Security PDF (Admin)

Tables of Contents

Securing connections to services with private service endpoints

You can configure isolated connectivity to your cloud-based services for production workloads with IBM Cloud service endpoints. When you enable IBM Cloud service endpoints in your account, you can expose a private network endpoint when you create a resource. You then connect directly to this endpoint over the IBM Cloud private network rather than the public network. Because resources that use private network endpoints don't have an internet-routable IP address, connections to these resources are more secure.

To use service endpoints:

1. Enable virtual routing and forwarding (VRF) in your account, if necessary, and enable the use of service endpoints.
2. Create services that support VRF and service endpoints.

See Enabling VRF and service endpoints.

Learn more

- Secure access to services using service endpoints
- Enabling VRF and service endpoints
- List of services that support service endpoints

Parent topic: Security

Configuring firewall access

Firewalls protect valuable data from public access. If your data sources reside behind a firewall for protection, and you are not using a Satellite Connector or Satellite location, then you must configure the firewall to allow the IP addresses for Cloud Pak for Data as a Service and also for individual services. Otherwise, Cloud Pak for Data as a Service is denied access to the data sources.

To allow Cloud Pak for Data as a Service access to private data sources, you configure inbound firewall rules using the security mechanisms for your firewall. Inbound firewall rules are not required for connections that use a Satellite Connector or Satellite location, which establishes a link by performing an outbound connection. For more information, see Connecting to data behind a firewall.

All services in Cloud Pak for Data as a Service actively use WebSockets for the proper functioning of the user interface and APIs. Any firewall between the user and the Cloud Pak for Data as a Service domain must allow **HTTPUpgrade**. If Cloud Pak for Data as a Service is installed behind a firewall, traffic for the **wss://** protocol must be enabled.

Configuring inbound access rules for firewalls

If data sources reside behind a firewall, then inbound access rules are required for Cloud Pak for Data as a Service. Inbound firewall rules protect the network against incoming traffic from the internet. The following scenarios require inbound access rules through a firewall:

- Firewall access for Cloud Pak for Data as a Service
- Firewall access for DataStage
- Firewall access for AWS Redshift
- Firewall access for Cloud Object Storage
- Firewall access for Spark
- Firewall access for watsonx.ai Runtime
- Firewall access for Data Virtualization
- Firewall access for watsonx.ai Studio

Learn more

- Connecting to data behind a firewall

Parent topic: Setting up the platform for administrators

Firewall access for the platform

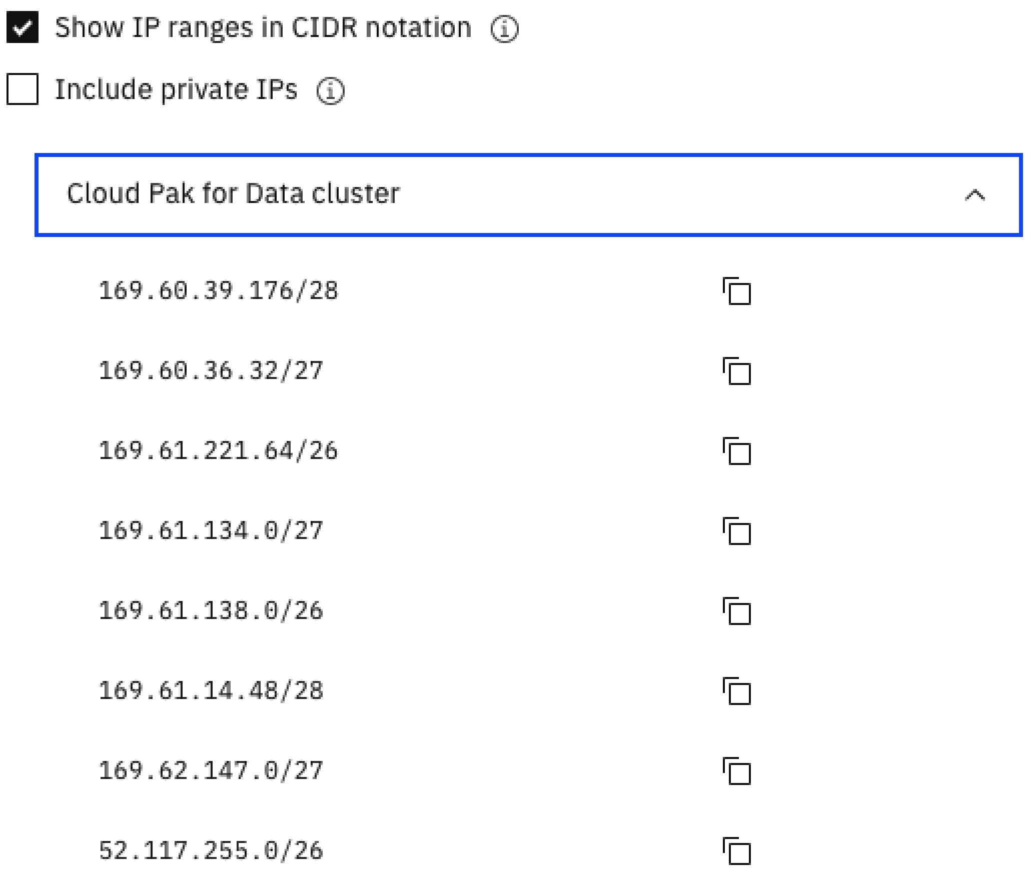
If a data source resides behind a firewall, then Cloud Pak for Data as a Service requires inbound access through the firewall in order to make a connection. Inbound firewall access is required whether the data source resides on a third-party cloud provider or in an data center. The method for configuring inbound access varies for different vendor's firewalls. In general, you configure inbound access rules by entering the IP addresses for the Cloud Pak for Data as a Service cluster to allow for access by Cloud Pak for Data as a Service.

You can enter the IP addresses using the starting and ending addresses for a range or by using CIDR notation. Classless Inter-Domain Routing (CIDR) notation is a compact representation of an IP address and its associated network mask. For start and end addresses, copy each address and enter them in the inbound rules for your firewall. Alternately, copy the addresses in CIDR notation.

The Cloud Pak for Data as a Service IP addresses vary by region. The user interface lists the IP addresses for the current region. The IP addresses apply to the base infrastructure for Cloud Pak for Data as a Service.

Follow these steps to look up the IP addresses for Cloud Pak for Data as a Service cluster:

1. Go to the **Administration > Cloud integrations** page.
2. Click the **Firewall configuration** link to view the list of IP ranges used by Cloud Pak for Data as a Service in your region.
3. View the IP ranges for the Cloud Pak for Data as a Service cluster in either CIDR notation or as Start and End addresses.
4. Choose **Include private IPs** to view the private IP addresses. The private IP addresses allow connections to IBM Cloud Object Storage buckets that are behind a firewall. See Firewall access for Cloud Object Storage.
5. Copy each of the IP ranges listed and paste them into the appropriate security configuration or inbound firewall rules area for your cloud provider.



☑ Show IP ranges in CIDR notation

□ Include private IPs

Cloud Pak for Data cluster

```
169.60.39.176/28
169.60.36.32/27
169.61.221.64/26
169.61.134.0/27
169.61.138.0/26
169.61.14.48/28
169.62.147.0/27
52.117.255.0/26
```

For example, if your data source resides on AWS, open the **Create Security Group** dialog for your AWS Management Console. Paste the IP ranges into the **Inbound** section for the security group rules.

Parent topic: Configuring firewall access

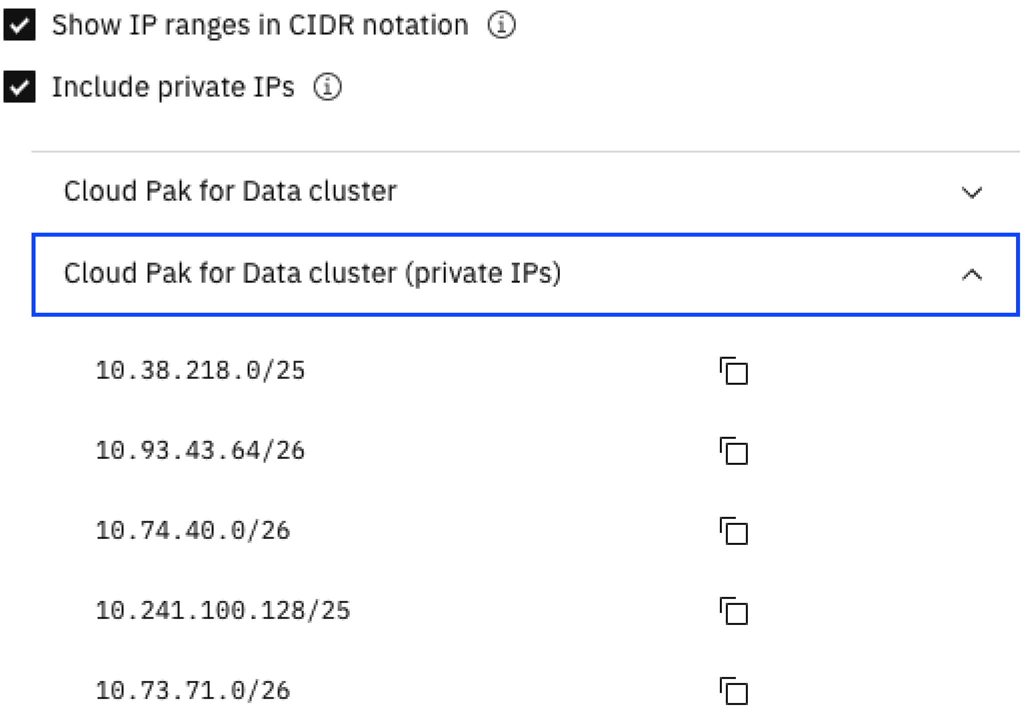
Firewall access for Cloud Object Storage

Private IP addresses are required when Cloud Pak for Data as a Service and Cloud Object Storage are located on the same network. When creating a connection to a Cloud Object Storage bucket that is protected by a firewall on the same network as Cloud Pak for Data as a Service, the connector automatically maps to private IP addresses for Cloud Pak for Data as a Service. The private IP addresses must be added to a **Bucket access policy** to allow inbound connections from Cloud Pak for Data as a Service.

Follow these steps to search the private IP addresses for the Cloud Pak for Data as a Service cluster and add them to the **Bucket access policy**:

1. Go to the **Administration > Cloud integrations** page.
2. Click the **Firewall configuration** link to view the list of IP ranges used by Cloud Pak for Data as a Service.

3. Choose **Include private IPs** to view the private IP addresses for the Cloud Pak for Data as a Service cluster.



☑ Show IP ranges in CIDR notation

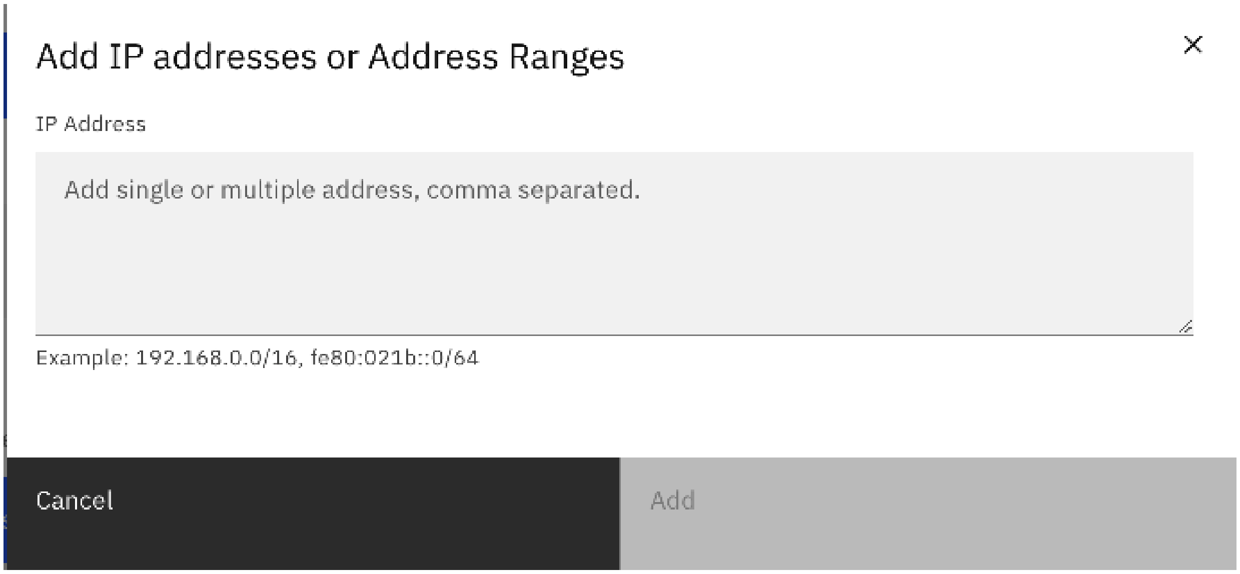
☑ Include private IPs

Cloud Pak for Data cluster

Cloud Pak for Data cluster (private IPs)

```
10.38.218.0/25
10.93.43.64/26
10.74.40.0/26
10.241.100.128/25
10.73.71.0/26
```

4. From your IBM Cloud Object Storage instance on IBM Cloud, open the **Buckets** list and choose the Bucket for the connection.
5. Copy each of the private IP ranges listed and paste them into the **Buckets > Permissions > IP address** field on IBM Cloud.



Add IP addresses or Address Ranges

IP Address

Add single or multiple address, comma separated.

Example: 192.168.0.0/16, fe80:021b::0/64

Learn more

- [IBM Cloud Object Storage connection]
- [IBM Cloud docs: Setting a firewall]

Parent topic: Configuring firewall access

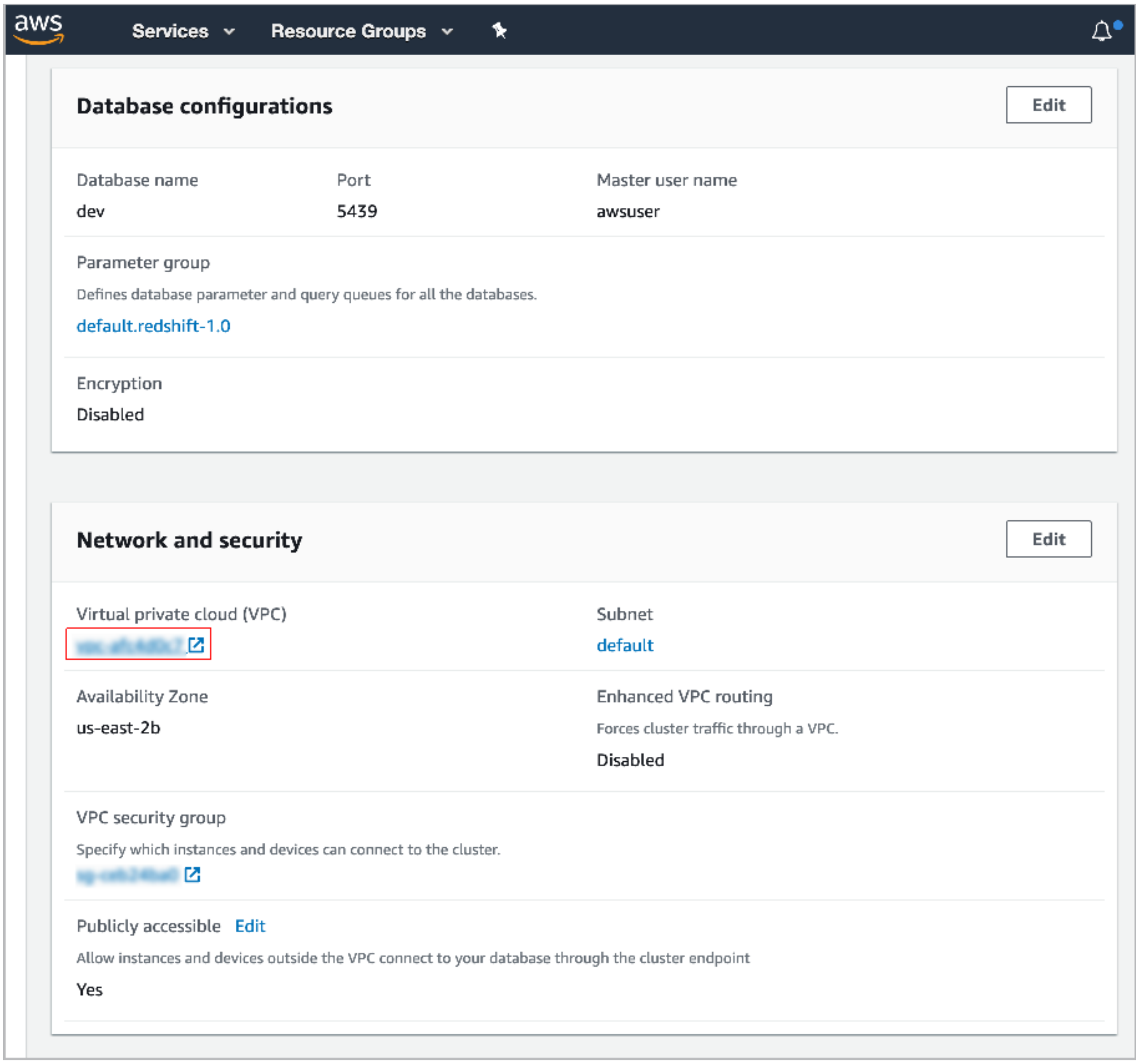
Firewall access for AWS Redshift

Inbound firewall access allows Cloud Pak for Data as a Service to connect to Redshift on AWS through the firewall. You need inbound firewall access to work with your data stored in Redshift.

To connect to Redshift from Cloud Pak for Data as a Service, you configure inbound access through the Redshift firewall by entering the IP ranges for Cloud Pak for Data as a Service into the inbound firewall rules (also called ingress rules). Inbound access through the firewall is configurable if Redshift resides on a public subnet. If Redshift resides on a private subnet, then no access is possible.

Follow these steps to configure inbound firewall access to AWS Redshift:

1. Go to your provisioned Amazon Redshift cluster.
2. Select **Properties** and then scroll down to **Network and security settings**.
3. Click the **VPC security group**.



Database configurations

Database name
dev

Port
5439

Master user name
awsuser

Parameter group
Defines database parameter and query queues for all the databases.
default.redshift-1.0

Encryption
Disabled

Network and security

Virtual private cloud (VPC)
[redacted]

Subnet
default

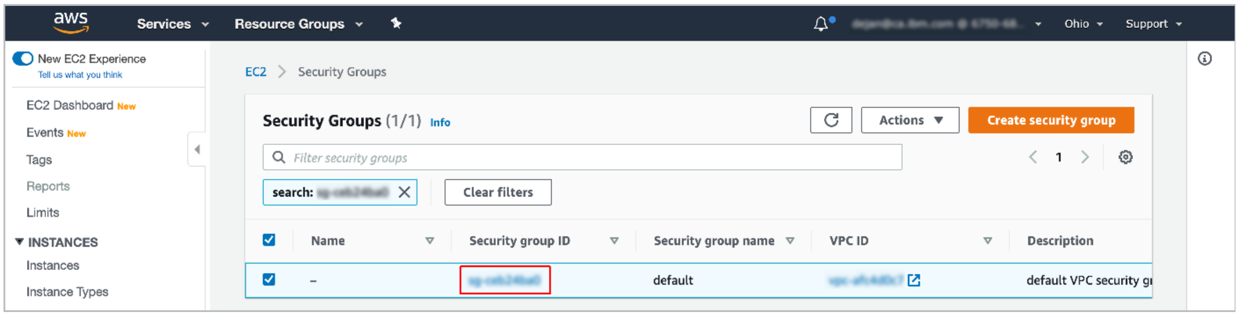
Availability Zone
us-east-2b

Enhanced VPC routing
Forces cluster traffic through a VPC.
Disabled

VPC security group
Specify which instances and devices can connect to the cluster.
[redacted]

Publicly accessible Edit
Allow instances and devices outside the VPC connect to your database through the cluster endpoint
Yes

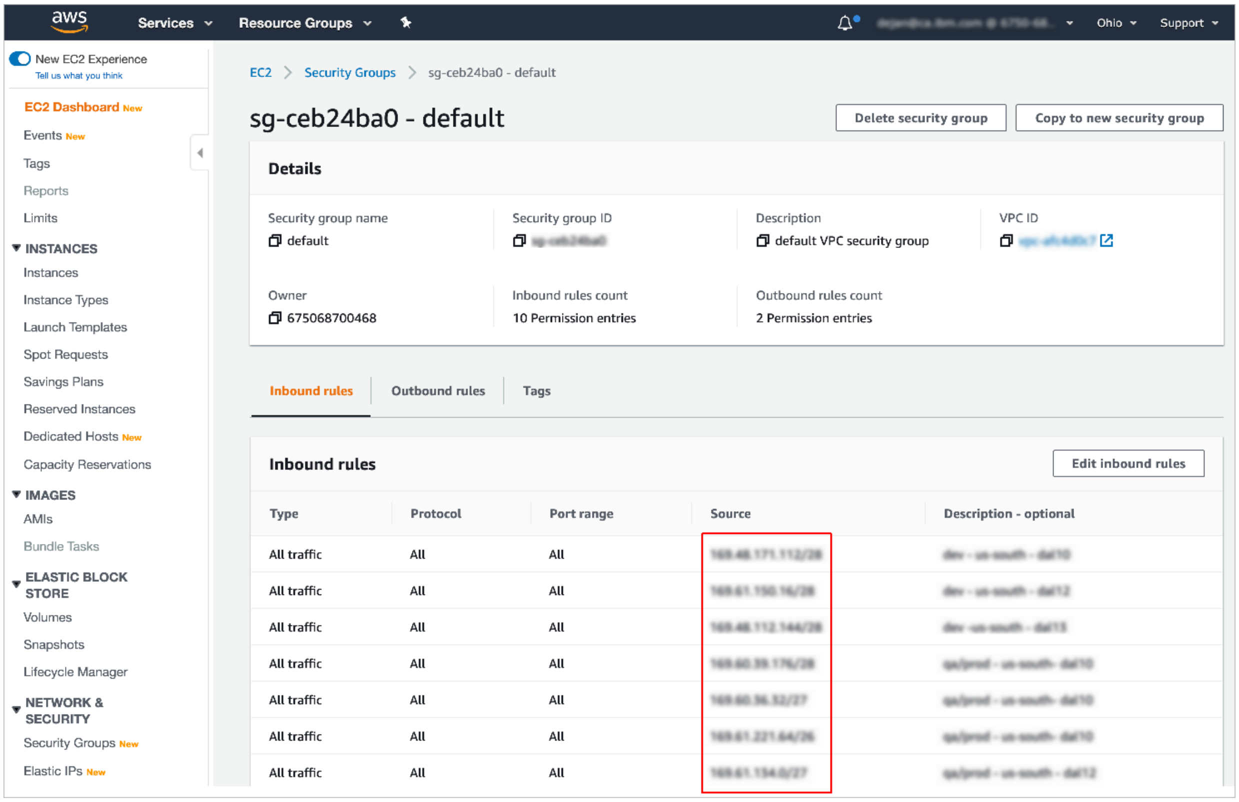
4. Edit the active/default security group.



Security Groups (1/1) Info

☑	Name	Security group ID	Security group name	VPC ID	Description
☑	–	[redacted]	default	[redacted]	default VPC security gr

5. Under **Inbound rules**, change the port range to 5439 to specify the Redshift port. Then select **Edit inbound rules > Add rule**.



sg-ceb24ba0 - default

Details

Security group name: default
Security group ID: [redacted]
Description: default VPC security group
VPC ID: [redacted]
Owner: 675068700468
Inbound rules count: 10 Permission entries
Outbound rules count: 2 Permission entries

Inbound rules

Type	Protocol	Port range	Source	Description - optional
All traffic	All	All	[redacted]	[redacted]
All traffic	All	All	[redacted]	[redacted]
All traffic	All	All	[redacted]	[redacted]
All traffic	All	All	[redacted]	[redacted]
All traffic	All	All	[redacted]	[redacted]
All traffic	All	All	[redacted]	[redacted]
All traffic	All	All	[redacted]	[redacted]

6. From Cloud Pak for Data as a Service, go to the **Administration > Cloud integrations** page.

7. Click the **Firewall configuration** link to view the list of IP ranges used by Cloud Pak for Data as a Service. IP addresses can be viewed in either CIDR notation or as Start and End addresses.

8. Copy each of the IP ranges listed and paste them into the **Source** field for inbound firewall rules.

Learn more

- Working with Redshift-managed VPC endpoints in Amazon Redshift

Parent topic: Configuring firewall access

Firewall access for Spark

To allow Spark to access data that is located behind a firewall, you add the appropriate IP addresses for your region to the inbound rules for your firewall.

Dallas (us-south)

- dal12 - 169.61.173.96/27, 169.63.15.128/26, 150.239.143.0/25, 169.61.133.240/28, 169.63.56.0/24
- dal13 - 169.61.57.48/28, 169.62.200.96/27, 169.62.235.64/26
- dal10 - 169.60.246.160/27, 169.61.194.0/26, 169.46.22.128/26, 52.118.59.0/25

London (eu-gb)

- lon05 - 141.125.70.64/26
- lon06 - 158.176.84.0/27, 158.176.166.128/26
- lon04 - 158.175.122.160/27, 158.175.170.128/26

Frankfurt (eu-de)

- fra04 - 161.156.76.64/27, 161.156.115.192/26
- fra05 - 149.81.74.128/27, 149.81.187.192/26
- fra02 - 158.177.124.32/27, 158.177.101.16/28, 158.177.166.0/26

Tokyo (jp-tok)

- tok02 - 169.56.44.128/25
- tok04 - 128.168.71.128/25
- tok05 - 165.192.72.0/25

Parent topic: Configuring firewall access

Firewall access for watsonx.ai Runtime

To allow watsonx.ai Runtime to access data that is located behind a firewall, you add the appropriate IP addresses for your region to the inbound rules for your firewall.

Dallas (us-south)

Subnet	Vlan
52.116.4.224/27	dal13.fcr01.1817
52.116.226.128/25	dal12.fcr01.1449
52.117.147.0/25	dal10.fcr03.752
52.117.204.128/25	dal13.fcr02.1380
52.118.34.96/27	dal10.fcr01.805
52.118.158.128/25	dal10.fcr01.1853
75.126.248.128/26	dal13.fcr01.1817
169.46.33.96/28	dal10.fcr01.1853

Subnet	Vlan
169.46.55.96/28	dal10.fcr01.805
169.46.78.128/27	dal10.fcr01.1853
169.47.73.0/27	dal12.fcr01.817
169.48.100.128/25	dal13.fcr01.1817
169.48.200.96/28	dal12.fcr01.817
169.60.139.16/28	dal13.fcr01.1817
169.61.150.96/27	dal12.fcr01.1449
169.61.159.64/26	dal12.fcr01.1449
169.62.168.160/27	dal13.fcr01.1174
169.62.190.176/28	dal13.fcr01.1174
169.63.234.192/26	dal10.fcr01.1853
169.46.17.168/29	dal10.fcr01.1853
169.46.34.64/29	dal10.fcr01.805
169.47.97.32/29	dal12.fcr01.817
169.48.198.96/29	dal12.fcr01.1449
169.48.224.0/27	dal12.fcr01.817
169.60.39.152/29	dal10.fcr03.752
169.60.131.80/29	dal13.fcr01.1174
169.60.145.0/27	dal13.fcr01.1174
169.61.47.128/29	dal13.fcr01.1817
169.62.162.88/29	dal13.fcr02.1380
169.63.249.192/27	dal10.fcr01.805

Frankfurt

Subnet	Vlan
149.81.71.64/27	fra05.fcr01.930
149.81.71.192/28	fra05.fcr01.899
149.81.78.224/27	fra05.fcr01.899
149.81.82.16/28	fra05.fcr01.872
149.81.130.0/28	fra05.fcr01.930
158.177.76.0/27	fra02.fcr02.800
158.177.125.32/27	fra02.fcr02.1164
158.177.176.240/28	fra02.fcr02.800
159.122.109.32/28	fra02.fcr01.758
161.156.29.64/26	fra04.fcr01.927
161.156.91.160/27	fra04.fcr01.927
161.156.185.96/28	fra04.fcr01.839
149.81.66.152/29	fra05.fcr01.899
149.81.76.40/29	fra05.fcr01.930
149.81.115.0/27	fra05.fcr01.872
149.81.176.168/29	fra05.fcr01.872
158.177.69.72/29	fra02.fcr02.1164
158.177.144.168/29	fra02.fcr02.800

Subnet	Vlan
161.156.65.32/29	fra04.fcr01.927
161.156.94.168/29	fra04.fcr01.839
161.156.158.224/27	fra04.fcr01.839
169.50.18.96/27	fra02.fcr01.758
169.50.21.16/29	fra02.fcr01.758

London

Subnet	Vlan
141.125.64.80/28	lon05.fcr01.778
141.125.74.32/27	lon05.fcr01.805
141.125.99.64/26	lon05.fcr01.805
141.125.141.128/25	lon05.fcr01.805
158.175.75.192/26	lon04.fcr01.1267
158.175.83.176/28	lon04.fcr01.909
158.175.103.128/25	lon04.fcr01.1267
158.175.110.96/27	lon04.fcr01.1267
158.176.66.64/27	lon06.fcr01.921
158.176.93.192/28	lon06.fcr01.780
158.176.142.192/26	lon06.fcr01.921
141.125.70.32/27	lon05.fcr01.778
141.125.73.248/29	lon05.fcr01.805
141.125.87.40/29	lon05.fcr01.778
158.175.79.88/29	lon04.fcr01.909
158.175.86.0/29	lon04.fcr01.1267
158.175.111.96/27	lon04.fcr01.909
158.176.107.0/27	lon06.fcr01.780
158.176.124.208/29	lon06.fcr01.921
158.176.163.120/29	lon06.fcr01.780

Tokyo

Subnet	Vlan
128.168.66.16/28	tok04.fcr01.777
128.168.70.16/28	tok04.fcr01.783
128.168.79.224/27	tok04.fcr01.777
161.202.94.144/28	tok02.fcr01.869
161.202.96.176/28	tok02.fcr01.891
165.192.89.160/27	tok05.fcr01.795
165.192.102.64/28	tok05.fcr01.901
169.56.17.0/27	tok02.fcr01.891
128.168.66.104/29	tok04.fcr01.777
128.168.97.136/29	tok04.fcr01.783
128.168.150.64/27	tok04.fcr01.783

Subnet	Vlan
161.202.139.16/29	tok02.fcr01.869
161.202.231.8/29	tok02.fcr01.891
165.192.66.200/29	tok05.fcr01.795
165.192.86.96/29	tok05.fcr01.901
165.192.91.96/27	tok05.fcr01.901
169.56.23.96/27	tok02.fcr01.869

Parent topic: Configuring firewall access

Firewall access for watsonx.ai Studio

Inbound firewall access is granted to the watsonx.ai Studio service by allowing the IP addresses for Cloud Pak for Data as a Service on IBM Cloud.

If watsonx.ai Studio is installed behind a firewall, you must add the WebSocket connection for your region to the firewall settings. Enabling the WebSocket connection is required for notebooks and RStudio.

Following are the WebSocket settings for each region:

Table 1. Regional WebSockets

Location	Region	WebSocket
United States (Dallas)	us-south	wss://dataplatform.cloud.ibm.com
Europe (Frankfurt)	eu-de	wss://eu-de.dataplatform.cloud.ibm.com
United Kingdom (London)	eu-gb	wss://eu-gb.dataplatform.cloud.ibm.com
Asia Pacific (Tokyo)	jp-tok	wss://jp-tok.dataplatform.cloud.ibm.com

Follow these steps to look up the IP addresses for Cloud Pak for Data as a Service and allow them on IBM Cloud:

1. From the main menu, choose **Administration > Cloud integrations**.
2. Click **Firewall configuration** to display the IP addresses for the current region. Use CIDR notation.
3. Copy each CIDR range into the **IP address restrictions** for either a user or an account. You must also enter the allowed individual client IP addresses. Enter the IP addresses as a comma-separated list. Then, click **Apply**.
4. Repeat for each region to allow access for watsonx.ai Studio.

When you configure the allowed IP addresses for watsonx.ai Studio, you include the CIDR ranges for the watsonx.ai Studio cluster. You can also allow individual client system IP addresses.

For step-by-step instructions for both user and account restrictions, see IBM Cloud docs: Allowing specific IP addresses

Parent topic: Configuring firewall access