. It means that the data to be uploaded to a public cloud is first stored locally and only then sent to the destination. For this reason, it is vital that the local storage is persistent and redundant so the data does not get lost. Using temporary disks may result in data loss.

- Choose a correct disk template to ensure desired backup performance (see example in the next paragraph). Make sure to plan ahead, because disk template cannot be changed. In such a case, you will need to add a new disk with the correct template to the VM, add the new disk to the storage cluster, release the old disk from the storage cluster, and delete it from the VM.

  Performance and size of a local VM disk depends on its template. For example, a **STANDARD_DS1** virtual machine has the dedicated bandwidth of 32 MB/s for premium storage disk traffic. In turn, a **P10** premium storage disk can provide the bandwidth of 100 MB/s. If a **P10** premium storage disk is attached to a **STANDARD_DS1** virtual machine, its performance will be capped at 32 MB/s instead of the maximum 100 MB/s it can provide. For more details on premium storage, see **Azure documentation**.

- A separate object container should be used for each Backup Gateway cluster.

- To increase the local storage space for Backup Gateway, add one or more disks to the virtual machine. Do not resize the VM’s existing disks, as it will not be detected by Acronis Cyber Infrastructure.

- Two-factor authentication (2FA) is not supported for Backup Gateway registration in Acronis Cyber Protect Cloud. To register Backup Gateway, mark a user as a service account, as described in the **Acronis Cyber Cloud documentation**, and specify the user credentials during the registration.
Creating Acronis Cyber Infrastructure virtual machine

First, you need to create a VM with Acronis Cyber Infrastructure. Do the following:

1. On the Dashboard, click **Create a resource**.

2. On the Home > Create a resource pane, find and click **Acronis Backup Gateway** in the Azure Marketplace.

3. On the Home > Create a resource > Acronis Backup Gateway pane, click **Create**.

   The VM creation wizard will open.

4. On the **Basics** tab:
a. In **Project details**, select a subscription type and resource group.

![Project details](image)

- **Subscription**: Pay-As-You-Go (Converted to EA)
- **Resource group**: (New) backup_gateway

b. In **Instance details**, select a region, and then specify a user name and password for the VM's admin account. The password must not contain special characters. Then, set the public access policies and specify a password for the Acronis Cyber Infrastructure web panel.

![Instance details](image)

- **Region**: East US
- **User name**: backup_gateway_admin
- **Authentication type**: Password
- **Password**: ************
- **Confirm password**: ************
- **Public SSH access to Acronis Storage node**: Restrict
- **Public access to Acronis Storage management panel**: Restrict
- **Acronis Storage management panel password**: ************
- **Confirm password**: ************

c. **Click Next: Gateway settings.**

5. On the **Gateway settings** tab:

a. In **Virtual machine size**, the recommended VM size, **Standard A4 v2**, should be selected by default.

b. In **Storage account**, create a new account. On the Create storage account pane, specify a name for the account, select **StorageV2 (general purpose V2)** in Account kind, and then click **OK**.
c. In **Storage account container**, specify a name.
d. In **Public IP address**, create a new IP address. On the **Create public IP address** pane, specify a name for the IP address, select **Static** in **Assignment**, and then click **OK**.

e. In **DNS prefix**, specify a DNS prefix for your Backup Gateway, for example, **backupgateway**.
6. On the **Acronis Backup Cloud settings** tab, provide the credentials of your partner account in Acronis Cyber Protect Cloud. The cloud management portal URL, https://cloud.acronis.com, should be specified by default. Click **Next: Review + create**.

**Important**
Make sure that two-factor authentication (2FA) is disabled for your partner account. You can also disable it for a specific user within a 2FA-enabled tenant, as described in **Acronis Cyber Cloud documentation**, and specify the user credentials. You can re-enable 2FA after Backup Gateway is deployed.

7. On the **Review + create** tab, make sure all the options are set correctly, wait until validation passes, and then click **Create**.
8. On the Create pane, read the terms of use and privacy policy, and then click Create.

After the VM is running, log in to the Acronis Cyber Cloud admin panel and check that the new Acronis Cyber Infrastructure is shown in the Locations section (for more details, refer to the Acronis Cyber Cloud documentation). Finally, perform a test backup to the Azure cloud to make sure that everything is working correctly.
Adding space to Acronis Cyber Infrastructure

Before you create new disks, consider the following recommendations for their sizing:

1. If you have a cluster of several nodes, the nodes should be the same size for redundancy reasons. Then, the data will be spread more evenly among them. For more information, refer to "How logical space is calculated" in the Administrator Guide.

2. Having the same-size disks helps distribute the loads more evenly. Inside a cluster, the disk usage is proportional to the disk size. For example, if you have a disk of 10 TB and a disk of 2 TB, a 50% cluster load will use 5 TB and 1 TB, respectively.

3. The disk performance depends on its size. In general, the greater the disk capacity, the higher the performance. However, in particular cases, the throughput of several smaller disks can exceed that of one larger disk. For example, the comparison of Premium SSD sizes in Azure shows that two 1-terabyte disks provide a higher total throughput than one 2-terabyte disk. Therefore, carefully consider your needs and your cloud provider's recommendations.

If you want to increase physical space in your storage cluster, you need to create and attach new data disks. Do not use the resize disk function of Azure on your Acronis Cyber Infrastructure VM, as the file system will not be resized correspondingly. Instead, create a new managed data disk and attach it as described below.

Create and attach a new disk to your Acronis Cyber Infrastructure VM, as outlined in Add a data disk. After that, the added disk will be listed in the node's disks in the admin panel of Acronis Cyber Infrastructure.

**To configure the new disk in the admin panel**

1. On the Infrastructure > Nodes screen, click the name of the node with the created disk. Go to the Disks tab to see all the node disks.

2. Click the disk without a role that you created earlier.

3. On the disk right pane, click Assign role.

4. In the Assign role window, select the Storage role, a storage tier, and enable checksumming, if
required. For more info, refer to "Configuring new disks manually" in the Administrator Guide.

Assign role

Select the role to assign to the disk "sdc"

- **Storage**
  Use the disk to store data.

- **Cache**
  Use the disk to store write cache. This disk does not add capacity to the cluster but improves its performance.

- **Metadata**
  Use the disk to store cluster metadata.

- **Metadata + Cache**
  Use the disk to store both cluster metadata and write cache.

You can also remove the virtual disk from a virtual machine, as described in Detach a data disk using the portal.
Performing additional tasks

Normally, you only need to create and run a VM with Acronis Cyber Infrastructure on Azure to be able to store backups in the Azure cloud. Logging in to Acronis Cyber Infrastructure itself is not required.

If, however, you need to perform some additional tasks that require you to log in to Acronis Cyber Infrastructure, you can access your Azure VM by using the domain name and user credentials specified during VM deployment. You will also need to open a port to the VM.

Note
Acronis Cyber Infrastructure always shows Microsoft Azure disks (even premium SSDs) as HDD, because Hyper-V does not provide information on the disk type.

The tasks related to Backup Gateway that you can perform in Acronis Cyber Infrastructure are described in the following sections of the Backup Gateway Quick Start Guide:

- Connecting to public cloud storage via Backup Gateway
- Changing the redundancy scheme for Backup Gateway
- Monitoring Backup Gateway
- Releasing nodes from Backup Gateway