IBM COS FA Gateway

SETUP GUIDE FOR KVM/OPENSTACK

This edition applies to IBM COS FA Gateway Setup and is valid until replaced by new editions.

CONTENTS

CHAPTER 1. THE IBM COS FA GATEWAY

IBM Cloud Object Storage File Access (COS FA) is a software defined offering that provides SMB and NFS protocol interfaces to applications to store, archive and retrieve infrequently accessed files on IBM Cloud Object Storage.

The IBM COS FA Solution includes the following components:

- IBM COS FA Portal
- IBM COS FA Gateway

The IBM COS FA Portal is the management component of the offering, which enables the creation, delivery and management of the services mentioned below. The IBM COS FA Portal interacts with the IBM COS FA Gateways and efficiently handles file data exchange between these applications and users and the private/public IBM Cloud Object Storage side. A centralized management console makes it possible to effectively manage a very large number of connected IBM COS FA Gateways.

The IBM COS FA Gateway is the component that the application and other data sources are connected to, and allows LAN speed writes via SMB and NFS protocols, and is in charge of onboarding the data to IBM Cloud Object Storage instantly and seamlessly.

The IBM COS FA Gateway works in caching mode, which means that it has a dedicated local disk space to allow local LAN speed ingestion. The main storage is on the IBM COS FA Portal in the cloud with stubs saved on the IBM COS FA Gateway. A stub is a file with a tiny footprint that contains the metadata about the file, such as the file name, size, and modification date. Only the folder and file metadata and not the actual file content is saved locally. This results in the cost of storage being significantly lower. Also, systems with many file changes, where only some of the files are required locally, don't over use bandwidth between the cloud and IBM COS FA Gateway. Only the required files are passed across the wire.

When a user accesses a file stub, the file is opened without delay, where possible by streaming the file content from the cloud. After the download has completed, the file is *unstubbed*. Any changes to the file are synced back to the IBM COS FA Portal. Folders that are always required can be pinned, in which case the files in the folders, and not the stubs, are stored on the IBM COS FA Gateway.

IBM COS FA Gateways are virtual appliances, which can be installed on any customer provided ESXi, Hyper-V, or KVM/OpenStack environment.

The IBM COS FA Portal was designed to scale from tens to hundreds and thousands of connected IBM COS FA Gateways and to support an easy to scale file system with PBs of data and more. The IBM COS FA Portal it is capable of supporting both *scale-up* and *scale-out* deployment schemes: administrators may deploy the IBM COS FA Portal software on increasingly more powerful compute platforms, thus scaling the deployment up. Alternatively, they can distribute the IBM COS FA Portal processes on multiple concurrent compute platforms, thus scaling the deployment out. In addition, the file system is fully scalable by enlarging the database to accommodate data capacity growth.

TECHNICAL SPECIFICATIONS

Port Requirements

- Firewall ports opened to clients.

Port	Protocol	Direction	Notes
443	TCP	Inbound and Outbound	HTTPS

- Firewall ports opened to the IBM COS FA Portal.

Port	Protocol	Direction	Notes
443	TCP	Inbound and Outbound	HTTPS
995	TCP	outbound	CTTP. Communications with IBM COS FA Gateways.

- Firewall ports opened for Active Directory:

Port	Protocol	Direction	Notes
389	TCP/UDP	Outbound	LDAP protocol
445	TCP	Outbound	SMB when joining to a domain as a Computer account
3268	TCP	Outbound	LDAP GC (Global Catalog) protocol

- Firewall ports opened for antivirus updates:

Port	Protocol	Direction	Notes
80	TCP	Outbound	HTTP

Warning: **IBM COS FA Gateways operate behind a firewall, and it is important to leave all other ports closed.**

Browser Requirements

The latest two releases of Google Chrome, Apple Safari, Mozilla Firefox, and Microsoft Edge.

Software Features

Feature	Description
Supported File Sharing Protocols	SMB 2.x/3.x (Windows File Sharing), NFS, WebDAV
Monitoring	SNMP

Cloud Service Features

Feature	Description
Protocol Security	TLS (Transport Level Security).
Efficiency	Incremental updates, data compression, block level deduplication, simultaneous synchronization.

Feature	Description
Versioning	Retention of previous file versions on the IBM COS FA Portal.
Additional Services	Centralized management, centralized monitoring, Cloud Drive caching and synchronization, reporting, logging, remote access.

CHAPTER 2. IBM COS FA GATEWAY PLANNING

During the planning stage for your IBM COS FA Gateway contact IBM COS FA Gateway support regardless of whether the installation is a new installation or an upgrade from an existing installation.

End users who are familiar with a given folder structure and shares, as well as a given permission scheme, while using the Windows file server, continue to see the same folder structure, shares, and permission scheme after migration to the IBM COS FA Gateway. This enables the migration from a current Windows Server-based file system to a IBM COS FA Gateway, without the need to apply any structural changes such as flattening the folder structure or simplifying the permissions scheme.

File and folder access continue to be available following the migration in the same way they were in the Windows Server-based file system. Access after the migration is through the SMB provided by the IBM COS FA Gateway. Users continue to access the files and folders through standard Windows client computers; for example, using Windows Explorer.

The following file server features are fully supported by IBM COS FA Gateway and are copied to IBM COS FA Gateway as part of the migration:

- ACL files/folder share permissions.
- Nested sharing.
- ACL emulation to allow files and folders management via standard SMB protocol using Windows Explorer.
- Shares can be mounted to users via standard administrator tools:
  - DFS Management
  - Group Policy (GPO)
  - Other tools based on Net use

In this chapter

PLANNING A MIGRATION FROM AN EXISTING FILE SERVER

When Planning the migration from a Windows or NetApp file server, IBM COS FA Gateway recommends creating a spreadsheet with the following data:

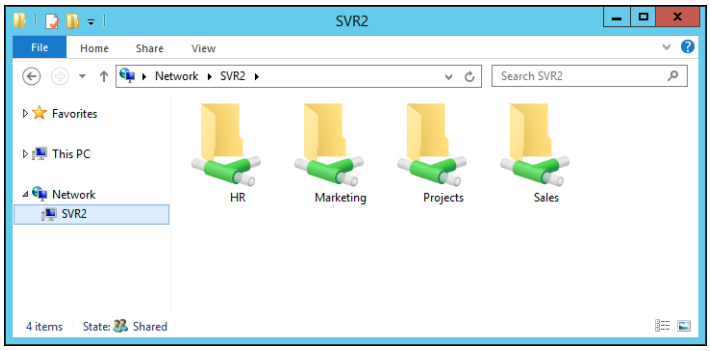
- Shares Names – The names of each share to migrate along with the following information:
  - Folders/Paths
  - Size
  - Number of Files
  - Average file size
- Shares security ACL – Enabled in the IBM COS FA Portal when defining each folder.

In addition, configure the file server to limit deduplication levels to 128TB or 128,000,000 files. IBM COS FA Gateway recommends setting the deduplication levels for the cloud drive in the IBM COS FA Portal settings, under **Default Settings for New User** to **Folder** and a folder group for each of the user account's devices, containing all of the device's cloud drive folders. Deduplication is performed separately for each of the user account's folder groups.

SHARE ARCHITECTURE

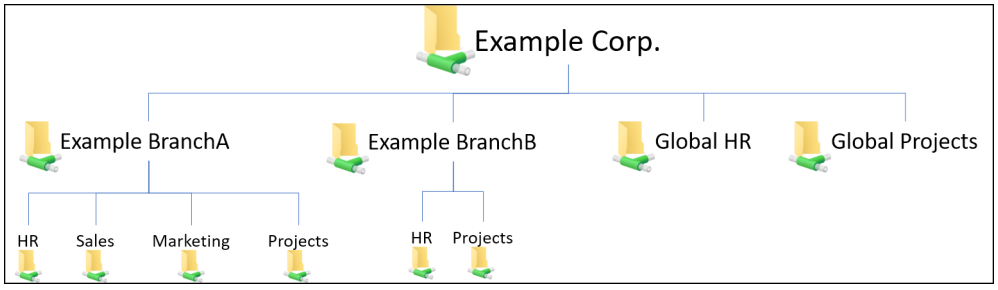
The proposed architecture assumes you want to keep the same shares configuration as in the original file server. For this share configuration, you map all the users to the top root of the Windows servers and all the shares are configured with team-based permissions.

For example, the following team folders exist on a Windows server named SRV2:

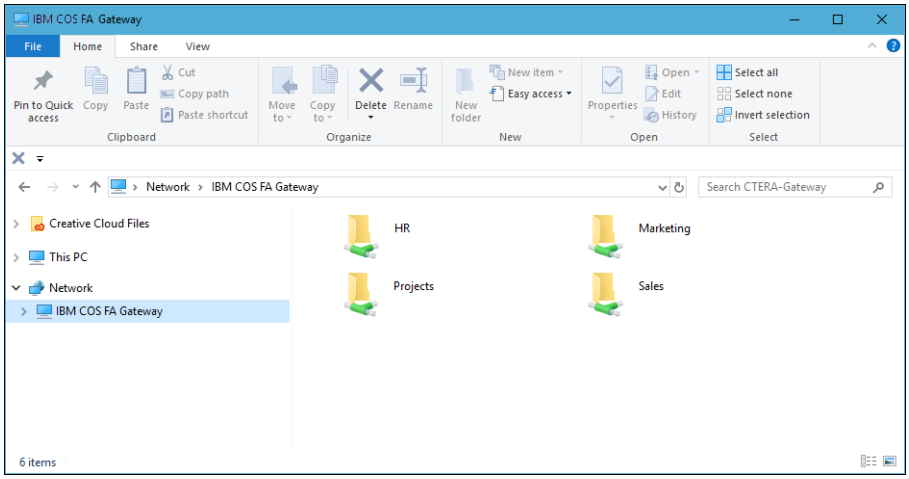


You create the corresponding folders in the IBM COS FA Portal and enable Windows ACLs and set the collaboration required for each folder and then sync them down to the IBM COS FA Gateway. Once the folders are synced to the IBM COS FA Gateway you need to create the shares pointing to these folders via the IBM COS FA Gateway user interface. The folder structure is critical to a smooth migration.

For example, where appropriate, IBM COS FA Gateway recommends creating site or company cloud folders. For example, if the migrated data will be used at multiple company sites, with similar share structures at each site, you should create a corporate cloud folder with all the folders that will be shared by all the sites underneath it and in addition have a site folder per site containing all the share folders for the site.



With this structure, you can edit the ACLs for each folder at the top level of the share and if you use a central IBM COS FA Gateway for failover or performing restores, it is clear which dataset you are working with.The view from Windows Explorer on the IBM COS FA Gateway will match the view from the original server.


IBM COS FA Gateway
File
Home
Share
View
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
Organize
New folder
New item
Easy access
New
Properties
Open
Edit
History
Open
Select all
Select none
Invert selection
Select
Network
IBM COS FA Gateway
Search CTERA-Gateway
Creative Cloud Files
This PC
Network
IBM COS FA Gateway
HR
Marketing
Projects
Sales
6 items

CHAPTER 3. INSTALLING THE IBM COS FA GATEWAY IN A KVM ENVIRONMENT

You can install a IBM COS FA Gateway on KVM via the OpenStack console or another console. The following instructions describe how to install the IBM COS FA Gateway using the OpenStack console and involves creating and configuring a virtual machine and then performing an initial setup.

In this chapter

INSTALLING THE IBM COS FA GATEWAY

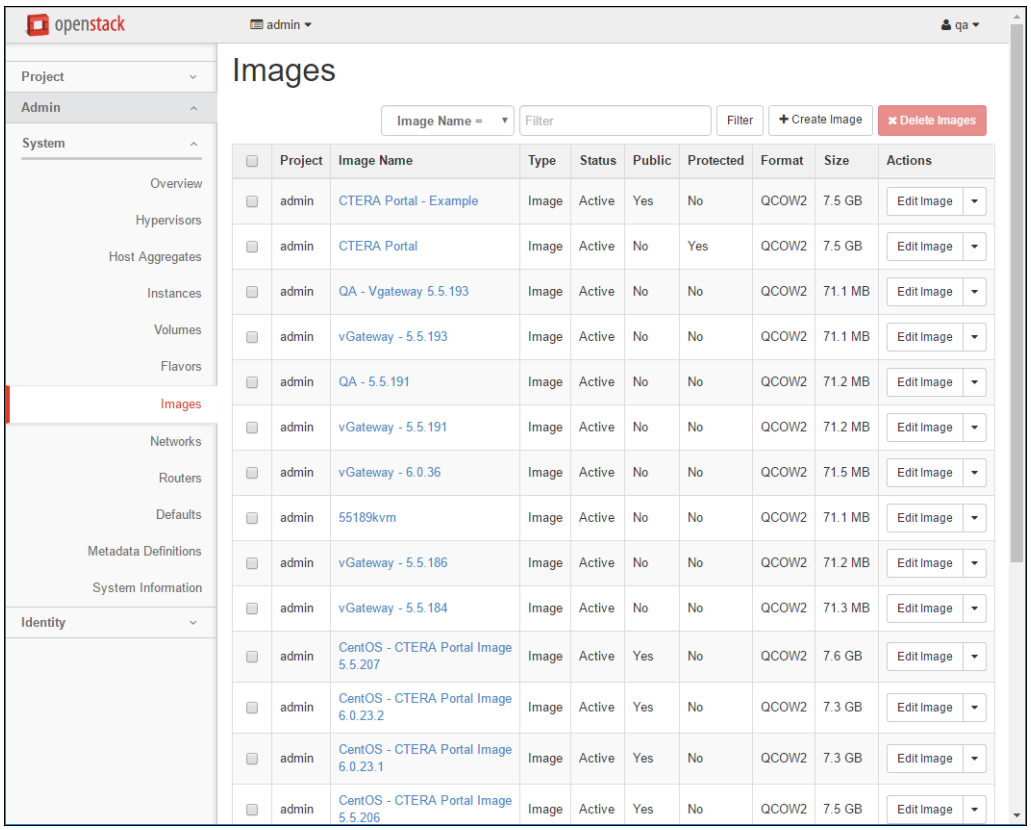
The IBM COS FA Gateway can be installed in a KVM environment.

- Linux machine with KVM virtualization
- Virtual Machine Manager (virt-manager) installed and running
- `*.qcow2` image file located on the machine

Contact IBM Networks, and request the latest `qcow2` IBM COS FA Gateway disk image.

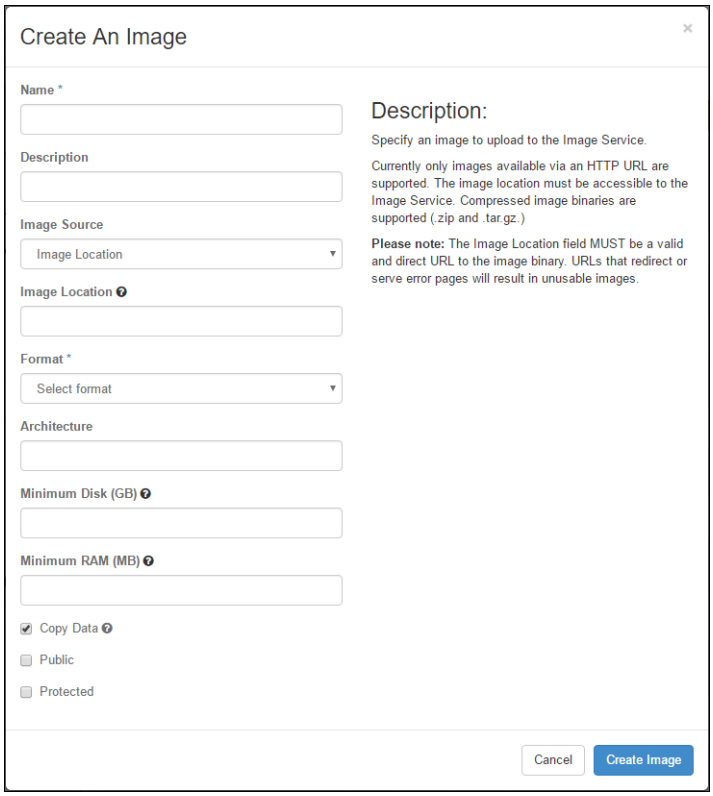
To install the IBM COS FA Gateway in OpenStack:

1 Log in to the OpenStack console and access **Admin > Images**.



2 Click **Create Image**.

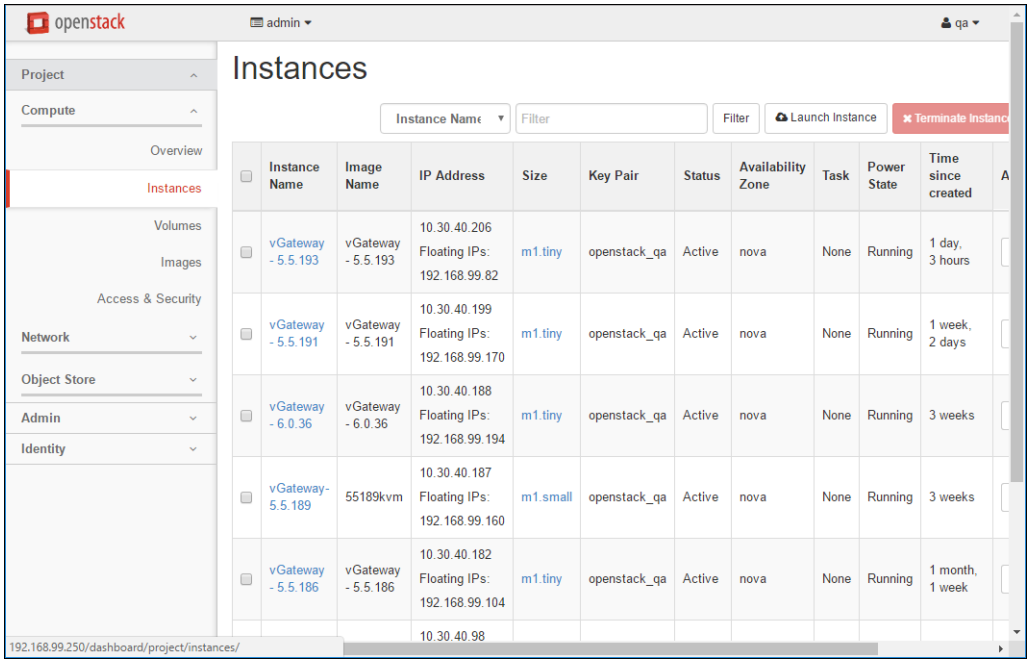
The **Create An Image** screen is displayed.



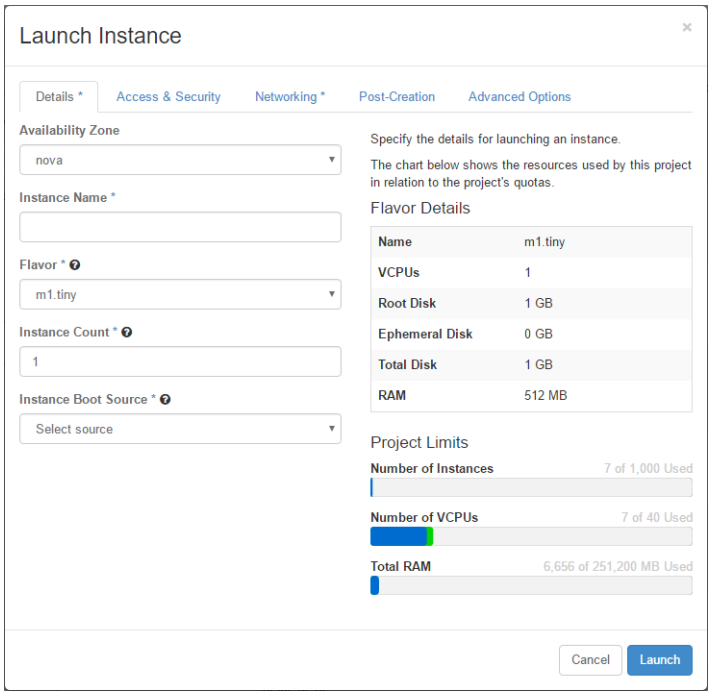
3 Specify the details for the image.
Name – A unique name to identify the image.
Description – An optional description of the image.
Image Source – Select `Image File`.
Image File – Browse to the OpenStack image received from IBM.
Format – Select `QCOW2 - QEMU Emulator`.
Architecture – Leave blank.
Minimum Disk – The recommended disk size is 16GB.
Minimum RAM – The minimum RAM requirement is 2GB (2048MB). The maximum RAM usage is 8GB.
You can leave both **Public** and **Protected** checkboxes with their default values.

4 Click **Create Image**.
The image is created. This can take a few minutes.

5 Access **Project > Compute > Instances**.



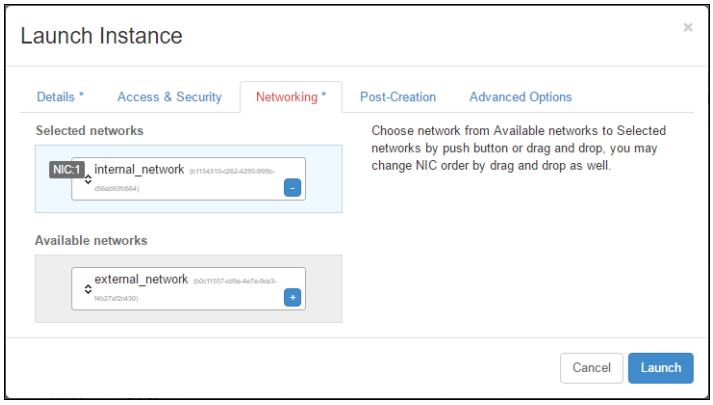
6 Click **Launch Instance**.
The **Launch Instance** screen is displayed.



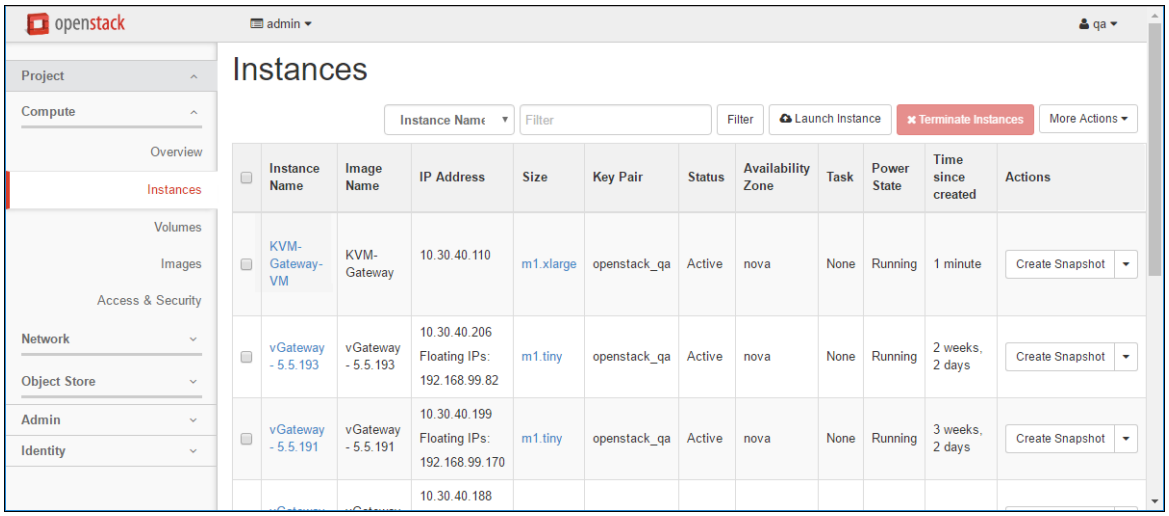
7 Specify the details for the image.
Availability Zone – Select the availability zone for the instance.
Instance Name – A unique name for the instance.
Flavor – Select a flavor for the IBM COS FA Gateway. The maximum CPUs is 4 with 8GB RAM, such as `m2.medium`.
Instance Count – Leave the default value, 1.

Instance Boot Source – Select `Boot from image`.
Image Name – Select the image you created for the IBM COS FA Gateway.

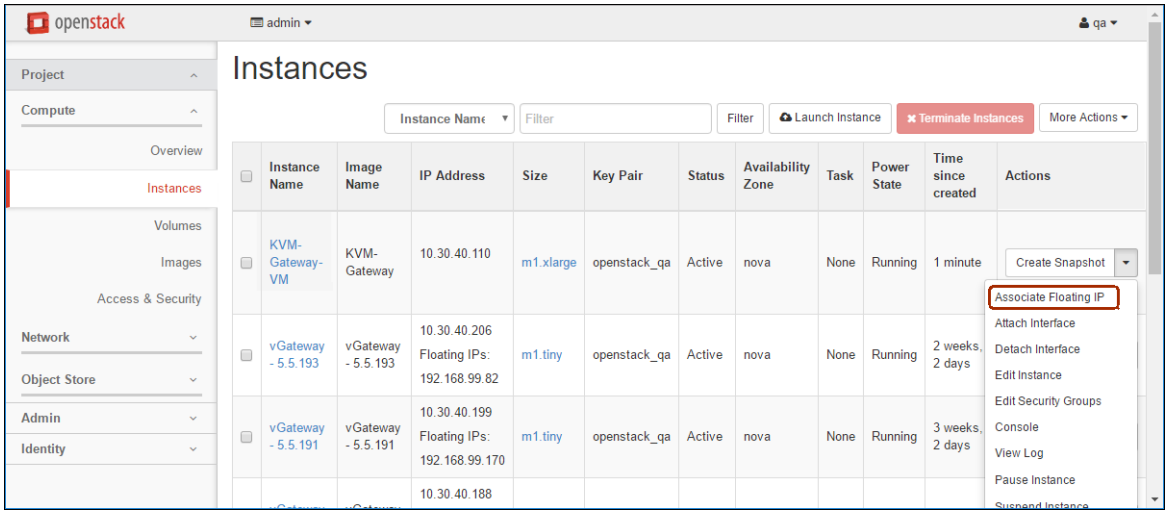
8 Click the **Networking** tab and drag the `internal_network` option to **Selected networks**.



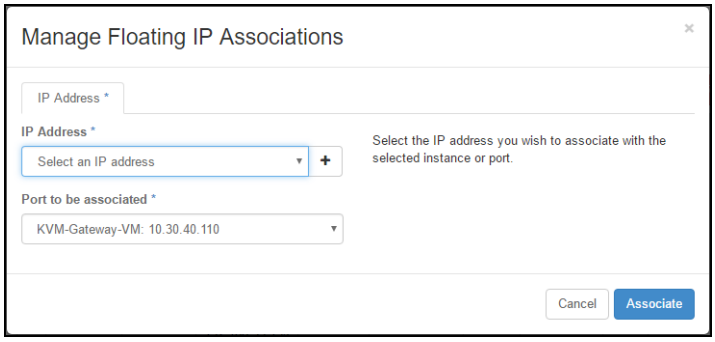
9 Click **Launch**.



10 Select the IBM COS FA Gateway instance and under **Actions** select **Associate Floating IP**.



The **Manage Floating IP Associations** dialog is displayed.

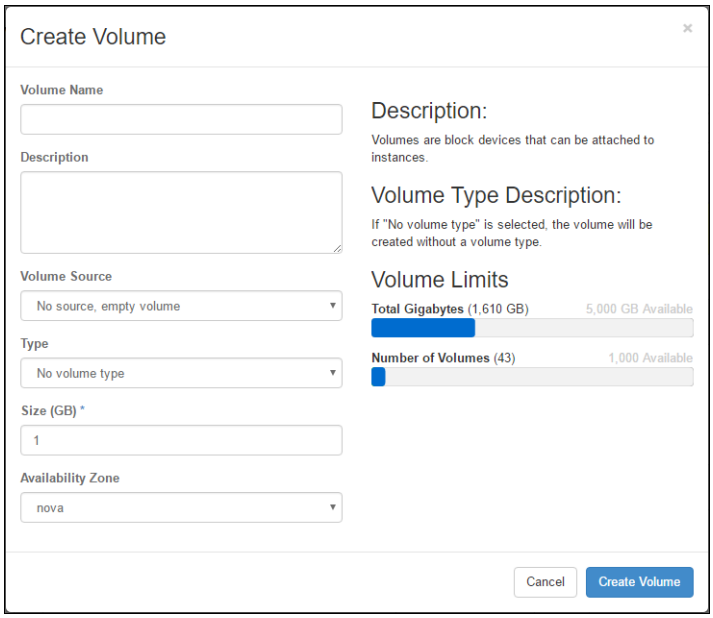


11 Select an IP address and click **Associate**.
Refreshing the Instances screen displays the IBM COS FA Gateway with the selected IP.

12 Access **Project > Compute > Volumes**.

13 Click **Create Volume**.

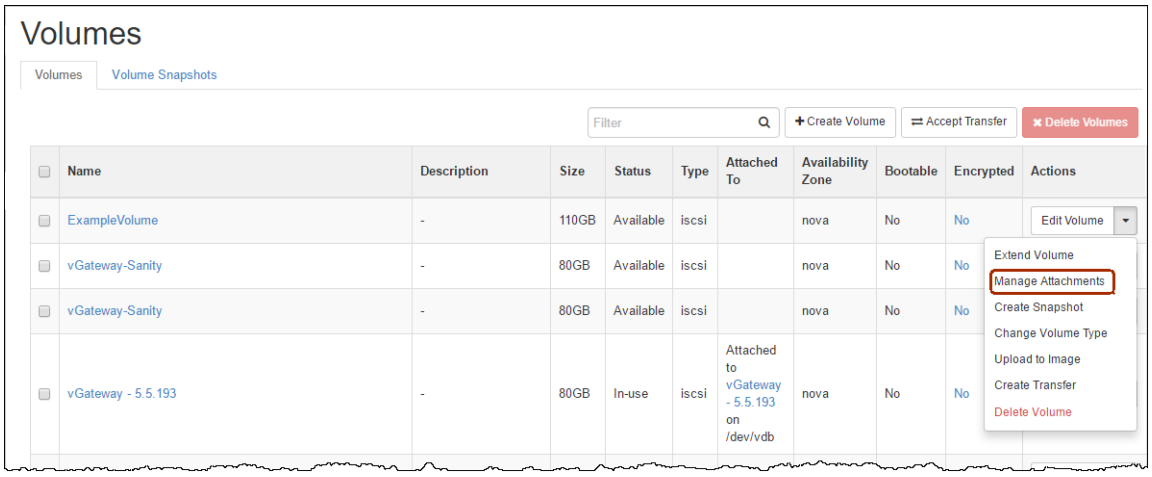
The **Create Volume** screen is displayed.



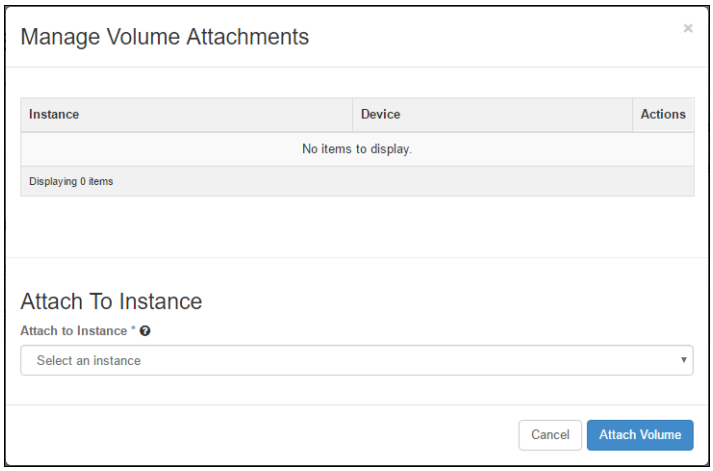
14 Specify the details for the image.
Volume Name – A unique name to identify the volume.
Description – An optional description of the volume.
Volume Source – Select `No source, empty volume`.
Type – Select `iscsi`.
Size – Specify the disk size. IBM COS FA Gateway recommends storage at least 20% of the IBM COS FA Portal storage. The maximum storage is 8TB.
Availability Zone – Select the same availability zone used for the image.

15 Click **Create Volume**.
The volume is created. This can take a few minutes.

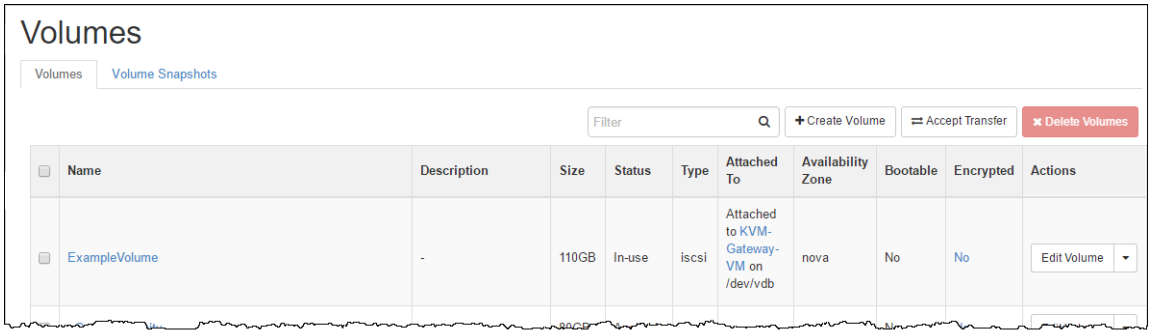
16 Select the new volume and under **Actions** select **Manage Attachments**.



The **Manage Volume Attachments** dialog is displayed.



17 Under **Attach To Instance**, select the IBM COS FA Gateway instance and click **Attach Volume**.



CONFIGURING THE IBM COS FA PORTAL AS A PRECONDITION TO SETTING UP THE IBM COS FA GATEWAY

Before setting up the IBM COS FA Gateway, you have to configure the IBM COS FA Portal to which the IBM COS FA Gateway will connect.

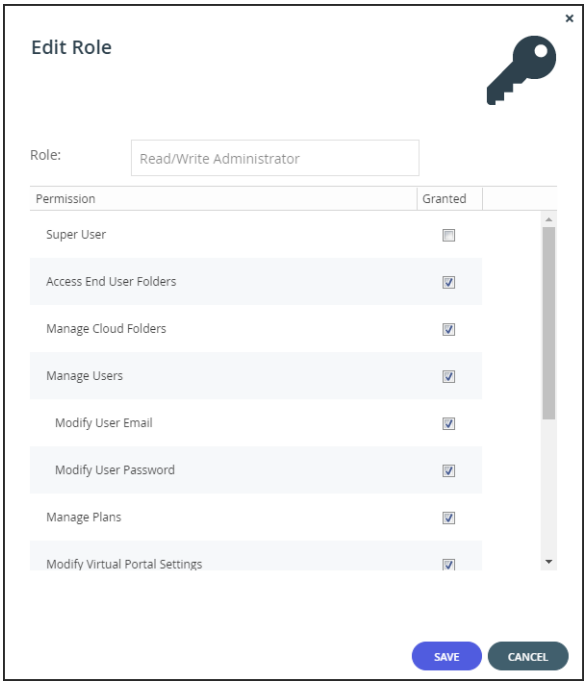
To configure the IBM COS FA Portal:

1 The user account on the IBM COS FA Portal used to connect the IBM COS FA Gateway to the IBM COS FA Portal must have read and write administrator permissions to enable syncing folders between the IBM COS FA Gateway and the IBM COS FA Portal.

a Sign in to the IBM COS FA Portal as an administrator and access the administration user interface.

b Select **Settings > User Roles** in the navigation pane.
The **Roles** window is displayed.

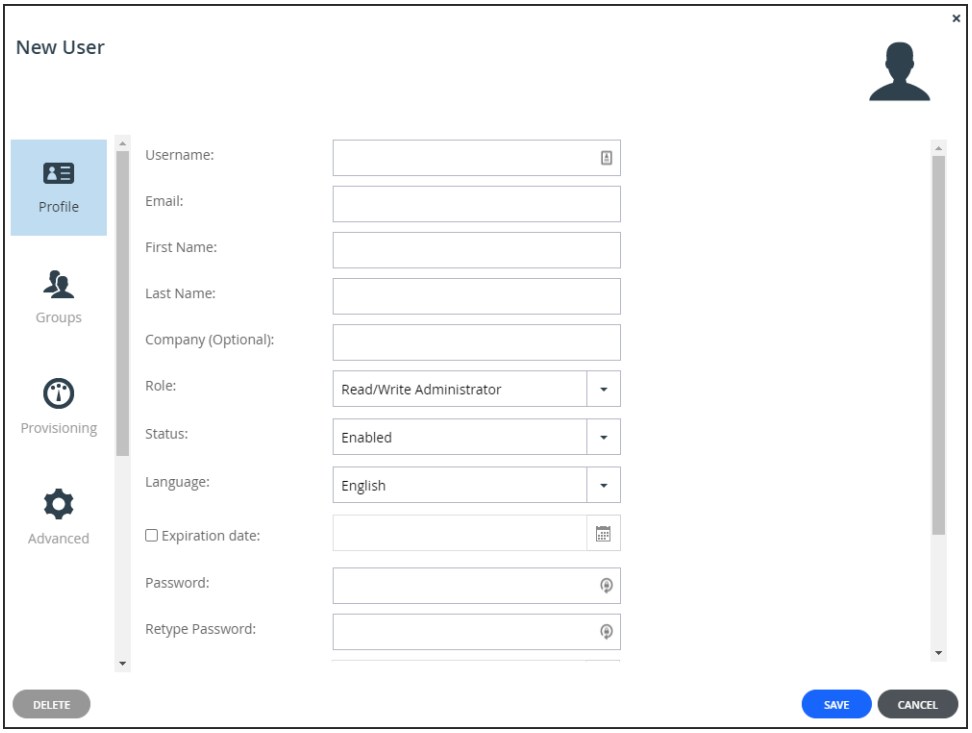
c Click **Read/Write Administrator** and in the **Edit Roles** window make sure that **Access End User Folders** is granted.



2 Create a designated user as an owner of the cloud folders and data. IBM COS FA Gateway recommends creating the owner as a local service account with administrator privileges and not a real user. Once the data is uploaded to the IBM COS FA Portal there is an owner for the data who can get elevated rights.

   a Select **Users > Users** in the navigation pane.
   The **USERS** page is displayed.

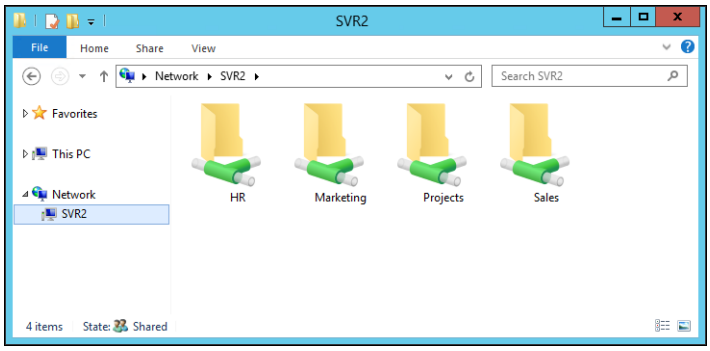
   b Click **New User**.
   The **New User** window is displayed.



c Complete the following fields in the **Profile** option.
Username – A name for the user's IBM COS FA Portal account.
Email – An email address.
First Name – A first name for the service account.
Last Name – A last name for the service account.
Role – Select **Read/Write Administrator**.
Password/Retype Password – A password for the account.

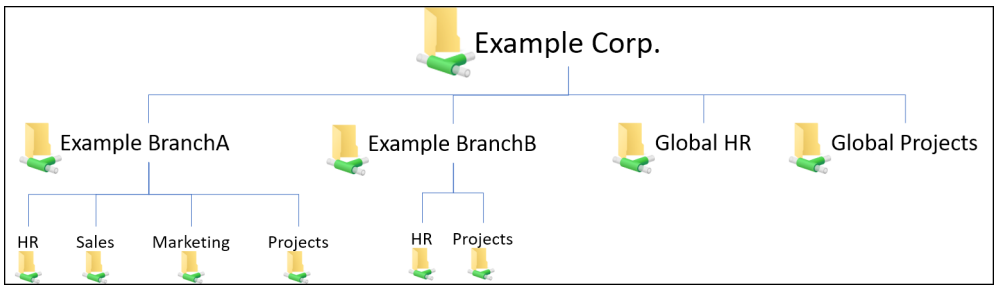
d Click **SAVE**.

3 When not using the migration tool, described in Migrating a File Server, set the folders to share with the same shares configuration as in the original file server, otherwise continue with Initial IBM COS FA Gateway Setup.
For example, the following team folders exist on a Windows server named SRV2:



Create the corresponding folders in the IBM COS FA Portal and then sync them down to the IBM COS FA Gateway. Once the folders are synced to the IBM COS FA Gateway you need to create the shares pointing to these folders via the IBM COS FA Gateway user interface.
Where appropriate, IBM COS FA Gateway recommends creating site or company cloud folders. For example, if the migrated data will be used at multiple company sites, with similar share structures

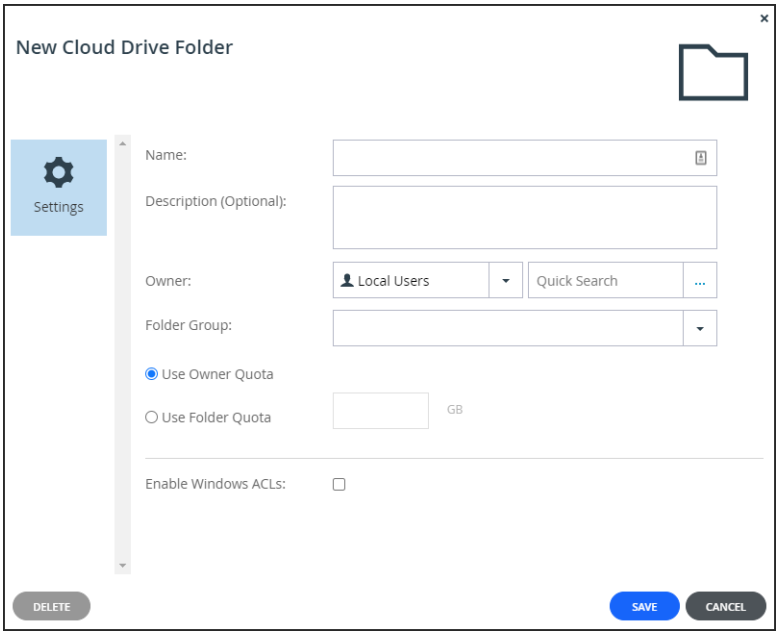
at each site, you should create a corporate cloud folder with all the folders that will be shared by all the sites underneath it and in addition have a site folder per site containing all the share folders for the site.



With this structure, you can edit the ACLs for each folder at the top level of the share.

a Select **Folders > Cloud Drive Folders** in the navigation pane.
The **Cloud Drive Folders** page is displayed.

b Click **New**.
Note: You cannot set up an existing folder that already contains files.



c Complete the fields:
Name – The name for the folder.
Description – An optional description for the folder.
Owner – The user who is the owner of the folder, defined in step 2.
Folder Group – A folder group for the folder.

d Check the **Enable Windows ACLs** check box.
ACL emulation enables files and folders management via standard SMB protocol using Windows Explorer.

e Click **SAVE**.

f Repeat steps a to e for all the share folders.

The new folders are added to the Cloud Drive folders.

4 Log on to the end user IBM COS FA Portal with the service account that owns the share folders.

5 Select each folder and click the **Share this folder** icon .

6 Add the domain users group and click and choose the *Read/write* permission.

Note: You can add individual users if you don't want the folder shared with every user from the domain users group.

INITIAL IBM COS FA GATEWAY SETUP

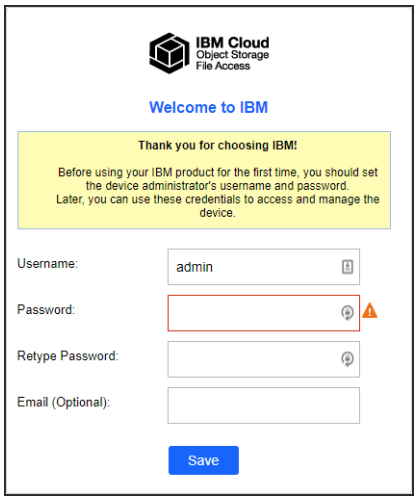
Before setting up the IBM COS FA Gateway, you have to configure the IBM COS FA Portal to which the IBM COS FA Gateway will connect, as described in Configuring the IBM COS FA Portal as a Precondition to Setting Up the IBM COS FA Gateway. After configuring the IBM COS FA Portal and installing the IBM COS FA Gateway, you need to perform an initial IBM COS FA Gateway setup. On first access to the IBM COS FA Gateway, you set up a IBM COS FA Gateway administrator and then a wizard guides you through connecting to a IBM COS FA Portal and storage and user setup. You can skip any of the wizard steps and perform them later, as described in the *IBM COS FA Gateway Administrator Guide*.

After this initial IBM COS FA Gateway setup, the file server structure is synced from the IBM COS FA Portal to the IBM COS FA Gateway.

To access the IBM COS FA Gateway and initial setup:

1 Open any web browser.

2 Enter the IBM COS FA Gateway's IP address from Select an IP address and click Associate. to navigate to the device.
When you connect to the web interface for the first time, your browser displays the **Welcome to** IBM page.



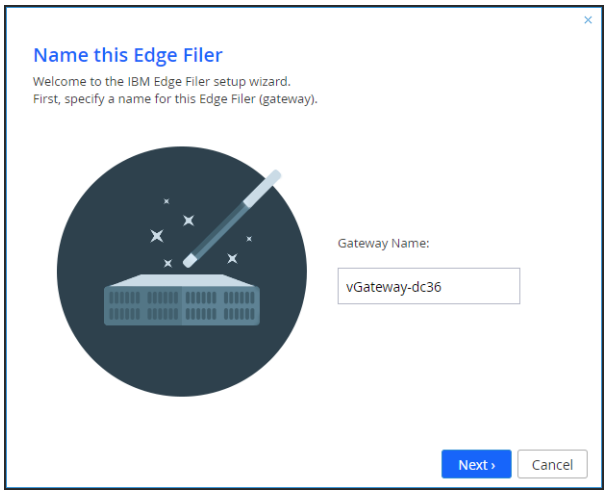
3 Choose a user name and password for the administrator. The password must be at least eight characters and must include at least a letter, digit and special character, such as ~, @, #, $, %, ^, & , (. Other administrators are defined in the IBM COS FA Gateway user interface from Active Directory.

Note: You can keep the default user name, `admin`.

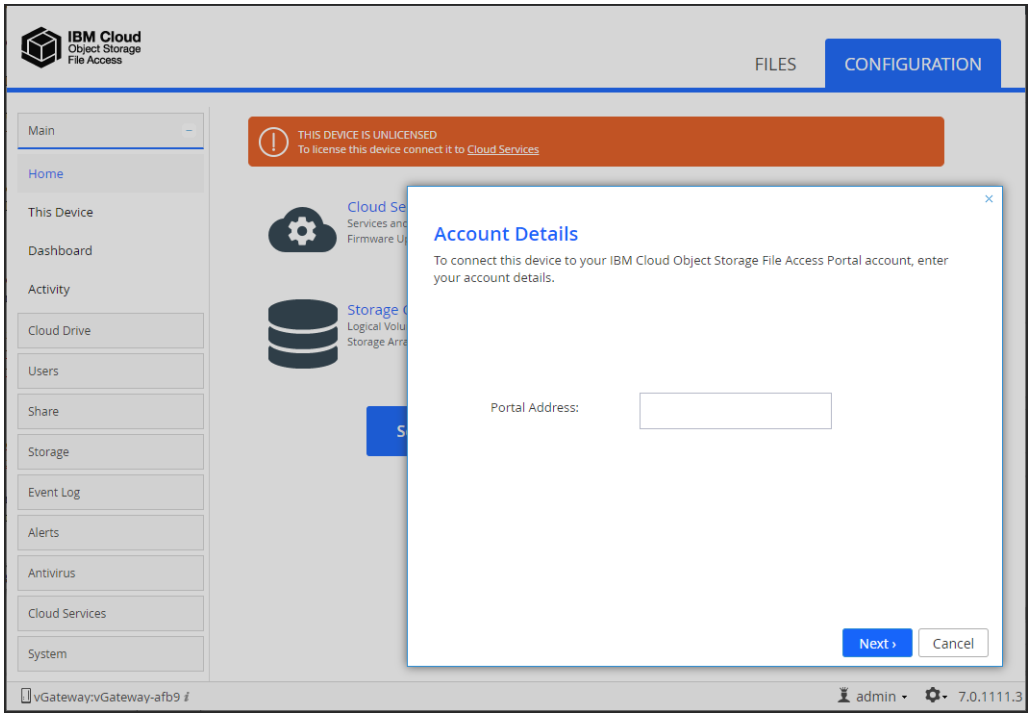
4 Optionally, enter an email for receiving notifications regarding the IBM COS FA Gateway.

5 Click **Save**.
If the IBM COS FA Gateway does not have a disk, a message window is displayed.
Shutdown the IBM COS FA Gateway and add a disk to the IBM COS FA Gateway virtual machine.

Otherwise, the **Name this IBM COS FA Gateway** window is displayed.



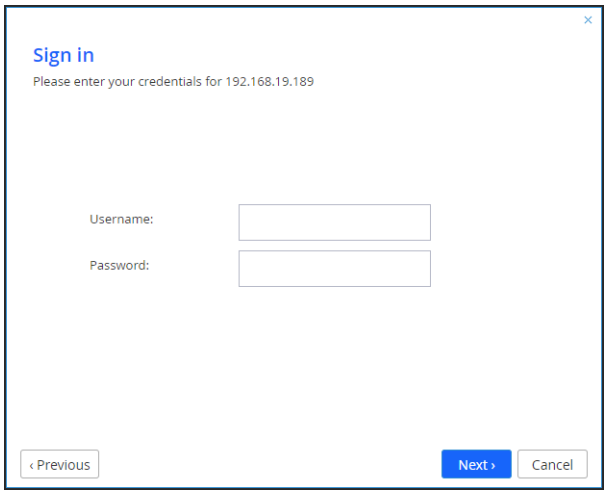
6 Either keep the IBM COS FA Gateway default name or enter a new name to identify the IBM COS FA Gateway and click **Next**.
The administration user interface is displayed to set up the IBM COS FA Gateway, starting with the **Account Details** window.



Note: You can also change the IBM COS FA Gateway name after the initial setup, as described in the *IBM COS FA Gateway Administrator Guide*.

7 Enter the DNS name of the IBM COS FA Portal to which you have an account and want to connect the IBM COS FA Gateway to, in the **Portal Address** field and click **Next**.

The **Sign in** window is displayed.

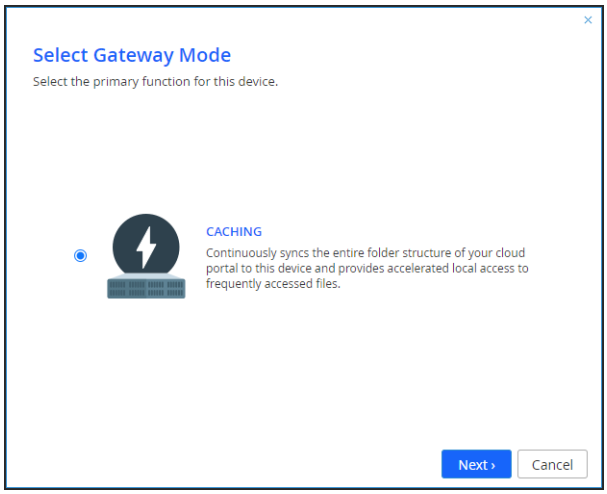


Note: If single sign-on has been implemented, you click the Sign-in button to continue.

8 Enter the IBM COS FA Portal designated user username and password, set in step **2** in Configuring the IBM COS FA Portal as a Precondition to Setting Up the IBM COS FA Gateway to access the IBM COS FA Portal and click **Next**.
The **Select License** window is displayed.

9 If required, select the license.

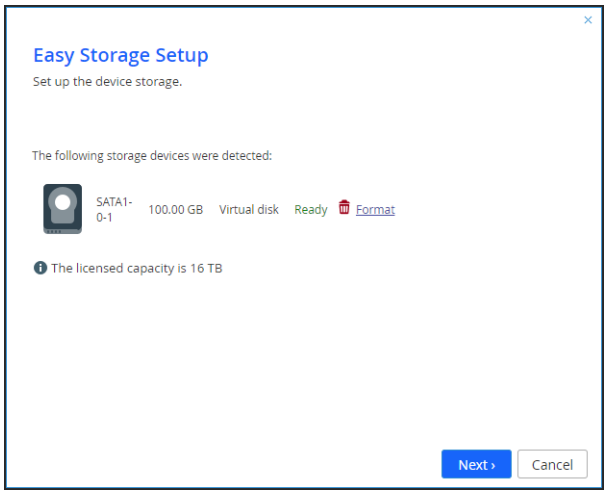
10 Click **Next**.
The **Select Gateway Mode** window is displayed.



CACHING provides users with LAN speed access to all the shared cloud folders on the IBM COS FA Portal. Shared storage is on the IBM COS FA Portal in the cloud with stubs saved on the IBM COS FA Gateway. A stub is a file with a tiny footprint that contains the metadata about the file, such as the file name, size, and modification date. Only the folder and file metadata and not the actual file content is saved locally. Thus, the IBM COS FA Gateway can have much less physical storage than is made available to users, who have access to both the local IBM COS FA Gateway storage and the IBM COS FA Portal storage. Systems with many file changes, where only some of the files are required locally, don't over use bandwidth between the cloud and IBM COS FA Gateway. Only the required files are passed across the wire. When a user accesses a file stub, the file is opened without delay, by streaming the file content from the cloud. After the download has completed, the

file is *unstubbed*. Any changes to the file are synced back to the IBM COS FA Portal. Folders that are always required can be pinned, in which case the files in the folders, and not the stubs, are stored on the IBM COS FA Gateway.

11 Click **Next**.
The **Easy Storage Setup** window is displayed.

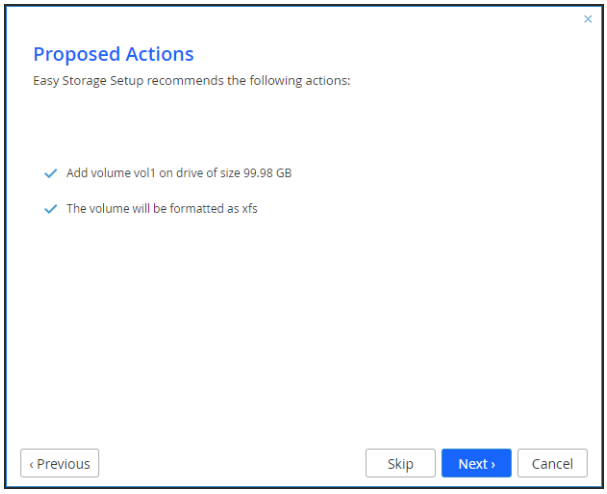


The maximum storage allowed for the IBM COS FA Gateway license is also displayed.

12 Format the virtual disks.

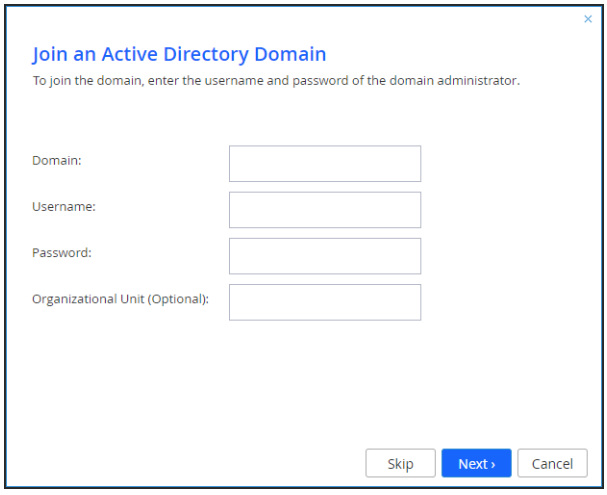
Note: Whenever a new disk is added to the IBM COS FA Gateway, it should always be formatted.

13 Click **Next**.
If the setup wizard determines that certain storage configuration changes would be beneficial, the **Proposed Actions** window is displayed describing the recommended changes.



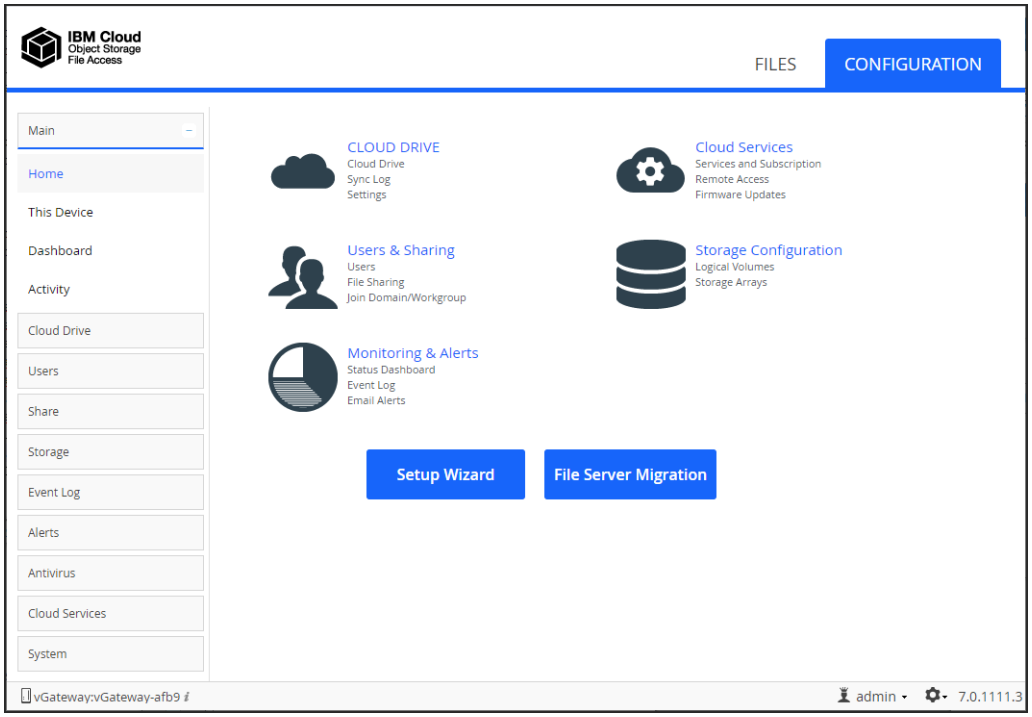
Note: An array is proposed only if the virtual machine has multiple disks.

14 Click **Next**.
The **Join an Active Directory Domain** window is displayed.



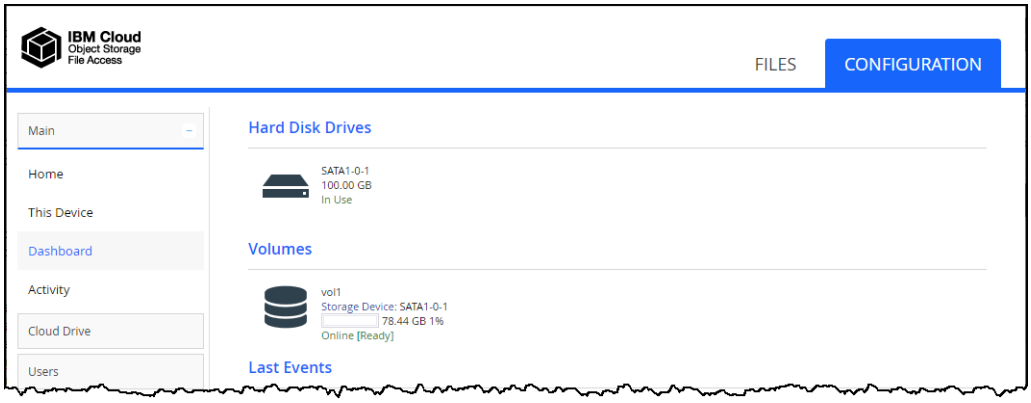
15 Specify the domain details so that the IBM COS FA Gateway is populated with the users from your Active Directory domain and click **Next**, or, if you want to set up Active Directory later, click **Skip**. The **Wizard Completed** window is displayed.

16 Click **Finish**.
The **CONFIGURATION** tab's **Main > Home** page is displayed.



If you selected CLOUD BACKUP, you can enable caching at a later date.

17 Select **Main > Dashboard** and verify that all the hard disk drives installed in the IBM COS FA Gateway are available.



Note: You can rerun the wizard by selecting **Main > Home** and click **Setup Wizard**.

You can migrate a file server to IBM COS FA Gateway so that end users who are familiar with a given folder structure and share, while using the file server, continue to see the same folder structure and shares after migration to the IBM COS FA Gateway. If you are replacing an exiting file server with the IBM COS FA Gateway, continue with Migrating a File Server.

For full details about managing the IBM COS FA Gateway, see the *IBM COS FA Gateway Administrator Guide*.

LOADING A SELF-SIGNED CERTIFICATE TO IBM COS FA GATEWAY

When the object storage used by theIBM COS FA Portal uses a X.509 Certificate signed by a private Certification Authority (a self-signed certificate) and not a public trusted certificate, this certificate must be uploaded to the IBM COS FA Gateway. You upload the certificate using the following procedure that requires a REST client tool such as Postman or HTTPie.

To upload a self-signed certificate to the IBM COS FA Gateway:

1 Get the certificate used by the object storage.

2 Launch the REST client.

3 Log in to the IBM COS FA Gateway with the following REST API, using HTTPS: `https://gateway_IP/admingui/api/login` with the following:

HTTP Method	POST	
Request Content-Type	`application/x-www-form-urlencoded`	
Request Body	**`Key`**	**`Value`**
	`username` `password`	*`username`* *`password`*
Expected Response Status	`200 OK` and an HTTP session cookie which is then used for the duration of the session. The session times out after 30 minutes of inactivity. If a response such as `403 Forbidden` is returned, check the user name and password provided.	

Where:
gateway_IP – The IP address of the gateway.
username – Mandatory: The name of a user with administrative rights to the gateway. This is the username set in step 3.
password – Mandatory: The password for the user. The login is over HTTPS to ensure that the

password is encrypted.This is the password set in step 3.
Upon receiving a successful login reply, the server sets HTTP session cookies. The client must return these cookies to the server in the next request.

Note: To ensure that the session cookie returned by the API login is automatically returned in subsequent requests to the server, the same HttpClient object must be used for all future requests.

4 Copy to your clipboard the contents of the certificate.

5 Upload the certificate using the following REST API:
`http://gateway_IP/admingui/api/config/extStorageTrustedCA?put` with the following:

HTTP Method	POST
Request Content-Type	`application/xml`

Request Body	`<obj class="ExtStorageTrustedCA">`
	`  <att id="certificate">`
	`  <val>`
	`-----BEGIN CERTIFICATE-----`
	`##### Certificate Content #####`
	`-----END CERTIFICATE-----`
	`  </val>`
	`  </att>`
	`</obj>`

Expected Response status	`200 OK`

Where:
gateway_IP – The IP address of the gateway.
Certificate Content – The content copied to the clipboard in step 4.

CHAPTER 4. MIGRATING A FILE SERVER

This chapter describes how to migrate a single file server to the IBM COS FA Gateway. After the migration has completed, end users who are familiar with a given folder structure and shares, as well as a given permission scheme continue to see the same folder structure, shares, and permission scheme. This enables the migration from a current file system to the IBM COS FA Gateway without the need to apply any structural changes such as flattening the folder structure or simplifying the permissions scheme.

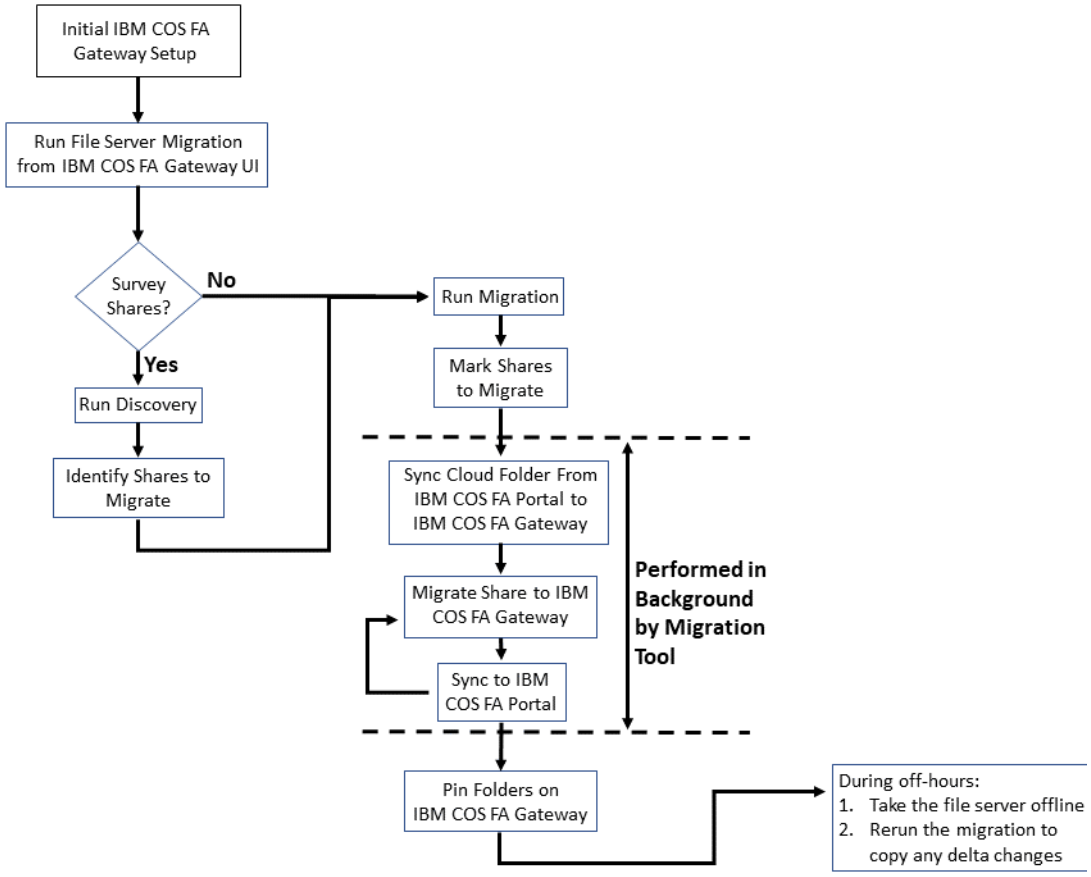
You can migrate file servers including Windows File Server, NetApp ONTAP, Panzura Freedom Filer.

Access to files and folders after the migration is through SMB provided by the IBM COS FA Gateway so that users continue to access the files and folders in the same way as with the old system. You can migrate more storage than is physically available on the IBM COS FA Gateway and the user has access to this storage, even when this is much larger than the storage available on the IBM COS FA Gateway.

Note: You can migrate a single file server to the IBM COS FA Gateway as a single cloud folder. After the migration, the cloud folder will start with the C: path as it represents a single server with all the shares/nested shares.

Migrating a file server to a IBM COS FA Gateway can be performed while the current file server remains in production.

The flow when performing a migration is as follows:



MIGRATING A FILE SERVER TO THE IBM COS FA GATEWAY

Before migrating the file server to the IBM COS FA Gateway, that IBM COS FA Gateway must be connected to the IBM COS FA Portal. After finishing the initial setup, make sure that syncing between the IBM COS FA Gateway and IBM COS FA Portal is not suspended.

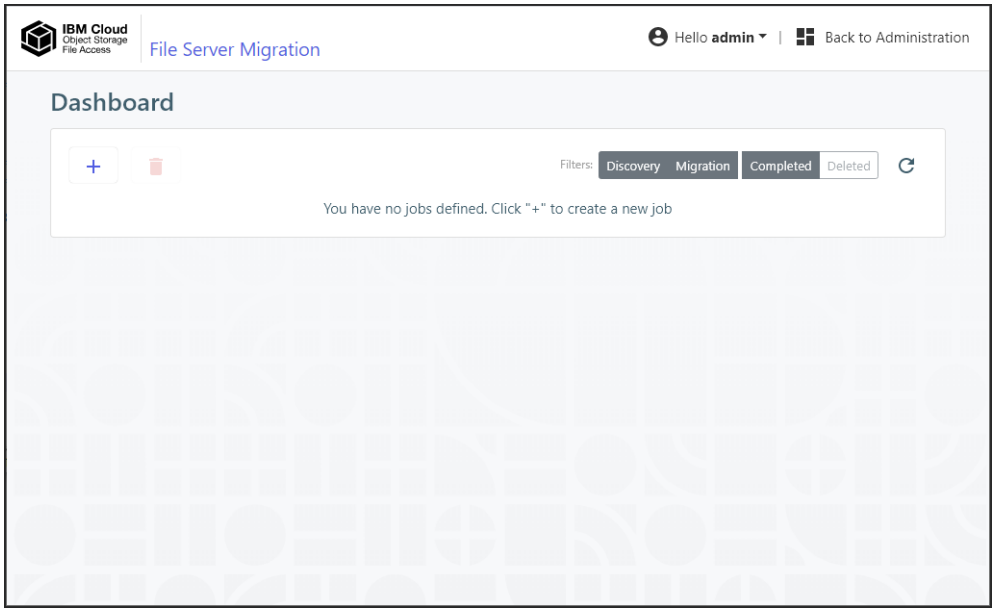
To migrate a single file server to the IBM COS FA Gateway as a single cloud folder involves the following procedures:
Discovering Shares – Optionally survey the current file server to discover which shares to migrate.
Migrating Shares – Migration shares to the IBM COS FA Gateway.

After the migration, the cloud folder will start with the C: path as it represents a single server with all the shares/nested shares.

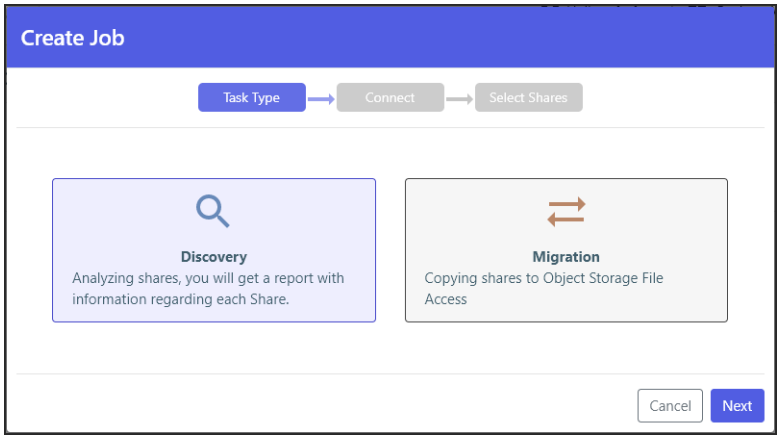
Discovering Shares

To discover the shares to migrate:

1 In the **CONFIGURATION** tab's **Main > Home** page, click **File Server Migration**.
The **File Server Migration** page is displayed.

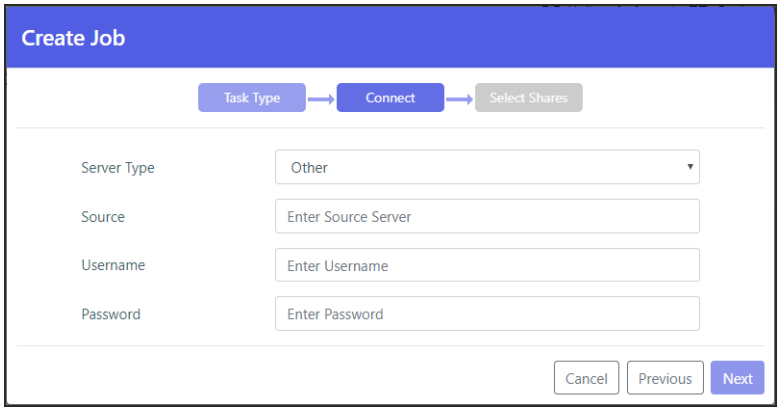


2 Click **+** to create a new job.
The **Create Job** wizard is displayed showing the **Task Type** step.



The default job is a **Discovery** job. This job analyses the file server that is being replaced to identify what data should be migrated.

3 Click **Next**.
The **Connect** step is displayed.

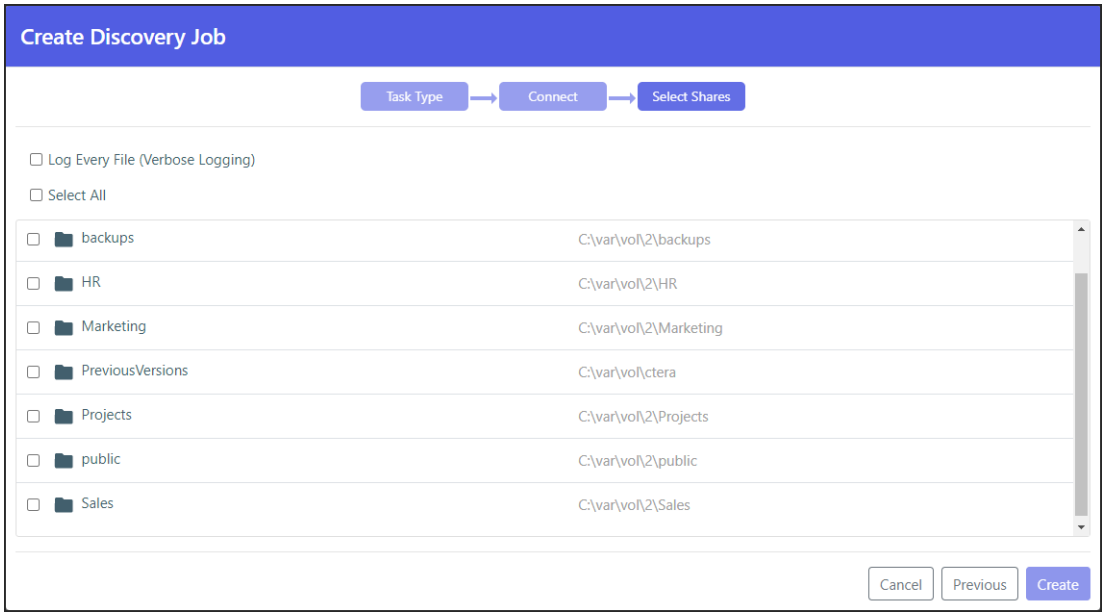


4 Select the server type to connect to from the drop-down box. You can connect to a **Windows Server**, **NetApp ONTAP**, **Panzura Freedom Filer** or another file server by selecting the **Other** option.

5 Enter the IP address or DNS name for the source file server and an administrator user name and password to access the filer server.

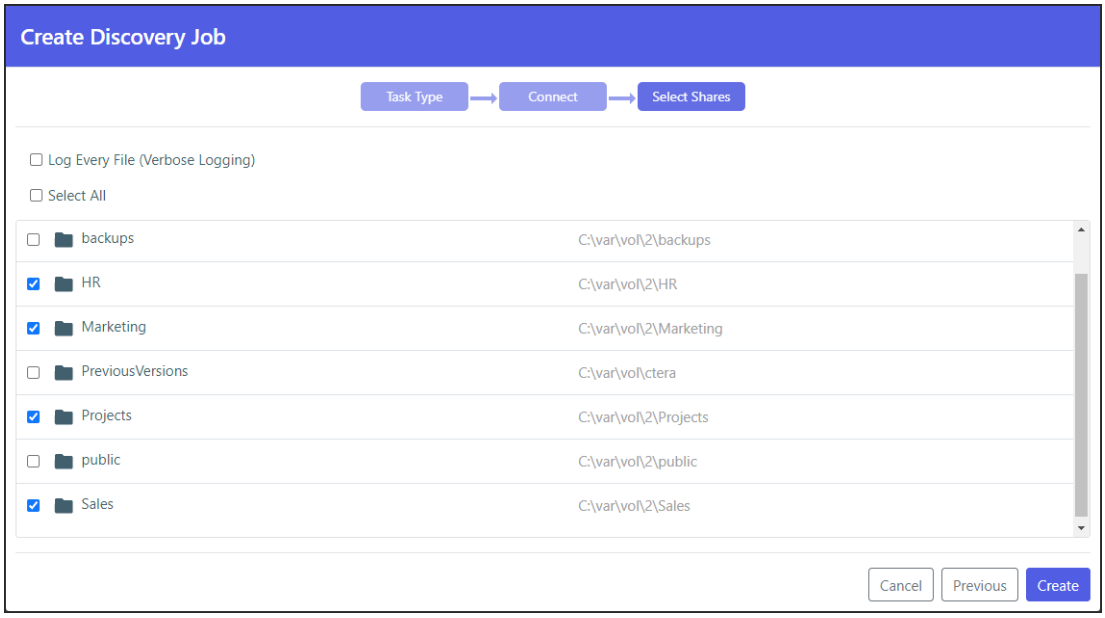
Note: The administrator used must have access to the files to migrate.

6 Click **Next**.
The **Select Shares** step is displayed.



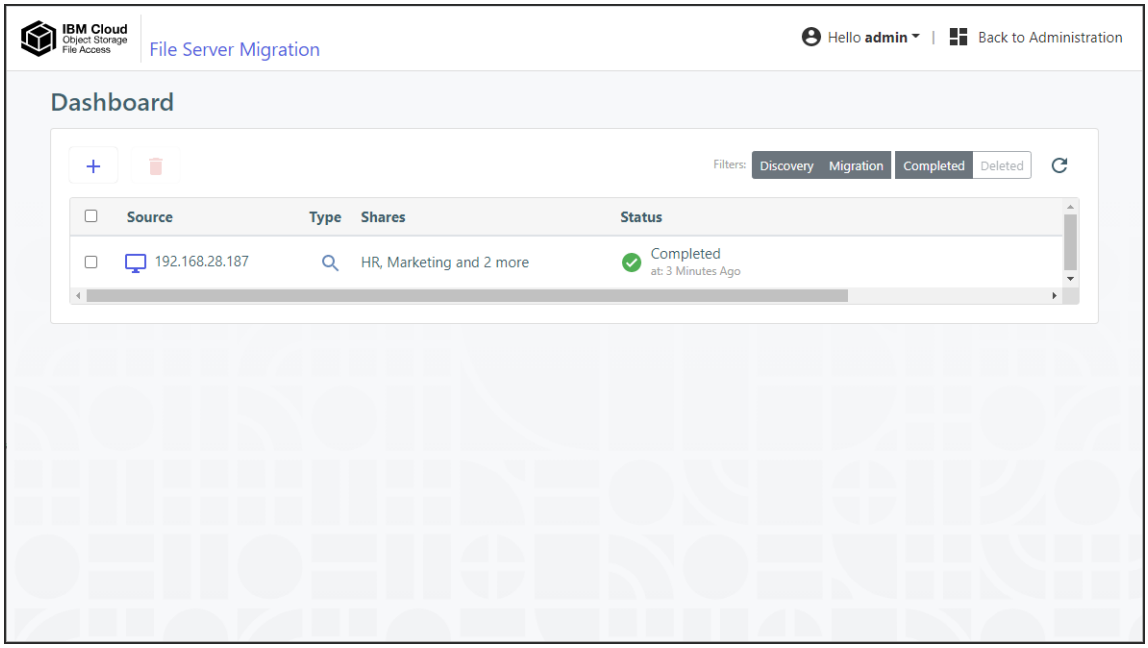
The shares on the file server are displayed and you can select the shares that you want to migrate to the IBM COS FA Gateway.

7 Select the shares to migrate.



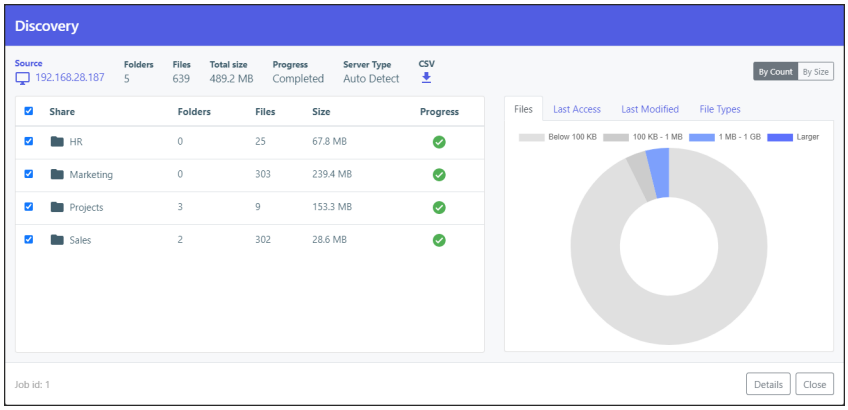
8 Click **Create**.

After analyzing the file server the job completes and you get a report as well as a full analysis of each share in the filer server that you selected.



If needed, scroll to the end of the job for buttons to access the discovery report and shares details.

9 Click  to display the discovery report.



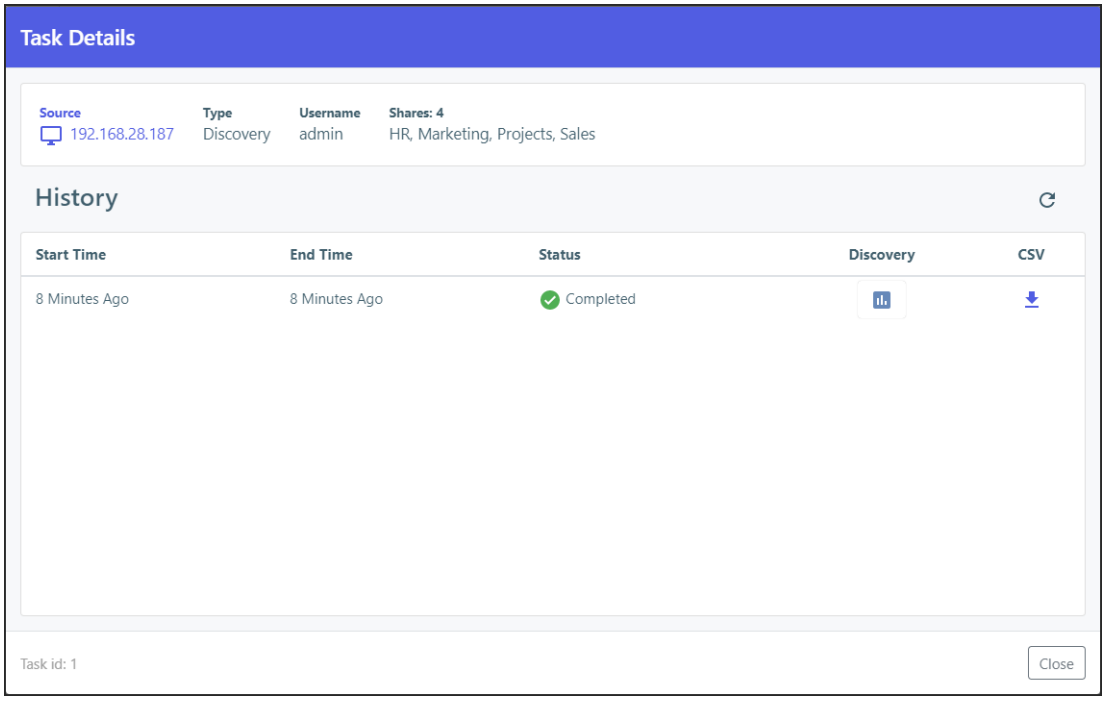
The first pane in the discovery report shows the list of shares with details of each share:

- The number of folders in the selected shares.
- The number of files in the selected shares.
- The size of the selected shares.
- The status of the report for the selected shares.

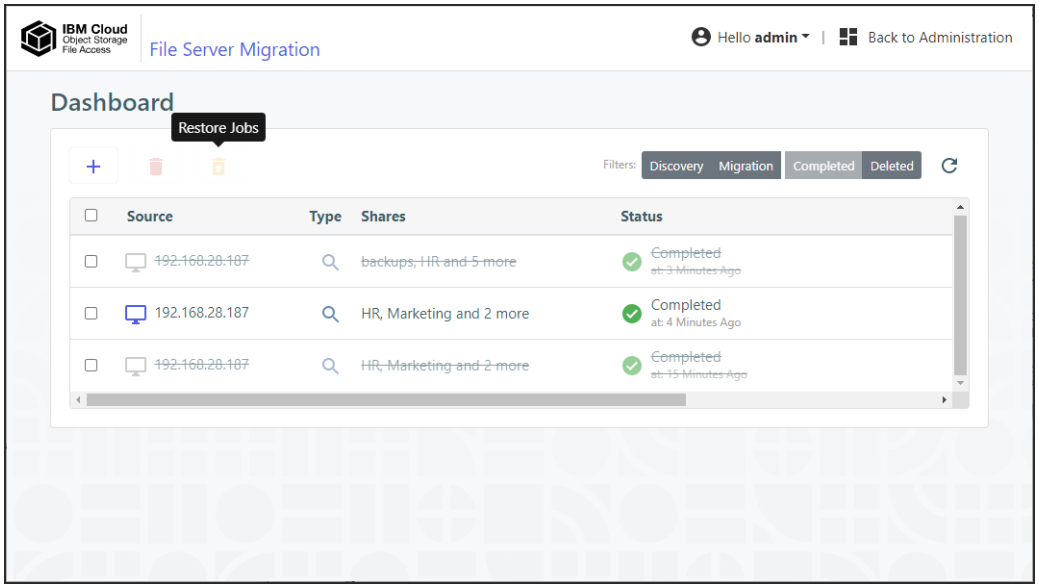
At the top of the window the sum of the information for the selected shares is displayed.
The second pane in the discovery report has tabs showing the following:
Files – A pie chart with the sizes of the files in the selected shares.
Last Access – A bar chart showing when the files in the selected shares were last accessed.
Last Modified – A bar chart showing when the files in the selected shares were last modified.
File Types – The list of the file types in the selected shares.

- Optionally, click CSV to export the report to a .csv file.
  The `discovery-IBM_COS_FA_Gateway_Ip-startTimestamp-endTimestamp.csv` report is downloaded, where:
  IBM_COS_FA_Gateway_Ip – The IP address of the IBM COS FA Gateway.
  startTimestamp – The starting date and time when the discovery was run.
  endTimestamp – The end date and time when the discovery was run.

10 Click ⓘ to display the list of every time this job was run with the results of each run.



11 Optionally, in the dashboard you can select a job and click 🗑 to delete it.
After deleting a job, you can display all the jobs including the deleted jobs by clicking the **Deleted** filter in the dashboard.

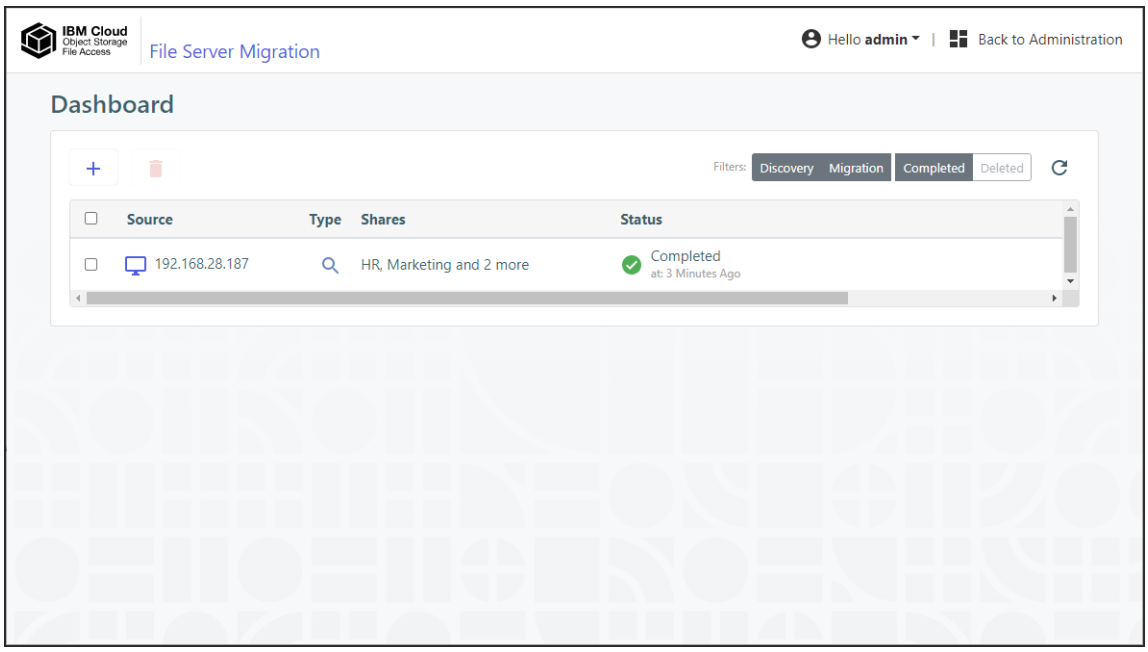


You can restore deleted jobs by selecting the deleted jobs to restore and clicking .

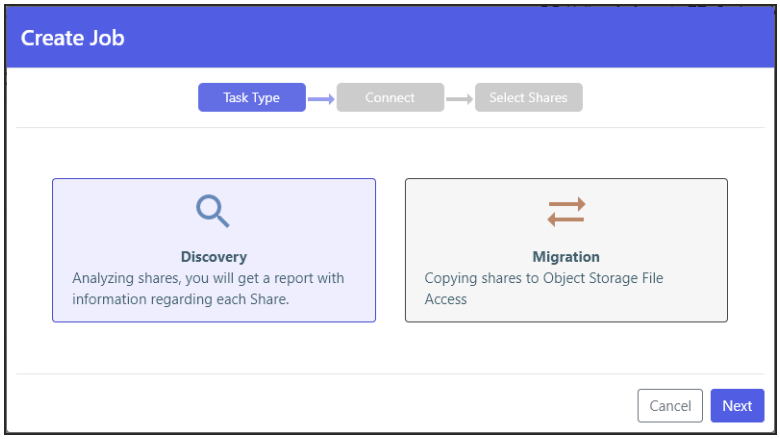
Migrating Shares

To migrate shares to the IBM COS FA Gateway:

1 In the **CONFIGURATION** tab's **Main > Home** page, click **File Server Migration**.
The **File Server Migration** page is displayed.

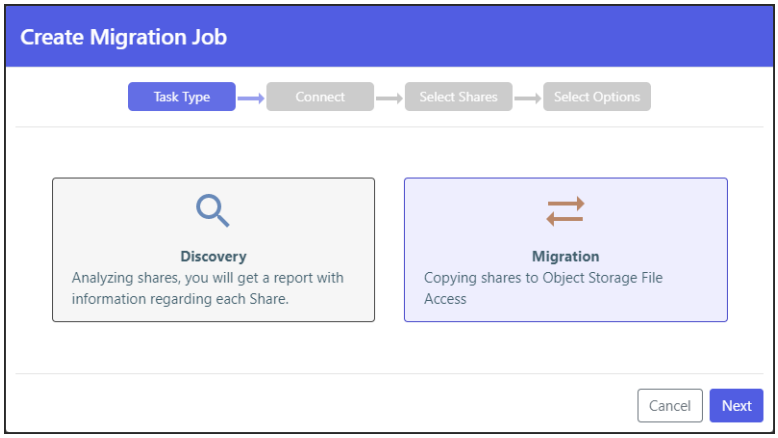


2 Click **+** to create a new job.
The **Create Job** wizard is displayed showing the **Task Type** step.

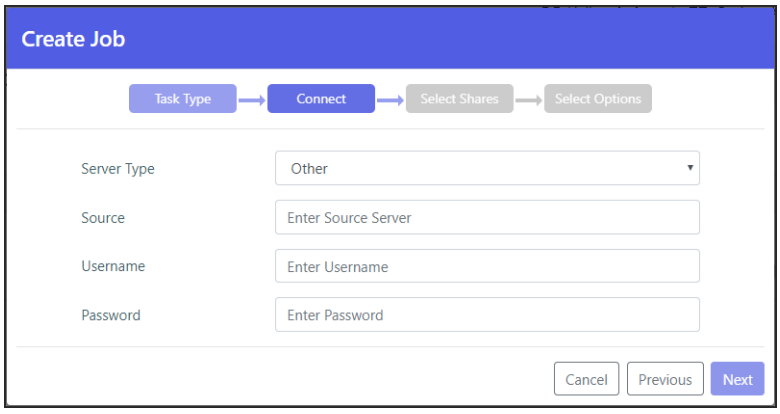


The default job is a discovery job.

3 Click the **Migration** job to change the job to migrate a file server.



4 Click **Next**.
The **Connect** step is displayed.



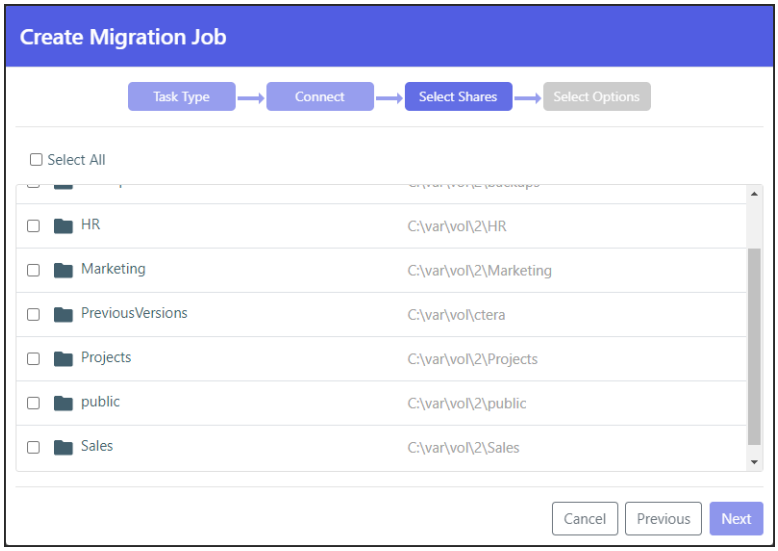
5 Select the server type to connect to from the drop-down box. You can connect to a **Windows Server**, **NetApp ONTAP**, **Panzura Freedom Filer** or another file server by selecting the **Other** option.

6 Enter the IP address or DNS name for the source file server and an administrator user name and password to access the filer server.

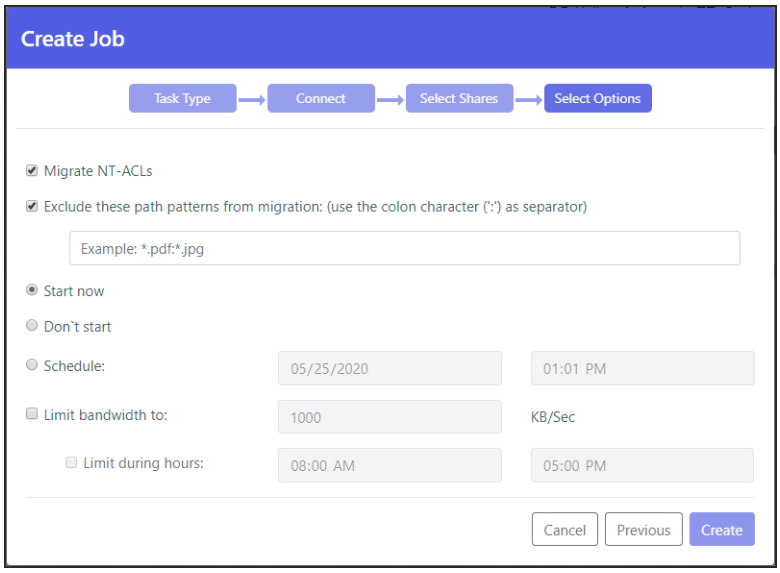
Note: The administrator used must have access to the files to migrate.

Note: The administrator used must have access to the files to migrate.

7 Click **Next**.
The **Select Shares** step is displayed.



8 Select the shares to migrate and click **Next**.
The **Select Options** step is displayed.

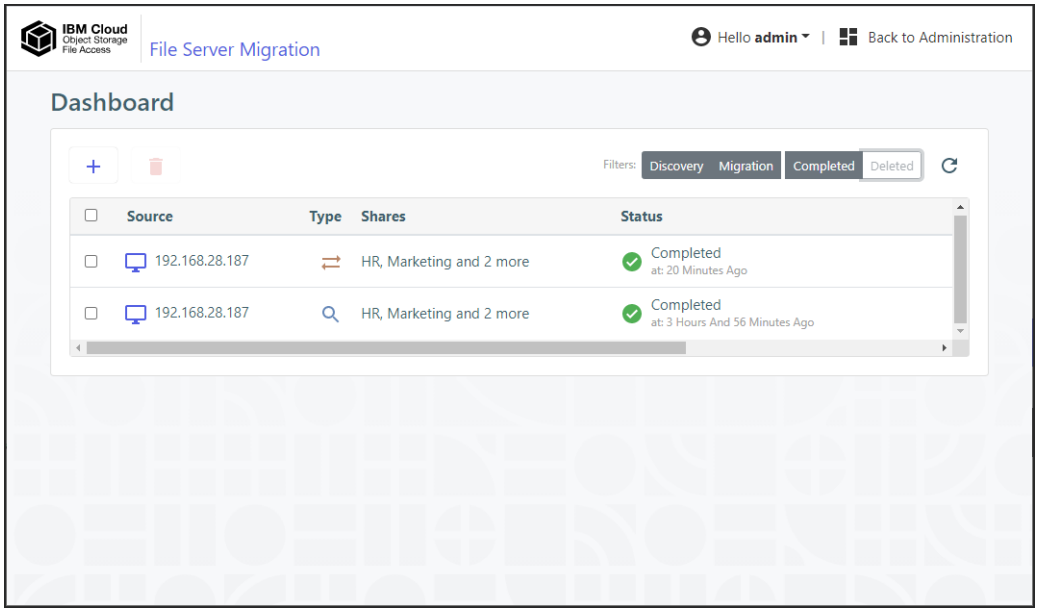


9 You can select to migrate the data from the file server with the ACLs.

10 You can specify patterns that you do not want to migrate, separating each pattern with a colon (:). You can include the asterisk (*) as a wildcard in the pattern.

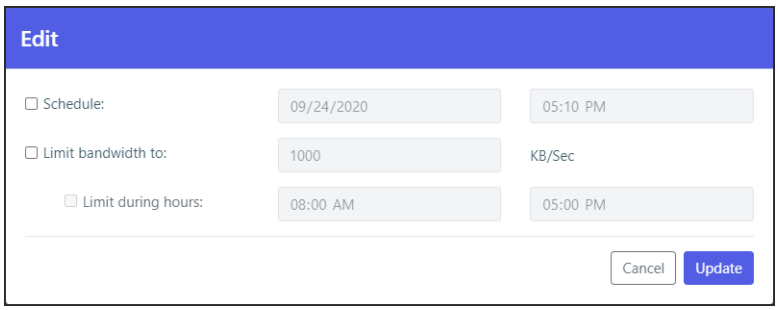
11 You can specify when to start the migration, either immediately or at a scheduled date and time. If you are migrating during working hours, you can throttle the bandwidth used for the migration so as not to adversely impact ongoing work.

12 Click **Create**.
After migrating all the shares, the job completes.

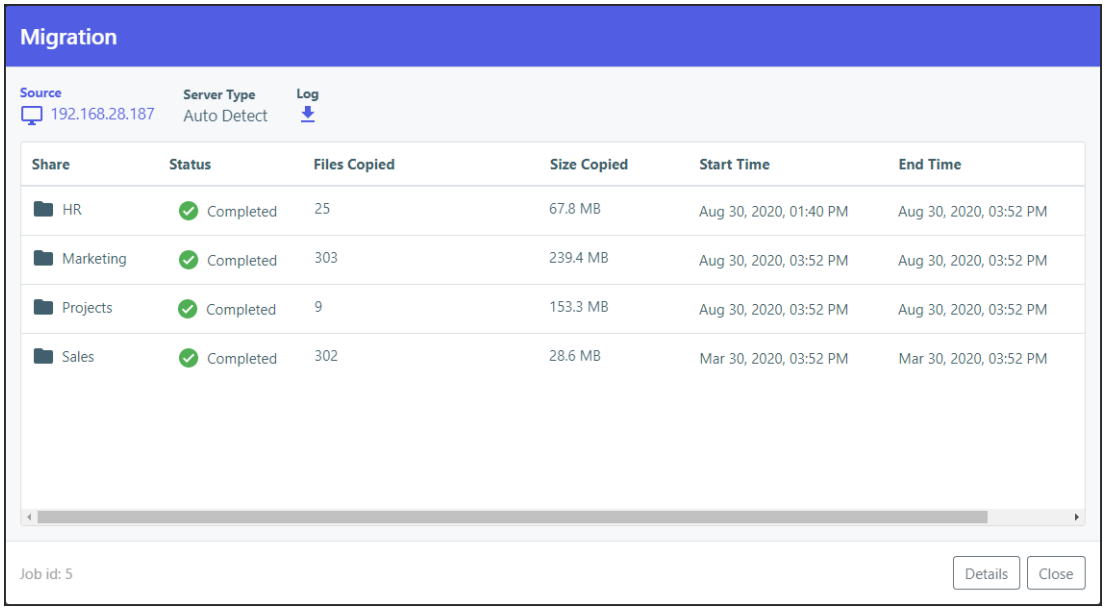


If needed, scroll to the end of the job for buttons to access the migration report and shares details.

13 Click  to edit the migration job schedule and throttling.



14 Click  to display the migration report.



- Optionally, click Log to export the migration log file to a .log text file.

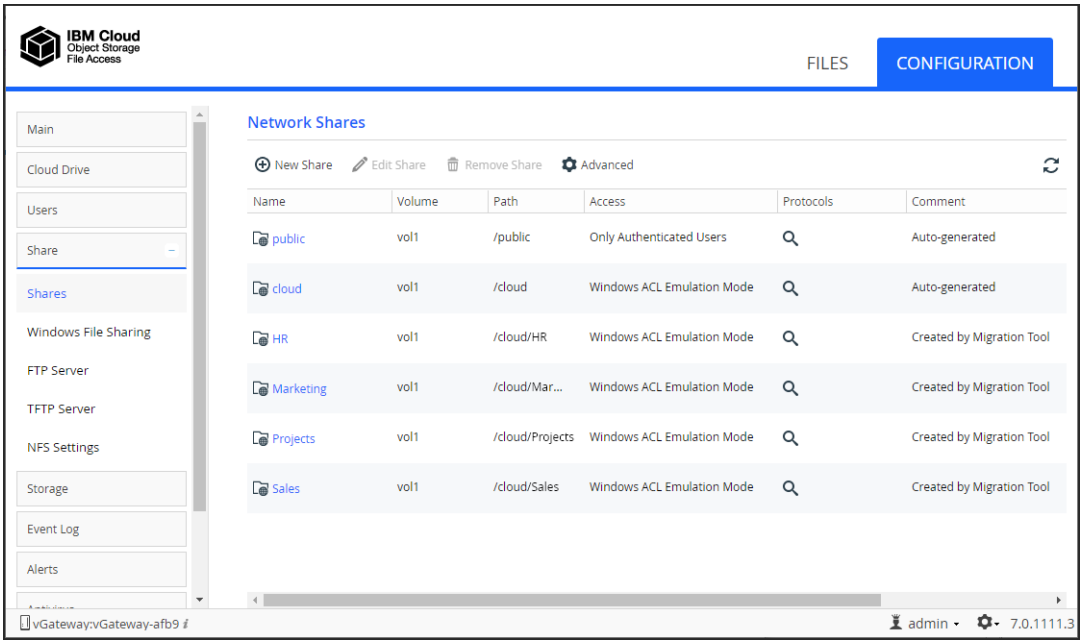
15 Click to display the list of every time this job was run with the results of each run, including the start and end times for the job, the number of files migrated and the total size of the migration, access to the report and the ability to download the log, which provides information about the migration and any errors that occurred during the migration.

16 Optionally, in the dashboard you can select a job and click to delete it.
After deleting a job, you can display all the jobs including the deleted jobs by clicking the **Deleted** filter in the dashboard.

You can restore deleted jobs by selecting the deleted jobs to restore and clicking .

The share structure from the source is recreated on the IBM COS FA Gateway, including nested shares and their permissions. If there are any recoverable errors during the copy process, retry the migration for the failed shares.

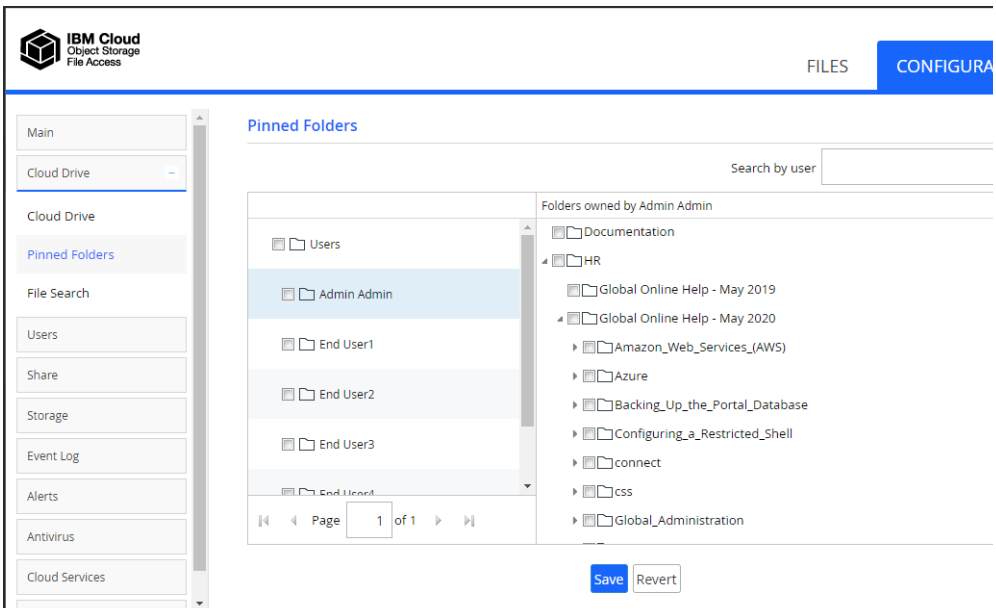
Note: Only ACLs are migrated with the files. Extended attributes are not migrated. In the IBM COS FA Gateway the shares are defined with Windows ACL Emulation Mode, as in the following example.



Unless the migration is completed when there is no access to the original file server, after completing the migration there may well be a number of new or changed files on the original file server that require migrating. Continue the migration process using the following procedure.

To complete a migration:

1. During off-peak hours, disconnect the filer server.
2. In the IBM COS FA Gateway user interface, pin the folders that you want to remain local to the IBM COS FA Gateway.
   a. In the **CONFIGURATION** tab, select **Cloud Drive > Pinned Folders** in the navigation pane. The **Pinned Folders** page is displayed.



The **Pinned Folders** area is separated into a users pane and folders pane, with paging in the users pane. This makes it easier to page through the users and select the folders to pin.

b Select a user to display the folders owned by the user and then select the folders that you want pinned for this user, so that the folder content is always available on the IBM COS FA Gateway. In addition, you can use the search field to jump to a specific user.

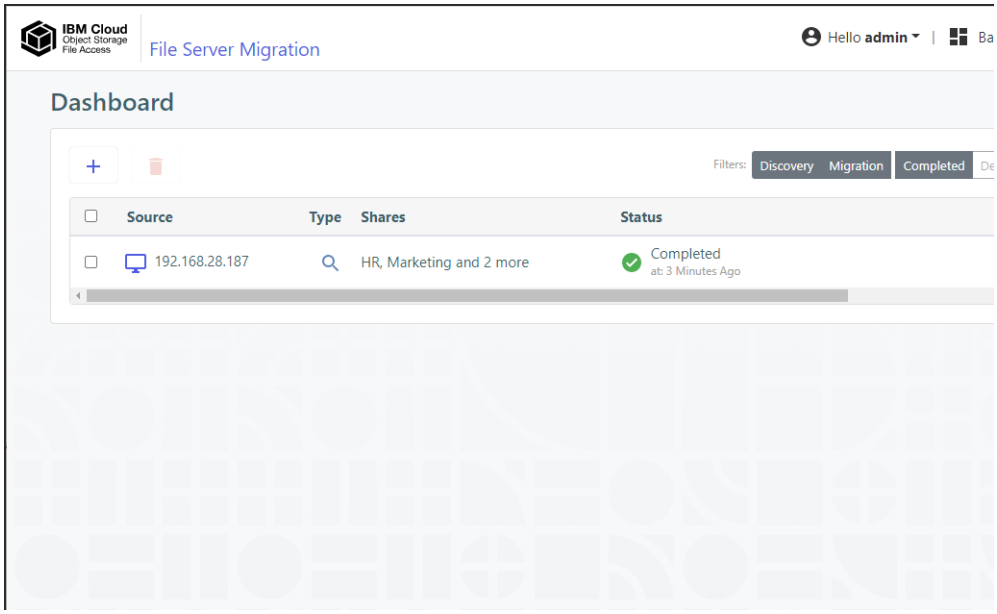
Note: You can select a a user to select all the folders and subfolders owned by the user. You can also select a higher level folder to select all the subfolders under it and then uncheck specific folders to unpin them. If you check a cloud folder, all the subfolders under the cloud folder are pinned and any folders added later under the cloud folder will be pinned automatically.

c Click **Save**.

The checked folders are pinned.

3 In the **CONFIGURATION** tab's **Main > Home** page, click **File Server Migration**.

The **File Server Migration** page is displayed.



4 Click  to rerun the migration (if needed, scroll to the end of the job for the button).

The migration reruns, migrating the deltas from the last migration.

Direct all the users to the IBM COS FA Gateway.

Users can now access and work on the IBM COS FA Gateway.