# Alibaba Cloud Lightning Cube

## Case Study

Issue: 20190522

# Legal disclaimer

**Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.**

1. **You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.**
2. **No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.**
3. **The content of this document may be changed due to product version upgrades , adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.**
4. **This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults " and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity , applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use**

or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

5. By law, all the content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of the Alibaba Cloud website, product programs, or content shall be used, modified , reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates . The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).
6. Please contact Alibaba Cloud directly if you discover any errors in this document.

# Generic conventions

Table -1: Style conventions

| Style | Description | Example |
| --- | --- | --- |
|  | This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results. |  Danger:<br>Resetting will result in the loss of user configuration data. |
|  | This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results. |  Warning:<br>Restarting will cause business interruption. About 10 minutes are required to restore business. |
|  | This indicates warning information, supplementary instructions, and other content that the user must understand. |  Notice:<br>Take the necessary precautions to save exported data containing sensitive information. |
| | This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user. |  Note:<br>You can use Ctrl + A to select all files. |
| > | Multi-level menu cascade. | Settings > Network > Set network type |
| Bold | It is used for buttons, menus , page names, and other UI elements. | Click OK. |
| `Courier font` | It is used for commands. | Run the `cd / d C :/ windows` command to enter the Windows system folder. |
| *Italics* | It is used for parameters and variables. | `bae log list --instanceid` *Instance_ID* |
| [] or [a\|b] | It indicates that it is a optional value, and only one item can be selected. | `ipconfig` *[-all\|-t]* |

| Style | Description | Example |
| --- | --- | --- |
| {} or {a\|b} | It indicates that it is a required value, and only one item can be selected. | `swich {stand \| slave}` |

# Contents

# 1 Seamless migration of business data to OSS

This section describes how to migrate data from a cloud service to Alibaba Cloud OSS.

## Background information

Company A is an Internet service provider that deploys the main business applicatio n in a cloud service provided by Cloud Service Provider B. The main business application of Company A provides online editing services for media files (such as images, videos). The existing data that is stored in Service Provider B includes 100, 000,000 files and has a total size of about 320 TB with a daily increase of 20 GB. The bandwidth for both the storage service of Service Provider B and OSS is 250 Mbit/s. The business application requires a maximum bandwidth of 50 Mbit/s.

The company is considering a switch to OSS because of its further development needs. When you switch over businesses between two data stores, you must migrate existing data and incremental data to OSS. To ensure a successful migration of large amounts of data and business continuity, the following needs must be met:

- During the migration job, you must ensure business continuity and diminish the impacts of normal data access from end users.
- After the migration job is complete, you must check data integrity to ensure a seamless switch of the business to OSS.

## Procedure

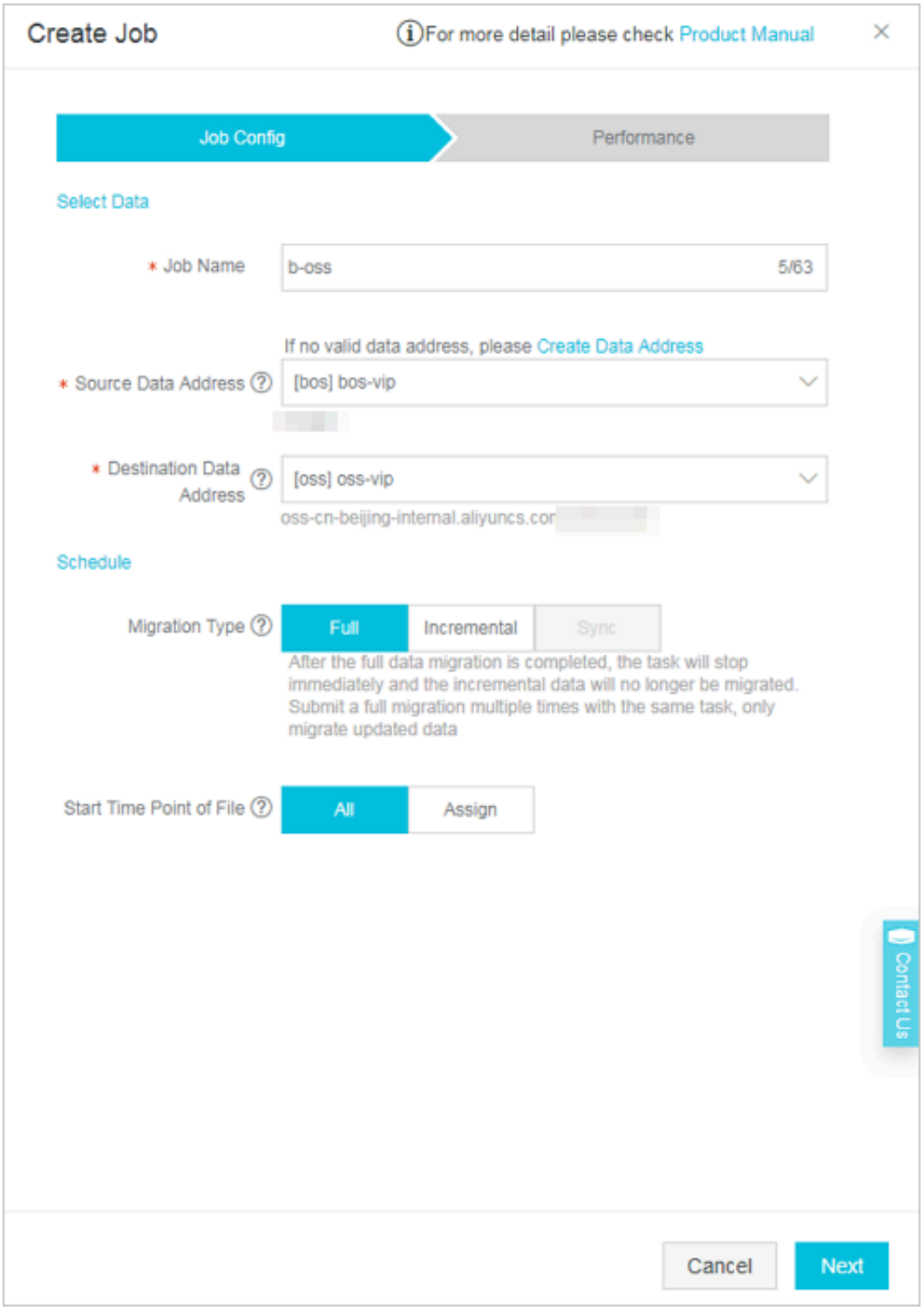
Based on the needs and background information, proceed as follows to migrate data:

1. With Data Transport, you can migrate existing data from a cloud service to OSS. Before a migration job is complete, ensure that no updates occur on the customer side.
2. After existing data is migrated, you can create back-to-origin rules in OSS for users to access un-migrated incremental data.
3. Switch businesses to OSS.
4. After the business switchover is complete, you can migrate incremental data to OSS using Data Transport.
5. After all data is migrated and validated, delete the data at the source data address.

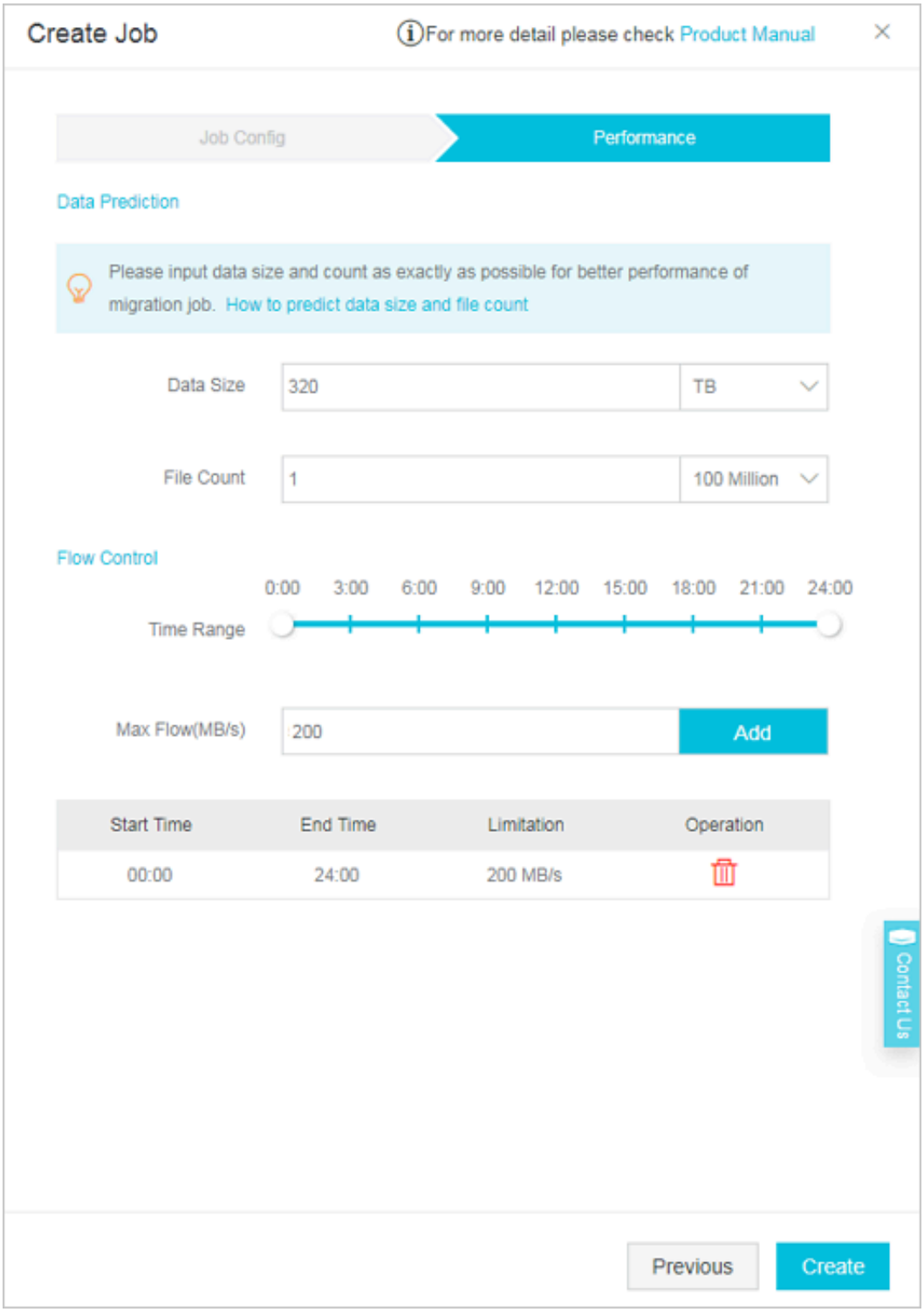
### Step 1: Migrate existing data

1. Create an OSS bucket to store migrated data. For more information, see *Create a bucket*.
2. Create the AccessKey of a RAM user that is used to migrate data.
   - To obtain the AccessKey of the storage service provided by Service Provider B, log on to storage service console to view the AccessKey.
   - To obtain the AccessKey of a RAM user, see *Create and authorize a RAM user*.

3. Create data addresses and a full migration job. For more information, see *Data Transport* documents. Configure the required options on the Job Config tab as follows.




Configure the required options on the Performance tab as follows.




4. To ensure that all data is migrated after migration, you need to *view a migration report* and compare data at both the source data address and the destination data address.

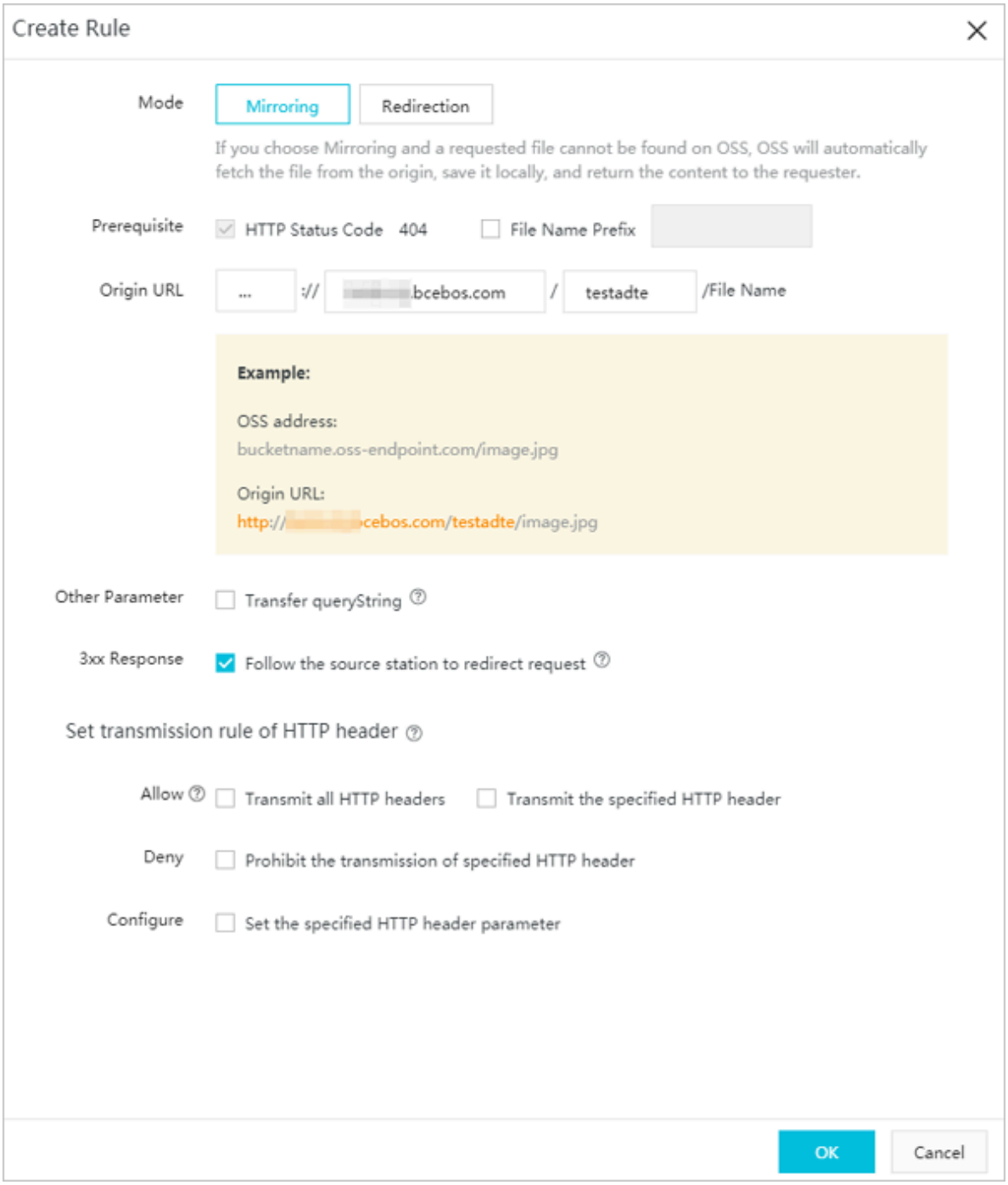
> **Note:**
> If a migration job fails, see *Common causes of a migration failure and solutions*.

### Step 2: Create back-to-origin rules

It takes about 25 days to migrate the existing data. During the migration process, data is continuously growing at the source data address. To ensure business continuity and a seamless switchover, you need to create `Back-to-Origin` rules. When files that are requested by end users do not exist in OSS, OSS fetches these files from the source data address and return them to end users.

1. Log on to the *OSS console*.
2. On the list of buckets, select the bucket where migrated data is located.
3. Select Basic Settings and click Configure in the Back-to-Origin section.

4. Click Create Rule. In the Create Rule dialog box, configure the required options.




- Mode: Select Mirroring.
- Prerequisite: HTTP Status Code 404 is selected by default. You can configure the File Name Prefix as needed.
- Origin URL: Enter the address of an endpoint.
- For more parameter settings, see *Create back-to-origin rules*.

**Note:**

You can create a maximum of five back-to-origin rules. The five rules take effect at the same time. For multiple source data addresses, you can create multiple back-to-origin rules. You can enable OSS to fetch various types of data by setting different values for the File Name Prefix.

5. Click OK.

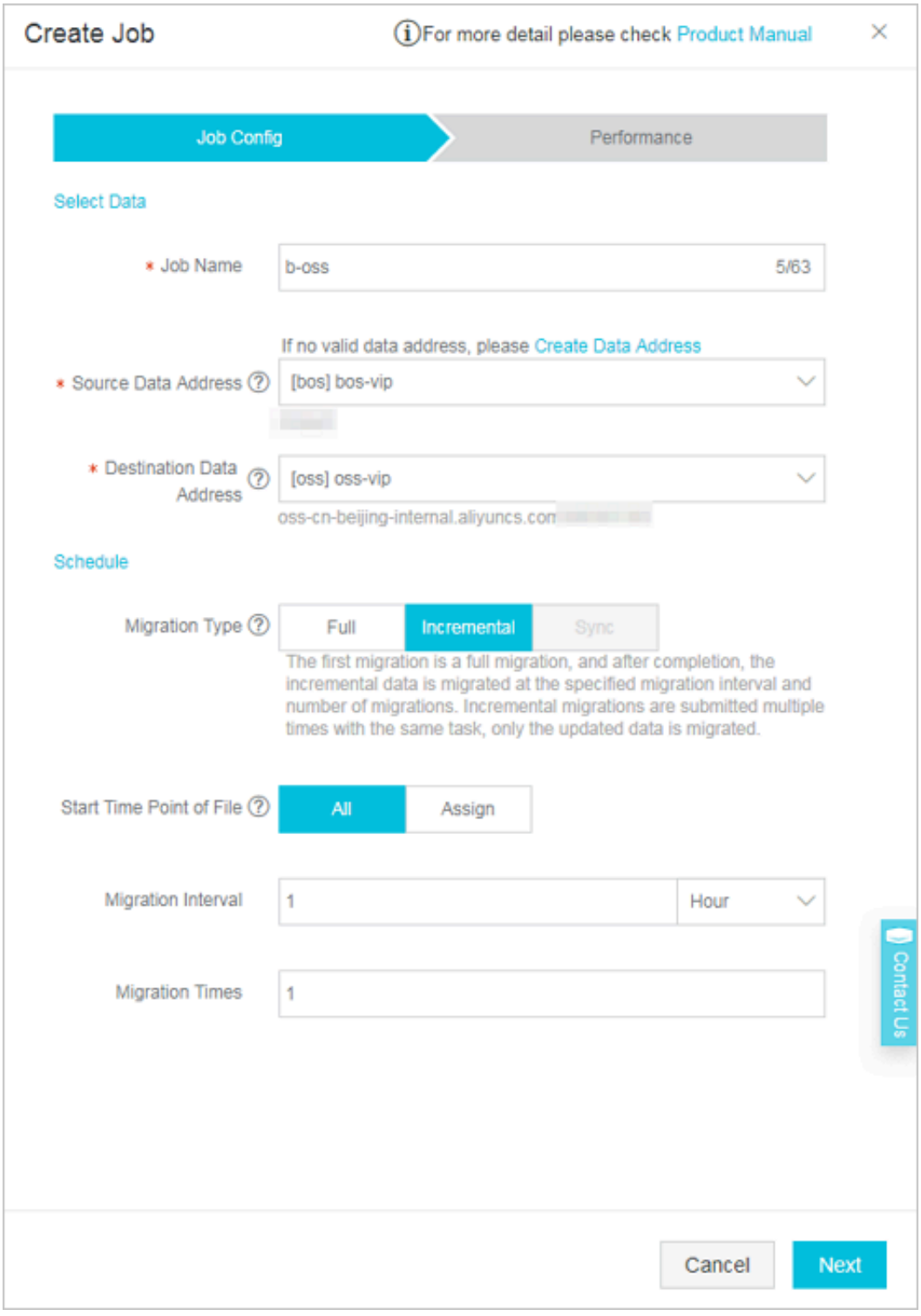
### Step 3: Switch businesses to OSS

Change the previous data address where the business application obtain data to OSS

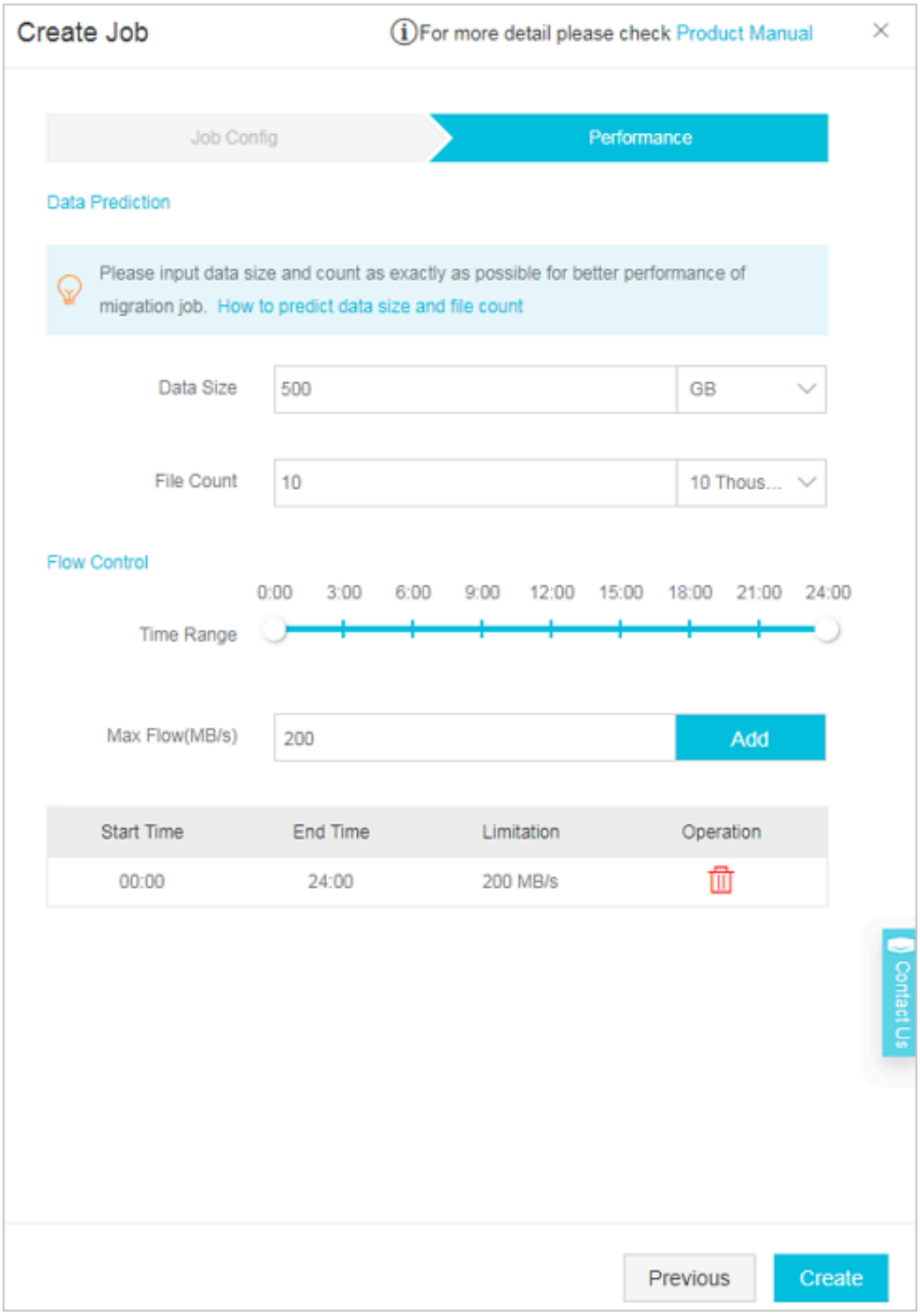
### Step 4: Migrate incremental data

During the migration of existing data, about 100,000 files that reach a total size of about 500 GB are generated. You must migrate these incremental files to OSS.

1. Create an incremental migration job based on the steps described in Step 1. Configure the required options on the Job Config tab as follows:




Configure the required options on the Performance tab as follows:




2. Click Create to create a migration job.
3. To ensure that all data is migrated after migration, you need to *view a migration report* and compare data at both the source data address and the destination data address.

> **Note:**
> If a migration job fails, see *Common causes of a migration failure and solutions*.

### Step 5: Delete data at the source data address

After a migration job is complete, you can create a lifecycle rule for files at the source data address to avoid extra charges for storage. This rule sets an expiration date for files of one day after the time when the migration job is complete. All data at the source data address is deleted on the expiration date.

# 2 Migrate data from a local NAS file system to OSS

This topic describes how to migrate data from a local Network Attached Storage (NAS) file system to Object Storage Service (OSS) for long-term storage.

## Background information

Assume that an entertainment company in Hangzhou needs to stores data, such as media files and documents on its local NAS file server. The data includes 5,000,000 files, which is about 20 TB. The NAS server is located in a local server room. The SMB protocol is used on the server that is enabled with a firewall. As no Internet connection exists, the private IP of the server is 10.0.0.254.

To facilitate maintenance and further development of online applications, the company needs to migrate data from the NAS server to OSS.

## Procedure

Based on the needs and background information, you can migrate data as follows:

1. Create a bucket in the China (Hangzhou) region and change the default storage location to the data address of this bucket.
2. Connect the NAS server to an Alibaba Cloud VPC by using a dedicated leased line. Modify the firewall settings of the NAS server and enable access to the NAS server by all IP addresses in the VPC.
3. With Data Transport, proceed as follows to migrate data from NAS to OSS.

## Step 1: Create a bucket and modify a storage location

1. In the China (Hangzhou) region, create a bucket to store data. For more information, see *Create a bucket*.
2. Set the bucket policy and only enable access to the bucket from company employees. For more information about configurations, see *Use bucket policies to authorize other users to access OSS resources*.
3. Inform internal employees of changing the default storage location to the data address of the bucket.

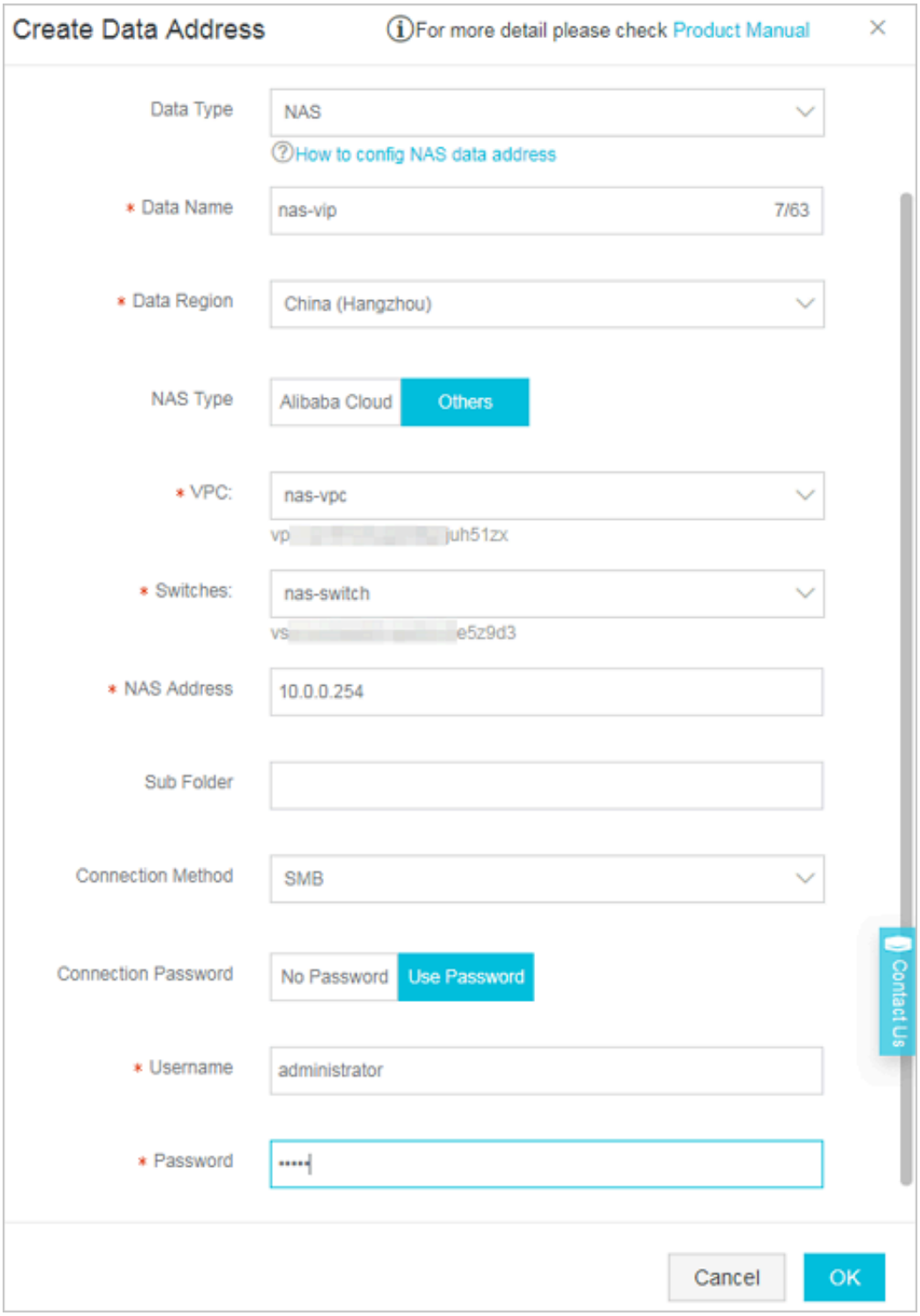
### Step 2: Connect the NAS server to the VPC

1. Connect the NAS server to the VPC using a dedicated data circuit with a maximum bandwidth of 1 Gbit/s. For more information, see *Connect an on-premises IDC to a VPC through a physical connection*.
2. Modify the firewall settings of the NAS server to enable access to the NAS server by all IP addresses in the VPC.

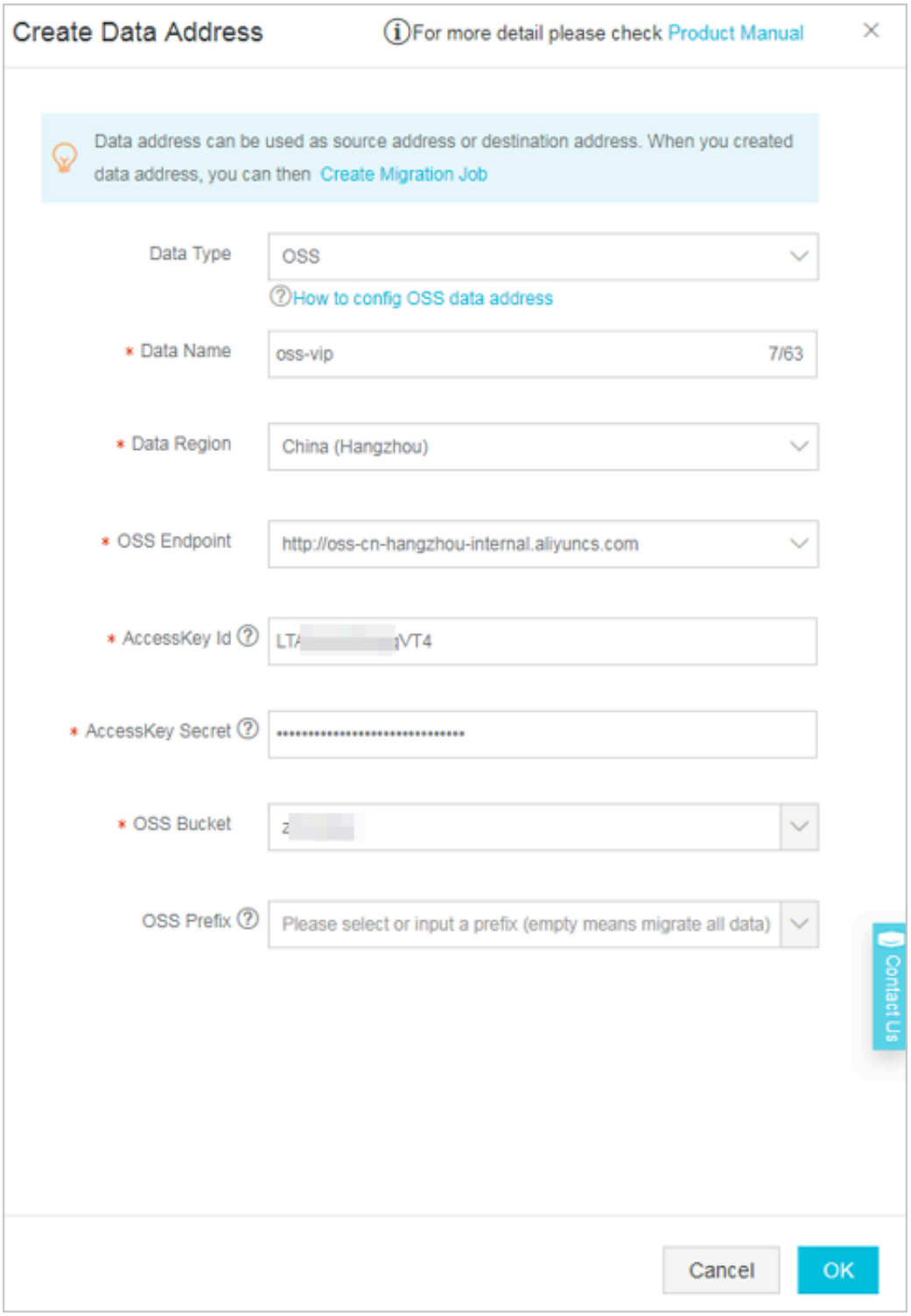
### Step 3: Migrate data from NAS to OSS by using Data Transport

1. Create a RAM user in Alibaba Cloud and grant the RAM user the permission to create migration jobs. Additionally, obtain the AccessKey of the RAM user. For more information, see *Create and authorize a RAM user*.

2. Create a NAS data address. For more information about options, see *Migrate data from NAS to OSS*. The options are shown in the following figure.

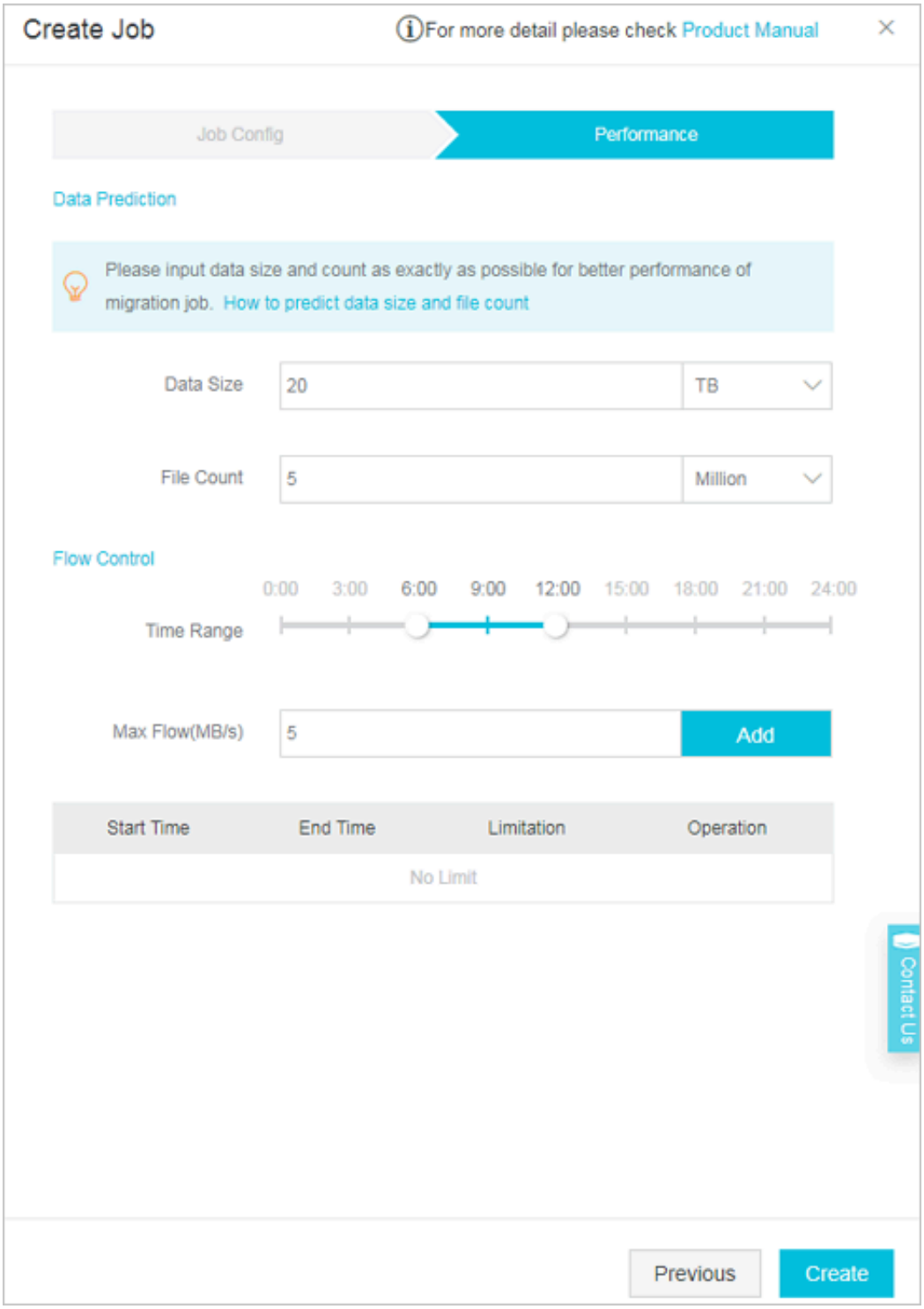


3. Create an OSS data address. For more information about options, see *Migrate data from NAS to OSS*. The options are shown in the following figure.




4. Create a full migration job and configure the required options in the Performance step. For more information about options, see *Migrate data from NAS to OSS*. The

options that you can configure in the Performance steps are shown in the following figure.




**Notice:**

**In this case, the entertainment company has no bandwidth needs for other applications while migrating data. Therefore, no flow control is set. In actual practice, you can set appropriate flow limits based on the usage of the bandwidth.**

5. A migration job requires about two days to complete. To ensure that all data is migrated, you need to *view a migration report* and compare data at both the source data address and the destination data address.

    Note:

   If a migration job fails, see *Common causes of a migration failure and solutions*.

6. After a migration job is complete, the storage of data, management of data, and other subsequent actions are all performed in OSS.

# 3 Migrate data between NAS files systems that are located in different VPCs

This topic describes how to migrate data between NAS file systems that are located in different VPCs.

## Background information

Assume that a Shenzhen company is named Company A. As Company A grows and needs to expand, this company establishes a sub-branch in Hangzhou, which is named Branch B. The data of Branch B is stored in a NAS file system. However, you must synchronize the data of Branch B to another NAS file system where the data of Company A is stored. Each day, Branch B generates about 100,000 files whose size is about 100 GB.

The NAS file system of Company A and the NAS file system of Branch B are located in separate VPCs. The 172.16.1.0/24 IP segment is used for the VPC where the file system of Company A is located, which is abbreviated as VPC A. The 10.0.0.0/24 IP segment is used for the VPC where the file system of Branch B is located, which is abbreviated as VPC B.

**Note:**
If you are using third-party NAS file systems, you must attach the NAS server to an Alibaba Cloud VPC by using a dedicated data circuit. For more information, see *Connect an on-premises IDC to a VPC through a physical connection*.

## Create a migration job

1. You can establish the connection between VPC A and VPC B by using Cloud Enterprise Network (CEN) and configure permission groups.
2. Create a synchronization job that synchronizes the data of Branch B to Company A on a regular basis.

## Step 1: Connect VPC A with VPC B by using CEN

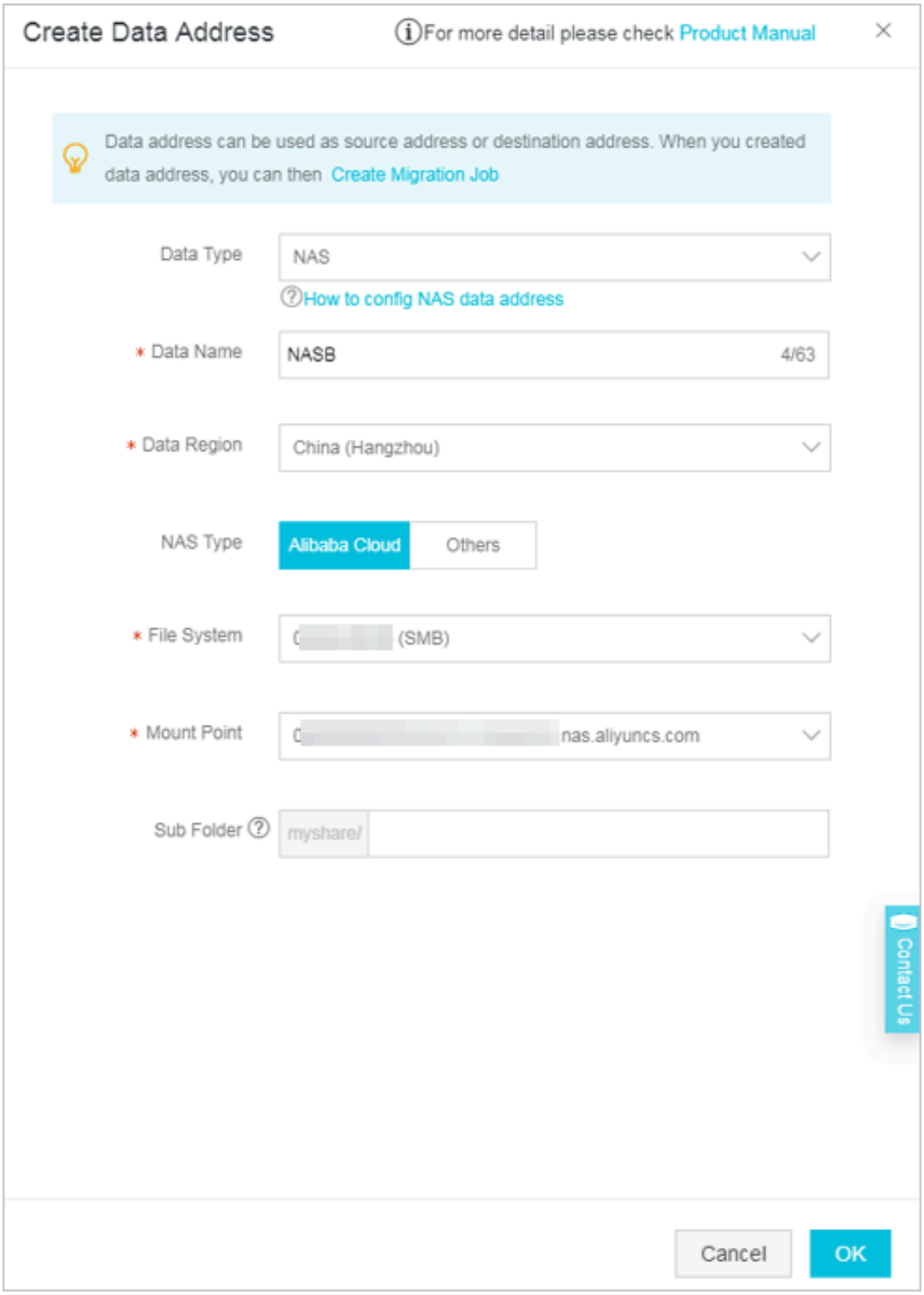
1. With CEN, you can connect VPC A with VPC B. For more information, see *Connect VPCs that are located in multiple regions and owned by different accounts*.

2. Modify the NAS permission groups of Company A and Branch B. This allows all devices in the 10.0.0.0/24 IP segment to read data from the NAS file system of Branch B and write data to the NAS file system of Company A. For more information, see *Use permission groups*.

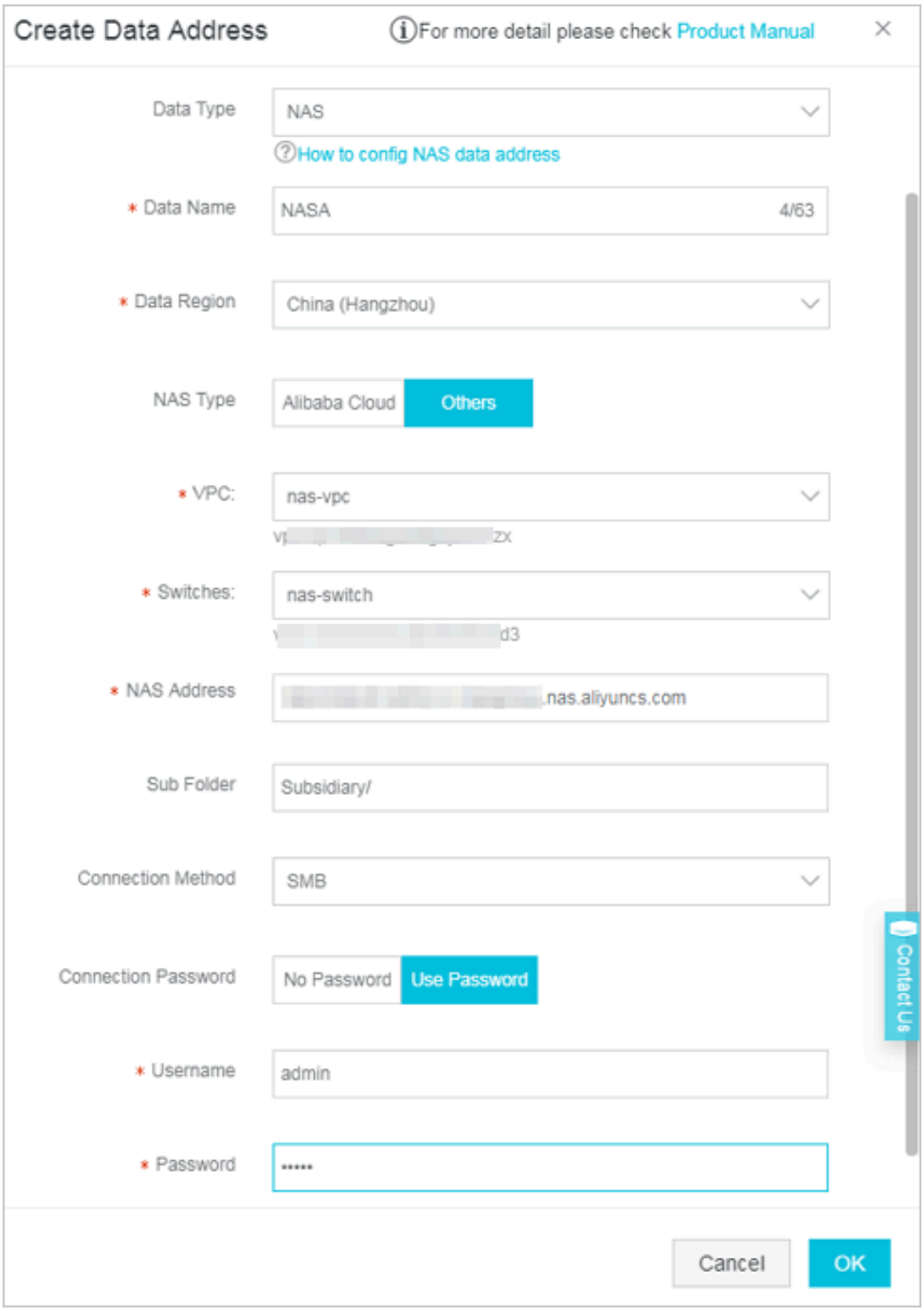
### Step 3: Create a migration job

1. Create a RAM user and grant the RAM user the permission to create migration jobs. For more information, see *Create and authorize a RAM user*.

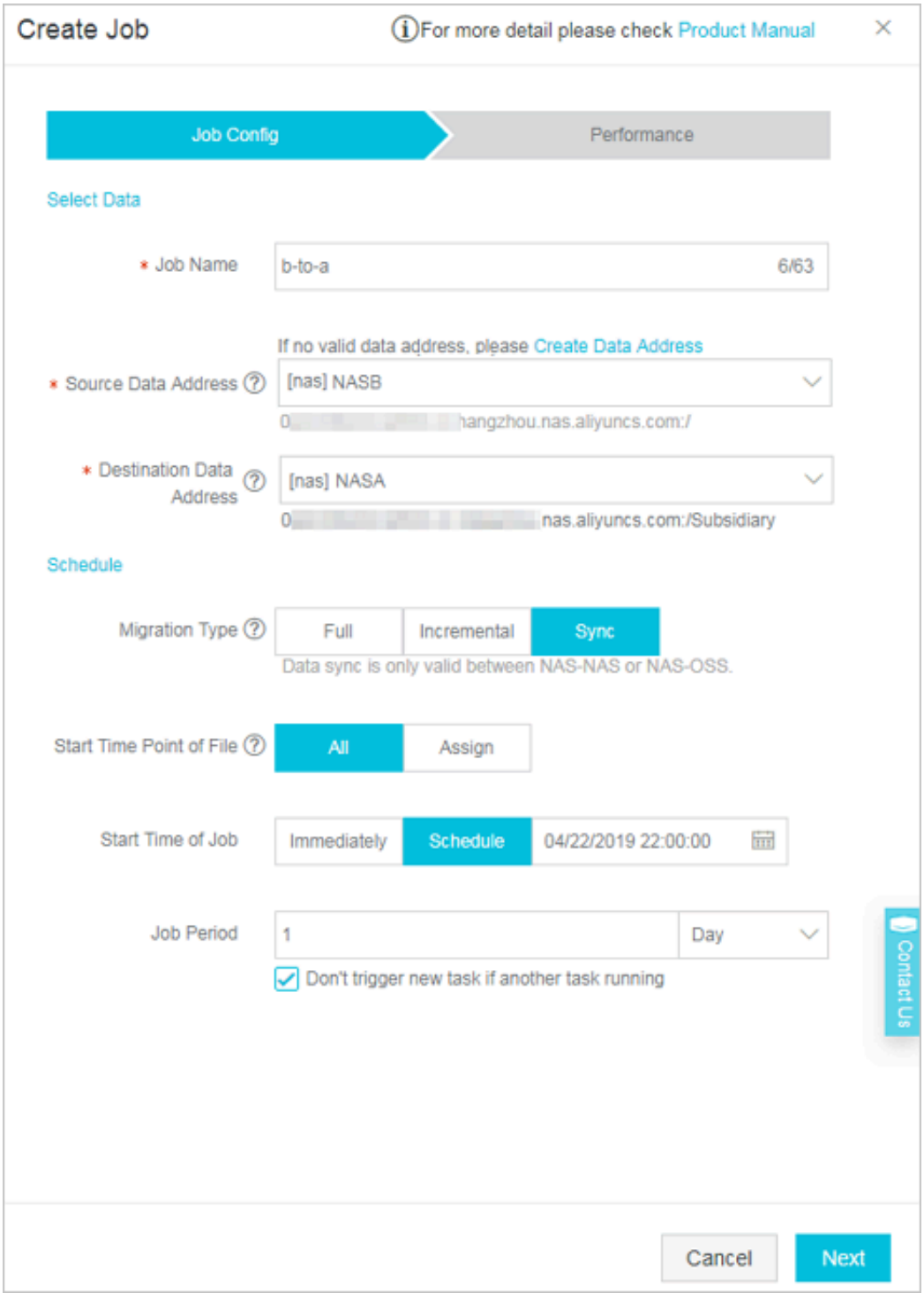
2. Create the source NAS data address. For more information about options, see *Create the source data address*. The options are shown in the following figure.



3. Create the destination NAS data address. For more information about options, see *Create the destination data address*. The options are shown in the following figure.



4. Create a Sync migration job. To ensure business continuity, set the daily start time of a synchronization job to 22:00. For more information about options, see *Create a migration job*. The options are shown in the following figure.




**Notice:**

- A synchronization job keeps running until you manually stop the job. Therefore, you only need to create one synchronization job to meet the needs of synchronizing data on a regular basis.
- In this case, as the customer synchronizes a small amount of data during off-peak hours, you can use the default settings in the Performance step. In actual practice, you can set appropriate performance options based on the usage status of the bandwidth.

5. After each synchronization subtask is complete, you must perform specific actions to ensure data is synchronized. These actions include viewing the status of a subtask, and comparing the data of the source data address with that of the destination data address. For more information about how to view the status of synchronization subtasks, see *Manage synchronization subtasks*.

# 4 Migrate data from a local NAS file system to Alibaba Cloud NAS

This topic describes how to migrate data from a local Network Attached Storage (NAS) file system to Alibaba Cloud NAS for long-term storage.

## Background information

Assume that a Hangzhou pharmaceutical enterprise stores data, such as product documents and experimental data on its local NAS file server. The data includes 10, 000,000 files, which is about 10 TB. The NAS server is located in a local s server room. The SMB protocol is used on the server that is enabled with a firewall. As no Internet connection exists, the private IP address of the server is 10.0.0.254.

Based on the considerations of data security and cost, the company needs to migrate data from the NAS server to Alibaba Cloud NAS.

## Procedure

Based on the needs and background information, you can migrate data as follows:

1. Create a NAS file system in the China (Hangzhou) region and mount the file system on an ECS instance that is located in a VPC.
2. Connect the NAS server to a VPC by using a dedicated data circuit. Modify the firewall settings of the NAS server and enable access to the NAS server by all IP addresses in the VPC.
3. Use Data Online Migration to migrate data from the NAS server to Alibaba Cloud NAS.

## Step 1: Create a file system in Alibaba Cloud NAS

1. In the China (Hangzhou) region, create a NAS file system whose protocol type is Network File System (NFS). For more information, see *Create a file system*.
2. Mount the file system on an ECS instance that is locate in the VPC For more information, see *Add a mount point*.
3. Modify the security group of the VPC to enable access to the NAS file system from all IP addresses in the VPC. For more information, see *Use permission groups*.

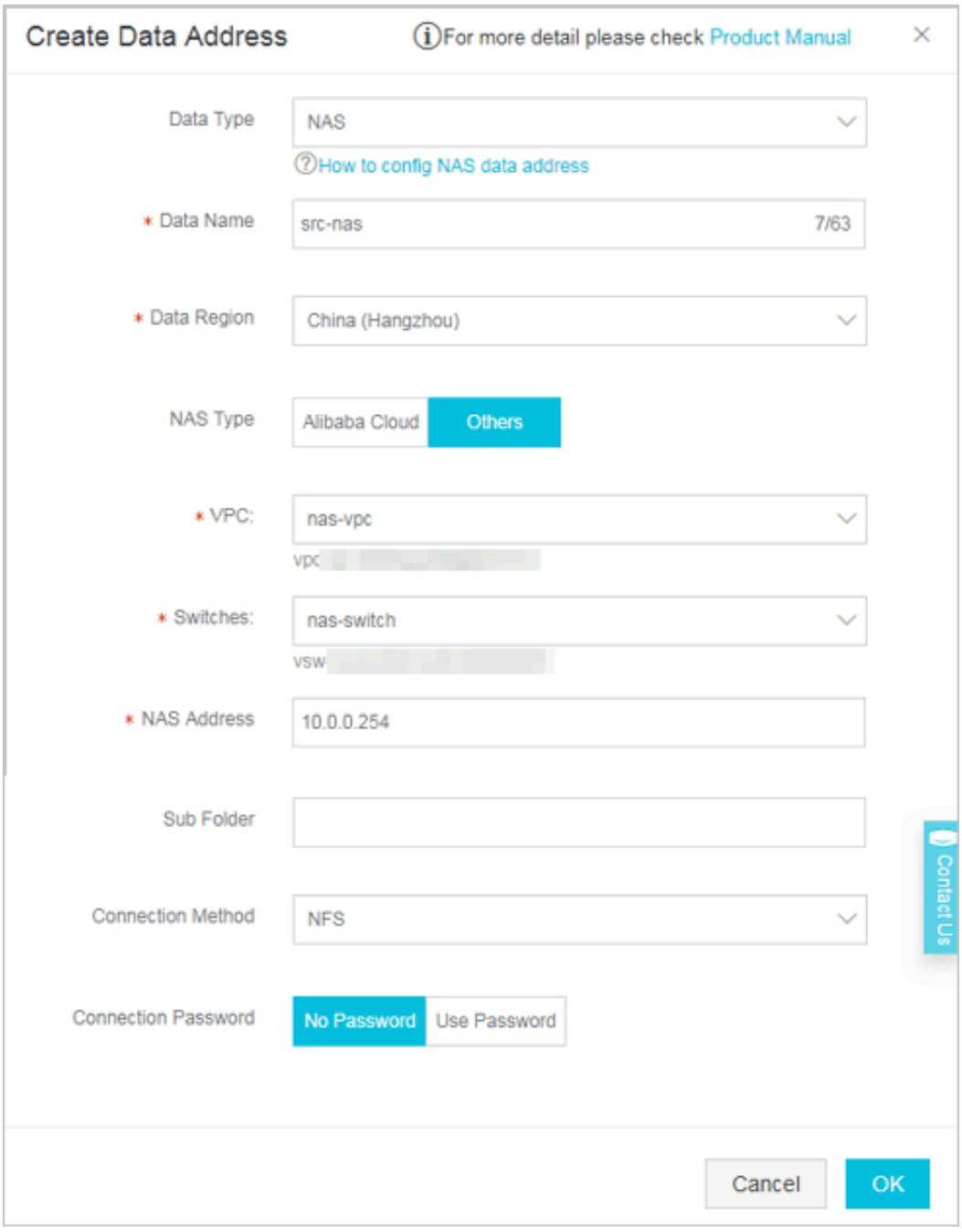
### Step 2: Attach the NAS server to the VPC

1. Connect the NAS server to the VPC where the ECS instance hosting the NAS file system is located. The connection is established using a dedicated data circuit with a maximum bandwidth of 1 Gbit/s. For more information, see *Connect an on-premises IDC to a VPC through a physical connection*.
2. Modify the firewall settings of the NAS server to enable access to the NAS server by all IP addresses in the VPC.

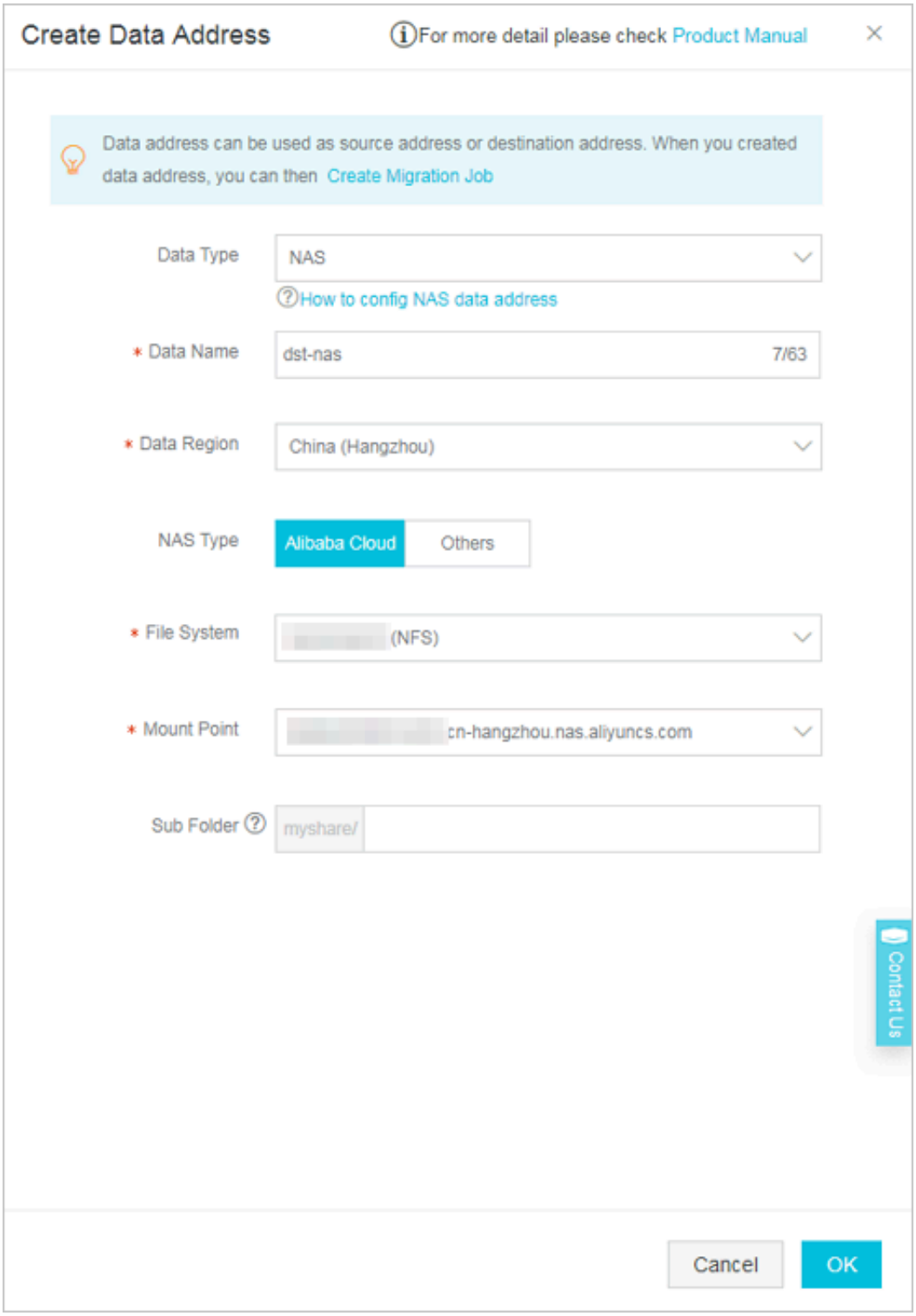
### Step 3: Create a migration job

1. Create a RAM user in Alibaba Cloud and grant the RAM user the permission to create a migration job. For more information, see *Create and authorize a RAM user*.
2. Log on to the *Data Transport* console by using the RAM user account. Use the information of the local NAS server to create the source data address. For more

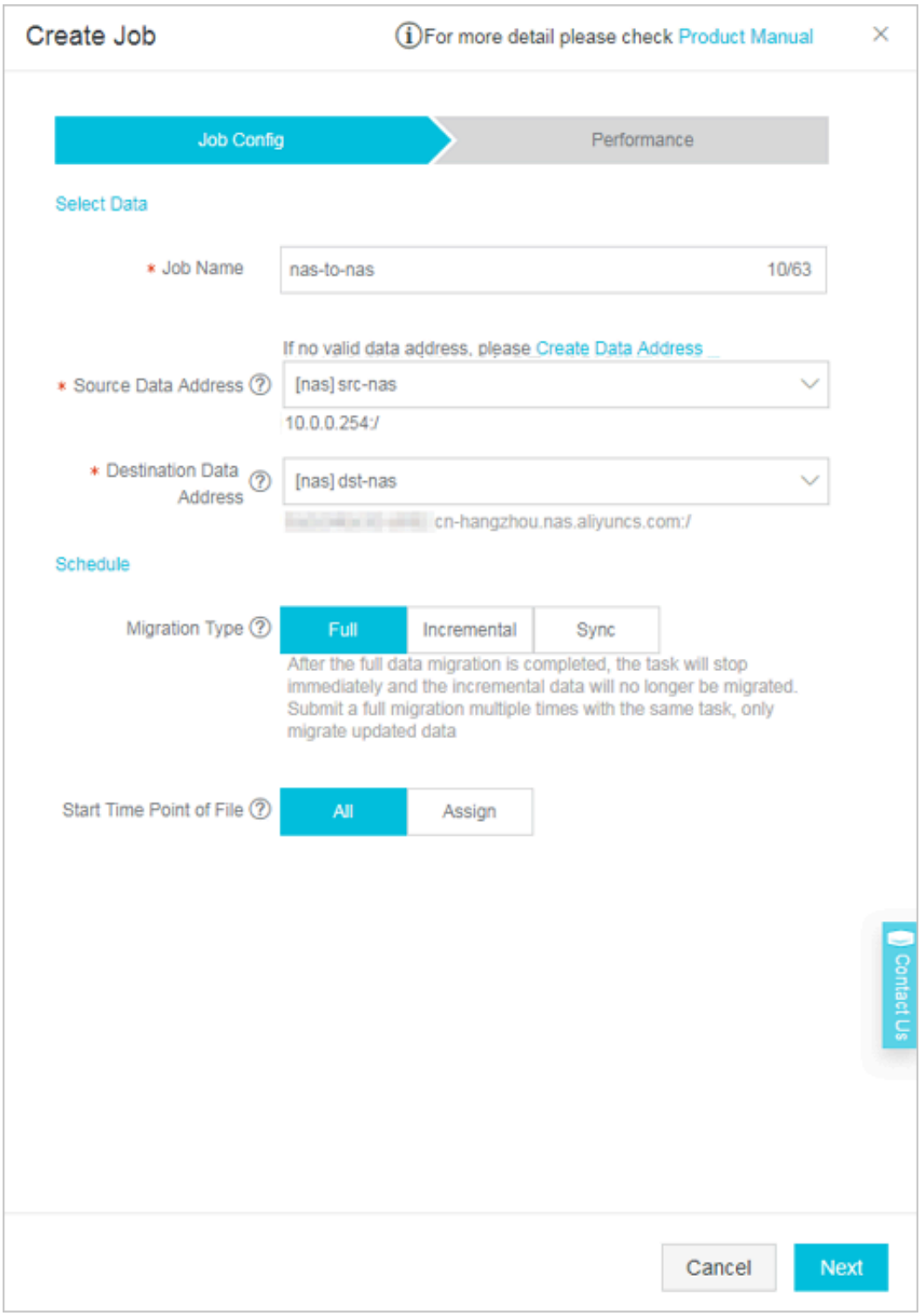
information about options, see *Create a source data address*. The configuration details are shown in the following figure.



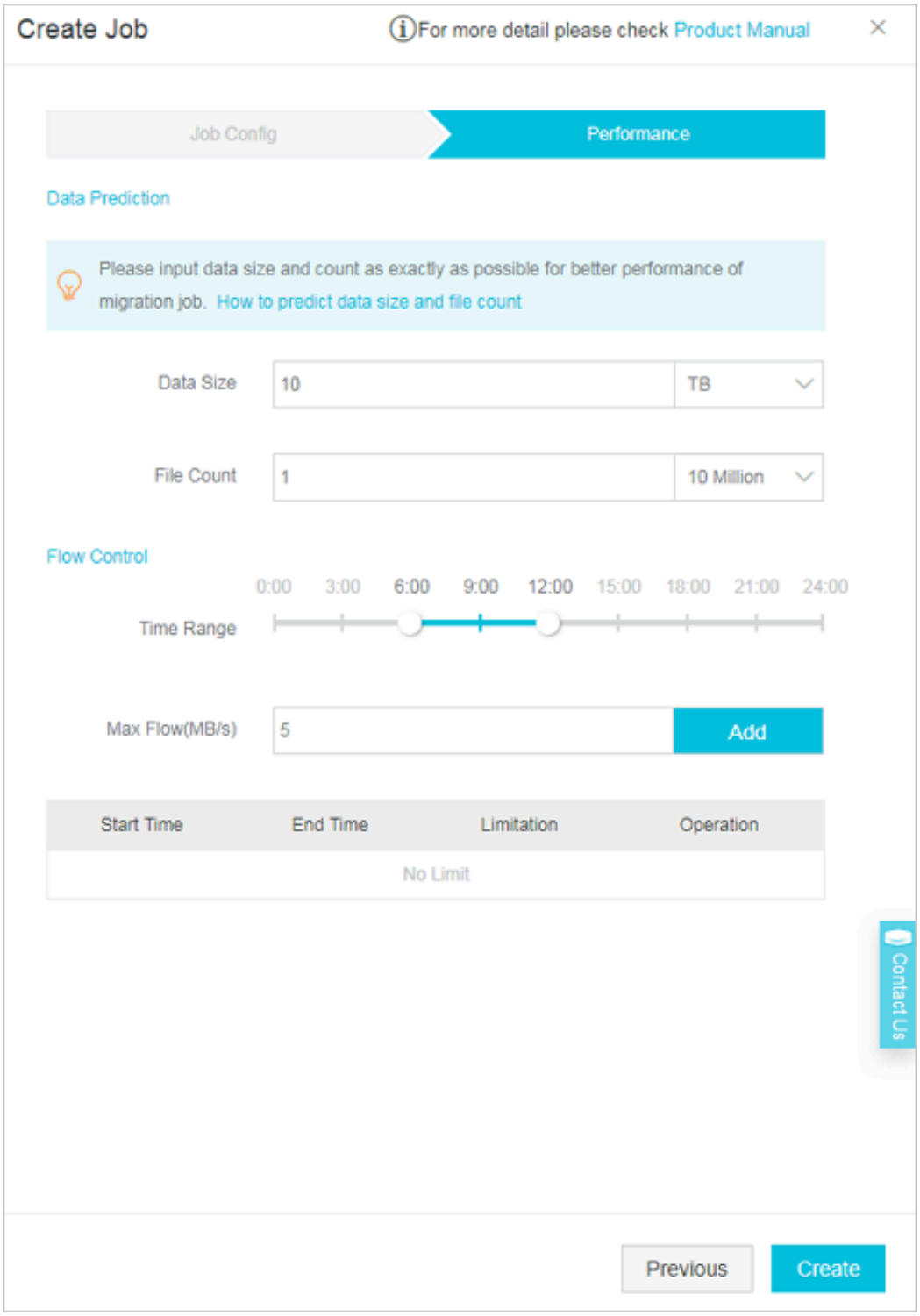
3. Use the information of the Alibaba Cloud NAS file system to create the destination data address. The configuration details are shown in the following figure.



4. Create a full migration job to migrate data from the NAS server to Alibaba Cloud NAS. For more information about options, see *Create a migration job*.




The options that you can specify in the Performance step are shown in the following figure.




5. A migration job requires about two days to complete. To ensure that all data is migrated, you need to *view a migration report* and compare data at both the source data address and the destination data address.

> **Note:**
> If a migration job fails, see *Common causes of a migration failure and solutions*.