Acronis

Acronis Storage Gateway

DEPLOYMENT GUIDE

Revision: 2/2/2017

Table of contents

1 Introducing Acronis Storage Gateway

Acronis Storage Gateway is intended for service providers who use Acronis Backup Cloud and want to organize a storage on their premises to store their clients' backed-up data.

Acronis Storage Gateway enables a service provider to easily adjust any supported back-end storage to the Acronis proprietary data format.

Acronis Storage Gateway is distributed as a package for installation on a machine running Linux.

This document explains the basics of Acronis Storage Gateway and describes how to:

- Install Acronis Storage Gateway
- Configure the gateway and a storage backend
- Register the storage in Acronis Backup Cloud

1.1 Supported storage backends

Acronis Storage Gateway supports the following storage backends:

- Local backend: a local directory or a mounted NFS
- A variety of S3 API-compatible storages: Amazon S3, Swisscom, IIJ GIO, Cleversafe
- Microsoft Azure Storage
- OpenStack Swift

The gateway does not provide data redundancy and thus does not create a storage overhead.

The gateway does not perform data deduplication. However, Acronis stores data in a deduplication-friendly format, which means that you can use hardware deduplication or third-party deduplication software. Block-level deduplication with a block size of 4 KB is supported. Encrypted backups cannot be deduplicated.

Consider the following factors when choosing the storage backend:

Factor	Local backend	S3, Azure, OpenStack
Storage space and scalability	Limited by the number of physical disks that can be connected to your storage server. A local disk or a mounted iSCSI target cannot be used in a high-availability configuration. This configuration will be available in future releases.	Easily scalable
Data redundancy	Configure RAID or use EMC NFS storage to ensure high reliability of your storage.	Various redundancy options

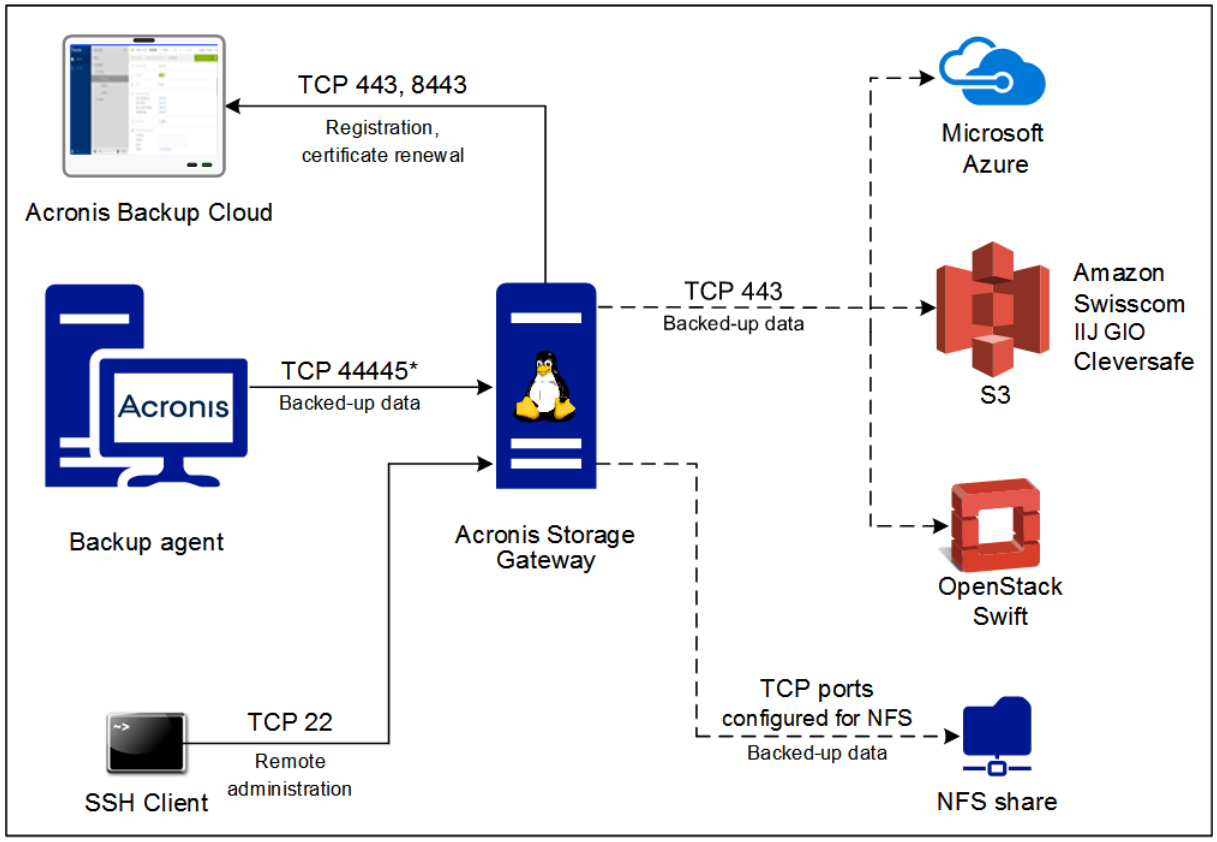
Data deduplication	Use hardware deduplication or deduplication software. For example, you can install Zettabyte File System (ZFS) modules on the machine running Acronis Storage Gateway, store the data in a ZFS storage pool, and enable the ZFS data deduplication.	Data deduplication is not exposed to customers. External deduplication options may be provided by third-parties.

1.2 Architecture and network diagram

Acronis Storage Gateway runs on a single Linux machine. The gateway does not store any data on this machine (except for logs), thus making the machine effectively "stateless." If the machine is virtual, you can take a snapshot and revert the machine to a previous state at any time. If the machine is physical and it goes down, you can easily deploy Acronis Storage Gateway from scratch and connect it to the same backend.

Multiple gateways may use a single Azure/S3/Swift account or a single NFS share, but the corresponding namespaces must not overlap. A gateway service must have exclusive access to all files inside its namespace. This means that you cannot configure multiple gateways for load balancing or high availability. This capability is planned for future releases.

The diagram below illustrates the network connections used by Acronis Storage Gateway. The dotted lines mean that a gateway can have only one backend at a time.



* The port is configurable. The diagram shows the default value.

1.3 System requirements

Hardware requirements

- A physical or virtual machine
- 2-4 (v)CPU
- 4 GB of RAM or more
- 100 GB of free disk space for logs

If you are planning to use an Azure or Amazon S3 backend, we recommend that you install Acronis Storage Gateway on a virtual machine in the corresponding cloud environment (Microsoft Azure or Amazon EC2).

A gateway can serve up to 2 gigabit of user traffic that is usually about 50-100 simultaneous backup sessions with a good speed.

Supported operating systems

Acronis Storage Gateway was tested and proven to work in the following operating systems:

- RHEL 7 x86_64
- CentOS 7 x86_64

2 Installing Acronis Storage Gateway

Acronis Storage Gateway is distributed in the RPM format.

To install Acronis Storage Gateway

1. As the **root** user, execute the following two commands:

```
rpm -i
http://dl.managed-protection.com/u/storage/repos/1.6/CentOS/7/x86_64/acronis-storage-repo-1.6.noarch.rpm

yum install acronis-storage-gateway
```

2. As the **root** user, execute one of the following commands, depending on the storage backend that you are planning to use:
   - Local backend

     ```
     yum install acronis-storage-backend-local
     ```
   - S3 backend

     ```
     yum install acronis-storage-backend-s3
     ```
   - Azure backend

     ```
     yum install acronis-storage-backend-azure
     ```
   - OpenStack Swift backend

     ```
     yum install acronis-storage-backend-swift
     ```

3 Configuring the gateway

After the installation is complete, configure the gateway to use a particular storage backend.

To configure Acronis Storage Gateway

1. Open the file **/etc/Acronis/acronis-storage-gateway.xml** in a text editor.
2. Locate the line **<FesfsPluginPath>...</FesfsPluginPath>**. Depending on the installed backend, specify one of the following values in this line:
   - Local backend
     ```
     /usr/lib/Acronis/acronis-storage-backend-local.so
     ```
   - S3 backend
     ```
     /usr/lib/Acronis/acronis-storage-backend-S3.so
     ```
   - Azure backend
     ```
     /usr/lib/Acronis/acronis-storage-backend-azure.so
     ```
   - OpenStack Swift backend
     ```
     /usr/lib/Acronis/acronis-storage-backend-swift.so
     ```
3. Locate the line **<FesfsParams>...</FesfsParams>**. Depending on the installed backend, specify one of the following values in this line:
   - Local backend

     The path to the directory where the data will be stored, for example **/var/lib/Acronis/storage.** If you use NFS storage, specify the NFS mount point.
   - S3 backend
     ```
     /etc/Acronis/acronis-storage-backend-s3.xml
     ```
   - Azure backend
     ```
     /etc/Acronis/acronis-storage-backend-azure.xml
     ```
   - OpenStack Swift backend
     ```
     /etc/Acronis/acronis-storage-backend-swift.xml
     ```
4. Locate the line **<InternetInterface>...</InternetInterface>**. In this line, specify the public IP address and port of this gateway. Ensure that this port is open for both incoming and outgoing requests through the firewall. Backup agents will use this address and port to upload the backed-up data.

   We recommend that you specify **0.0.0.0:44445** in this line. In this case, Acronis Storage Gateway will listen on all local IP addresses.

   If you change this port at a later time, you must restart, and then re-register (p. 11) Acronis Storage Gateway in Acronis Backup Cloud with the same UID.

4 Configuring the storage backends

4.1 Local backend

The following is a checklist for those who use a local directory or a mounted NFS as a back-end storage.

- If you are going to use a mounted NFS storage, ensure that the NFS share is properly mounted, as described in the following RedHat help article: https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Storage_Administration_Guide/nfs-clientconfig.html

  Important *The* **`local_lock=all`** *mount option must be used.*

- Acronis Storage Gateway creates a Linux user named **`acronis`**. This user must have the read and write permissions for the directory where the data is stored.

  We recommend that you set this directory owner to **`acronis`** by using the **`chown acronis:acronis <directory_path>`** command.

- The user **`acronis`** must be able to traverse the path to the directory where the data is stored.

  For example, if the path is **/var/lib/Acronis/storage**, you can set the permissions for the **var**, **lib**, and **Acronis** directories to **711** by using the **`chmod 711 <directory_name>`** command.

4.2 S3 backend

To configure the S3 backend

1. Open the file **/etc/Acronis/acronis-storage-backend-s3.xml** in a text editor.
2. Locate the line **`<Flavour>...</Flavour>`**. Depending on the S3 API flavour that you want to use, specify one of the following values in this line:
   - Amazon
     ```
     amz
     ```
   - Swisscom
     ```
     swisscom
     ```
   - IIJ GIO
     ```
     iij
     ```
   - Cleversafe
     ```
     cleversafe
     ```
3. Define two POSIX paths inside the S3 namespace that the gateway will use to store file objects and their content: **HomePath** and **ChunkStoragePath**. Ensure that all of the following is true:
   - **ChunkStoragePath** is not a subdirectory of **HomePath**.
   - **HomePath** and **ChunkStoragePath** are globally unique within the entire S3 storage. We recommend that you use name patterns like "/<company>_<department_or_region>_<storage_name>".

     For example, **/acronis-us-west-gateway-files** and **/acronis-us-west-gateway-chunks**
4. Locate and uncomment the line **`<HomePath>...</HomePath>`**. In this line, specify the value for **HomePath**.

5. Locate and uncomment the line **<ChunkStoragePath>...</ChunkStoragePath>**. In this line, specify the value for **ChunkStoragePath**.
6. Locate and uncomment the line **<Account>...</Account>**. In this line, specify your S3 access key ID. This account must have write permissions for the bucket where the data will be stored.
7. Locate and uncomment the line **<AccessKey>...</AccessKey>**. In this line, specify your S3 secret access key.
8. [Only for Amazon] Locate and uncomment the line **<Region>...</Region>**. In this line, specify your S3 region name (for example **us-west-2**). To find out which region you are using, refer to the following Amazon documentation article: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html

4.3 Microsoft Azure backend

To configure the Microsoft Azure backend

1. Open the file **/etc/Acronis/acronis-storage-backend-azure.xml** in a text editor.
2. Locate and uncomment the line **<HomePath>...</HomePath>**. In this line, specify the POSIX path inside your Azure container where the file objects will be stored.

   For example, **<HomePath>/acronis-us-test-gateway-files</HomePath>**

   Note *Due to Azure requirements on container names, HomePath should be at least three characters long.*
3. Locate and uncomment the line **<Account>...</Account>**. In this line, specify your Microsoft Azure account name.
4. Locate and uncomment the line **<AccessKey>...</AccessKey>**. In this line, specify your Microsoft Azure secondary access key.

4.4 OpenStack Swift backend

The OpenStack Swift backend uses the Keystone identity service for locating the resources and authentication. To configure the backend, you must provide the Keystone project name, user name, and password.

To configure the OpenStack Swift backend

1. Open the file **/etc/Acronis/acronis-storage-backend-swift.xml** in a text editor.
2. Locate the line **<Endpoint>...</Endpoint>**. In this line, specify the Keystone identity service URL.

   For example, **https://keystone.example.com:5000/**
3. Locate the line **<ApiVersion>...</ApiVersion>.** In this line, specify one of the following values, depending on the API version used by the Keystone identity service:
   - **v1**
   - **v2**
   - **v3**
4. Locate the line **<UserName>...</UserName>**. In this line, specify your Keystone user name. This account must have write permissions for the container where the data will be stored.
5. Locate the line **<Password>...</Password>**. In this line, specify the Keystone password.
6. Locate the line **<ProjectName>...<ProjectName>**. In this line, specify the Keystone project name.
7. Define two POSIX paths inside the Swift namespace that the gateway will use to store file objects and their content: **HomePath** and **ChunkStoragePath**. Ensure that all of the following is true:

- **ChunkStoragePath** is not a subdirectory of **HomePath**.
- **HomePath** and **ChunkStoragePath** are globally unique within the entire Swift storage. We recommend that you use name patterns like "/<company>_<department_or_region>_<storage_name>".

  For example, **/acronis-us-west-gateway-files** and **/acronis-us-west-gateway-chunks**

8. Locate and uncomment the line **<HomePath>...</HomePath>**. In this line, specify the value for **HomePath**.
9. Locate and uncomment the line **<ChunkStoragePath>...</ChunkStoragePath>**. In this line, specify the value for **ChunkStoragePath**.

5 Registering and starting Acronis Storage Gateway

After the gateway is configured, you need to register it in Acronis Backup Cloud and start the gateway services.

To register the gateway in Acronis Backup Cloud

As the **root** user, execute the following command in any directory:

```
acronis-storage-registration -u USERNAME -p PASSWORD -s HOST -a GATEWAYADDRESS -i "UID"
-o "/etc/pki/tls/certs/Acronis/storage/"
```

- **USERNAME** is the login for your administrator account in Acronis Backup Cloud
- **PASSWORD** is the password for the above account

  If the password contains Linux Bash special characters (for example, **^**, **$**, or **&**), the password must be enclosed in single quotes.

  If the password contains single quote characters ('), they must be properly escaped according to the Linux Bash syntax.
- **HOST** is the address of the Acronis Backup Cloud management console (for example, **baas.acronis.com**)
- **GATEWAYADDRESS** is the public DNS name and port of this gateway, as specified in the gateway configuration (for example, **storage.example.com:44445**)
- **UID** is a unique ID of the storage, as it will appear on the **Storage** tab in Acronis Backup Cloud (for example, **"My Storage 123"**)

To start the gateway

As the **root** user, execute the following commands in any directory:

```
service acronis-storage-mds start
service acronis-storage-gateway start
```

Copyright Statement

Acronis patented technologies

Technologies, used in this product, are covered and protected by one or more U.S. Patent Numbers: 7,047,380; 7,275,139; 7,281,104; 7,318,135; 7,353,355; 7,366,859; 7,475,282; 7,603,533; 7,636,824; 7,650,473; 7,721,138; 7,779,221; 7,831,789; 7,886,120; 7,895,403; 7,934,064; 7,937,612; 7,949,635; 7,953,948; 7,979,690; 8,005,797; 8,051,044; 8,069,320; 8,073,815; 8,074,035; 8,145,607; 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 and patent pending applications.