Acronis Cyber Infrastructure 3.0

Backup Gateway Quick Start Guide for Amazon S3 and EC2

November 26, 2019

Copyright Statement

Copyright ©Acronis International GmbH, 2002-2019. All rights reserved.

"Acronis" and "Acronis Secure Zone" are registered trademarks of Acronis International GmbH.

"Acronis Compute with Confidence", "Acronis Startup Recovery Manager", "Acronis Instant Restore", and the Acronis logo are trademarks of Acronis International GmbH.

Linux is a registered trademark of Linus Torvalds.

VMware and VMware Ready are trademarks and/or registered trademarks of VMware, Inc. in the United States and/or other jurisdictions.

Windows and MS-DOS are registered trademarks of Microsoft Corporation.

All other trademarks and copyrights referred to are the property of their respective owners.

Distribution of substantively modified versions of this document is prohibited without the explicit permission of the copyright holder.

Distribution of this work or derivative work in any standard (paper) book form for commercial purposes is prohibited unless prior permission is obtained from the copyright holder.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Third party code may be provided with the Software and/or Service. The license terms for such third-parties are detailed in the license.txt file located in the root installation directory. You can always find the latest up-to-date list of the third party code and the associated license terms used with the Software and/or Service at http://kb.acronis.com/content/7696.

Acronis patented technologies

Technologies, used in this product, are covered and protected by one or more U.S. Patent Numbers: 7,047,380; 7,246,211; 7,275,139; 7,281,104; 7,318,135; 7,353,355; 7,366,859; 7,383,327; 7,475,282; 7,603,533; 7,636,824; 7,650,473; 7,721,138; 7,779,221; 7,831,789; 7,836,053; 7,886,120; 7,895,403; 7,934,064; 7,937,612; 7,941,510; 7,949,635; 7,953,948; 7,979,690; 8,005,797; 8,051,044; 8,069,320; 8,073,815; 8,074,035; 8,074,276; 8,145,607; 8,180,984; 8,225,133; 8,261,035; 8,296,264; 8,312,259; 8,347,137; 8,484,427; 8,645,748; 8,732,121; 8,850,060; 8,856,927; 8,996,830; 9,213,697; 9,400,886; 9,424,678; 9,436,558; 9,471,441; 9,501,234; and patent pending applications.

Contents

CHAPTER 1

About This Guide

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

Briefly, you will need to do the following:

1. Deploy an instance with Acronis Cyber Infrastructure from an Amazon Machine Image (AMI) on Amazon EC2.
2. Obtain the password and log in to the Acronis Cyber Infrastructure admin panel.
3. Set up Backup Gateway to work with the Amazon cloud.

All these steps are described in the next chapters.

Note: Common tasks related to Backup Gateway are described in the more general *Backup Gateway Quick Start Guide*:

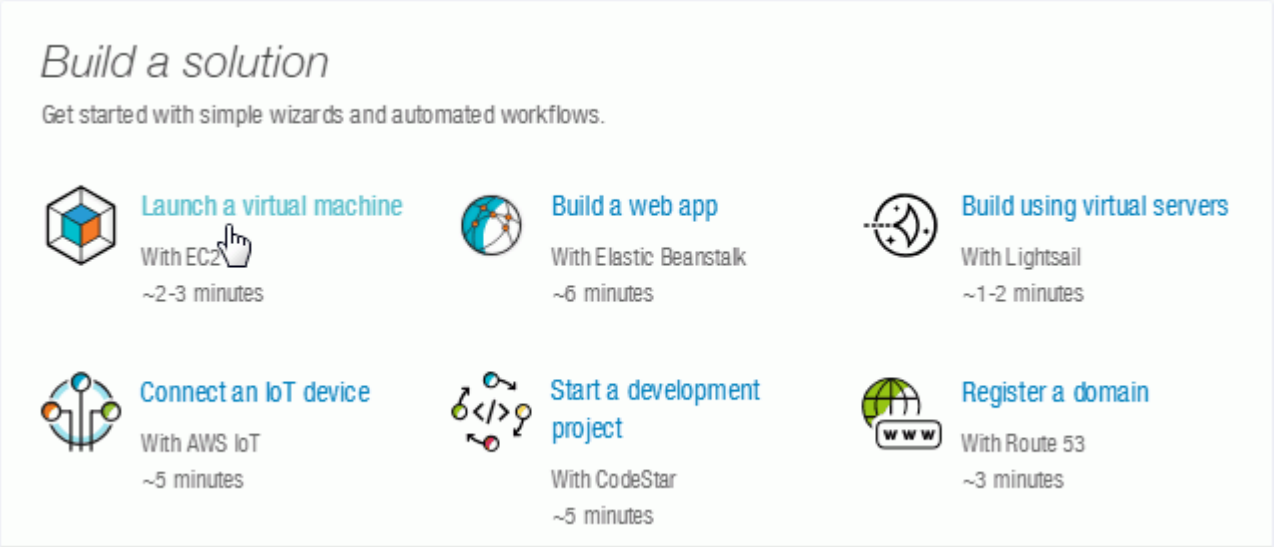
- Connecting to Public Cloud Storage via Backup Gateway
- Migrating Backups from Older Solutions
- Monitoring Backup Gateway
- Releasing Nodes from Backup Gateway

CHAPTER 2

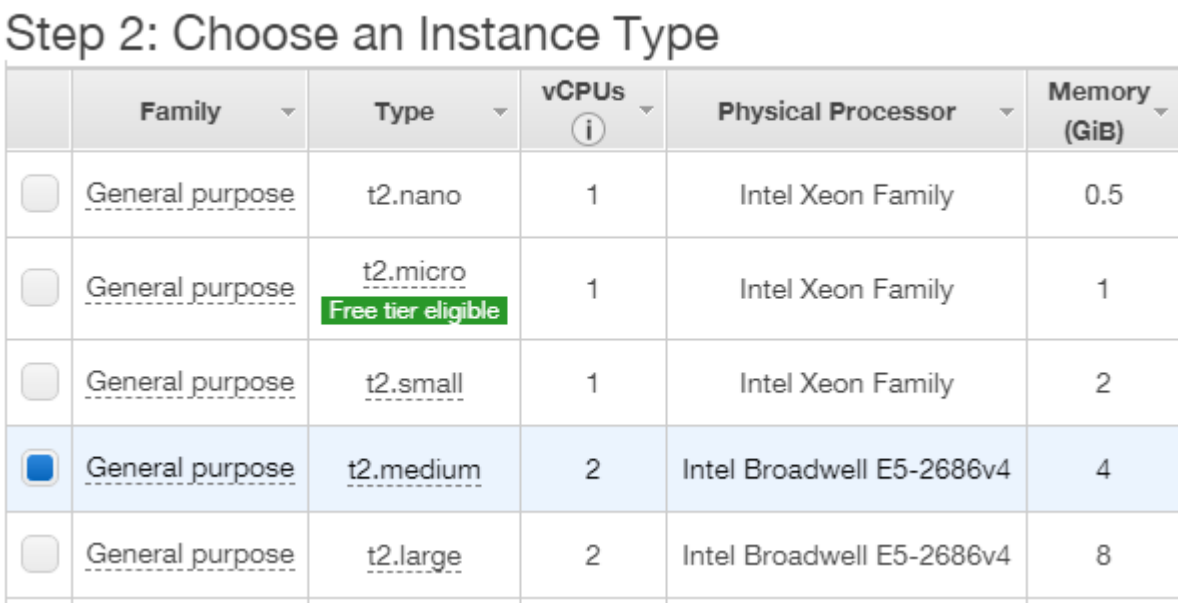
Launching Acronis Cyber Infrastructure Instance

First, you need to create and launch an instance with Acronis Cyber Infrastructure. Do the following:

1. In the AWS Console Home, click **Launch a virtual machine** and search for “Acronis Cyber Infrastructure” on the AWS Marketplace.



2. Click **Select** by the found AMI.
3. On wizard step 2, choose the **t2.medium** type for the instance.



Step 2: Choose an Instance Type

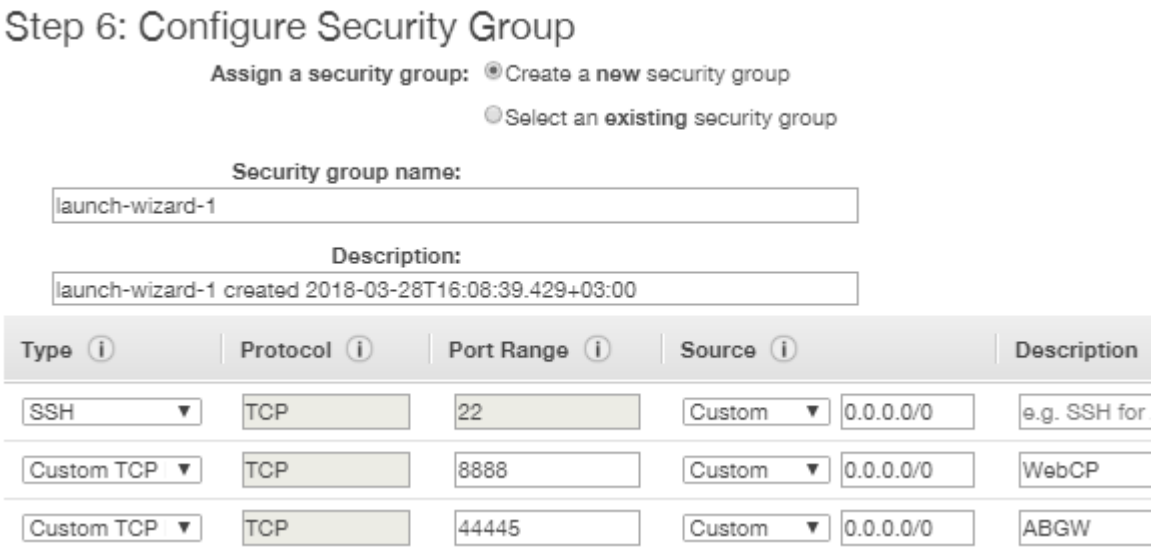
	Family	Type	vCPUs	Physical Processor	Memory (GiB)
☐	General purpose	t2.nano	1	Intel Xeon Family	0.5
☐	General purpose	t2.micro Free tier eligible	1	Intel Xeon Family	1
☐	General purpose	t2.small	1	Intel Xeon Family	2
☑	General purpose	t2.medium	2	Intel Broadwell E5-2686v4	4
☐	General purpose	t2.large	2	Intel Broadwell E5-2686v4	8

4. Wizard steps 3 to 5—**Configure Instance Details**, **Add Storage**, and **Add Tags**—are optional. You can skip them by clicking **NEXT**.

   Make sure, however, that the storage cluster deployed in the instance has plenty of logical space for staging (keeping backups locally before sending them to the cloud). For example, if you perform backups daily, provide enough space for at least 1.5 days' worth of backups. For more details, see the section "Connecting to Public Cloud Storage via Backup Gateway" in the *Administrator's Guide*.

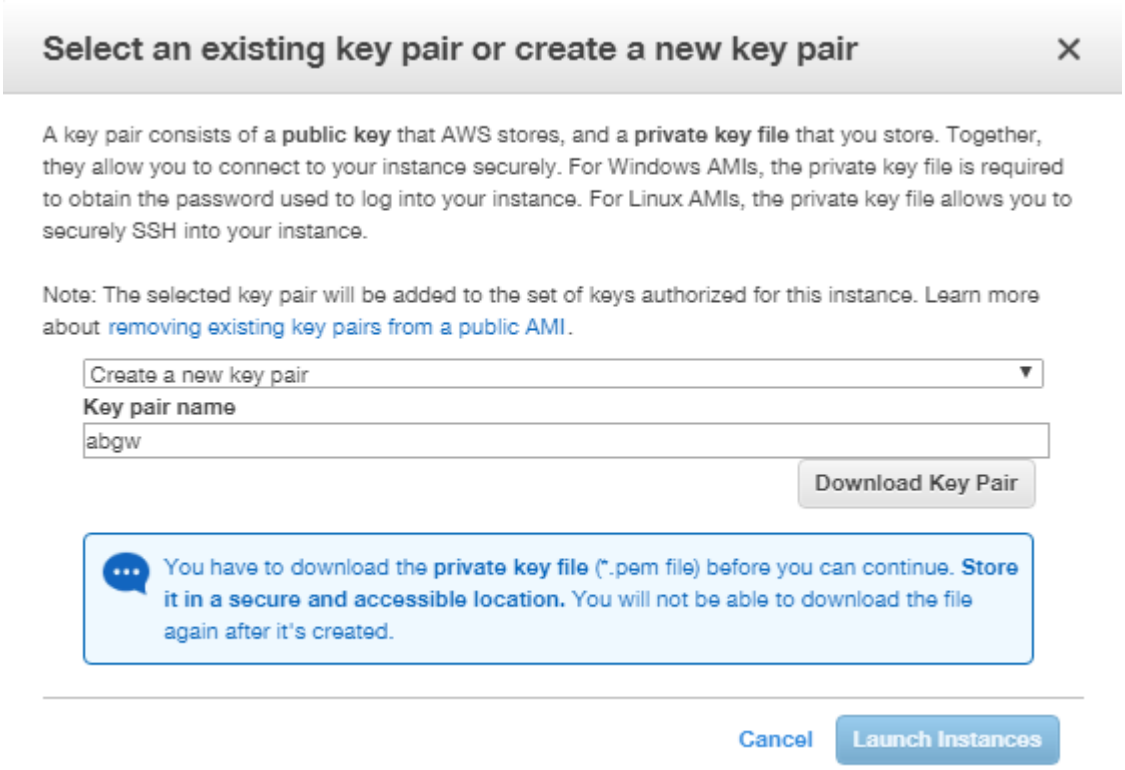
5. On wizard step 6, add two rules to a new security group to open ports 8888 and 44445 in addition to port 22 opened by default. Ports 22 (SSH) and 8888 (admin panel) are required for instance administration and, for safety, must only be open to a narrow IP address range, from which the administrator will access the instance. Port 44445 is needed to receive backup traffic and connect with Cloud Management Console, so it must be open to all IP addresses.

   Having added the rules, click **Review and Launch**



6. On wizard step 7, generate a new key pair to be able to access the instance via SSH. Download the key pair.

Important: Save the key in a safe place: make the key file readable only by you (e.g., `chmod 400 <key_file>` on Linux or Mac) and place it in a directory that only you can access (e.g., `chmod 700 <dir>` on Linux or Mac).



7. Click **Launch Instance**.
8. Associate an elastic IP address with your instance as described in the Amazon AWS documentation. This will make your instance available from the Internet.

Once the instance is running, you can access it by hostname found in instance details. For example: https://ec2-18-197-117-93.eu-central-1.compute.amazonaws.com.

CHAPTER 3

Obtaining Password and Logging in to Acronis Cyber Infrastructure

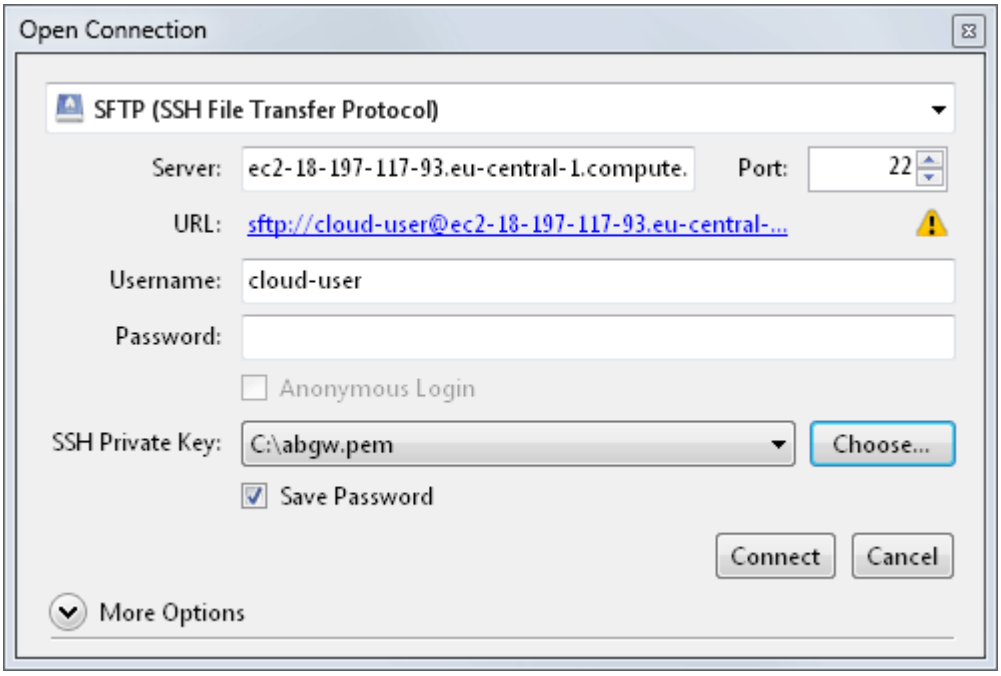
After launching the instance, you need to obtain the default Acronis Cyber Infrastructure admin panel password, which is stored inside the instance in `/.initial-admin-password`.

You can access the instance via SSH, using the previously generated key. For example, on Linux or Mac:

```
# chmod 400 astor-23.pem
# ssh -i astor-23.pem cloud-user@ec2-18-197-117-93.eu-central-1.compute.amazonaws.com
# cat /.initial-admin-password
```

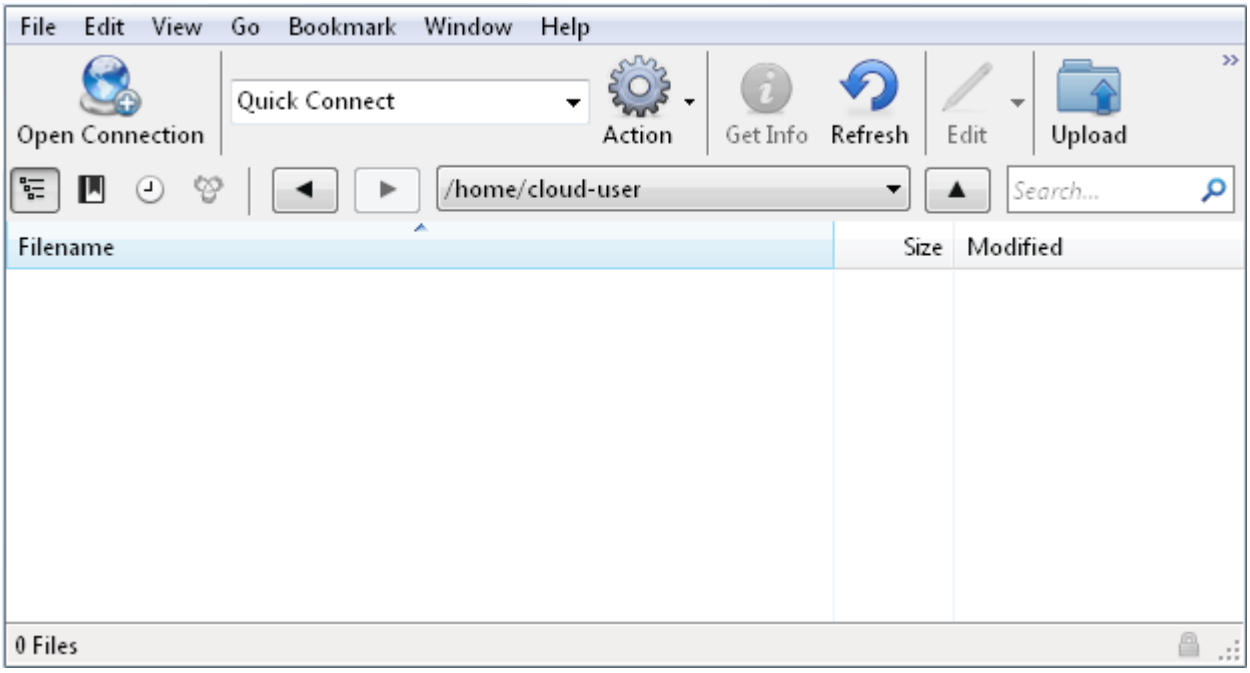
Alternatively, you can access the password file via SFTP. For example, on Windows and Mac, you can use a program like CyberDuck:

1. Click **Open Connection**.
2. Fill out the connection details: select **SFTP** as protocol, paste the instance hostname, enter user name `cloud-user`, and specify the previously generated key.

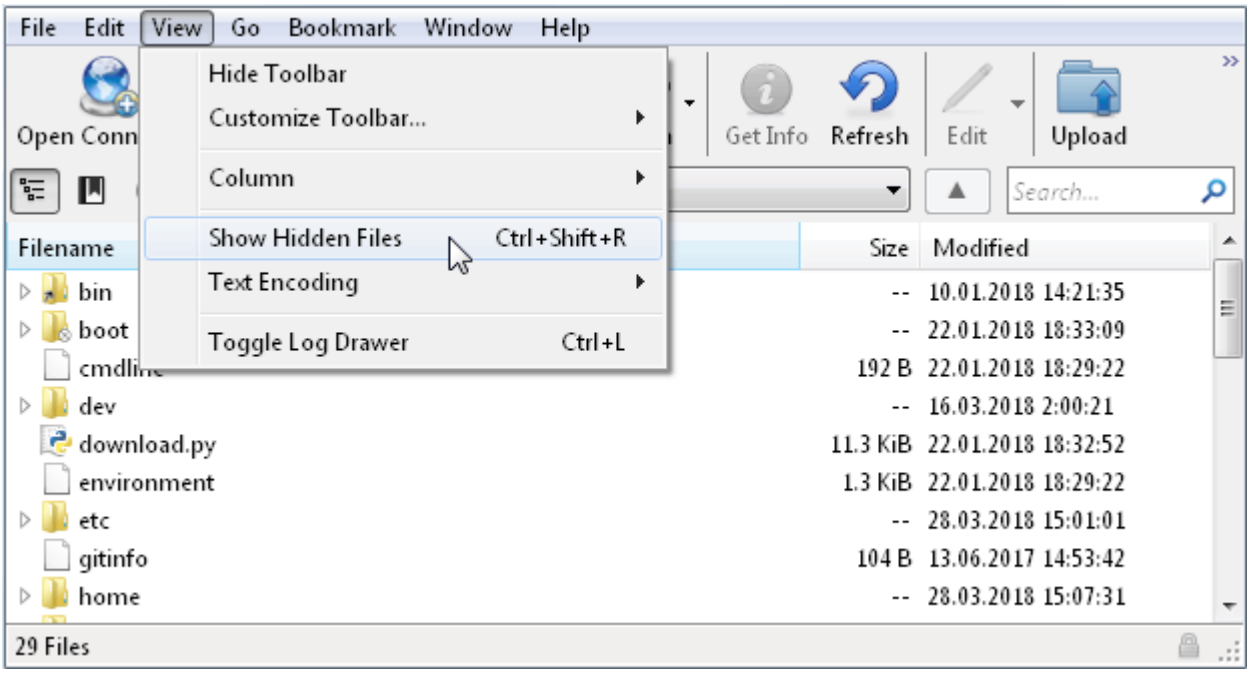


3. Click **Connect** and accept the server fingerprint.

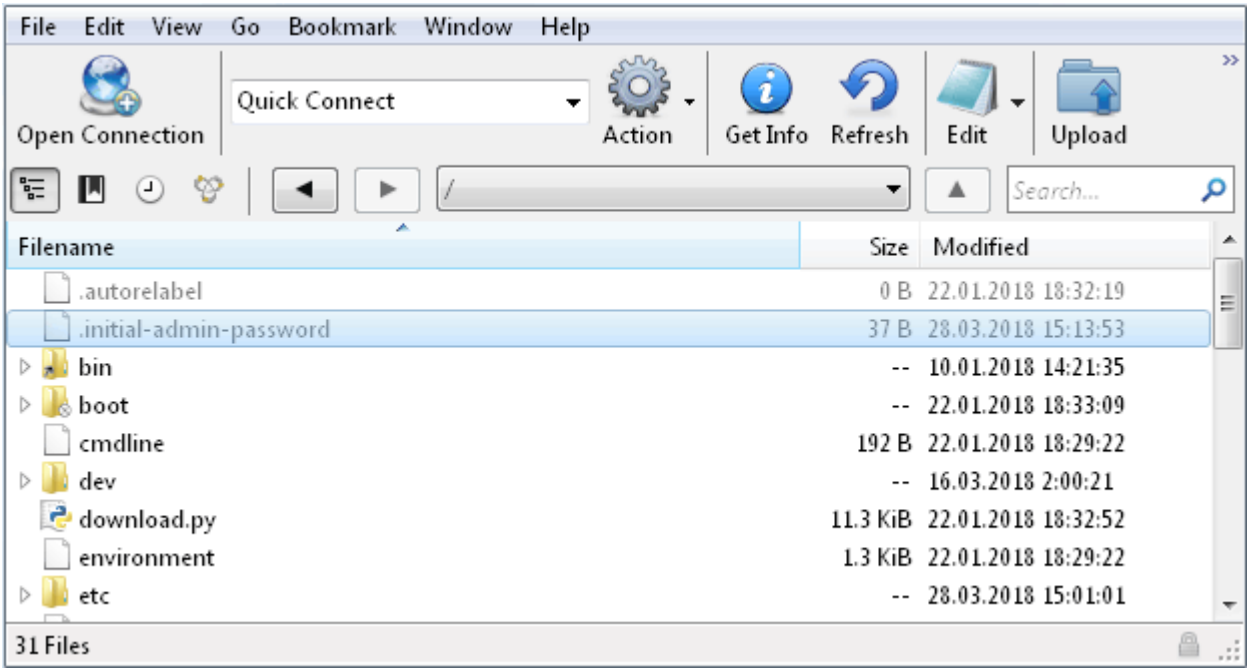
4. Navigate to the home directory, i.e. `/home/cloud-user`.



5. The password file is hidden, so click **View** > **Show Hidden Files** in order to make it visible in the SFTP client.



6. Download and open the password file `.initial-admin-password`.



Using the password, log in to the Acronis Cyber Infrastructure admin panel as `admin` at the instance hostname and port 8888. For example, https://ec2-18-197-117-93.eu-central-1.compute.amazonaws.com:8888/.

Take note of the following:

1. Consider changing the password to one that you will remember and that will be complex enough to

resist a brute-force attack.

2. The instance will be using a self-signed certificate by default, so you will need to either accept it in the web browser or upload a valid certificate issued by a trusted authority.

Normally, the first step after installing Acronis Cyber Infrastructure is to create a storage cluster. This is done automatically, however, when you launch an instance with Acronis Cyber Infrastructure on Amazon EC2, so you can proceed directly to setting up Backup Gateway.

CHAPTER 4

Setting Up Backup Gateway

4.1 Important Requirements and Restrictions

- When working with public clouds, Backup Gateway uses the local storage (inside the VM) as the staging area as well as to keep service information. It means that the data to be uploaded to the cloud is first stored locally and only then sent to the destination. Because of this, you must make sure that the local storage is redundant and permanent. Using temporary disks may result in data loss.
- If you are to store backups in an Amazon S3 cloud, keep in mind that Backup Gateway may sometimes block access to such backups due to the eventual consistency of Amazon S3. It means that Amazon S3 may occasionally return stale data as it needs time to render the most recent version of the data accessible. Backup Gateway detects such delays and protects backup integrity by blocking access until the cloud updates.
- Use a separate object container for each Backup Gateway cluster.

4.2 Creating Backup Gateway

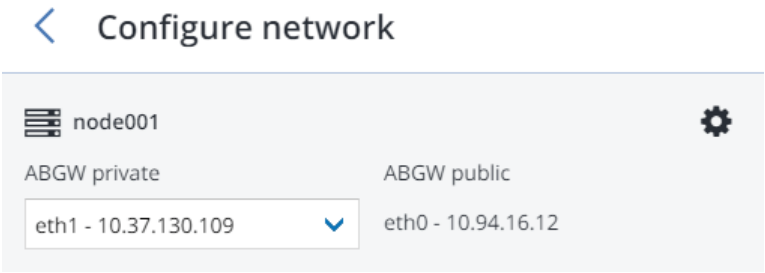
Before you proceed, make sure that the destination storage has enough space for backups.

To set up Backup Gateway, do the following:

1. On the **INFRASTRUCTURE** > **Networks** screen, make sure that the **ABGW private** and **ABGW public** traffic types are added to your networks.
2. In the left menu, click **STORAGE SERVICES** > **Backup storage**.
3. Select the node(s) to run the gateway services on and click **Create gateway** in the right menu.

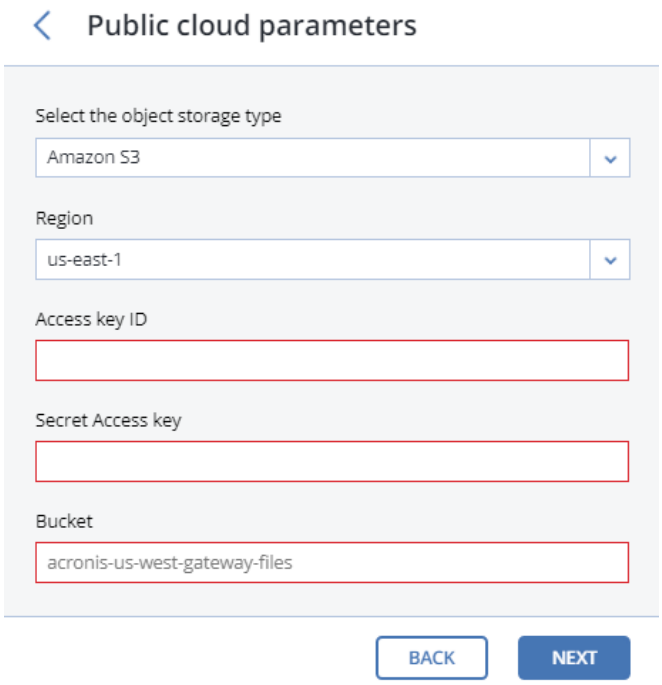
4. Select **Public Cloud** as storage type.
5. Make sure the correct network interface is selected in the drop-down list. Click **NEXT**.

   If necessary, click the cogwheel icon and configure node's network interfaces on the **Network Configuration** screen.

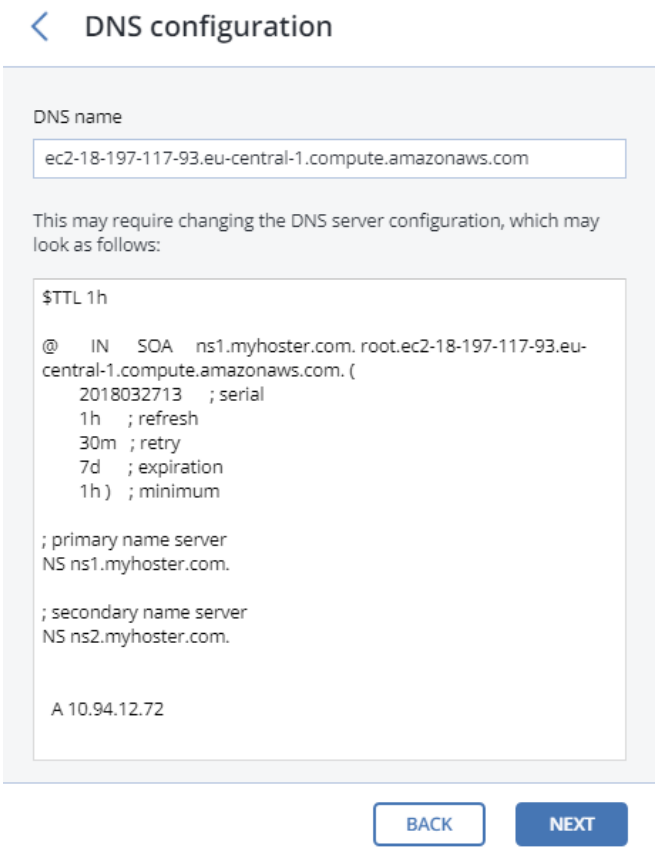


6. On the **Public cloud parameters** pane, select **Amazon S3**, the desired region, and fill out the keys and bucket information.

Important: The specified bucket folder must be writeable.



7. On the **Volume parameters** pane, leave volume parameters as they are.
8. On the **DNS configuration** pane, paste the instance hostname in the **DNS name** field.



9. On the **Register in backup software** pane, specify the following information for your Acronis product:
   - In **Address**, specify the address of the Acronis Backup Cloud management portal (e.g., https://cloud.acronis.com/) or the hostname/IP address and port of the Acronis Backup Advanced management server (e.g., http://192.168.1.2:9877).
   - In **Account**, specify the credentials of a partner account in the cloud or of an organization administrator on the local management server.
10. Finally, click **DONE**.

After setting up the Backup Gateway, log in to Acronis Backup Cloud and perform a test backup to the Amazon cloud to make sure that everything is working correctly.