

Qloud Cover Connection Guide For Azure Blob Storage



Content

Introduction	1
Preparing your Qlik Cloud tenant	2
Prerequisites	2
Step 1: Creating a Qlik Cloud Service Account.....	2
Step 2: Enabling API-Keys on your Qlik Cloud tenant.....	6
Step 3: Generating an API-Key	7
Setting up an Azure Blob Storage Container	10
Setting up your Qlik Cloud connection and Azure Blob Storage in Qloud Cover	17
Prerequisites	17
Qlik Cloud Connection	17
Storage Connection.....	19

Introduction

Welcome to the comprehensive guide for setting up and integrating your Qlik Cloud and Azure Blob Storage with Qloud Cover - the leading backup and restore tool for Qlik Cloud tenants.

The power of Qloud Cover lies in its ability to automate and streamline the often time-consuming task of backing up and restoring your Qlik Cloud data. However, to unleash this power, there are some preliminary setup steps that must be completed. These steps include establishing a secure connection with Qlik Cloud, setting up an Azure Blob Storage account, and finally integrating these two connections within Qloud Cover.

This guide is designed to walk you through each of these steps in detail. We'll start by setting up a secure connection with Qlik Cloud, achieved through the creation of a dedicated Service User Account and the generation of an API key. This setup allows Qloud Cover to communicate seamlessly with your Qlik Cloud environment.

Next, we'll guide you through the process of creating an Azure Blob Storage account and a container, which will serve as the storage location for your Qlik Cloud backups.

Lastly, we'll take you through the steps of integrating these connections in Qloud Cover. This final step is what allows the tool to perform its core functions - backing up and restoring your Qlik Cloud tenants.

The aim of this guide is to provide you with a clear, step-by-step roadmap that you can follow to get your Qloud Cover up and running. Whether you're a seasoned IT professional or a first-time user of Qlik Cloud and Azure, this guide has got you covered.

Preparing your Qlik Cloud tenant

This guide is designed to take you through the steps of creating a service user account and generating an API-Key in Qlik Cloud for use with the Qloud Cover backup and restore tool.

Prerequisites

- A working Qlik Cloud tenant with a valid license.
- A valid Qlik Cloud account with sufficient privileges to create a new user and generate an API key.
- An already-configured Qlik Cloud service user account for your tenant, or a fresh e-mail account for creating a service user account.

Step 1: Creating a Qlik Cloud Service Account

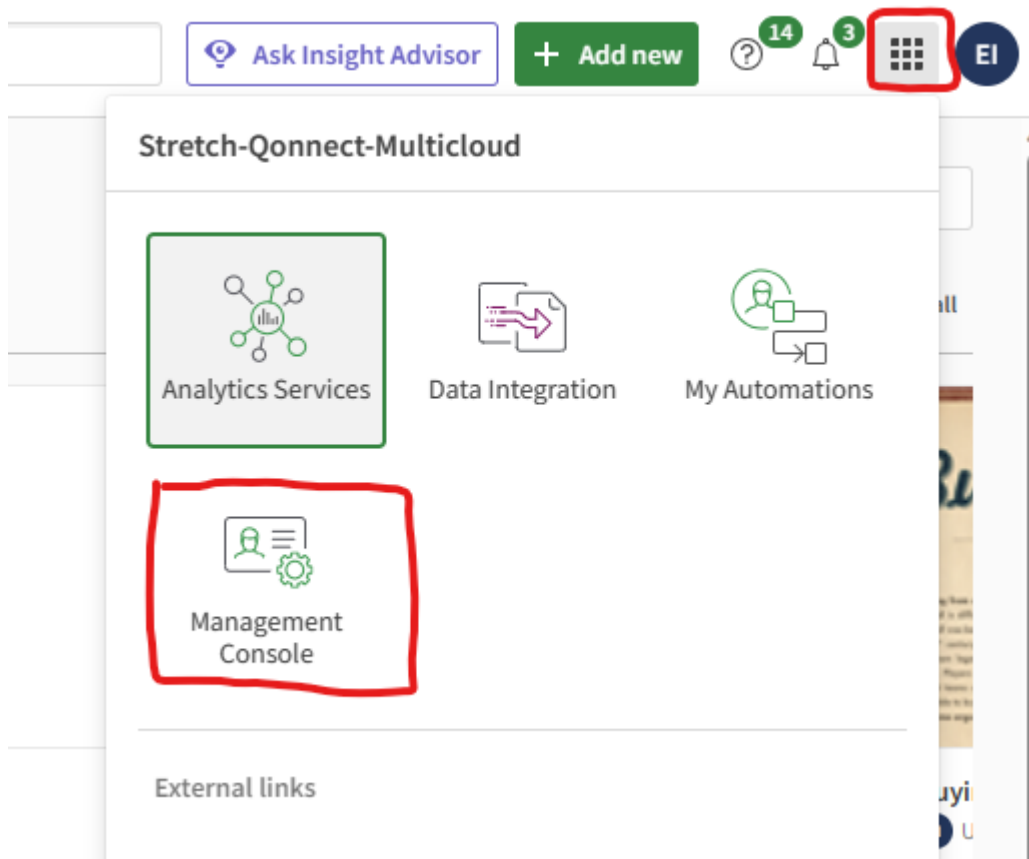
A Service User account is a non-human user account that you can use to interact with your Qlik Cloud environment programmatically. Since Qloud Cover will be doing some permission-heavy tasks, such as exporting apps and creating objects, we recommend creating a specific service user account with the exact permissions needed for this purpose.

Follow the steps below to create a service user account:

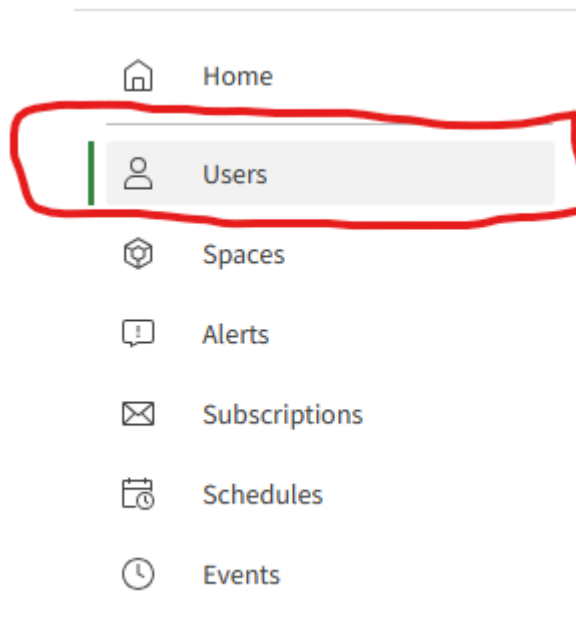
1. **Login to your Qlik Cloud account:** Open your web browser and navigate to your Qlik Cloud tenant. Enter your login credentials to access your account.

Note: If you are using AD to authenticate in your Qlik Cloud tenant, or if you already have a Qlik Cloud service user account that you would wish to use for Qloud Cover, you may skip to step 4 for assigning roles and permissions.

2. **Navigate to the Management Console:** From your Qlik Cloud tenant starting page, locate and click on the icon with nine squares next to your initials in the upper right corner, and select “Management Console”.



3. **Navigate to the Users tab:** In the left-hand menu, click on the *Users* tab.

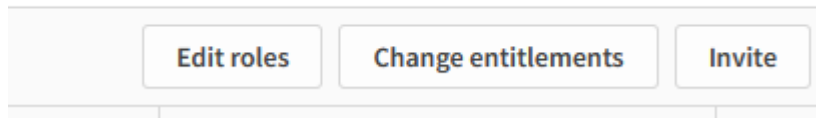


4. **Invite New User:** Click “Invite user” in the right-hand corner. In the pop-up form that appears, fill out the e-mail address for your new service user.

A screenshot of a pop-up form titled "Invite users to 'stretch-qconnect'" with a close button (X) in the top right corner. Below the title is the label "Email addresses" followed by a text input field containing the email address "qloudcoverserviceaccount@yourcompany.com" and a small X icon to its right. At the bottom of the form are three buttons: "Manage invites", "Cancel", and "Invite" (which is highlighted in green).

Note: Make sure to use a unique email address for the service user, as Qlik Cloud does not allow duplicate emails.

5. **Assign Entitlement and Roles to User:** Locate the invited service user in the list of users, and assign them following entitlement and roles:

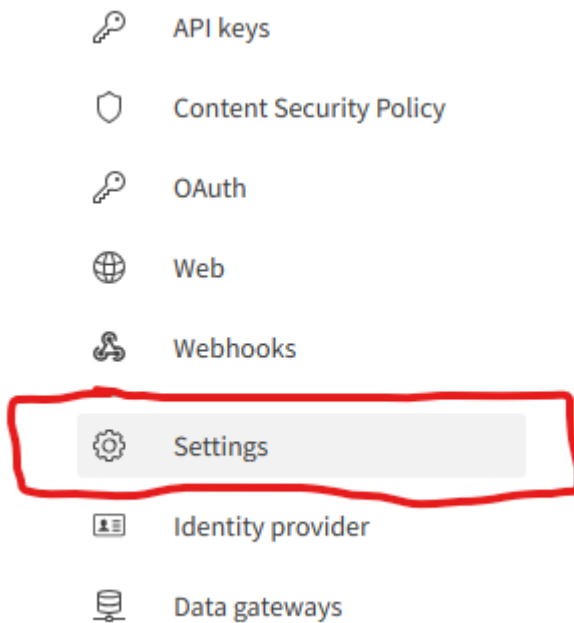


- **Entitlement:** Professional
 - **User Roles:**
 - Data Services Contributor
 - Data Space Creator
 - Developer
 - Managed Space Creator
 - Private Analytics Creator
 - Shared Space Creator
 - **Admin Roles:**
 - Tenant Admin
6. **Save User Account:** After filling all the required details and assigning a role, click on the "Save" button to create the service user account.
 7. **Service User Account Ready:** Your service user account is now ready.

Step 2: Enabling API-Keys on your Qlik Cloud tenant

Before we can generate API-keys, we need to make sure that they are activated on your Qlik Cloud tenant. By default, API-keys might be deactivated, so follow these steps to activate them:

1. **Navigate to the Settings tab.** In the Qlik Management Console (you should still be here from step 1), navigate to the “Settings” tab in left-hand panel.



2. **Enable API-keys:** Scroll down until you see the **API keys** section, and toggle the *Enable API keys* toggle button. Additionally, you may set the *Change maximum token expiration* to a custom number of days. A good recommendation is 9999 days, as seen below. Now, API-keys should be enabled on your tenant!

API keys

Enable API keys
 Enable management and retrieval of API keys.

Generate API keys
 Redirect to API key generation [Generate new](#)

Change maximum token expiration
 Set the maximum value (number of days), for API keys expiration.

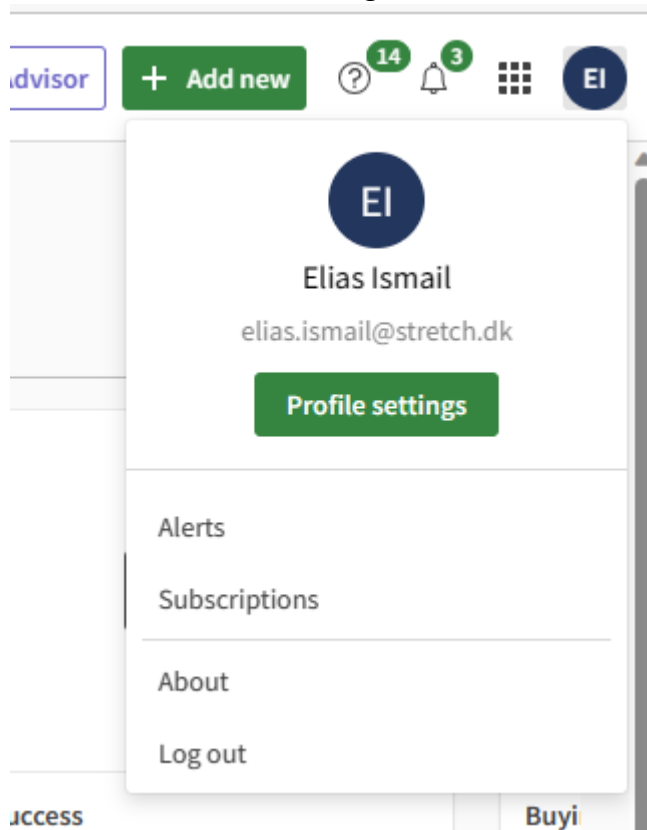
Change maximum of active API keys per user
 Set the maximum number of active API keys per user.

Step 3: Generating an API-Key

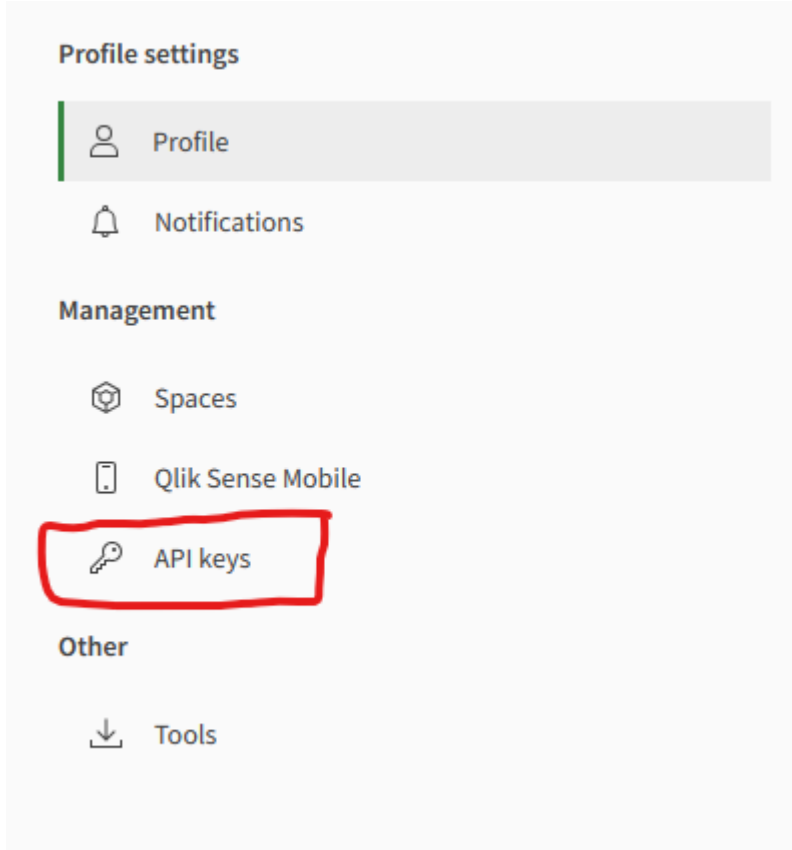
After creating the Service User, and enabling the API-keys on your Qlik Cloud tenant, the next step is generating the API key. This key will enable Qloud Cover to programmatically access the Qlik Cloud, and give Qloud Cover the same permissions as the service user who generated the API key.

Follow the steps below to generate an API key:

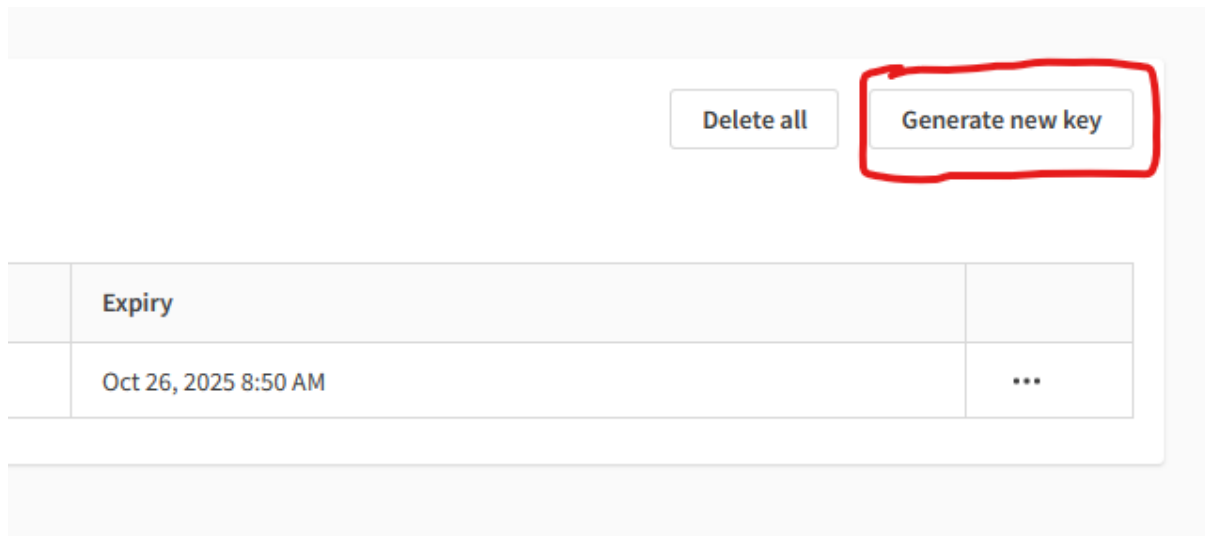
1. **Login with your Service User Account:** Make sure that you are now logged in with the newly generated service account before continuing!
2. **Navigate to Your Profile Settings:** After logging in with the Service User account, locate and click on your account name in the top right corner. From the dropdown menu, select "Profile settings."



- 3. Access the API-Key Section:** In the Profile settings page, locate and select "API Keys."



- 4. Generate a New API-Key:** Click on "Generate new key." In the pop-up form that appears, provide a name for your new API key (such as QloudCover) and select the longest expiration date possible – this is dependent on the input you made in the API key expiration settings earlier in the guide.





Generate new API key



API key description

QloudCover

Expires in

27 years



Cancel

Generate

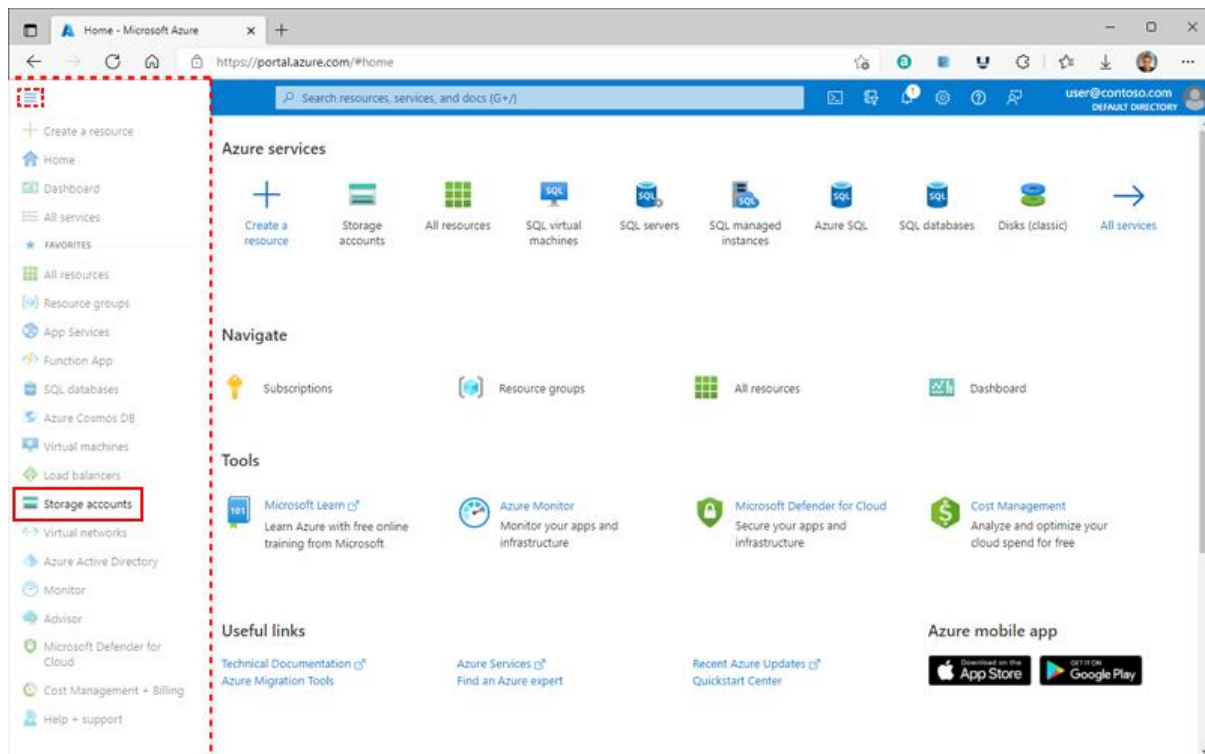
-
- 5. Create the API-Key:** After providing all the necessary details, click on the "Create" button to generate the API-Key.
 - 6. Save Your API-Key:** Your new API key will be displayed only once after creation. Make sure you copy and save it in a safe and secure location.

Setting up an Azure Blob Storage Container

Qloud Cover needs a Cloud Storage account, in order to be able to store the backups of your Qlik Cloud tenant. As of currently, Qloud Cover supports Azure Blob Storage connections.

To create an Azure Blob Storage account with the Azure portal, follow these steps:

1. **Navigate to the Azure Portal:** Navigate to and login with your credentials at <https://portal.azure.com>
2. **Navigate to Storage Accounts:** From the left portal menu, select Storage accounts to display a list of your storage accounts. If the portal menu isn't visible, click the menu button to toggle it on.





3. Create Storage Account: On the Storage accounts page, select Create.

The screenshot shows the Microsoft Azure portal interface for 'Storage accounts'. The page title is 'Storage accounts' and it is under the 'Default Directory'. A red box highlights the '+ Create' button in the top left corner of the main content area. Below the button are various utility icons like 'Manage view', 'Refresh', 'Export to CSV', 'Open query', 'Assign tags', and 'Delete'. There are also filter buttons for 'Subscription == all', 'Resource group == all', and 'Location == all'. A table below shows a list of storage accounts with columns for Name, Type, Kind, Resource group, Location, and Subscription. The table contains three rows of data. At the bottom, there are navigation controls for 'Previous', 'Page 1 of 1', 'Next', and 'Showing 1 to 4 of 4 records'. A 'Give feedback' link is also present.

<input type="checkbox"/>	Name ↑↓	Type ↑↓	Kind ↑↓	Resource group ↑↓	Location ↑↓	Subscription ↑↓
<input type="checkbox"/>	groovystorageaccount	Storage account	StorageV2	myGroovyResourceGroup	West US	My Example Subscription ...
<input type="checkbox"/>	hepcatstorageaccount	Storage account	StorageV2	myGroovyResourceGroup	West US	My Example Subscription ...
<input type="checkbox"/>	righteousstorageacct	Storage account	StorageV2	myResourceGroup	West US	My Example Subscription ...



Create a storage account ...

- Basics**
- Advanced
- Networking
- Data protection
- Encryption
- Tags
- Review

Azure Storage is a Microsoft-managed service providing cloud storage that is highly available, secure, durable, scalable, and redundant. Azure Storage includes Azure Blobs (objects), Azure Data Lake Storage Gen2, Azure Files, Azure Queues, and Azure Tables. The cost of your storage account depends on the usage and the options you choose below. [Learn more about Azure storage accounts](#)

Project details

Select the subscription in which to create the new storage account. Choose a new or existing resource group to organize and manage your storage account together with other resources.

Subscription *

Resource group * [Create new](#)

Instance details

If you need to create a legacy storage account type, please click [here](#).

Storage account name ⓘ *

Region ⓘ * [Deploy to an edge zone](#)

Performance ⓘ * **Standard:** Recommended for most scenarios (general-purpose v2 account)
 Premium: Recommended for scenarios that require low latency.

Redundancy ⓘ *

Make read access to data available in the event of regional unavailability.

4. Choose a subscription
5. Choose the resource group (a new one can be created with a name of your choosing)
6. Give the storage account a relevant name like: **qloudcoverstorageaccount**
7. Choose the region (depends on the region you're in, we suggest **(Europe) North Europe** for Denmark)
8. Choose performance **Standard**
9. Choose redundancy (choice is up to you, but we recommend): **Geo-Redundant storage (GRS)**



10. Click **Next : Advanced >**

Review

< Previous

Next : Advanced >

11. Keep everything default except for under the step **Blob Storage**, select **Cool** as the access tier:

Basics Advanced Networking Data protection Encryption Tags Review

ⓘ Certain options have been disabled by default due to the combination of storage account performance, redundancy, and region.

Security

Configure security settings that impact your storage account.

Require secure transfer for REST API operations ⓘ

Allow enabling public access on individual containers ⓘ

Enable storage account key access ⓘ

Default to Azure Active Directory authorization in the Azure portal ⓘ

Minimum TLS version ⓘ

Permitted scope for copy operations (preview) ⓘ

Hierarchical Namespace

Hierarchical namespace, complemented by Data Lake Storage Gen2 endpoint, enables file and directory semantics, accelerates big data analytics workloads, and enables access control lists (ACLs) [Learn more](#)

Enable hierarchical namespace

Access protocols

Blob and Data Lake Gen2 endpoints are provisioned by default [Learn more](#)

Enable SFTP ⓘ

ⓘ To enable SFTP, 'hierarchical namespace' must be enabled.

Enable network file system v3 ⓘ

ⓘ To enable NFS v3 'hierarchical namespace' must be enabled. [Learn more about NFS v3](#)

Blob storage

Allow cross-tenant replication ⓘ



Access tier ⓘ



Hot: Frequently accessed data and day-to-day usage scenarios



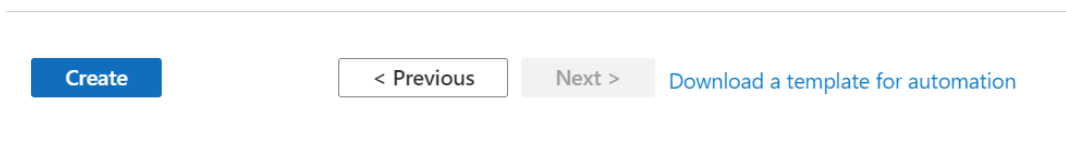
Cool: Infrequently accessed data and backup scenarios

Azure Files

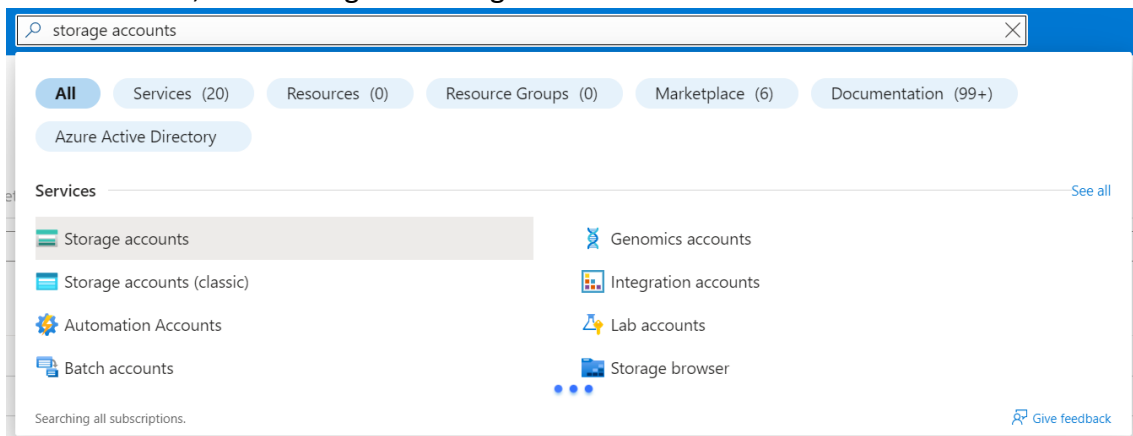
Enable large file shares ⓘ



12. The next steps should also be kept default, click on **Review** on the top menu bar and click **Create**

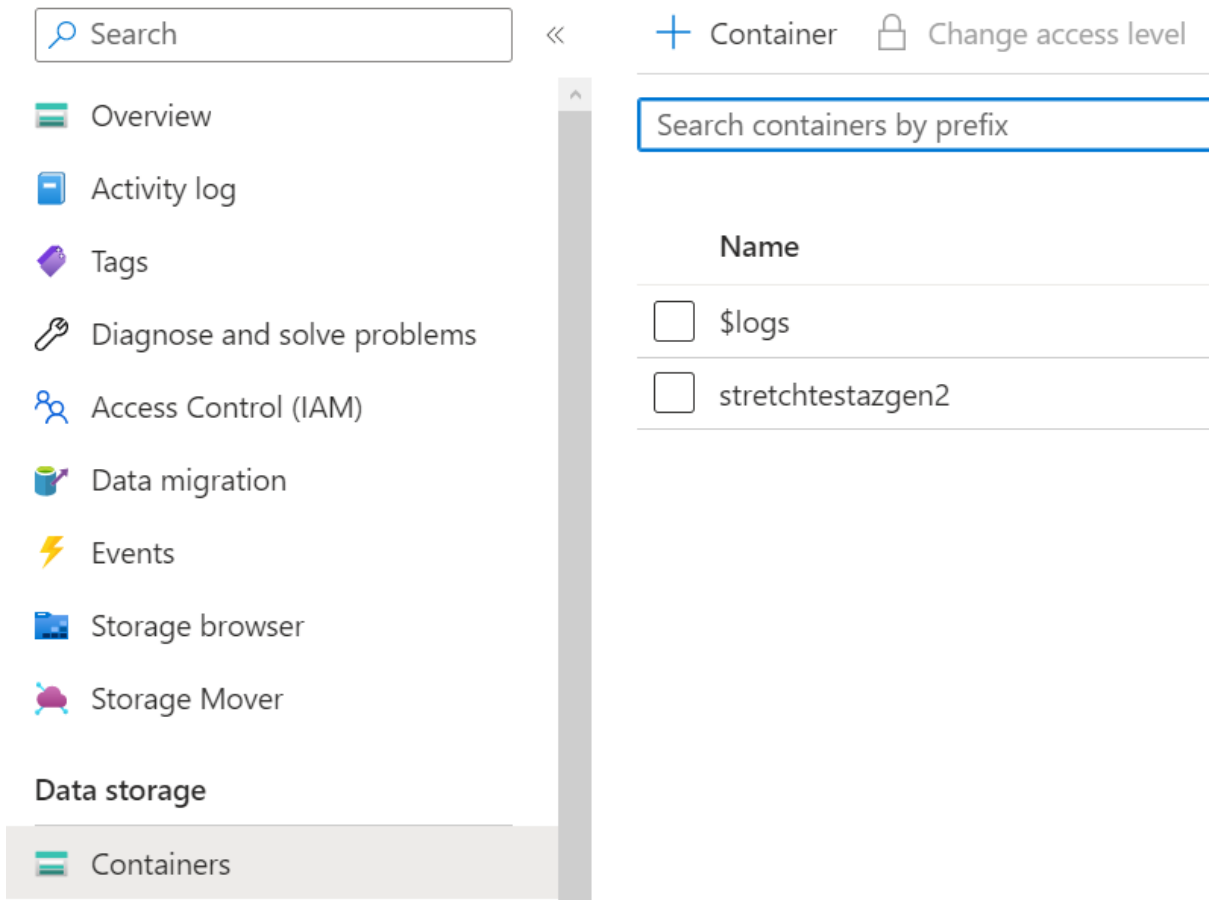


13. Next, find the newly created storage account by searching for “storage accounts” in the search bar, and clicking on “Storage accounts” under the **Services** tab.

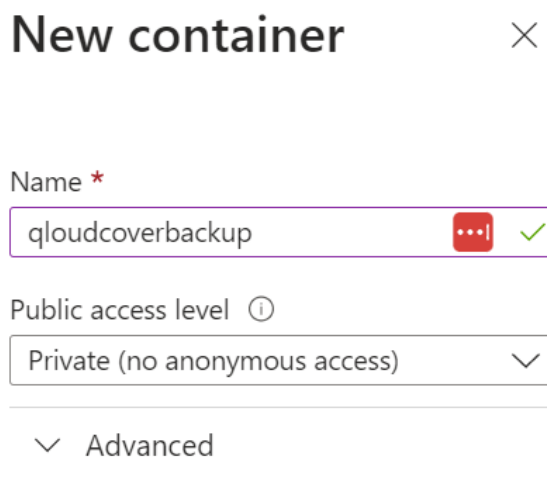


14. Within the storage account, click on **Containers**

15. Click on the + **Container** icon, to create a new Container.



16. Give the container a name, like **qloudcoverbackup**. Keep the Public access level to **Private (no anonymous access)**, unless otherwise needed.



17. You have now successfully created a storage account, as well as a container. For the last step, navigate to the storage account panel, and click on the **Access keys** tab in the left-hand panel.



Home > qloudcoverstorageaccount

qloudcoverstorageaccount | Access keys

Storage account

Search

Set rotation reminder Refresh Give feedback

Access keys authenticate your applications' requests to this storage account. Keep your keys in a secure location like Azure Key Vault, and replace them often with new keys. The two keys allow you to replace one while still using the other.

Remember to update the keys with any Azure resources and apps that use this storage account. [Learn more about managing storage account access keys](#)

Storage account name: qloudcoverstorageaccount

key1 Rotate key
Last rotated: 6/13/2023 (0 days ago)
Key: [Redacted] **Show**
Connection string: [Redacted] **Show**

key2 Rotate key
Last rotated: 6/13/2023 (0 days ago)
Key: [Redacted] **Show**
Connection string: [Redacted] **Show**

- Overview
- Activity log
- Tags
- Diagnose and solve problems
- Access Control (IAM)
- Data migration
- Events
- Storage browser
- Storage Mover
- Data storage
 - Containers
 - File shares
 - Queues
 - Tables
- Security + networking
 - Networking
 - Azure CDN
 - Access keys**
 - Shared access signature
 - Encryption
 - Microsoft Defender for Cloud

- Under the **key1** section, click the **Show** button next to the *Connection String* box, and copy the connection string. This string will be used in the next step, in which the connections are created in Qloud Cover.

Setting up your Qlik Cloud connection and Azure Blob Storage in Qloud Cover

The final step of this guide is to use the generated API-key and Azure Blob Storage Account details, to create connections within the Qloud Cover application, such that the mapping between your Qlik Cloud tenant and Storage account can be created.

Prerequisites

- A valid Qlik Cloud API-key
- A valid Azure Blob Storage Connection String
- A valid Azure Blob Storage Container Name

Qlik Cloud Connection

1. **Navigate to Qloud Cover:** Access the Qloud Cover web application using a browser at <https://demo.qcloudcover.com>
2. **Navigate to the Connections tab:** In the left-hand side panel, click the **Connections** tab.
3. **Create a Qlik Cloud connection:** Click the “+ Create New” button, above the **Qlik Cloud Connections** table

Qlik Cloud Connections + Create New

Name	URL	Actions
Stretch Qconnect - Qlik Cloud	https://stretch-qconnect.eu.qlikcloud.com	Edit Delete
Stretch Qconnect - Qlik Multicloud	https://stretch-qconnect-multicloud.eu.qlikcloud.com	Edit Delete

4. **Input the Qlik Cloud connection details:** Three different inputs are needed:
 - **Connection Name:** This name will serve as a reference to the connection in Qloud Cover only, such that you can use it in later steps.
 - **Tenant URL:** This is the URL to your Qlik Cloud tenant, e.g. <https://stretch-qconnect.eu.qlikcloud.com>.
 - **API Key:** This is the API-key that you generated in the previous step. Simply paste it here.

Add Qlik Cloud Connection Go back to list

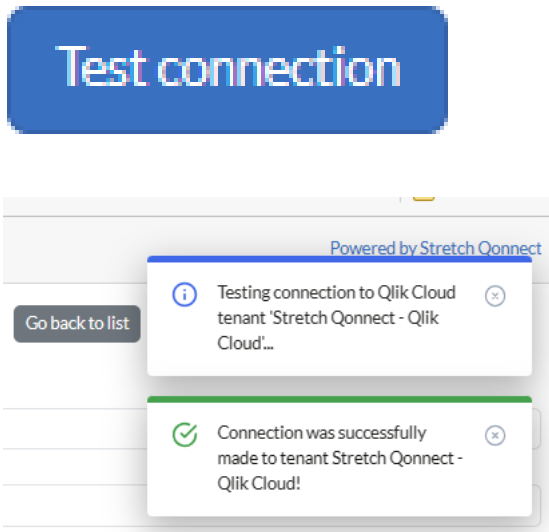
Connection Name

Tenant URL (<https://tenant.region.qlikcloud.com>)

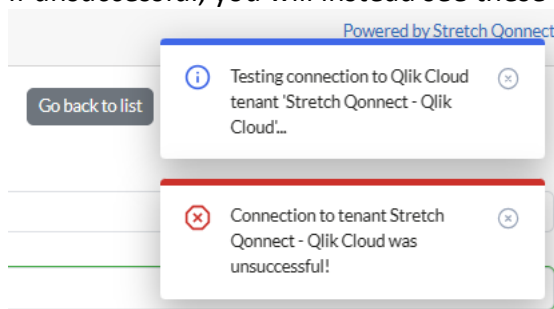
API Key ([Qlik Guide](#))

[Create connection](#) [Test connection](#)

5. **Test Connection:** When you have filled out the details, click the **Test connection** button to check the validity of the connection, so that Qloud Cover can access your tenant. If filled out correctly, you should see the following toast messages:

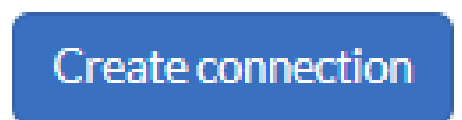


If unsuccessful, you will instead see these toast messages:



If this is the case, make sure that you have correctly input your Qlik Cloud tenant URL, and that the input API-key is valid and is generated on the same Qlik Cloud tenant.

6. **Create Connection:** If the connection was successful, click on the **Create Connection** to create the connection. This will take you back to the Connection Overview, in which you should now see your newly created connection.



Storage Connection

1. **Navigate to Qloud Cover:** Access the Qloud Cover web application using a browser at <https://demo.qcloudcover.com>
2. **Navigate to the Connections tab:** In the left-hand side panel, click the **Connections** tab.
3. **Create a Storage connection:** Click the “+ Create New” button, above the **Storage Connections** table

Storage Connections

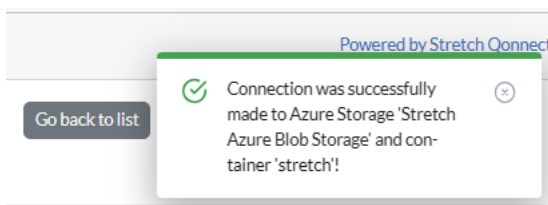


Name	Type	Actions
Stretch Azure Blob Storage	AzureStorage	Edit Delete
QcloudCoverStorageAccount	AzureStorage	Edit Delete

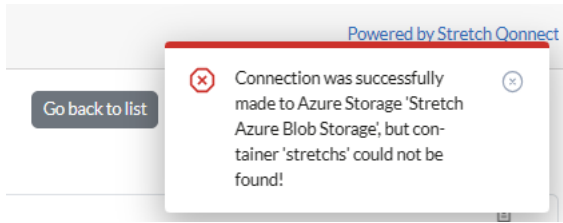
4. **Input the Azure Blob Storage connection details:** Three different inputs are needed:
 - **Azure Storage Name:** This name will serve as a reference to the Azure Blob Storage in Qloud Cover only, such that you can use it in later steps.
 - **Blob Connection String:** This is the connection string to your Azure Blob Storage, that you copied from the previous steps. It should be on the form “DefaultEndpointsProtocol=https;...”
 - **Blob Container Name:** This is the name of the Azure Blob Storage Container that you generated in the previous steps. If you followed the naming convention of this guide, the name will be **qloudcoverbackup**.
5. **Test Connection:** When you have filled out the details, click the **Test connection** button to check the validity of the connection, so that Qloud Cover can access your tenant.



If filled out correctly, you should see the following toast message:



If unsuccessful, you will instead see the following toast message:



If this is the case, make sure that you have correctly input your Azure Blob Storage account connection string, and that the container name is valid.

6. **Create Connection:** If the connection was successful, click on the **Create Connection** to create the connection. This will take you back to the Connection Overview, in which you should now see your newly created connection.

