

IBM COS FA Portal
Version 6.1.0

SETUP GUIDE FOR VMWARE ESXI



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

© Copyright International Business Machines Corporation 2020.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

CHAPTER 1. PLANNING YOUR INSTALLATION	1
Scalability and Load Balancing.....	1
Data Replication and Failover.....	1
Security.....	2
Requirements	2
CHAPTER 2. INSTALLING IBM COS FA PORTAL	5
Importing the IBM COS FA Portal OVA File	5
Preparing for Production Deployment	6
Logging In to the IBM COS FA Portal Server	6
Configuring Network Settings	6
Additional Installation Instructions for Customers Without Internet Access.....	15
CHAPTER 3. CONFIGURING THE IBM COS FA PORTAL MASTER SERVER.....	16
Performing Initial IBM COS FA Portal Setup	16
Installing an SSL Certificate.....	20
Creating DNS Records.....	27
Configuring a Public NAT Address	28
Installing the License Key	30
Setting Up the Time Zone.....	31
CHAPTER 4. INSTALLING ADDITIONAL IBM COS FA PORTAL SERVERS	32
CHAPTER 5. MANAGING IBM COS FA PORTAL SERVERS.....	36
Backing Up the IBM COS FA Portal	36
Backing Up the Database.....	36
Enabling FIPS	47
Enabling/Disabling Remote Support	47
Extending the IBM COS FA Portal Main Database or Catalog Node Storage Pool.....	47
Load Balancing IBM COS FA Portal Servers	48
Protecting the IBM COS FA Portal Main Database using vSphere HA	51
CHAPTER 6. UPGRADING IBM COS FA PORTAL	54

CHAPTER 1. PLANNING YOUR INSTALLATION

This guide describes how to install the IBM COS FA Portal, how to set it up for initial use, and how to perform a minor upgrade.

If you require assistance in setting up your IBM COS FA Portal, contact IBM support.

A IBM COS FA Portal installation comprises a cluster of one or more servers. Each server can host any combination of the following services:

- **Main database.** Only one server can host the main database. The server that hosts the main database is called the master server.
- **Catalog node.** A database service that stores file metadata. It can be hosted together with the main database or on a separate server.
- **Application service.** This service accepts connections and handles requests from Web and CTTTP clients.
- **Database replication server.** A passive database service set to replicate an active database server (main database or a catalog node). During server installation, you can turn on the replication service and select the database server from which to replicate.

By default, the first installed server is a master server, hosting the main database, application server, and catalog node. You can install any number of additional servers, for [Scalability and Load Balancing](#) and for [Data Replication and Failover](#).

SCALABILITY AND LOAD BALANCING

IBM COS FA Portal is horizontally scalable. Additional servers can be added:

- As catalog node servers, to increase metadata storage handling capacity and performance.
- As application servers, to increase client handling capacity. Any servers that are enabled as application servers automatically balance the connected clients between them, allowing for maximized capacity and availability.

DATA REPLICATION AND FAILOVER

The main database and catalog node services are stateful and any servers hosting these services contain critical data. You must replicate all such servers to maintain the availability of critical data. The application service is stateless, and therefore, any dedicated application servers do not require replication or backup. Failover between application servers is automatic.

For details about replicating the database, see [Backing Up the Database](#).

IBM COS FA Portal includes a built-in replication function for achieving higher level of availability. For more information, refer to the document *Configuring Database Backup and Replication*.

Replication can be achieved using other platform dependent replication methods (such as SAN or VMWare-level replication).

SECURITY

All internal communications between IBM COS FA Portal servers is authenticated to prevent unauthorized access. Nevertheless, to follow the *defense in-depth* security philosophy, the master and catalog node servers, which store sensitive data, should be placed in their own firewalled, isolated network, and only the application server should be allowed to face the Internet.

REQUIREMENTS

Requirements for the VMWare ESXi platform

IBM COS FA Portal must be installed on a machine that meets the following requirements:

- The IBM COS FA Portal ESXi image, obtainable from IBM support.
- VMware ESXi 6.5 or later.
- The IBM COS FA Portal can be managed in VMware vCenter and in VMware vCloud Director.
- In a production environment, with a multi-node deployment, the application and database servers each require a 64-bit virtual machine with minimum 16GB RAM, 4 CPU cores and 110GB local hard disk drive. In a small or test environment, with a single server deployment, the requirement is a 64-bit virtual machine with minimum 8GB RAM, 2 CPU cores and 110GB local hard disk drive.
- The size of the database should be around 2% of the target data. IBM Recommends seeking guidance from IBM support for a more accurate estimation of the required database size.
- Access from the virtual machine to a Storage Area Network (SAN) or directly attached hard drives.
- The virtual disk, VMDK, attached to the IBM VMs running the IBM database, applicable for main database or catalog node, must yield a minimum of 700 TPS (transactions per second). To test the TPS on your installation, contact IBM support.

Note: All resources allocated to a server should be dedicated to that server and not shared with other servers. You must not run non-IBM COS FA Portal applications on any of the IBM COS FA Portal servers.

Requirements for administrator device

- Web browser: The latest two releases of Google Chrome, Apple Safari, Mozilla Firefox, and Microsoft Edge.
- SSH and SCP clients. For example, the freeware PuTTY.

Other Requirements

Prepare the following:

- A public DNS name for the IBM COS FA Portal installation.
- An SMTP mail server for sending notifications

Port requirements

To allow access to and from the Internet on the firewall on each machine that will operate as an application server or database server, ensure the following network ports are open:

Port	Protocol	Direction	Notes
22	TCP	Inbound and Outbound	SSH. IBM recommends limiting SSH access to specific IP addresses that may require access to the IBM COS FA Portal application servers, for example to perform scheduled maintenance and support related work.
53	UDP	Inbound and Outbound	DNS
80	TCP	Inbound and Outbound	HTTP
123	UDP	Outbound	NTP
443	TCP	Inbound and Outbound	HTTPS
995	TCP	Inbound	CTTP. Communications with IBM COS FA Gateways.
xx ^a	TCP	Outbound	SMTP

a. Use the port number that is used at your site for SMTP. The default port for SMTP is 25.

The following ports must be opened towards storage nodes:

Port	Protocol	Direction	Notes
80	TCP	Outbound	IBM COS FA Portal local filesystem
80 or 443 (for HTTPS)	TCP	Outbound	Object Storage ^a
111, 2049	TCP	Outbound	NFS

a. When **Direct Mode** is set for the storage node, only HTTPS is available

If you are running a separated environment that consists of multiple IBM COS FA Portal servers residing on separate firewalled network segments, open the following additional ports between the IBM COS FA Portal servers. These ports do not need to be accessible from the Internet:

Port	Protocol	Direction	Notes
22	TCP	Inbound and Outbound	SSH management between the servers.
443	TCP	Inbound and Outbound	Updates between the servers.
5432	TCP	Inbound	PostgreSQL. Applicable for master server, catalog nodes and database replication servers only.

If IBM COS FA Portal will be connected to Active Directory, open the following ports towards the Active Directory servers

Port	Protocol	Direction	Notes
53	TCP/UDP	Outbound	DNS
389	TCP/UDP	Outbound	LDAP/LDAP GC (Global Catalog)
3268	TCP		
636, 3269	TCP	Outbound	LDAP and LDAP GC with SSL ^a

a. IBM recommends using LDAP and LDAP GC with SSL instead of LDAP and LDAP GC.

IBM COS FA Portal requires the following port open for RSync for database replication between the main and secondary databases. This port does not need to be accessible from the Internet:

Port	Protocol	Direction	Notes
873	TCP	Inbound	—

IBM COS FA Portal requires the following port open for antivirus scanning. This port does not need to be accessible from the Internet:

Port	Protocol	Direction	Notes
1344	TCP	Outbound	—

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

CHAPTER 2. INSTALLING IBM COS FA PORTAL

Use the following workflow to install IBM COS FA Portal on each server.

- 1 [Importing the IBM COS FA Portal OVA File.](#)
- 2 [Preparing for Production Deployment.](#)
- 3 [Logging In to the IBM COS FA Portal Server](#) and changing the password.
- 4 [Configuring Network Settings.](#)
- 5 [Additional Installation Instructions for Customers Without Internet Access](#)
- 6 For the first server you install, follow all of the steps in [Configuring the IBM COS FA Portal Master Server.](#)
- 7 For any additional servers beside the master server, configure the server as an additional server as described in [Installing Additional IBM COS FA Portal Servers.](#)
- 8 Make sure that you replicate the database, as described in [Backing Up the Database.](#)

Note: You can use snapshots block-storage-level snapshots for backup, but snapshots are periodical in nature, configured to run every few hours. Therefore, using snapshots, you cannot recover the metadata to any point-in-time, and can lose a significant amount of data on failure. Also, many storage systems do not support block-level snapshots and replication, or do not do so efficiently.

IMPORTING THE IBM COS FA PORTAL OVA FILE

Contact IBM, and request the latest ESXi IBM COS FA Portal OVA file.

Note: The following procedure uses the vSphere Client. You can also use the vSphere Host Client. When using the vSphere Host Client, because the OVA file is larger than 2GB, you must unpack the OVA file, which includes the OVF file, VMDK and MF files. Use the OVF and VMDK files to deploy the IBM COS FA Portal.

To install the IBM COS FA Portal Server using the vSphere Client console:

- 1 In the vSphere Client console click **File > Deploy OVF Template**. The **Deploy OVF Template** wizard is displayed.
- 2 Browse to the IBM COS FA Portal OVA file and choose it.
- 3 Click **NEXT**.
- 4 Continue through the wizard specifying the following information, as required for your configuration:
 - A name to identify the IBM COS FA Portal in vCenter.
 - The location for the IBM COS FA Portal: either a datacenter or a folder in a datacenter.
 - The host or cluster to run the IBM COS FA Portal.
 - The virtual disk format for the IBM COS FA Portal software and the storage to use for this software. Refer to VMware documentation for a full explanation of the disk provisioning formats. Select either **Thick Provision Lazy Zeroed** or **Thick Provision Eager Zeroed** according to your preference.

Thick Provision Lazy Zeroed – Creates a virtual disk in a default thick format. Space required for the virtual disk is allocated when the virtual disk is created. Data remaining on the device is not erased during creation, but is zeroed out on demand at a later time on first write from the virtual machine. Using the default flat virtual disk format does not zero out or eliminate the possibility of recovering deleted files or restoring old data that might be present on this allocated space.

Thick Provision Eager Zeroed – Creates a virtual disk that supports clustering features such as Fault Tolerance. Space required for the virtual disk is allocated at creation time. In contrast to the flat format, the data remaining on the device is zeroed out when the virtual disk is created. It might take much longer to create disks in this format than to create lazy zeroed disks.

- The network that the IBM COS FA Portal will use.
- 5 Review the configuration details and click **FINISH**.
The IBM COS FA Portal is created and powered off.
 - 6 Start the IBM COS FA Portal virtual machine.

PREPARING FOR PRODUCTION DEPLOYMENT

- When deploying a main database server or a catalog node to production: It is recommended to remove the default 50GB and 60GB VMDKs included in the IBM COS FA Portal OVA, and attach a VMDK sized 2% of the overall cloud storage you intend to allocate for the service. Prior to going to production, contact IBM Support to evaluate whether the attached drive's performance meets IBM COS FA Portal's main database and catalog node performance requirements.
- When deploying an application server to production: It is recommended to remove the default 60GB VMDK included in the IBM COS FA Portal OVA.

LOGGING IN TO THE IBM COS FA PORTAL SERVER

To log in to the IBM COS FA Portal server:

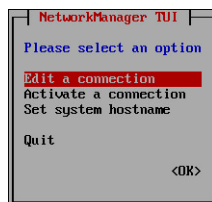
- Log in as the **root** user using SSH.
The default password is **portal321**.
You are prompted to change the password on your first login.

CONFIGURING NETWORK SETTINGS

By default, the IBM COS FA Portal server obtains an IP address using DHCP. In a production environment it is recommended to use a static IP address. Also when your infrastructure includes more than one network, you have to configure IBM COS FA Portal for the appropriate network. You configure network settings by using **nmmtui**, the built-in network manager.

To use **nmmtui**:

- 1 Log in as **root**, using SSH or through the console.
- 2 Run the following command: **nmmtui**
The **NetworkManager TUI** screen is displayed.

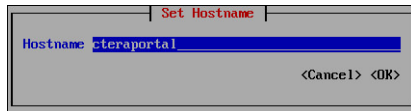


- 3 Use your keyboard arrows or the **TAB** key to navigate between options.

Changing the IBM COS FA Portal Server's Hostname

To change the IBM COS FA Portal server's hostname:

- 1 In nmtui, navigate to **Set system hostname** and press **Enter**.
The **Set Hostname** screen opens, displaying the current IBM COS FA Portal hostname.
- 2 In the field provided, type the server hostname.



- 3 In the field provided, enter the server hostname.
- 4 Navigate to **OK** and press **Enter**.
A confirmation message is displayed.
- 5 Press **Enter**.
The new hostname is configured.
- 6 Navigate to **Quit** and press **Enter** to exit nmtui.
- 7 You need to reboot the system for the change to take effect. You can reboot the system by entering the command: `reboot`

Configuring a Network Interface

Listing Network Interfaces

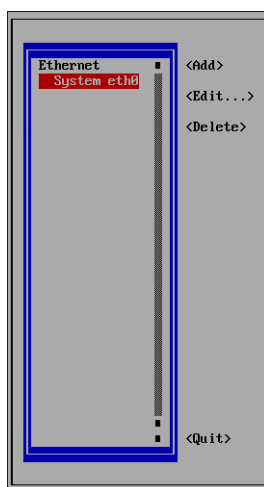
To list all network interfaces:

- Run the following command: `ifconfig`

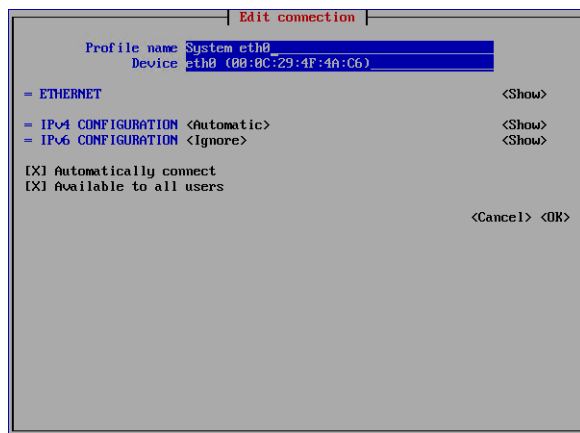
Configuring a Static IP Address for a Network Interface

To configure a static IP address for a network interface:

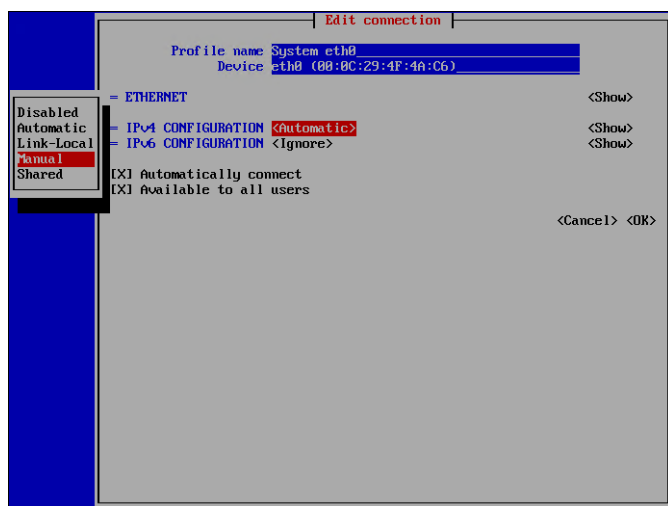
- 1 In nmtui, navigate to **Edit a connection** and press **Enter**.
The following window opens, displaying all network adapters attached to the IBM COS FA Portal server.



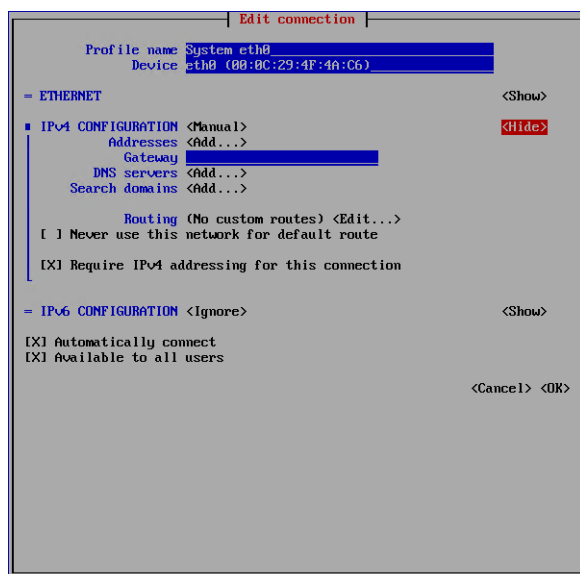
- 2 Navigate to the network adapter for which you want to set a static IP address and press **Enter**.
The **Edit connection** window is displayed.



- 3 Navigate to **Automatic** next to **IPv4 CONFIGURATION**, press **Enter**, and then select **Manual**.



- 4 Navigate to **Show** next to **IPv4 CONFIGURATION** and press **Enter**. Additional fields are displayed.



5 Navigate to **Add** next to **Addresses** and press **Enter**.

6 Type the static IP address.

To specify a subnet mask, use the classless inter-domain routing (CIDR) notation. For example:

- To set a class C subnet mask [255.255.255.0], use: *IP_Address/24*, for example, 192.168.93.204/24
- To set a class B subnet mask [255.255.0.0], use: *IP_Address/16*, for example, 192.168.93.204/16

You can refer to the following link for a full IPv4 CIDR reference:

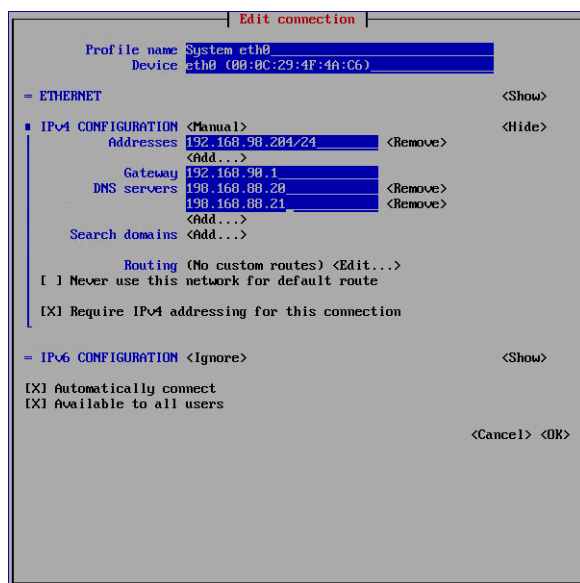
https://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing#IPv4_CIDR_blocks

7 To configure a default gateway for the current network interface, navigate to **Gateway**, and then type the IP address of the default gateway.

8 To configure a DNS server, navigate to **Add** next to **DNS servers**, press Enter, and then enter the IP address of the DNS server.

Note: You can add multiple DNS servers if desired, by repeating this step.

In the following example, the network interface named eth0 has the static IP address 192.168.98.204, the default gateway address 192.168.90.1, and the two DNS servers 192.168.88.20 and 192.168.88.21.



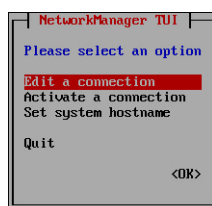
- 9 Navigate to **OK** and press **Enter**.
 - 10 Navigate to **Quit** and press **Enter** to exit nmtui.
 - 11 Restart the network service by typing the command: `service network restart`
- Your changes take effect.

Enabling DHCP for a Network Interface

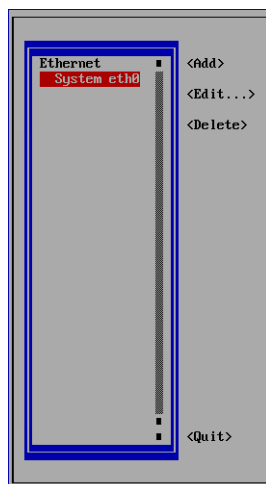
If you want to use DHCP, for example, for a demo, and you are configured to use a static IP, you can change to DHCP using nmtui.

To enable DHCP for a network interface:

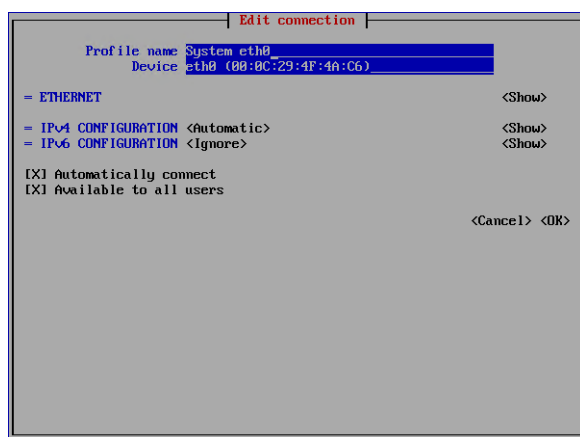
- 1 In nmtui, navigate to **Edit a connection** and press **Enter**.



The following screen opens, displaying all network adapters attached to the IBM COS FA Portal server.



- 2 Navigate to the network adapter for which you want to enable DHCP, and then press Enter. The **Edit connection** screen is displayed.



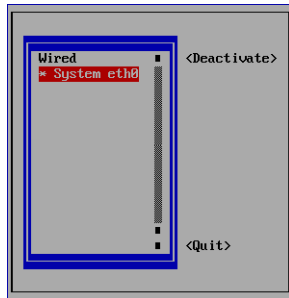
- 3 Navigate to **Manual** next to **IPv4 CONFIGURATION**, press Enter, and then select **Automatic**.
- 4 Navigate to **OK** and press Enter.
- 5 Navigate to **Quit** and press Enter to exit nmtui.
- 6 Restart the network service, by entering the command: `service network restart`

Your changes take effect.

Deactivating a Network Interface

To deactivate a network interface:

- 1 In nmtui, navigate to **Activate a connection** and press Enter.
The following screen opens, displaying all network adapters attached to the IBM COS FA Portal server.



The asterisk (*) to the left of a network adapter's name indicates that the network adapter is activated.

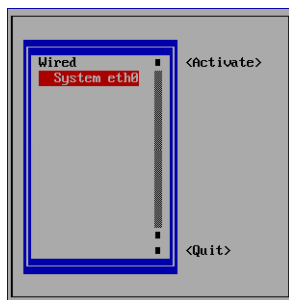
- 2 Navigate to the activated network adapter you want to deactivate, a network adapter with an asterisk, and press Enter.
- 3 Navigate to **Quit** and press **Enter** to exit nmtui.

The network adapter is deactivated.

Activating a Network Interface

To activate a network interface

- 1 In nmtui, navigate to **Activate a connection** and press Enter.
The following screen opens, displaying all network adapters attached to the IBM COS FA Portal server:



- 2 Navigate to the deactivated network adapter you want to activate, a network adapter without an asterisk, and press Enter.
- 3 Navigate to **Quit** and press **Enter** to exit nmtui.

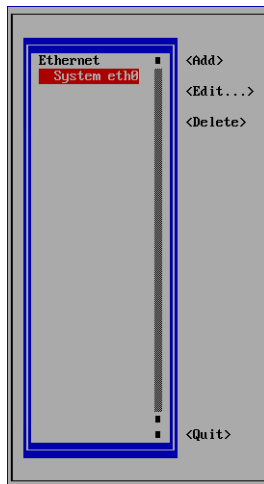
The network adapter is deactivated.

The asterisk (*) to the left of a network adapter's name indicates that the network adapter is activated.

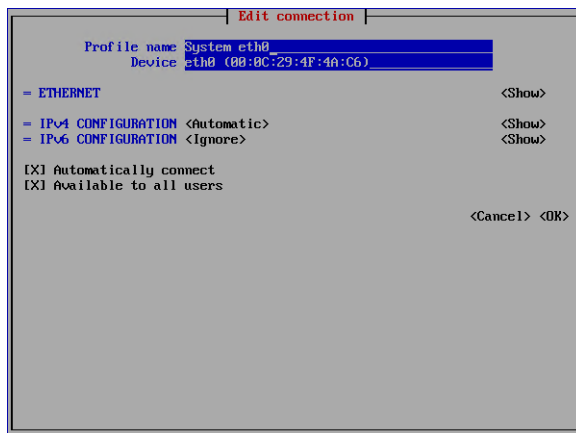
Configuring Static Routes

To configure a static route for a network interface:

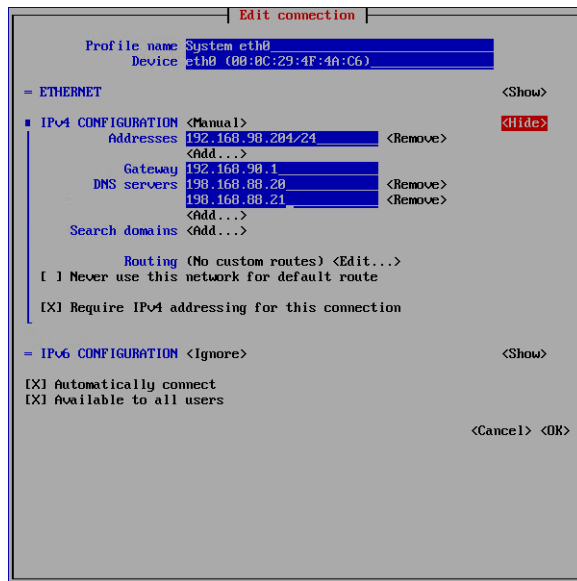
- 1 In nmtui, navigate to **Edit a connection** and press Enter.
The following screen opens, displaying all network adapters attached to the IBM COS FA Portal server.



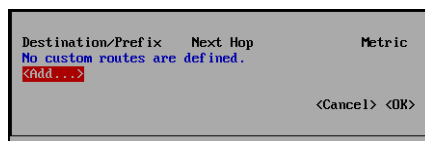
- 2 Navigate to the network interface for which you want to set a static route and press Enter.
The **Edit connection** screen is displayed.



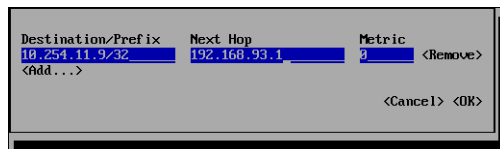
- 3 Navigate to **Show** next to **IPv4 CONFIGURATION** and press Enter.
Additional fields are displayed.



- 4 Navigate to **Edit** next to **Routing** and press **Enter**. The following screen is displayed.



- 5 Navigate to **Add** and press **Enter**.
- 6 In the fields provided, type the network destination/prefix, the next hop, and the route metric.



Note: To add another static route, navigate to **Add** and press **Enter**, and then specify the route details.

To remove an existing route, navigate to **Remove** next to the static route you want to remove and press **Enter**.

- 7 When done configuring static routes, navigate to **OK** and press **Enter**.
- 8 Navigate to **OK** and press **Enter**.
- 9 Navigate to **Quit** and press **Enter** to exit nmtui.
- 10 Restart the network service, by running the following command: `service network restart`. Your changes take effect.
- 11 To view the list of static routes, run the following command: `netstat -rn`

```

[root@portal ~]# netstat -rn
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
0.0.0.0 255.255.255.0 0.0.0.0 UG 0 0 0 eth0
192.168.12.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
255.255.255.0 0.0.0.0 255.255.255.255 UH 0 0 0 eth0
[root@portal ~]#

```

Configuring a Default Gateway

To set a default gateway for the IBM COS FA Portal server:

- 1 Run the following command:
`echo "GATEWAY=default_gateway_ip_address" > /etc/sysconfig/network`
 Where *default_gateway_ip_address* is your default gateway IP address.
 For example: `echo "GATEWAY=192.168.90.1" > /etc/sysconfig/network`
- 2 Restart the network service, by running the following command: `service network restart`
 Your changes take effect.

ADDITIONAL INSTALLATION INSTRUCTIONS FOR CUSTOMERS WITHOUT INTERNET ACCESS

The IBM COS FA Portal image requires packages for enhanced syslog functionality. During a IBM COS FA Portal image installation, these packages are downloaded from the Internet and automatically installed. If you do not have access to the Internet, you can install these packages manually, using the archive file provided with the image installation file.

To install the syslog enhanced functionality archive:

- 1 Install the IBM COS FA Portal image with the latest image file, as described above, prior to running the setup wizard.
- 2 Copy the provided archive file, **exported_images.tar.gz**, to a local folder on the IBM COS FA Portal machine.
- 3 Run the following CLI command on all servers (including main, Replica, and DB servers):
`portal-syslog-client load_images images_archive_path`
 where *images_archive_path* is the path to the local folder where you copied the archive file.
- 4 Run the setup wizard.

Troubleshooting

If the setup wizard was run prior to loading the new packages, an error message is generated. To resolve it, run the CLI `portal-syslog-client load_images images_archive_path` and restart all servers.

Note: If you do not run the CLI command, the enhanced syslog functionality will not work and an error message is generated. For these reasons it is recommended to run the command, however if you don't, apart from the error message, there is no impact on IBM COS FA Portals where syslog functionality is not used.

CHAPTER 3. CONFIGURING THE IBM COS FA PORTAL MASTER SERVER

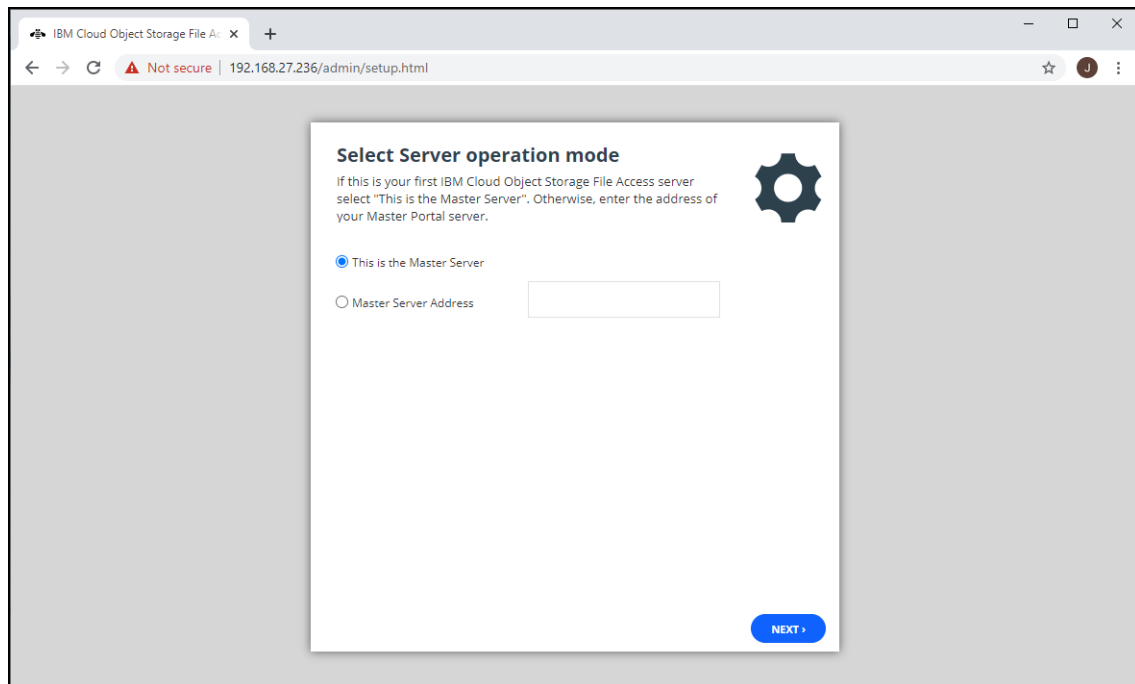
Configuring the master server is a one-time operation, the first time you access the IBM COS FA Portal. If you are installing an additional server, proceed directly with [Installing Additional IBM COS FA Portal Servers](#).

PERFORMING INITIAL IBM COS FA PORTAL SETUP

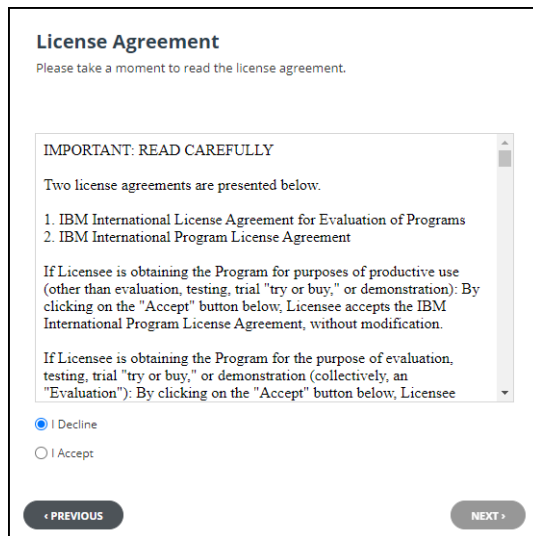
This procedure is performed only once, on the master server.

To perform initial IBM COS FA Portal setup of the master server:

- 1 Using a Web browser, browse to the IBM COS FA Portal, via the IP address or public DNS. The **Setup** wizard opens, displaying the **Select Server operation mode** window.



- 2 Choose **This is the Master Server**.
- 3 Click **Next**.



License Agreement

Please take a moment to read the license agreement.

IMPORTANT: READ CAREFULLY

Two license agreements are presented below.

1. IBM International License Agreement for Evaluation of Programs
2. IBM International Program License Agreement

If Licensee is obtaining the Program for purposes of productive use (other than evaluation, testing, trial "try or buy," or demonstration): By clicking on the "Accept" button below, Licensee accepts the IBM International Program License Agreement, without modification.

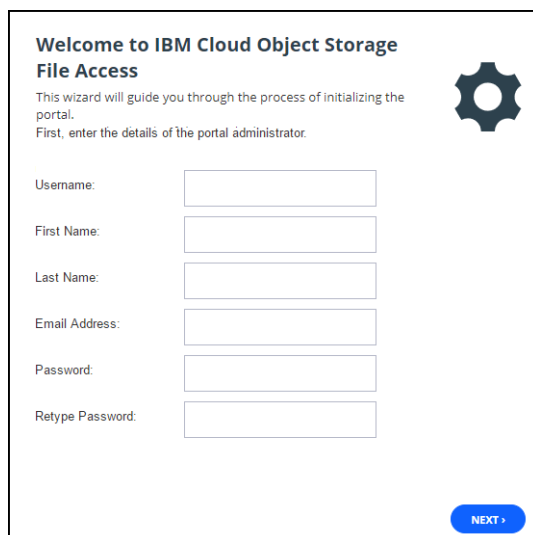
If Licensee is obtaining the Program for the purpose of evaluation, testing, trial "try or buy," or demonstration (collectively, an "Evaluation"): By clicking on the "Accept" button below, Licensee

☒ I Decline
☐ I Accept

[< PREVIOUS](#) [NEXT >](#)

4 Accept the license and click **Next.**

The database is initialized and then the **Welcome to IBM COS FA Portal** dialog box is displayed.



Welcome to IBM Cloud Object Storage File Access

This wizard will guide you through the process of initializing the portal.

First, enter the details of the portal administrator.



Username:

First Name:

Last Name:

Email Address:

Password:

Retype Password:

[NEXT >](#)

5 Complete the fields as follows:

Username – The name for your IBM COS FA Portal administrator account.

First Name – The first name of the administrator.

Last Name – The last name of the administrator.

Email Address – The email address of the administrator for notifications.

Password – The password administrator will use to access the IBM COS FA Portal.

Retype Password – The password.

6 Click **Next.**

The **Email Settings** window is displayed.

Email Settings
Specify the settings to use when sending an email message.

SMTP Server:

SMTP Port:

Sender:

☐ Enable TLS

☐ Server Requires Authentication

Username:

Password:

[< PREVIOUS](#) [NEXT >](#)

7 Complete the fields as follows:

SMTP Server – The outgoing mail server address for sending email messages from IBM COS FA Portal to users.

SMTP Port – The port number for sending email messages from IBM COS FA Portal to users. This port is usually TCP 25.

Sender – The email address that should appear in the From field of notifications. For example: *IBM Customer Service <support@IBM.com>*.

Enable TLS – Select this option to use Transport Layer Security (TLS) encryption for sending email messages from IBM COS FA Portal to users.

Server requires authentication – Select this option if the SMTP server requires authentication.

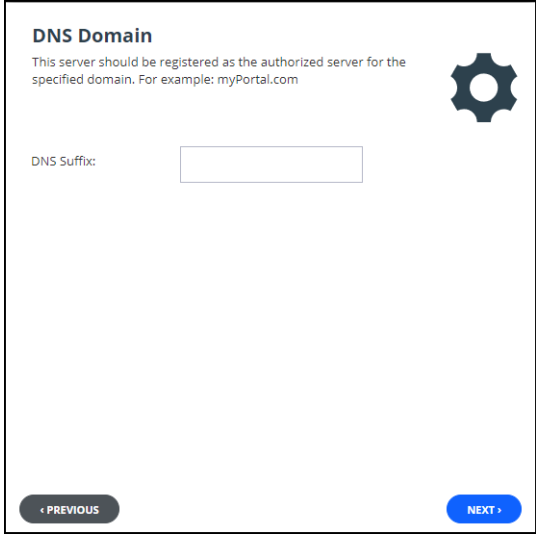
User Name – Type the user name that IBM COS FA Portal should use when authenticating to the SMTP server.

Password – Type the password that IBM COS FA Portal should use when authenticating to the SMTP server.

Warning: The username and password you specified for the IBM COS FA Portal administrator are sent to the email address using the information specified here. If the address is incorrect, the email will not arrive and if you have not recorded the administrator username and password details and they are forgotten, you will not be able to access the IBM COS FA Portal.

8 Click Next.

The **DNS Domain** window is displayed.



DNS Domain

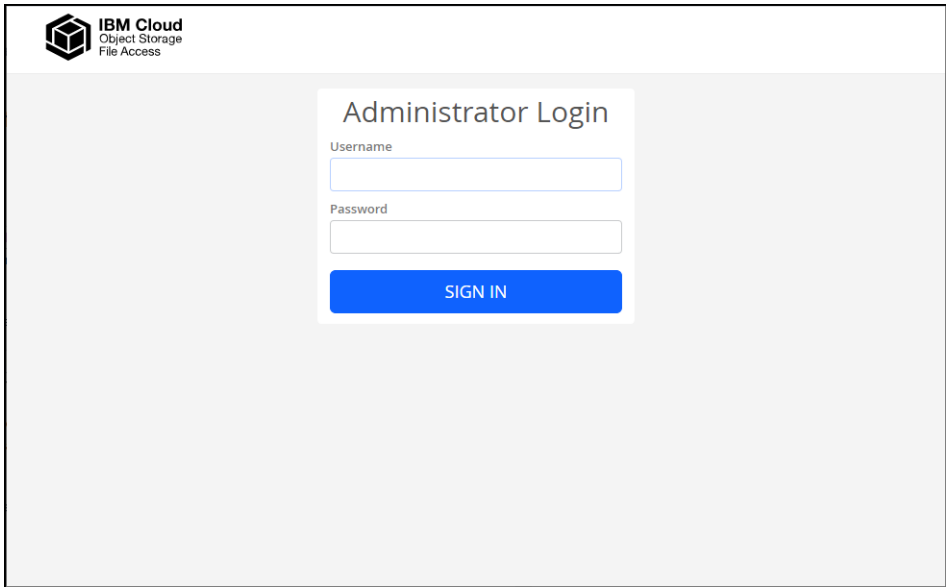
This server should be registered as the authorized server for the specified domain. For example: myPortal.com

DNS Suffix:

◀ PREVIOUS

NEXT >

- 9 In the **DNS Suffix** field, type the DNS suffix to append to each virtual IBM COS FA Portal's name, in order to create the virtual IBM COS FA Portal's DNS name.
For example, if a virtual IBM COS FA Portal's name is *myportal*, and the DNS suffix is *example.com*, then the virtual IBM COS FA Portal's DNS name is *myportal.example.com*.
- 10 Click **Next**.
The **Wizard Completed** window is displayed.
- 11 Click **Finish**.
The data is saved and a success message is displayed.
- 12 Click **OK**.
IBM COS FA Portal opens, displaying the **Administrator Login** page.



IBM Cloud
Object Storage
File Access

Administrator Login

Username

Password

SIGN IN

- 13 Enter the user name and password you specified in the Setup Wizard.
- 14 Click **SIGN IN**.
The IBM COS FA Portal opens, displaying the **Main > Dashboard** page. By default, IBM COS FA

Portal creates a team portal called *portal*.

Warning: The initial setup includes initializing the PostgreSQL database used by the IBM COS FA Portal. The database must be backed up. Backing up the database is described in [Backing Up the Database](#).

INSTALLING AN SSL CERTIFICATE

Perform the following steps to install a certificate on IBM COS FA Portal:

- 1 [Note your IBM COS FA Portal's DNS Suffix](#)
- 2 [Obtain an SSL Certificate](#)
- 3 [Generate a Certificate Signing Request](#)
- 4 [Sign the Certificate Request](#)
- 5 [Validate and Prepare Certificates for Upload](#)
- 6 [Install the Signed Certificate on IBM COS FA Portal](#)

Note your IBM COS FA Portal's DNS Suffix

Note your IBM COS FA Portal's DNS suffix so that you have it for later steps.

To view your IBM COS FA Portal's DNS suffix:

- 1 In the global administration view, select **Settings** in the navigation pane.
- 2 Select **Global Settings** under **SETTINGS** in the **Control Panel** page.
The **Global Settings** window is displayed.

The screenshot displays the 'Global Settings' window of the IBM COS FA Portal. The left sidebar contains a navigation menu with options: Main, Users, Provisioning, Settings (selected), Control Panel, License, Skins, Email Template, Seeding, Antivirus, Data Loss Prevention, and Logs & Audit. The main content area is titled 'Global Settings' and includes the following fields and sections:

- DNS Suffix:** A text input field containing 'c.me' with a small icon to its right.
- Timezone:** A dropdown menu showing '(GMT) Greenwich Mean Time : Dublin, Edinburgh, List' with a note '*Requires Restart'.
- Retain deleted portals for:** A text input field containing '30' followed by 'days'.
- Database Replication:** A section containing 'Alert when lag is more than: 60 seconds'.
- Administration Console:** A section containing 'Redirect from HTTP to HTTPS: ☒'.
- HTTPS Port:** A text input field containing '443' with a note '*Requires Restart'.
- End User Portal:** A section containing 'Redirect from HTTP to HTTPS: ☒'.
- Web Session Control:** A section with a text input field.

At the bottom right of the window are 'SAVE' and 'CANCEL' buttons. The bottom left corner shows the version '6.1.1170.8'.

- 3 The **DNS Suffix** field displays the IBM COS FA Portal's DNS suffix.

Obtain an SSL Certificate

It is necessary to obtain a valid certificate for production services signed either by a well-known certificate authority or by your own internal certificate authority.

Note: You can connect with a device to the IBM COS FA Portal using a dummy certificate. Using a dummy certificate is recommended for testing purposes only and user confirmation is required upon every attempt to connect to the IBM COS FA Portal in order to proceed with the connection.

If you intend to generate a signed certificate using your own internal certificate authority, contact IBM Support beforehand.

The SSL certificate can be either of the following:

- **A wildcard certificate**
A wildcard SSL certificate secures your website's URL and an unlimited number of its subdomains. For example, a single wildcard certificate for *.example.com can secure both company01.example.com and company02.example.com.
A wildcard certificate is mandatory if you plan for your service to consist of more than one virtual IBM COS FA Portal.
- **A domain certificate**
A domain certificate secures a single domain or subdomain only. For example: company01.example.com.
This option is relevant if you are planning to provision a single virtual IBM COS FA Portal only.
Note: IBM COS FA Portal also supports certificates with Subject Alternative Names (SAN certificates). This option enables you to secure multiple domain names with a single certificate.

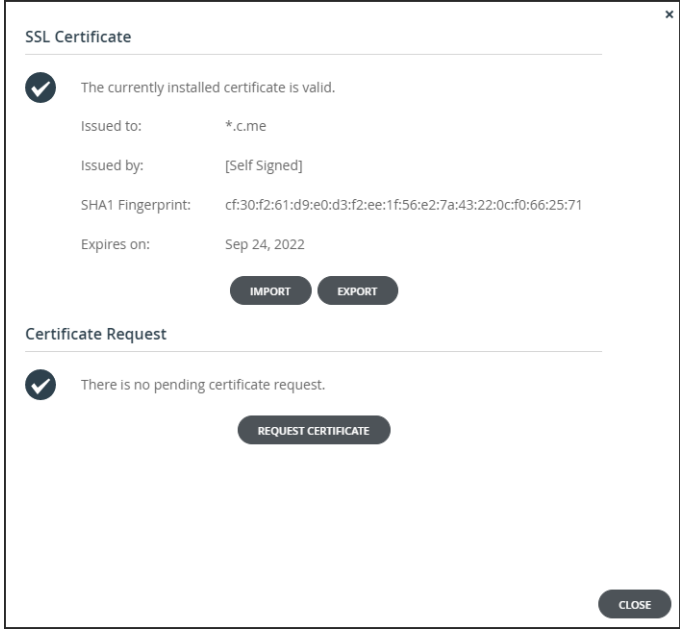
Generate a Certificate Signing Request

The next step is to generate a certificate signing request (CSR) for your domain using IBM COS FA Portal. This requires a IBM COS FA Portal Administrator account.

Warning: IBM COS FA Portal generates a built-in certificate that is not suitable for production. This certificate is valid for testing purposes only, as it is not signed by a well-known certificate authority.

To generate a certificate signing request for your domain:

- 1 In the global administration view, select **Settings** in the navigation pane.
- 2 Select **SSL Certificate** under **SETTINGS** in the **Control Panel** page.
The **SSL Certificate** window is displayed.



SSL Certificate

✓ The currently installed certificate is valid.

Issued to: *.c.me

Issued by: [Self Signed]

SHA1 Fingerprint: cf:30:f2:61:d9:e0:d3:f2:ee:1f:56:e2:7a:43:22:0cf0:66:25:71

Expires on: Sep 24, 2022

IMPORT EXPORT

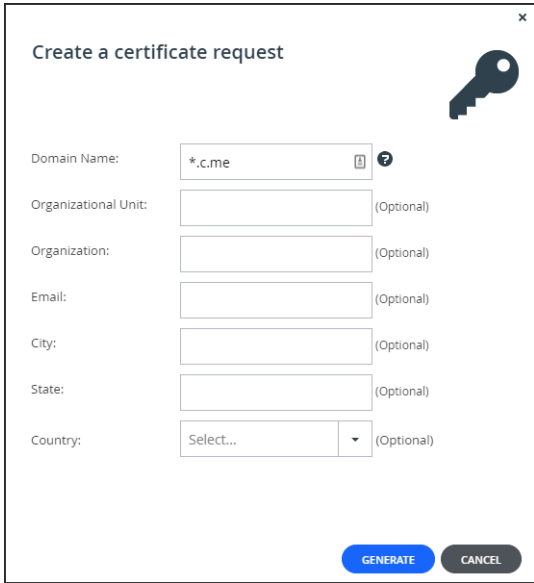
Certificate Request

✓ There is no pending certificate request.

REQUEST CERTIFICATE

CLOSE

- 3 Click **REQUEST CERTIFICATE**.
The **Create a Certificate Request** window is displayed.



Create a certificate request

Domain Name: *.c.me ⓘ ?

Organizational Unit: (Optional)

Organization: (Optional)

Email: (Optional)

City: (Optional)

State: (Optional)

Country: Select... (Optional)

GENERATE CANCEL

- 4 Specify the following mandatory field:
Domain Name – The domain name for which you would like to request a certificate.
The value entered must match the type of certificate you chose to use. For example, if you chose a wildcard certificate, the domain name might be *.ibm.com. If multiple virtual IBM COS FA Portals are configured, each virtual IBM COS FA Portal has its own DNS name and the SSL certificate should be a wildcard certificate.
If you have only one IBM COS FA Portal, and do not intended to configure multiple virtual IBM COS FA Portals, then it is sufficient to purchase a regular SSL certificate and not a wildcard certificate.
To request a certificate that specifies multiple alternative names, type the multiple names in this

field, separated by semicolons. The certificate will include the subjectAltName certificate extension.

- 5 You can also specify the following optional fields:

Organizational Unit – The name of your organizational unit.

Organization – The name of your organization.

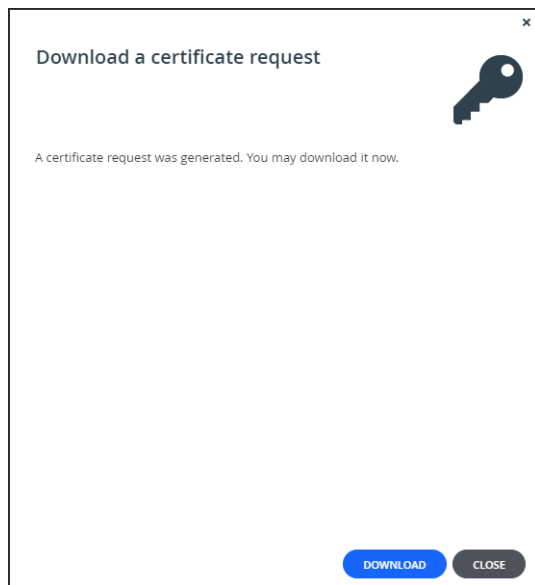
City – Your city.

State – Your state.

Country – Your country.

- 6 Click **GENERATE**.

A key pair is generated and stored on the IBM COS FA Portal and the **Download a certificate request** screen is displayed.

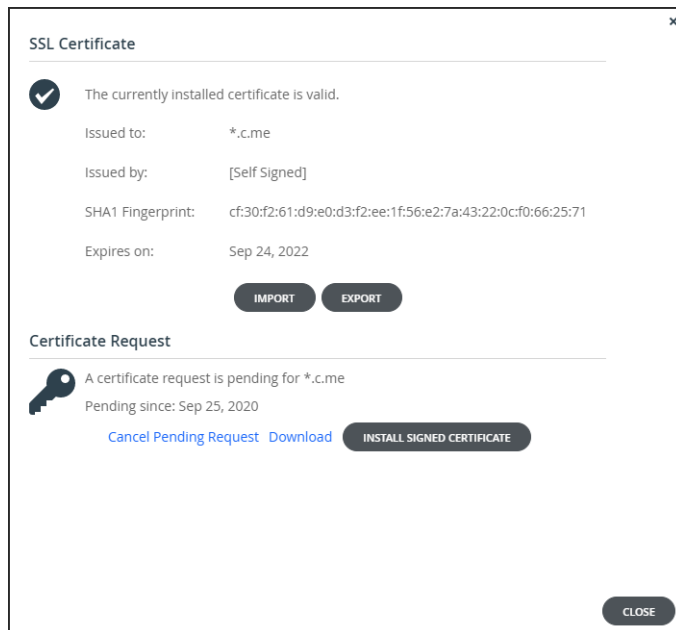


- 7 Click **DOWNLOAD**.

The certificate request file *certificate.req* is downloaded to your computer.

- 8 Click **CLOSE**.

The **SSL Certificate** window **Certificate Request** area indicates that the certificate request is pending.



Warning: When you generated the CSR, a `private.key` file was registered in the IBM COS FA Portal. If you now generate a new CSR, it will override the existing `private.key` file, and signing the old CSR will result in an error message indicating that the CSR does not match the `private.key` file. Therefore, do not generate a new CSR before installing the signed certificate.

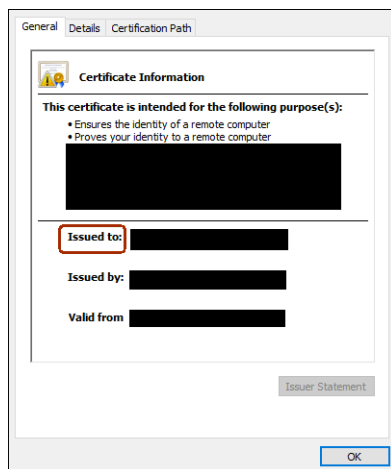
Sign the Certificate Request

To sign the certificate request:

- 1 Send the `certificate.req` file you generated to your certificate authority for signing. If the request is successful, the certificate authority will send back an identity certificate that is digitally signed with the certificate authority's private key.

Note: The certificate authority should return a base-64 encoded identity certificate.

- 2 Open the identity certificate and verify that the **Issued to** field includes the DNS suffix you provided upon creating the certificate request.



- 3 Build a certification chain from your identity certificate to your trusted root certificate. In order to do this, you will need to obtain all of the intermediate certificates, as well as your root

certificate authority's self-signed certificate.

If you are using a well-known certificate authority, the intermediate certificates and the root certificate authority's self-signed certificate can be downloaded from your certificate authority website. If you are using your own internal certificate authority, contact the necessary entity to provide you with the required intermediate and self-signed certificate.

Validate and Prepare Certificates for Upload

To validate and prepare certificates for upload:

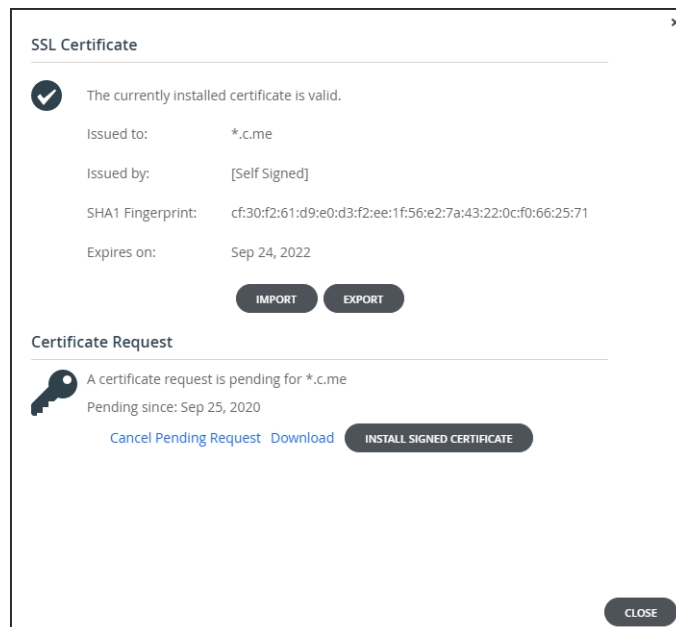
- 1 Verify that none of the certificates in the certificate chain are corrupted or using invalid encoding. To do so, open each certificate in a program such as Notepad or Word, and verify that it contains the following:

```
----- BEGIN CERTIFICATE -----
<CERTIFICATE CONTENT>
----- END CERTIFICATE -----
```
- 2 Rename the identity certificate issued to "*.ibm.com" to `certificate.crt`.
- 3 Change the file extension of the other certificates in the certificate chain to ".crt". For example, `certificate-name.crt`.
- 4 Archive all of the certificates – the identity certificate, the intermediary certificates, and the root self-signed certificate – in a ZIP file called `certificate.zip`.

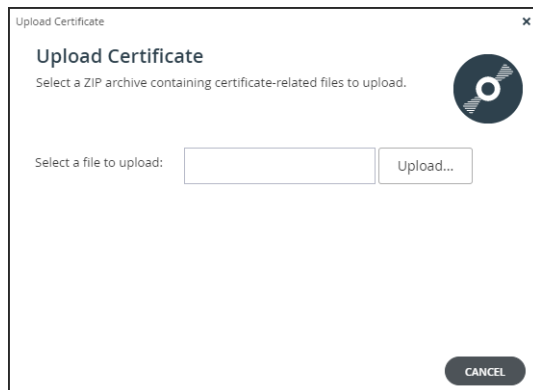
Install the Signed Certificate on IBM COS FA Portal

If you have a valid signed certificate, install it and replace the built-in certificate.

- 1 In the global administration view, select **Settings** in the navigation pane.
- 2 Select **SSL Certificate** under **SETTINGS** in the **Control Panel** page.
The **SSL Certificate** window is displayed. The **Certificate Request** area indicates that the certificate request is pending.



- 3 Click **INSTALL SIGNED CERTIFICATE**.
The **Upload Certificate** window is displayed.



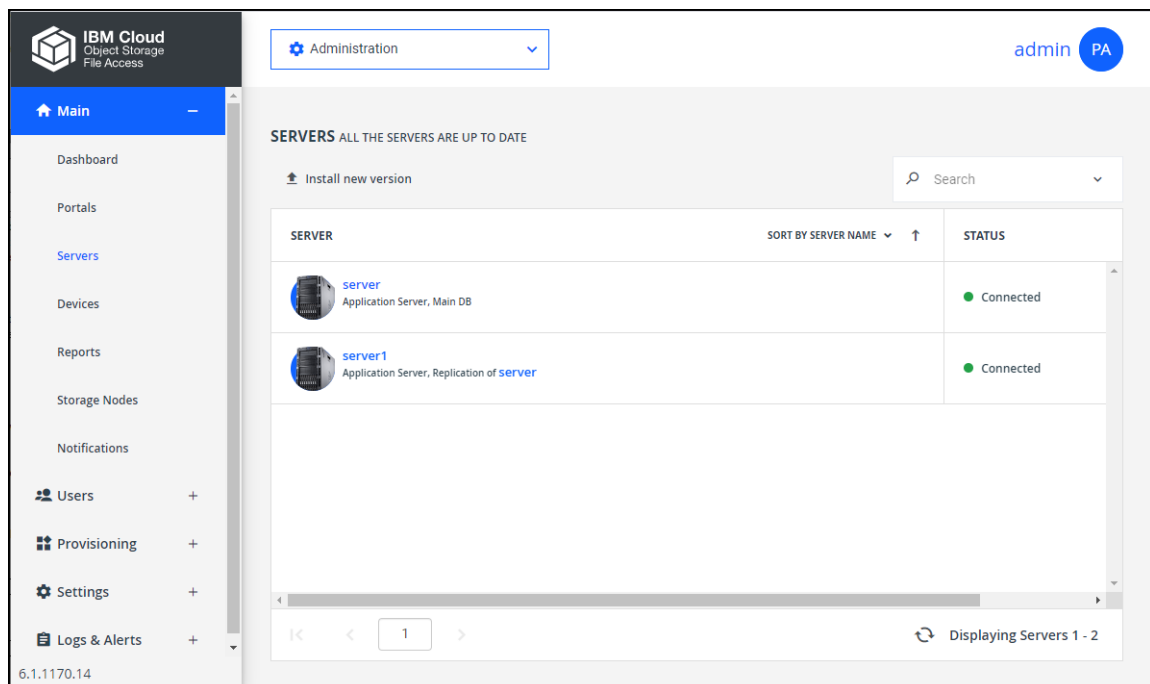
- 4 Click **Upload** and browse to the file you created.
All the certificates in the certificate chain must be present in the ZIP file in Base-64 encoded X.509 format, and each file must have a `.crt` extension.
- 5 Click **FINISH**.
The certificate is installed on IBM COS FA Portal.
- 6 Restart all the IBM COS FA Portal servers. See [Restart Servers](#).
- 7 Browse to your IBM COS FA Portal and verify that the certificate updated successfully.
You should not receive any security exception messages.

Restart Servers

IBM COS FA Portal servers can be restarted from the IBM COS FA Portal web page.

To restart a server:

- 1 In the global administration view, select **Main > Servers** in the navigation pane.
The **SERVERS** page is displayed, listing all the servers for the IBM COS FA Portal.



- 2 Select the server to restart and click **Restart**.

A confirmation window is displayed.

- 3 Click **RESTART** to confirm.

The server is restarted.

CREATING DNS RECORDS

The IBM COS FA Portal includes a built-in DNS server. This server automatically resolves the domain names of all the defined virtual IBM COS FA Portals, as well as names of devices using the remote access service. In order for this DNS server to work, you must register it using an NS (Name Server) record on your DNS server.

The procedure used for configuring the DNS for remote access depends on whether you have purchased a dedicated domain (the DNS suffix includes only records for the IBM COS FA Portal) or not (the DNS suffix includes records that are unrelated to the IBM COS FA Portal).

If you have a dedicated domain:

- If you have a dedicated domain for the IBM COS FA Portal – no servers other than the IBM COS FA Portal – then the NS record can be created just once, in that zone.
For example, for a DNS suffix called *storage.example.com* and two IBM COS FA Portal servers with IPs 123.168.0.3 (master) and 123.168.0.4 (secondary), you would register:

A	srv1.example.com	123.168.0.3
A	srv2.example.com	123.168.0.4

Next, you would create an NS record for each server to the zone *storage.example.com*:

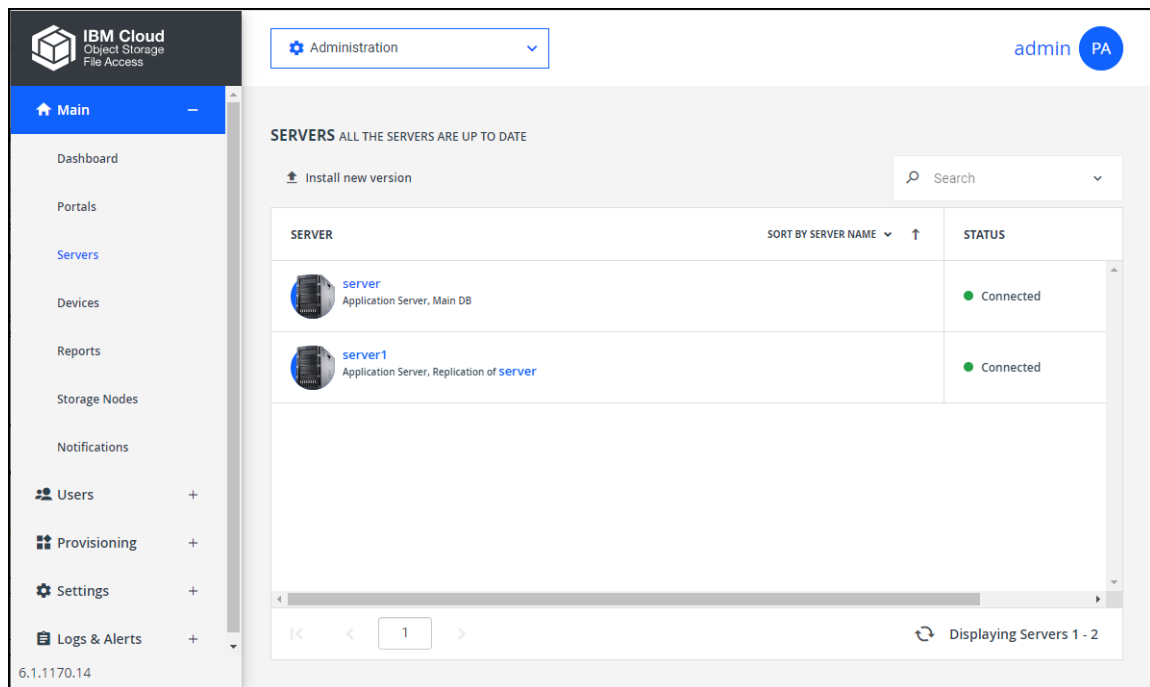
NS	storage.example.com	srv1.example.com
NS	storage.example.com	srv2.example.com

CONFIGURING A PUBLIC NAT ADDRESS

Immediately after deploying a IBM COS FA Portal instance, the IBM COS FA Portal server will respond to DNS requests with its private internal IP address. In order to make the IBM COS FA Portal available via the Internet, and to enable the IBM COS FA Portal to respond to DNS queries with the public IP address, you must configure the IBM COS FA Portal's public NAT address.

To configure a Public NAT address:

- 1 In the global administration view, select **Main > Servers** in the navigation pane. The **SERVERS** page is displayed, listing all the servers for the IBM COS FA Portal.



- 2 Click the server to edit.

The server window is displayed with the server name as the window title.

The screenshot shows a configuration window titled 'server' with a status bar indicating 'CONNECTED'. On the left is a sidebar with icons for 'General Settings' (selected), 'Address Mappings', 'Clients', 'DB Replication', and a heartbeat icon. The main area contains the following fields and options:

- Name:** A text box containing 'server'.
- Application server:** A checked checkbox.
- Antivirus Background Scanner:** An unchecked checkbox.
- Replication of:** An unchecked checkbox followed by a dropdown menu.
- Network section:**
 - Default Address:** A text box containing '192.168.27.221'.
 - Public NAT Address:** An unchecked checkbox followed by four empty text boxes for IP address segments.
- Advanced section:**
 - Read Cache Size Limit:** A text box containing '256' followed by 'MB'.

At the bottom are three buttons: 'DELETE', 'SAVE', and 'CANCEL'.

3 Check **Public NAT Address** and enter public IP address.

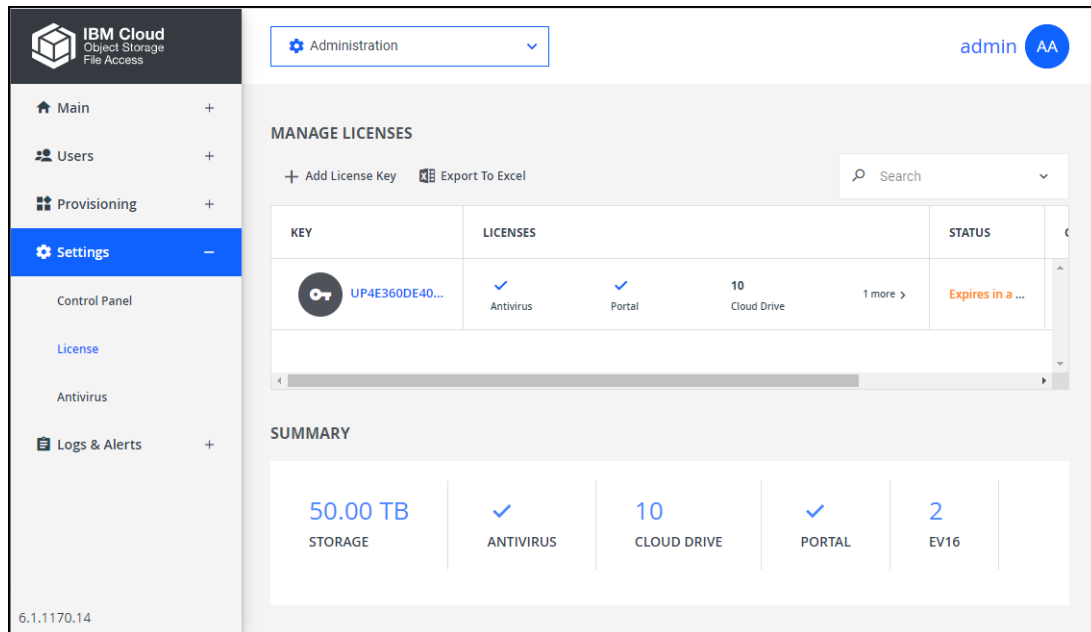
4 Click **SAVE**.

INSTALLING THE LICENSE KEY

Your IBM COS FA Portal includes a default license for 30 days. If you have a permanent license, install it using the following procedure.

To install a new license key:

- 1 In the global administration view, select **Settings > License** in the navigation pane. The **MANAGE LICENSES** page is displayed.



- 2 Click **Add license key**. The **Add License Keys** dialog box opens.

Add License Keys

Type or paste one or more license keys in text area below.

Type the license keys to add:

Comment (Optional):

SAVE **CANCEL**

- 3 Copy the license key you received from IBM, and paste it into the text box. The system verifies and activates the license key by contacting the IBM Activation service. When

the license key is activated, it is associated with this installation of IBM COS FA Portal.

- 4 Optionally add a comment In the **Comment** field.
The comment is displayed in the **License** page. You can use this comment to document the purchase order number associated with the license, and the like.
- 5 Click **Save**.

SETTING UP THE TIME ZONE

To configure the IBM COS FA Portal server's time zone:

- 1 In the global administration view, select **Settings** in the navigation pane.
- 2 Select **Global Settings** under **SETTINGS** in the **Control Panel** page.
The **Global Settings** window is displayed.

The screenshot shows the 'Global Settings' window of the IBM COS FA Portal. The left sidebar contains a navigation menu with options: Main, Users, Provisioning, Settings (highlighted), Control Panel, License, Skins, Email Template, Seeding, Antivirus, Data Log, and Logs & Reports. The main content area is titled 'Global Settings' and contains several sections:

- DNS Suffix:** A text field containing 'c.me' with a small icon to its right.
- Timezone:** A dropdown menu showing '(GMT) Greenwich Mean Time : Dublin, Edinburgh, List' with a downward arrow. To its right is the text '*Requires Restart'.
- Retain deleted portals for:** A text field containing '30' followed by the word 'days'.
- Database Replication:** A section header.
- Alert when lag is more than:** A text field containing '60' followed by the word 'seconds'.
- Administration Console:** A section header.
- Redirect from HTTP to HTTPS:** A checkbox that is checked.
- HTTPS Port:** A text field containing '443' with '*Requires Restart' to its right.
- End User Portal:** A section header.
- Redirect from HTTP to HTTPS:** A checkbox that is checked.
- Web Session Control:** A section header.

 At the bottom right of the window are two buttons: 'SAVE' (in blue) and 'CANCEL' (in gray). The bottom left corner of the window shows the version '6.1.1170.8'.

- 3 Select the correct time zone for the IBM COS FA Portal from the list.
- 4 Click **SAVE**.

CHAPTER 4. INSTALLING ADDITIONAL IBM COS FA PORTAL SERVERS

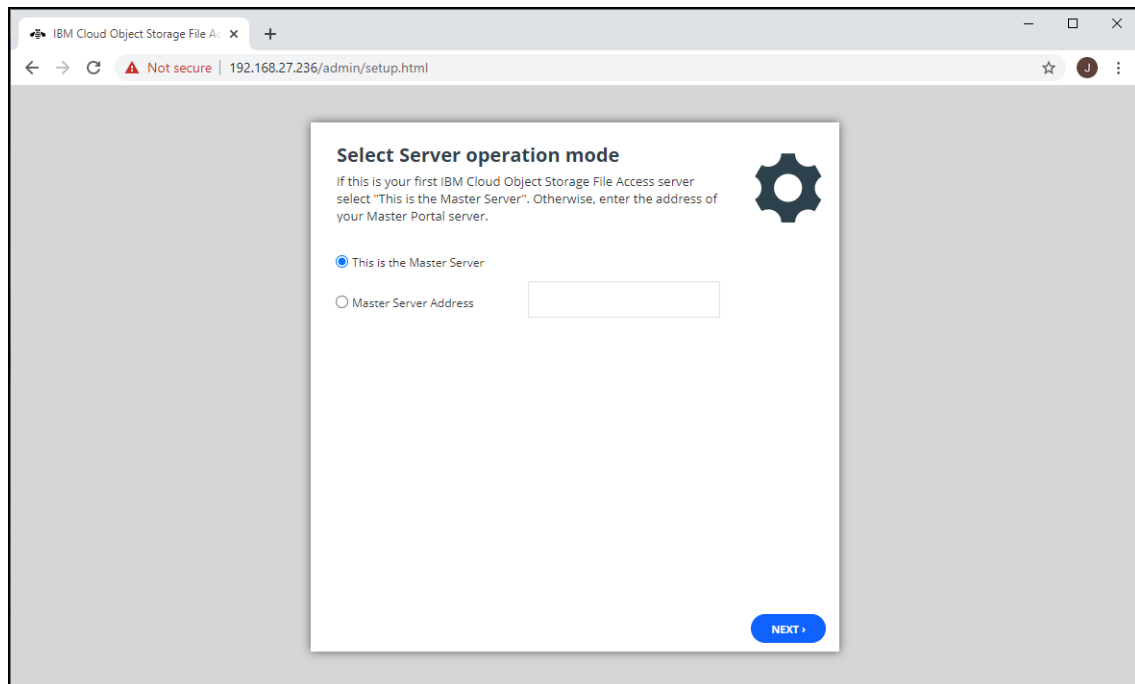
When installing an additional server, follow this procedure after performing the steps in [Installing IBM COS FA Portal](#). All servers except the master server are additional servers.

By default, the server will be an application server running no other service. After initial setup, the application service and catalog node service can each be enabled or disabled through the IBM COS FA Portal user interface. See the *IBM COS FA Portal Global Administrator Guide* for details.

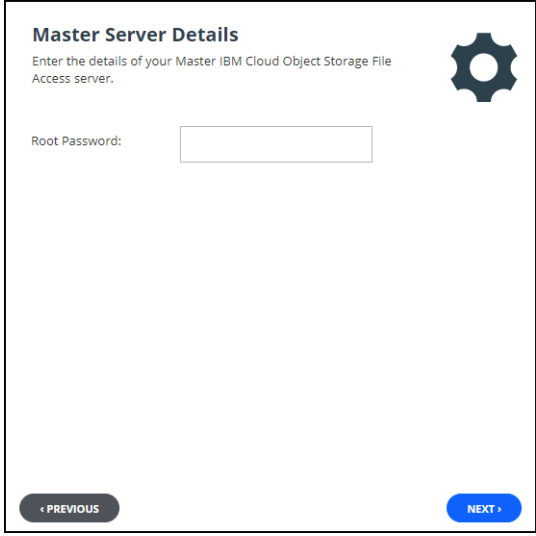
To configure an additional server:

Note: If the HTTPS administration port was changed on the master server, you must enable the relevant port on all servers.

- 1 Using a Web browser, browse to the new server, via the IP address or public DNS. The **Setup** wizard opens, displaying the **Select Server operation mode** window.



- 2 Choose **Master Server Address** and enter the address of the master server.
- 3 Click **Next**.



Master Server Details

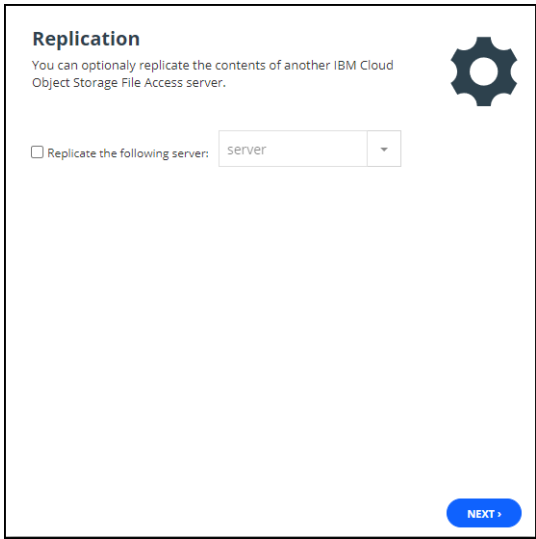
Enter the details of your Master IBM Cloud Object Storage File Access server.

Root Password:



[< PREVIOUS](#) [NEXT >](#)

- 4 Enter the root password for the master server and click **Next**. The server is started and the **Replication** window is displayed.



Replication

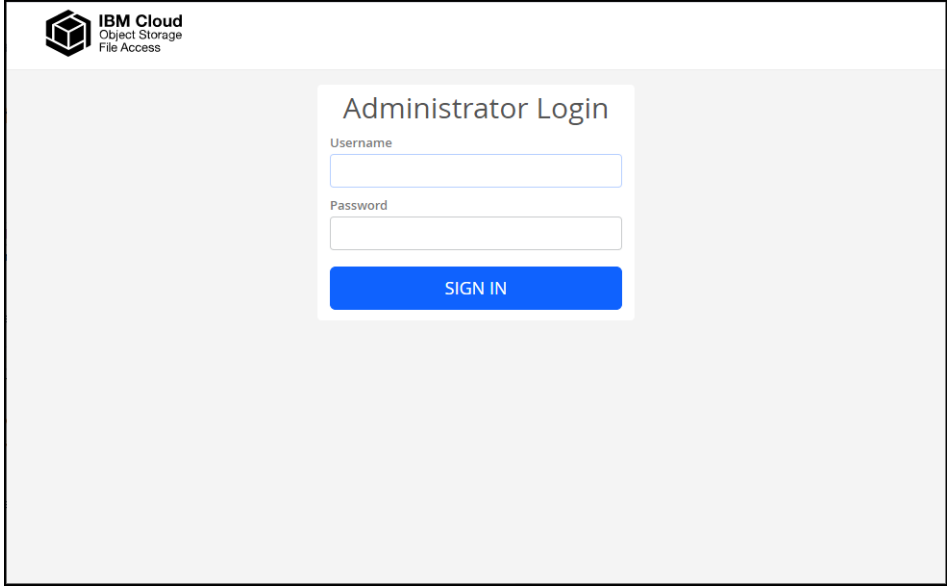
You can optionally replicate the contents of another IBM Cloud Object Storage File Access server.

☐ Replicate the following server: 



[NEXT >](#)

- 5 To configure this server as a replica of the main database or a catalog node, select the **Replicate the following server** check box, and then select the server you want to replicate in the drop-down list.
- 6 Click **Next**. The wizard completes and a success message is displayed.
- 7 Click **OK**. IBM COS FA Portal opens, displaying the **Administrator Login** page.



8 Enter the user name and password you specified in the Setup Wizard.

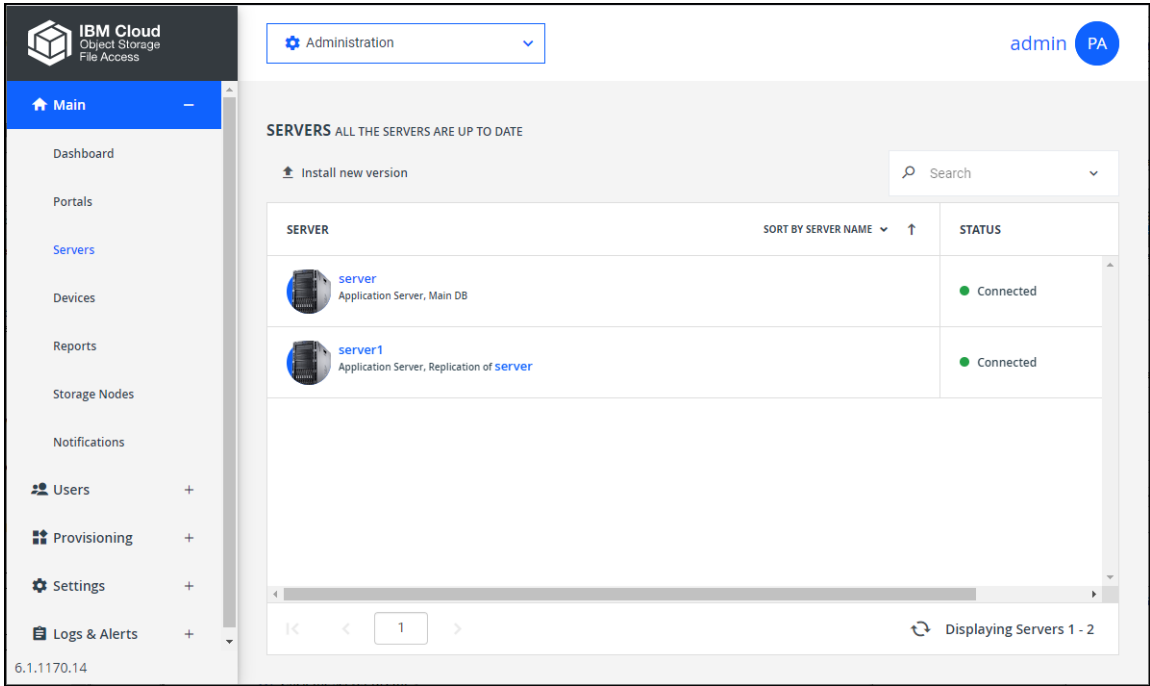
9 Click **SIGN IN**.

The IBM COS FA Portal opens, displaying the **Main > Dashboard** page.

By default, IBM COS FA Portal creates a team portal called *portal*. For information about how to rename, view and edit this IBM COS FA Portal, see the *IBM COS FA Portal Global Administrator Guide*.

10 In the global administration view, select **Main > Servers** in the navigation pane.

The **SERVERS** page is displayed, listing all the servers for the IBM COS FA Portal.



11 Click the server to edit.

The server window is displayed with the server name as the window title.

server CONNECTED

General Settings

Address Mappings

Clients

DB Replication

Name: server

☒ Application server

☐ Antivirus Background Scanner

☐ Replication of: [dropdown]

Network

Default Address: 192.168.27.221

☐ Public NAT Address: [input]

Advanced

Read Cache Size Limit: 256 MB

DELETE SAVE CANCEL

- 12 Check the boxes of the services to be provided by this server.
The server can act as an application server, or catalog node server.
- 13 Click **SAVE**.

CHAPTER 5. MANAGING IBM COS FA PORTAL SERVERS

In this chapter

- [Backing Up the IBM COS FA Portal](#)
- [Backing Up the Database](#)
- [Enabling FIPS](#)
- [Enabling/Disabling Remote Support](#)
- [Extending the IBM COS FA Portal Main Database or Catalog Node Storage Pool](#)
- [Load Balancing IBM COS FA Portal Servers](#)
- [Protecting the IBM COS FA Portal Main Database using vSphere HA](#)

BACKING UP THE IBM COS FA PORTAL

To back up the IBM COS FA Portal servers and storage, such as NetApp NFS mount, you need to use third-party recovery tools.

For database backup, see [Backing Up the Database](#).

Using third-party tools can result in a recovery after a disaster not being consistent with the database with the recovery being either older or newer than the database recovery.

If the IBM COS FA Portal recovery is older than the database, it will be missing some recent blocks. In this situation, you should rollback the database to an earlier point-in-time that matches the latest IBM COS FA Portal recovery.

If the IBM COS FA Portal recovery is newer than the database, since deleted blocks are kept for a minimum of 30 days and these blocks are never modified, as long as the database is no more than 30 days older, there will be no data loss.

Note: Running FSCK is usually recommended following a disaster recovery.

BACKING UP THE DATABASE

IBM COS FA Portal uses PostgreSQL to store metadata. This database **must** be backed up to ensure continued use of IBM COS FA Portal in order to ensure data and metadata persistence and consistency on the IBM COS FA Portal platform, and to keep Recovery Time Objective (RTO) and Recovery Point Objective (RPO) values to a minimum.

Calculating the Minimum Space Required for the Database Backup

The database storage used for backup does not have SSD storage. You require double the storage for the backup. For example, if the master database uses 1TB storage and a slave database uses another 1TB, then each of these databases require 2TB for backup. The storage pool must be at least 6TB: 1TB for the master database, 1TB for the slave database and 4TB for the master and slave backup (2TB for each backup).

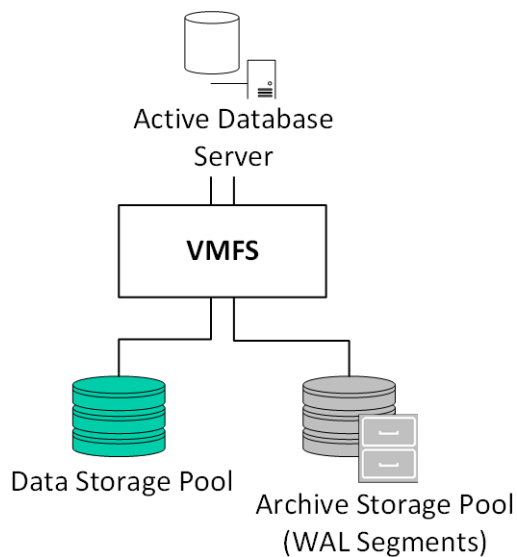
Note: You **must** define a database archive pool, whether using PostgreSQL continuous archiving or PostgreSQL Streaming Replication. Both [Using PostgreSQL Continuous Archiving](#) and [Using PostgreSQL Streaming Replication](#) procedures describe how to create an archive pool.

Using PostgreSQL Continuous Archiving

IBM COS FA Portal uses PostgreSQL's built-in continuous archiving mechanism, known as Point-In-Time Recovery (PITR).

After backing up the database for the first time, the *base backup*, Incremental backups of the database are performed using Write Ahead Log (WAL) files, which include all the database transactions and changes. Running a base backup and incremental backups is non-disruptive: the database continues running, without losing any data.

The following diagram illustrates continuous archiving and point-in-time recovery:



Using WAL logs has the following major benefits:

- Ensures data integrity
- Significantly reduces the number of disk writes

Note: The IBM COS FA Portal database WAL files are located in `$pgdatadir/pg_wal`, which is commonly called the WAL directory.

The WAL file size is 16MB. Once a WAL file reaches 16MB, a new WAL file is created.

The maximum number of WAL files stored in the WAL directory is 128. This means that the WAL directory size can reach $16 \text{ (MB)} * 128 \text{ (files)} = 2\text{GB}$.

When the 128-file threshold is reached, WAL files are recycled.

The database base backup and WAL logs are compressed upon backup:

- The base backup is typically 20%-30% of the size of the original database size. By default, there are always two base backups in the archive storage pool so the archived base backups typically consume around 40%-60% of the original database size.
- An archived WAL file size is typically 20% the size of the original WAL file.

Configuring PostgreSQL Continuous Archiving

To configure PostgreSQL continuous archiving:

- 1 Using SSH, log in as root to your IBM COS FA Portal server.
- 2 In the command line, enter the following command to create the database archive pool:
`portal-storage-util.sh create_db_archive_pool device`
 Where *device* is the name of the disk on which the database archive pool is created.

For example: `portal-storage-util.sh create_db_archive_pool sdd`

Note: This command creates both a logical volume and an LVM volume group using the specified device. Multiple devices can be specified. For example:

```
portal-storage-util.sh create_db_archive_pool sdd sde sdf
```

The logical volume size can be extended at a later time, as described in [Extending the Database Archive Pool](#).

Note: When using NFS storage, use the following command to create the database archive pool:

```
portal-storage-util.sh create_db_archive_pool -nfs
<NFS_IP>:/export/db_archive_dir
```

where *NFS_IP* is the IP address of the NFS mount point.

- 3 In the command line, enter the following command to configure the maximum number of days to keep the backups: `portal.sh configure-db-recovery backup-history-days`

Where *backup-history-days* is the number of days you want to retain a base backup archive before a new one is created. For example, to retain an archive for seven days, run:

```
portal.sh configure-db-recovery 7
```

An initial base backup of the database is created and the next backup is scheduled based on the *backup-history-days* parameter. Starting from the second base backup, the first scheduled base backup, there is always two base backups in the archive storage pool. WAL files are created after the first base backup. When a scheduled base backup is performed, the new base backup replaces both the old base backup that exceeded the *backup-history-days*, as well as the WAL files created in the period of time between the old base backup and the new base backup.

Warning: The minimum retention period recommended by IBM is 7 days. If you set the retention period to less than 7 days, you must also have a secondary backup method in order to protect the IBM COS FA Portal from disasters.

When the command finishes successfully a message is displayed, similar to the following:

```
NOTICE: pg_stop_backup complete, all required WAL segments have been
archived
Done
```

You can roll back to any older version of the database up until the previous base backup.

Rolling Back PostgreSQL Continuous Archiving to a Previous Point-in-Time

After continuous archiving has been set up, you can roll back to an older version of the IBM COS FA Portal database.

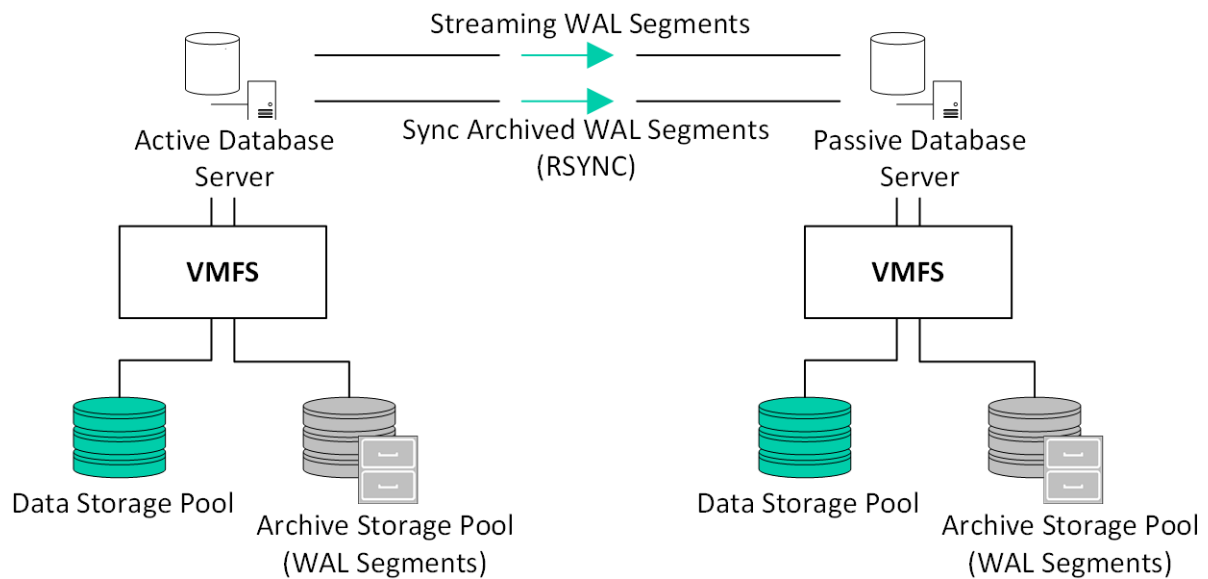
To roll back PostgreSQL continuous archiving to a previous point in time:

- 1 Using SSH, log in as root to your IBM COS FA Portal server.
- 2 In the command line, enter the following command to view the oldest time possible to roll back to:
`portal.sh db-rollback -p`
- 3 Enter the following command to roll back to a point in time within the available backup range:
`portal.sh db-rollback -r "point-in-time"`
Where *point-in-time* is the desired point in time, in the format YYYY-MM-DD hh:mm:ss.
- 4 When rolling back a Primary DB Server, Master DB or Catalog Node, from which a replication server is streaming, described in [Using PostgreSQL Streaming Replication](#), restart the IBM COS FA Portal on the secondary DB server, the replicating server, by running:
`portal-manage.sh restart`

Using PostgreSQL Streaming Replication

Streaming replication enables the continuous streaming and replication of WAL segments from the WAL directory and archived WAL segments from a primary server (either the IBM COS FA Portal master database server, or a catalog node) to a secondary database server.

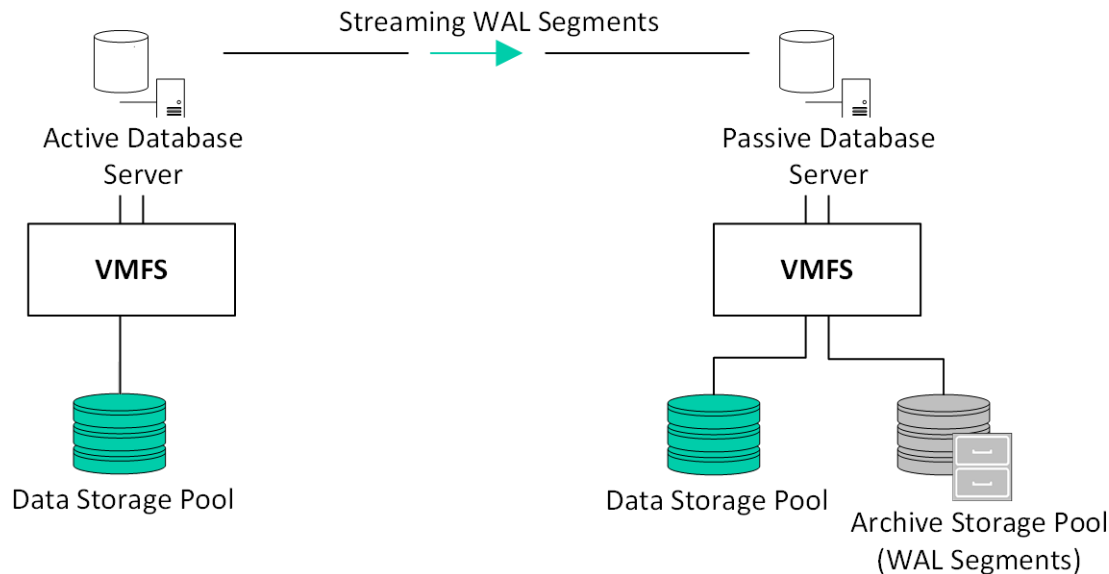
The following diagram illustrates streaming replication with continuous archiving and point-in-time recovery:



Note: Syncing archived WAL segments is done only on the first setup of the replica.

This process is complementary to configuring continuous archiving, described in [Using PostgreSQL Continuous Archiving](#). It protects against failures occurring on the primary database server, by streaming the WAL directory and synchronizing the database's archived WAL logs to a secondary database server.

You can also configure the replication so that the archive storage pool is on the passive, slave, database and not the active database server with point-in-time recovery on the slave.



Configuring PostgreSQL Streaming Replication

The secondary server continuously streams the master server's WAL segments, and synchronizes the master's archived WAL segments every 10 minutes. Streaming replication traffic runs on TCP port 5432, which means you must open these ports for communication between the master and secondary database servers. The secondary IBM COS FA Portal database server acts as a standby/passive server and cannot be used for load balancing purposes.

Before setting up streaming replication, the following conditions must be met:

- The IBM COS FA Portal Storage Pool has to be created.
- Add dedicated disks to the host for the PostgreSQL database archive in order to create a separate storage pool that contains the database backup archive.
- The allocated disk space for the PostgreSQL archive storage pool should be at least twice the size of the storage space allocated for the IBM COS FA Portal storage pool, as described in [Calculating the Minimum Space Required for the Database Backup](#).

Note: The locations of the streaming and archived WAL segments are `$pgdatadir/pg_wal` and `$DBarchive` respectively.

To configure streaming replication:

- 1 Using SSH, log in as root to your IBM COS FA Portal server.
- 2 In the command line, enter the following command to create the database archive pool:

```
portal-storage-util.sh create_db_archive_pool device
```

 Where *device* is the name of the disk on which the database archive pool should be created. For example: `portal-storage-util.sh create_db_archive_pool sdd`
Note: This command creates both a logical volume and an LVM volume group using the specified device. Multiple devices can be specified. For example:

```
portal-storage-util.sh create_db_archive_pool sdd sde sdf
```

The logical volume size can be extended at a later time, if needed. See [Extending the Database Archive Pool](#).

Note: When using NFS storage, use the following command to create the database archive pool:

```
portal-storage-util.sh create_db_archive_pool -nfs
<NFS_IP>:/export/db_archive_dir
where NFS_IP is the IP address of the NFS mount point.
```

3 Do one of the following:

- If the secondary server has not been initialized, browse to the server's IP address or public DNS.
- If the secondary server has been initialized but without replication, and you want to set it up as a replication server, open an SSH session to the IBM COS FA Portal database server, by running the following command: `portal-manage.sh resetdb`

The **Setup** wizard opens, displaying the **Select Server operation mode** window.

4 Set the server as a replication of the desired database server.

You can choose to replicate either the main IBM COS FA Portal database server or a IBM COS FA Portal catalog node.

Note: After completing the setup wizard on an already initialized server, a new server entry is created representing the newly configured server. This makes the old server entry obsolete. You can remove the obsolete server entry by doing the following:

- i** Log in to the IBM COS FA Portal as a global administrator.
- ii** In **Main > Servers** locate the obsolete server entry, displayed as *Not Connected*.
- iii** Select the server and click **Delete**.

Failing Over PostgreSQL Streaming Replication to the Secondary Database Server

The secondary database acts as a passive database, meaning it can only process read requests. In the event that the primary database fails, you have to fail over to the secondary database server, making it active, in order to assure proper continuity of the platform.

Note: You can also switch between the primary and secondary database servers, making the secondary database server the master and the primary database server a slave, when the primary database server is still up.

To switch between the master and the slave:

- 1** Using SSH, log in as root to secondary database server.
- 2** In the command line, enter the following command: `portal-failover.sh become_master`

The primary database server becomes the slave, and the secondary database server becomes the master.

To failback to the master database server, when the primary database server becomes online:

- 1** Once the former primary database is running again, using SSH, log in as root to the original secondary database server.
- 2** In the command line, enter the following command: `portal-failover.sh become_replica`

Log in to the IBM COS FA Portal as a global administrator and In the global administration view, select **Main > Servers** in the navigation pane and click the replication server name. Click **DB Replication** in the server window that is displayed and under **Database Replication** verify that the **Status** value is set to **OK**.

Note: If there is a mismatch between the requested WAL files and their location on the server the **Status** value can be set to **Failed** until the mismatch is resolved when the WAL file position reaches the location, which can take a few hours. IBM recommends the following manual procedure to resolve this issue:

- i** Log in to the IBM COS FA Portal as a global administrator and In the global administration

view, select **Main > Servers** in the navigation pane.

The **SERVERS** page is displayed, listing all the servers for the IBM COS FA Portal.

- ii Click the replication server name and in the server window that is displayed, under **General Settings**, uncheck **Replication of**.
- iii Click **SAVE**.
- iv Click the replication server name again and in the server window that is displayed, under **General Settings**, recheck **Replication of**.
- v Click **SAVE**.

The replication process will reinitialize which can be monitored by clicking **DB Replication** in the server window and under **Database Replication** verify that the **Status** value is set to **Reinitializing**. After the replication has reinitialized, which can take some time, depending on the IBM COS FA Portal size and the amount of data to be replicated, and the **Status** value is set to **OK**.

Extending the Database Archive Pool

In both PostgreSQL continuous archiving and streaming replication, the database archive storage pool is created using LVM. This means that if at any point the pool requires additional disk space, it is possible to increase the pool's size by adding additional disks (or partitions) to the LVM volume group, thereby extending the logical volume in which the database archive resides.

To extend the database archive storage pool:

- 1 Using SSH, log in as root to your IBM COS FA Portal server.
- 2 Run the following command: `portal-storage-util.sh extend_db_archive_pool device`
Where *device* is the disk you would like to add to the LVM volume group.
For example: `portal-storage-util.sh extend_db_archive_pool sde`

Monitoring the Database Backup and Streaming Replication

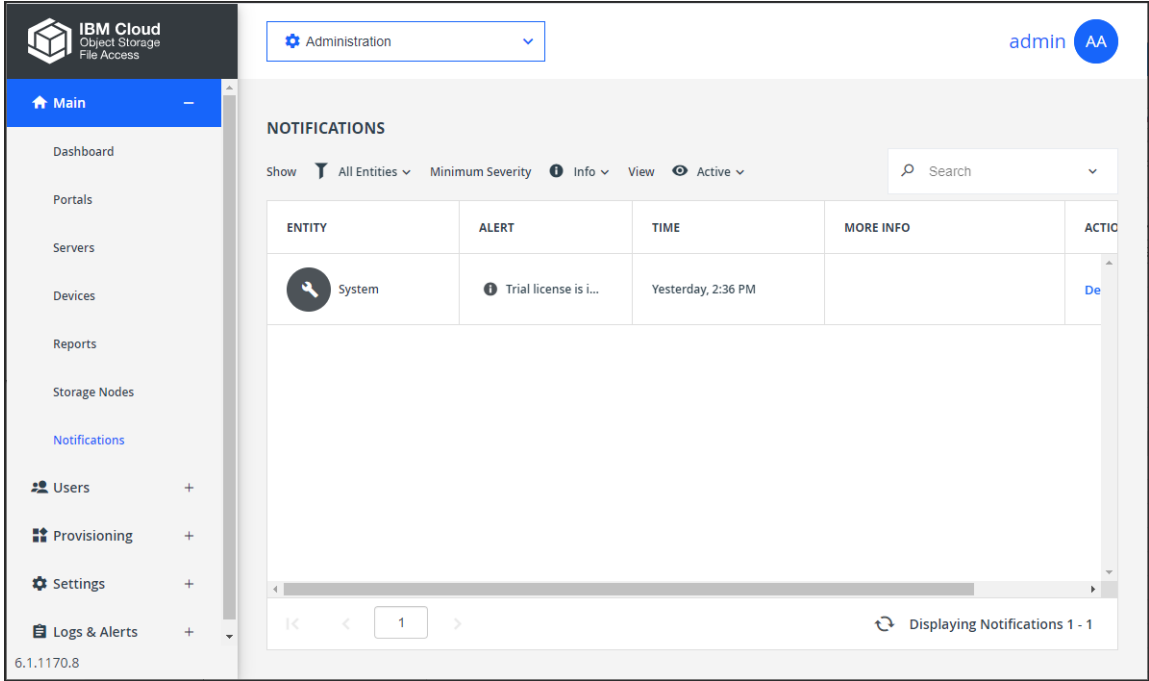
You can monitor every database backup and replication component running on the server, including:

- Streaming replication
- Base backup
- WAL archive (continuous archive)

Monitoring Database Backup and Replication from the Notifications Pane

To monitor database backup and replication from the NOTIFICATIONS page:

- In the global administration view, select **Main > Notifications** in the navigation pane. The **NOTIFICATIONS** page is displayed.



Any alerts related to database backup or streaming replication are displayed.

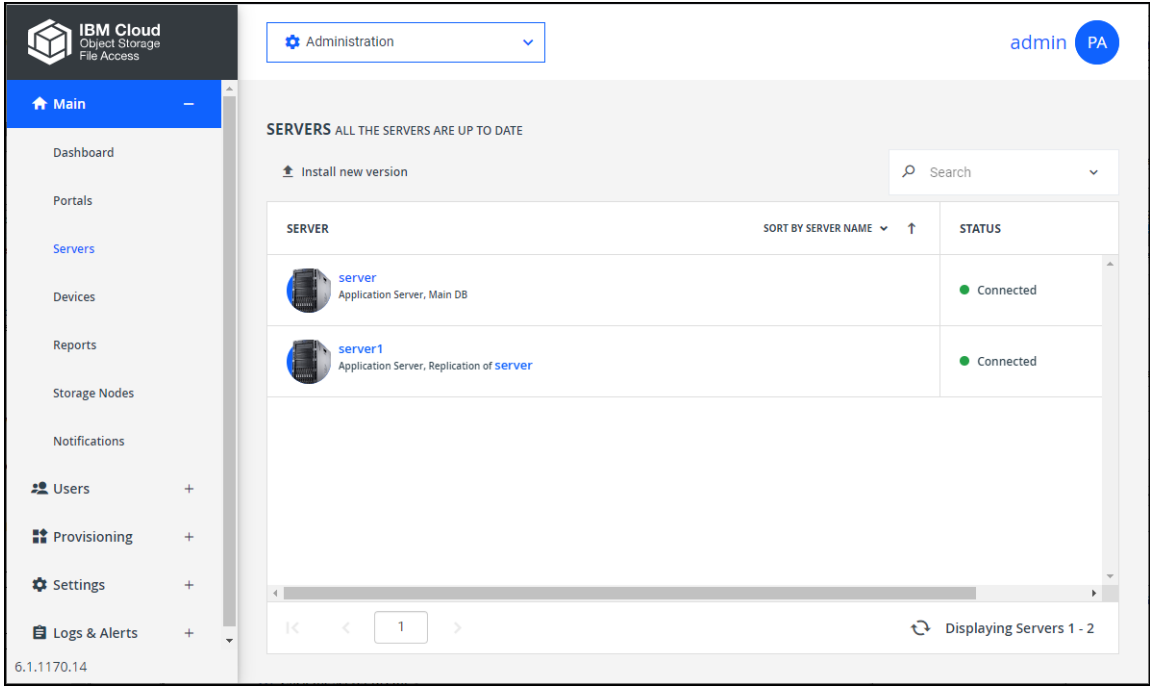
Monitoring Database Backup and Replication from the Server Task Manager

If streaming replication is set up, you can monitor it from the Server Task Manager. The IBM COS FA Portal runs a task every few minutes to verify that replication is working as expected. If any issues are detected, the task fails, and the IBM COS FA Portal displays an appropriate notification in the **NOTIFICATIONS** page, and also sends an email alert to the IBM COS FA Portal administrators.

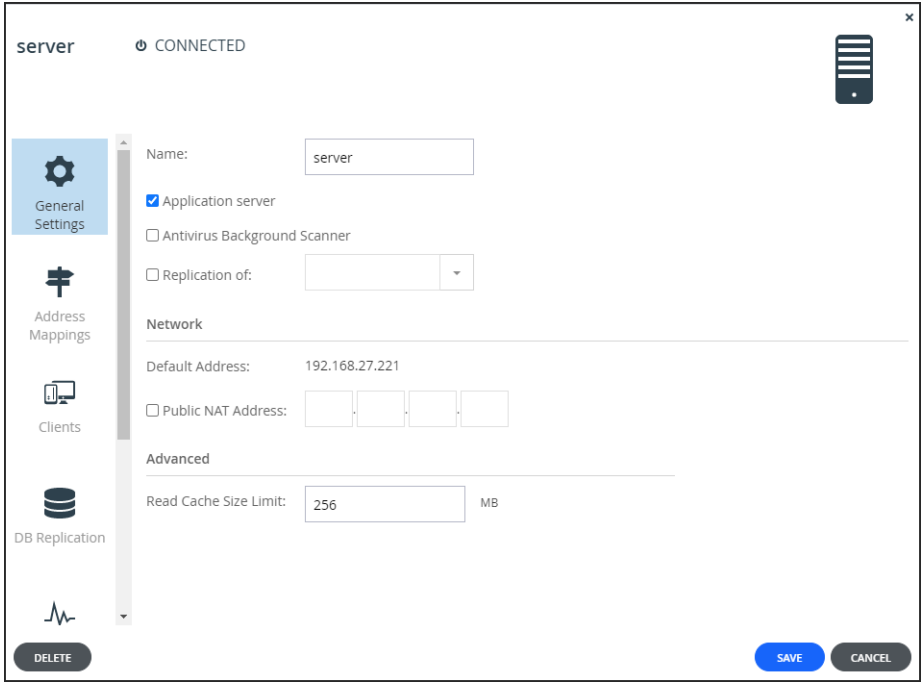
Note: The task runs the `portal.sh replication_status` command and analyzes the output. For more information see [Monitoring Database Backup and Replication from the Server Console](#).

To monitor database backup and replication from the Server Task Manager:

- In the global administration view, select **Main > Servers** in the navigation pane. The **SERVERS** page is displayed, listing all the servers for the IBM COS FA Portal.

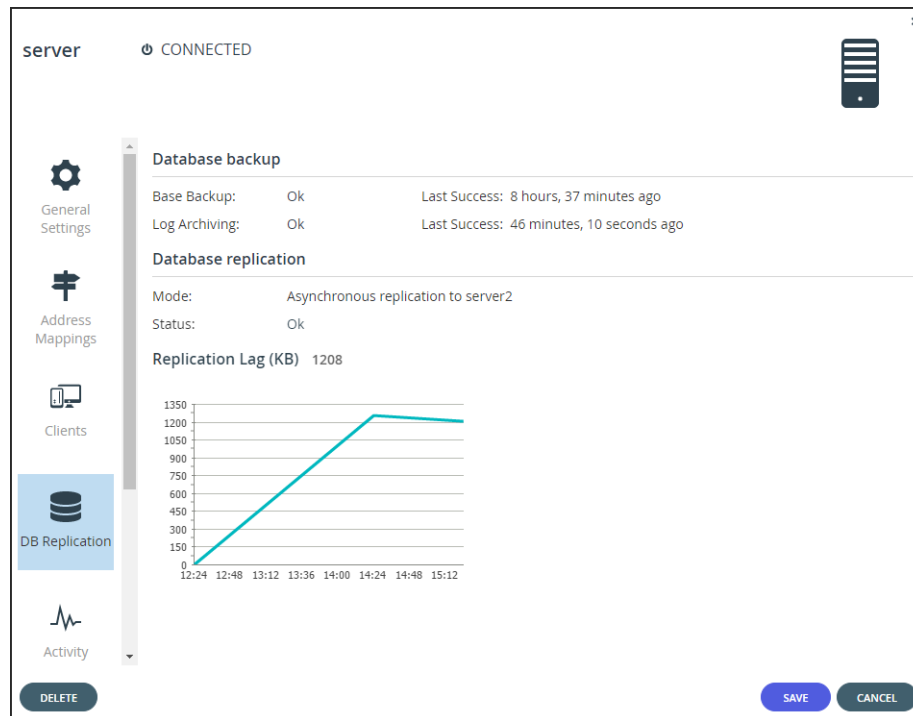


- 3 Click the replicating secondary server name.
The server window is displayed with the server name as the window title.



- 4 Click the **DB Replication** option.
The IBM COS FA Portal reports the status of its scheduled base backups and transaction log

archiving process, as well as additional metrics to help detect when database replication falls behind due to lags in the process. In the event that replication falls behind, IBM COS FA Portal administrators are notified via email. The relevant email templates are *Replication setup failed* and *Replication has errors*.



Monitoring Database Backup and Replication from the Server Console

You can view the status of each database backup and replication component.

To monitor database backup and replication from the server console:

Note: This procedure can be performed on both the master server and on secondary servers.

- 1 Using SSH, log in as root to the master or secondary server.
- 2 Run the following command: `portal-storage-util.sh extend_db_archive_pool device`
- 3 Run the following command: `portal.sh replication_status | json_reformat`
The output is displayed in JSON format. For example:

```
{
  "streaming_replication": {
    "status": "ok",
    "lastSuccess": "256KB"
  },
  "base_backup": {
    "status": "ok",
    "lastSuccess": "none"
  },
  "wal_archive": {
    "status": "failed",
    "lastSuccess": "3 hours"
  }
}
```

}

Both the master and secondary servers have the same output structure. However, the fields have slightly different meanings:

Field	Master Server	Secondary Server
streaming_replication		
status	Indicates whether a secondary server is streaming from the master server: ok – Streaming replication is running. failed – Streaming replication failed. not configured – Streaming replication is not configured on this server.	Indicates whether this server is streaming from the master server: ok – Streaming replication is running. failed – Streaming replication failed.
lastSuccess	The difference in size (in KB) between the last sent WAL segment and the secondary server's last checkpoint, a point in the WAL logs at which all data files have been written to the disk. In other words, the amount of data the master database sent to the secondary database, which has not been processed by the secondary database.	The difference in size (in KB) between the last received WAL segment and the secondary server's last checkpoint, a point in the WAL logs at which all data files have been written to the disk. In other words, the amount of data the master database sent to the secondary database, but which has not been processed by the secondary database. If the value is <code>none</code> , then the secondary database is up to date.
base_backup		
status	Indicates whether the last base backup was completed successfully: ok – Last base backup ended successfully. failed – Last base backup failed. not configured – Base backup is not configured for this server. Continuous archiving was not configured on the server.	Indicates whether the last base backup was completed successfully: ok – Last base backup completed successfully. failed – Last base backup failed.
lastSuccess	The last time a successful backup was run (in days). If the value is <code>none</code> , the <code>status</code> field is <code>ok</code> , and the last base backup was completed successfully.	
wal_archive		
status	Indicates whether a WAL was successfully archived in the past hour: ok – WAL directory was archived successfully in the past hour. failed – WAL directory was not archived in the past hour. This does not indicate a problem. You can change the status to <code>ok</code> , by running a manual command that forces archiving. For more information, contact support. not configured – WAL archiving, that is continuous archiving, is not configured on this server. Archiving occurs after 16MB of data has been written or during a system restart.	Indicates whether a WAL was successfully synchronized in the past hour: ok – WAL directory was synchronized successfully in the past hour. failed – WAL directory was not synchronized in the past hour.

Field	Master Server	Secondary Server
lastSuccess	The last time a WAL log was archived successfully (in hours). If the <code>status</code> field's value is <code>ok</code> , then <code>none</code> is output.	

- Run the following command on the slave server to view the slave archive synchronization log:
`portal-log.sh replication [-f]`
Include the `-f` flag to display the log in the command window. Otherwise, the log is displayed in `vim`.

ENABLING FIPS

The Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2), is a U.S. government computer security standard used to approve cryptographic modules. Setting the IBM COS FA Portal to be FIPS compliant requires a IBM COS FA Portal restart and impacts performance.

To change the IBM COS FA Portal to be FIPS compliant, contact IBM support.

ENABLING/DISABLING REMOTE SUPPORT

You can enable remote assistance by the IBM support team, by using the `portal-support.sh` script. This script adds a user called "support", which the IBM Support Team can use to remotely access and log in to your IBM COS FA Portal.

To enable remote support:

- Open an SSH session to the IBM COS FA Portal instance.
- Log in as **root** user.
- In the command line, enter the following command: `portal-support.sh enable`

The **support** user is created.

To disable remote support:

- Open an SSH session to the IBM COS FA Portal instance.
- Log in as **root** user.
- In the command line, enter the following command: `portal-support.sh disable`

The **support** user is deleted.

EXTENDING THE IBM COS FA PORTAL MAIN DATABASE OR CATALOG NODE STORAGE POOL

Note: IBM recommends changing the storage with the help of IBM Support.

To extend the IBM COS FA Portal main database or catalog node storage pool:

- For each IBM COS FA Portal instance you have installed, stop IBM COS FA Portal services, by doing the following:
 - Open an SSH session to the IBM COS FA Portal instance.
 - Log in as **root** user.
 - Run the command to stop the IBM COS FA Portal services: `portal-manage.sh stop`
- Attach a VMDK drive to the IBM COS FA Portal server, by doing the following:
 - In the vSphere Web Client, right-click the IBM COS FA Portal virtual machine and click **Edit**

Settings.

The virtual machine settings are displayed.

- b** In the Virtual **Hardware** tab, click select **New Hard Disk** for **New Device** and click **Add**.
A new hard disk is added to the settings.
- c** Specify the disk size you want for the new disk.
- d** Click **OK**.

The new VMDK hard disk is added.

Note: In certain cases, you may be required to reboot the IBM COS FA Portal server in order for the new VMDK drive to be identified.

- 3** Extend the IBM COS FA Portal storage pool, by doing the following:
 - a** Log in as **root** user to your IBM COS FA Portal server over SSH.
 - b** Run the following command to identify the name of the device you attached: `fdisk -l`
Locate the device name according to its size and usage information.
 - c** Run the following command to stop the IBM COS FA Portal services: `portal-manage.sh stop`
 - d** Run the command to extend the storage pool:
`portal-storage-util.sh extend_storage deviceName`
Where *deviceName* is the device name copied in the previous step.
The main database or catalog node storage pool is extended.
- 4** To view the storage pool size, run the following command: `df -h /usr/local/lib/ibm`
- 5** For each IBM COS FA Portal instance you installed, starting from the IBM COS FA Portal main database and catalog node and proceeding to the application servers, start IBM COS FA Portal services.
 - a** Log in as **root** user to each IBM COS FA Portal server over SSH.
 - b** Run the following command to start the IBM COS FA Portal services: `portal-manage.sh start`

LOAD BALANCING IBM COS FA PORTAL SERVERS

General Load Balancing Best Practices

- Probing to test tomcat reachability: Most load balancers have a health check/probing mechanism that checks for ports and services availability. The best scenario is to only use port tests that check if the port is available (checking ports 995 and 443). If a more accurate probing is required, use port 995 probe. With HTTPS use: `portalurl/admin/startup`.
- It is not recommended to use source NAT on the load balancer as this makes it hard to monitor and troubleshoot networking issues, since all the connections come to the tomcat servers from the same IP. This will also open the possibility that the IBM COS FA Portal will be locked due to too many retries if any user gets his password wrong 3 times and it will affect all users since this mechanism is based on IP.

Using F5 Load Balancer

The following describes setting up load balancing using a version of F5 software that is not the latest version. If your version is different, contact IBM support for help with your configuration.

Using F5 load balancing to perform SSL offloading requires the following configuration:

- Create an F5 iRule to add **Secure** and **HttpOnly** flags to the JSESSIONID cookie.
- Create an F5 iRule to add **HSTS** flags.
- Disable old insecure encryption algorithms like RC4.

F5 Best Practices

The following best practices are recommended by IBM:

- Configure the **tcp** TCP protocol profile.
 - If **Idle Timeout** is configured, make sure the value is at least 5 minutes, 300 seconds, as IBM COS FA Portal handles its own TCP sessions with keep alives.
 - If **Keep Alive Interval** is configured, make sure the value is greater than the value specified for **Send CTTTP keepalive messages every** in the virtual IBM COS FA Portal settings. IBM recommends setting **Send CTTTP keepalive messages every** less than half the value specified for **Keep Alive Interval**.

Virtual Portal Settings

Remote Access Settings

Remote Access Redirection: Private IP Redirect

☐ Use HTTPS for remote access

Advanced

☐ Send CTTTP keepalive messages every seconds

SAVE CANCEL

- If **Zero window Timeout** is configured, make sure it is as high as possible. For example, 30000. The following shows recommended F5 settings for the **tcp** TCP protocol profile.

Hostname: f5-clera.me Date: Aug 21, 2017 User: admin
IP Address: 127.0.0.1 Time: 12:22 PM (IDT) Role: Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

Main Help About

Local Traffic » Profiles: Protocol: TCP » tcp

Properties

General Properties

Name: tcp
Partition / Path: Common

Timer Management

Close Wait: Specify... 5 seconds
Fin Wait: Specify... 5 seconds
Idle Timeout: Specify... 180 seconds
Keep Alive Interval: Specify... 1800 seconds
Minimum RTO: 0 milliseconds
Reset On Timeout: ☒ Enabled
Time Wait: Specify... 2000 milliseconds
Time Wait Recycle: ☒ Enabled
Zero Window Timeout: Specify... 30000 milliseconds

Memory Management

Proxy Buffer High: 49152 bytes
Proxy Buffer Low: 32768 bytes

- Configure the **source_addr** Persistence profile.
The following shows recommended F5 settings for **source_addr** Persistence profile.

The screenshot shows the F5 configuration interface for the 'source_addr' Persistence profile. The breadcrumb trail is 'Local Traffic >> Profiles : Persistence >> source_addr'. The 'Properties' tab is selected.

General Properties

Name	source_addr
Partition / Path	Common
Persistence Type	Source Address Affinity

Configuration

Match Across Services	☐
Match Across Virtual Servers	☐
Match Across Pools	☐
Hash Algorithm	Default
Timeout	Specify... 180 seconds
Mask	None
Map Proxies	☒ Enabled
Override Connection Limit	☐

Update

- After setting the profiles, set up the load balancing for the IBM COS FA Portal virtual servers.

The screenshot shows the F5 configuration interface for the 'vs_clera' Virtual Server List. The breadcrumb trail is 'Local Traffic >> Virtual Servers : Virtual Server List >> vs_clera'. The 'Resources' tab is selected.

Load Balancing

Default Pool	pl_clera
Default Persistence Profile	source_addr
Fallback Persistence Profile	None

Update

iRules Manage...

Name	No records to display.
------	------------------------

Policies Manage...

Name	No records to display.
------	------------------------

PROTECTING THE IBM COS FA PORTAL MAIN DATABASE USING VSPHERE HA

The IBM COS FA Portal platform must be protected from datacenter and virtualization host failure and maintain data integrity and business continuity. This can be achieved through IBM COS FA Portal's native, application level, database archiving and replication procedures but can also be managed at the ESXi layer.

To protect the IBM COS FA Portal platform from datacenter and virtualization host failure at the ESXi layer:

- [vSphere HA Hardware and Software Requirements](#)
- [Configuring vSphere HA](#)
- [Testing vSphere HA Failover](#)

vSphere HA Hardware and Software Requirements

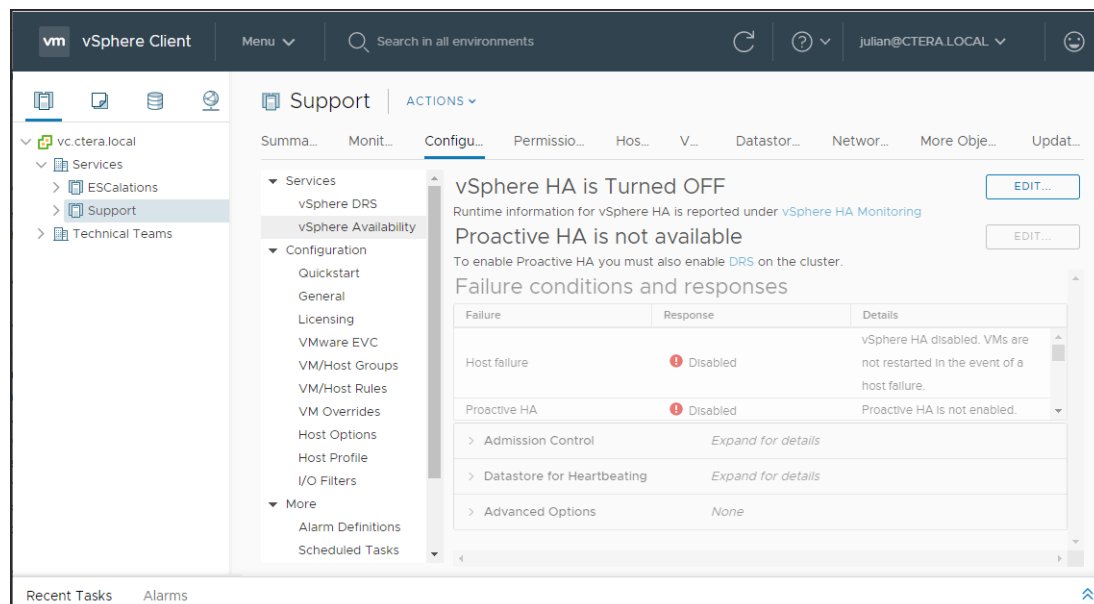
Before starting to configure vSphere HA and protect the IBM COS FA Portal Main Database VM, review VMware's [vSphere HA Hardware and Software requirements](#). These requirements must be addressed prior to any configuration and VM deployments.

Configuring vSphere HA

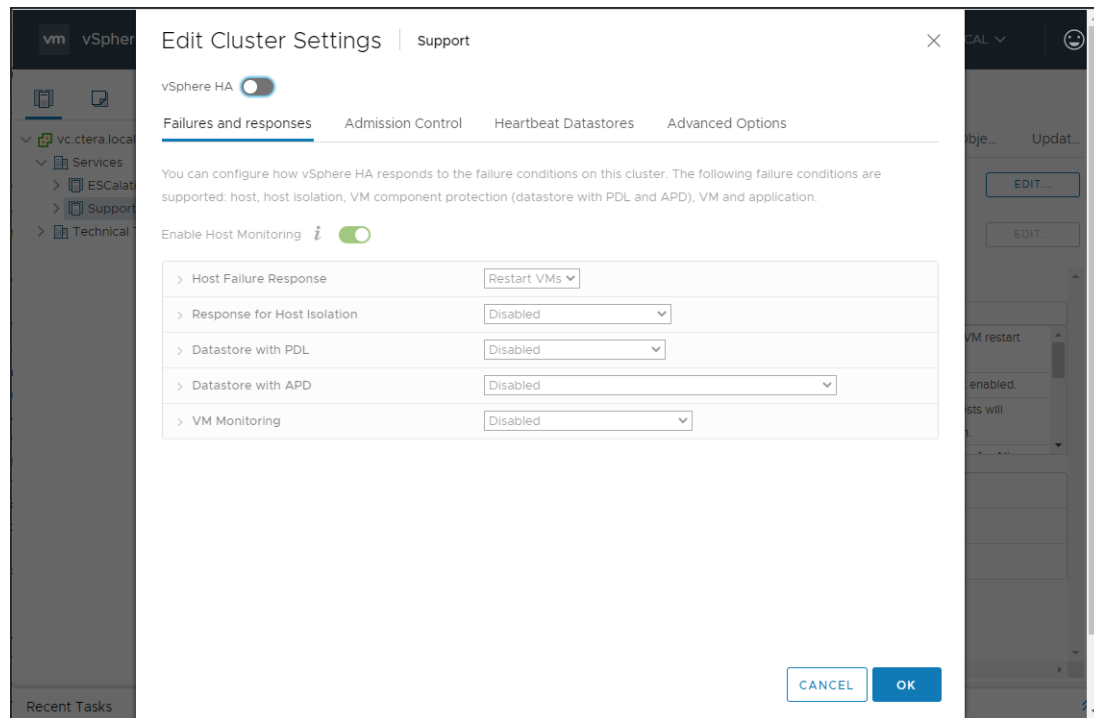
Perform the following procedure to enable vSphere HA for your datacenter.

To configure vSphere HA:

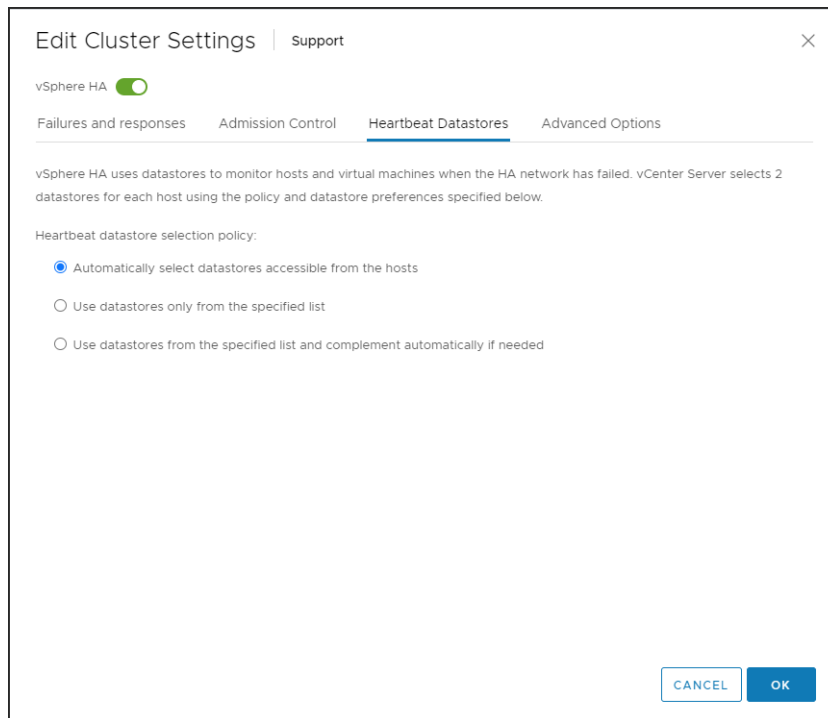
- 1 Login in to your vCenter Server using vSphere client.
- 2 Right-click on the cluster you want to protect using vSphere HA on and click **Settings**.
- 3 Browse to **vSphere Availability** under **Services**.



- 4 Click **EDIT** for vSphere HA.
The **Edit Cluster Settings** window is displayed.



- 5 Enable **vSphere HA**.
 - 6 In the **Failures and responses** tab make sure that **Enable Host Monitoring** is on and set **Host Failure Response** to **Restart VMs**.
 - 7 In the **Heartbeat Datastores** tab, select the shared datastores that will be used for vSphere HA.
- Note:** You must select a minimum of two datastores. For automatic detection of accessible datastores, choose **Automatically select datastores accessible from the hosts**.



8 Click OK.

vSphere HA is now enabled on the cluster.

Once vSphere HA is enabled, using the dedicated, shared datastores, virtual machines deployed to hosts participating in your cluster are automatically protected.

Testing vSphere HA Failover

Virtual machines deployed to hosts participating in the vSphere HA-enabled cluster are protected.

To perform a failover test:

- 1** Deploy the IBM COS FA Portal Main Database VM to one of the hosts in the cluster with vSphere HA set.
- 2** Upload sample data to the IBM COS FA Portal Global File System through IBM COS FA Portal's web application or via SMB using a IBM COS FA Gateway.
- 3** After successfully uploading files to the IBM COS FA Portal Global File System, power off the vSphere host running the IBM COS FA Portal Main Database.

vSphere will provide an alert indicating that the failover process has started and will begin restarting the IBM COS FA Portal Main Database VM on a second host.

Upon completing the failover, vSphere will provide an alert indicating that the IBM COS FA Portal Main Database virtual machine is back up and running.

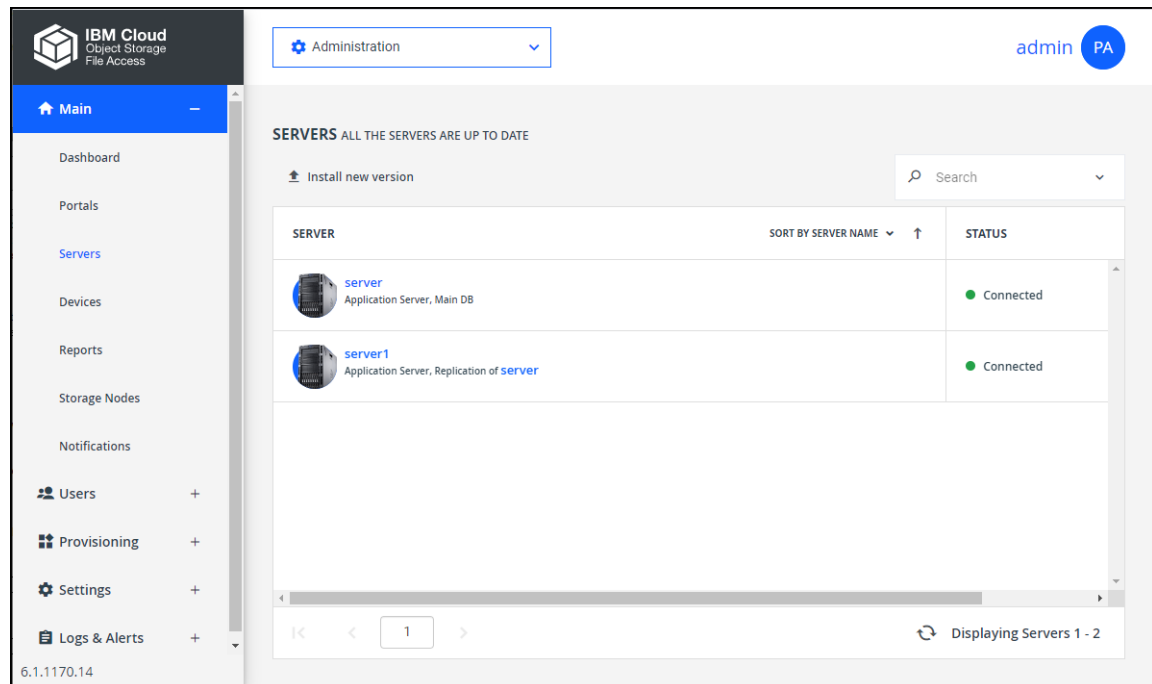
The failover and failback processes are performed automatically, requiring no manual intervention.

CHAPTER 6. UPGRADING IBM COS FA PORTAL

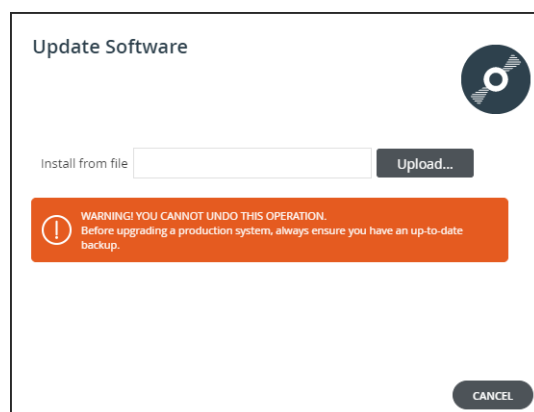
IBM recommends installing a new image and software with the help of IBM Support.

To upgrade the IBM COS FA Portal software via the IBM COS FA Portal user interface:

- 1 In the global administration view, select **Main > Servers** in the navigation pane.
The **SERVERS** page is displayed, listing all the servers for the IBM COS FA Portal.



- 2 Click **Install new version**.
The **Update Software** window is displayed.



- 3 Upload the IBM COS FA Portal version provided by IBM.
All servers in your IBM COS FA Portal installation are upgraded.

To upgrade the IBM COS FA Portal software via the command line:

- 1** Stop the IBM COS FA Portal servers.
First stop all application servers. Next stop the main database server and finally stop the replication database server, if available.
 - a** Using SSH, log in as root to your IBM COS FA Portal server.
 - b** Run the following command: `portal-manage.sh stop`
Once services are stopped, the Done message is displayed on the screen.
- 2** When all servers are in a stop state, upgrade the IBM COS FA Portal software.
 - a** Using SSH, log in as root to your IBM COS FA Portal server.
 - b** Upgrade the IBM COS FA Portal software: `portal-manage.sh upgrade upgrade_file`
where *upgrade_file* is the software file provided by IBM.
- 3** Restart the servers.
First start the main database server. Next start the replication database server, if available. Finally start the application servers.
 - a** Using SSH, log in as root to your IBM COS FA Portal server.
 - b** Start the IBM COS FA Portal: `portal-manage.sh start`