Alibaba Cloud Lightning Cube

Migrate data from ECS instances to OSS

Issue: 20190509

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: 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: 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: 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: 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 Background information

This guide describes how to migrate shared files from ECS instances to Object Storage Service (OSS).

Alibaba Cloud Data Migration Service is used as a data channel between various data stores. With Data Migration Service, you can migrate shared files from ECS instances to OSS.

To migrate these shared files, you only need to enter the data addresses for both shared files and OSS, and then create a migration job. After starting a migration job, you can perform management tasks for the job such as viewing the process and status of the job. Additionally, you can view the list of files to be migrated and the list of files that failed to be migrated.

This guide includes the following sections:

- *Prerequisites*
- *Create a migration job*
- *Manage a migration job*

2 Prerequisites

This section describes what you need to do before creating a migration job.

ECS instances

On an ECS instance, you can use the following steps to share folders:

- Windows

  If Windows is running on the instance, proceed as follows:

  1. Place data to be migrated in a folder and share the folder. Follow the version-specific instructions to share a folder.
  2. Modify the settings of Windows Defender Firewall and anti-virus software to enable access to port 445 of the instance (by all IP addresses in the VPC where the instance is located). Skip this step if both Windows Defender Firewall and anti-virus software are disabled.
  3. Add ECS *security group rules* to enable access to port 445 of the instance by all IP addresses in a VPC where the instance is located.

- Linux

  If Linux is running on the instance, proceed as follows:

  1. Start the NFS service and share the folder to be migrated. For more information, see *Start the NFS service*. Skip this step if the NFS service is enabled.
  2. Modify the settings of Linux firewalls to enable access to the corresponding port of the NFS service. You can use the `rpcinfo -p localhost` command to view the corresponding ports to be enabled of the `portmapper`, `mountd`, and `nfs` services. For more information, see *Firewall settings*. If firewalls are not enabled, skip this step.
  3. Add ECS *security group rules* to enable access to the corresponding port of the NFS service by all IP addresses in a VPC where the instance is located.

     Warning:
     To ensure data security, disable access to the port of the NFS service by external networks.

Alibaba Cloud Object Storage Service

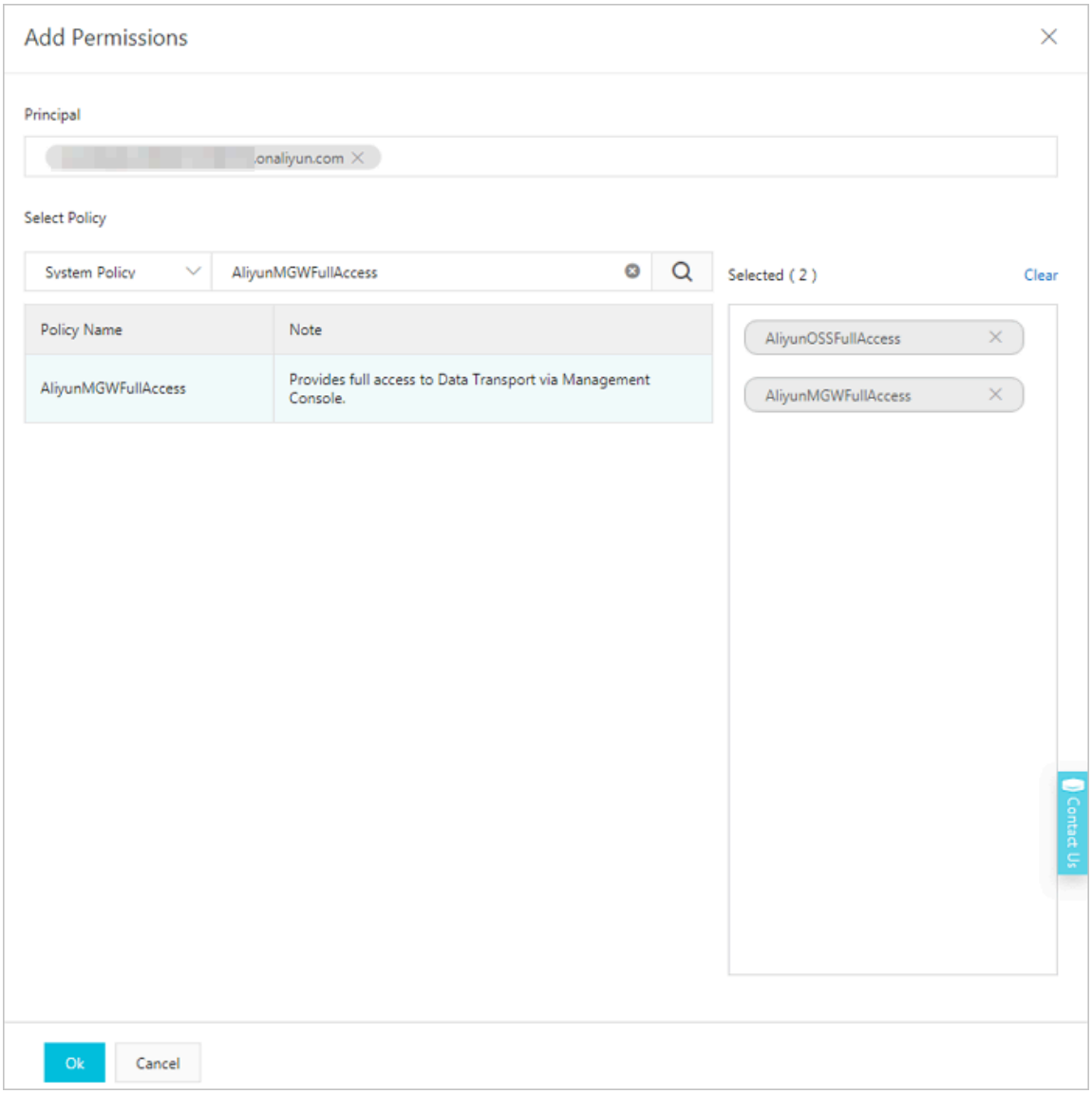
- **Create a bucket**

  Create the target bucket that is used to store migrated data For more information, see *Create a bucket*.

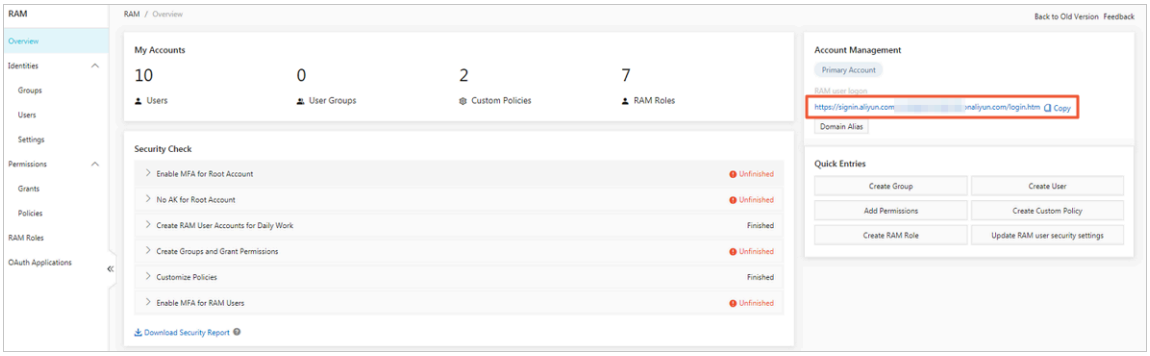
- **Create and authorize a RAM user**

  1. Log on to the *RAM console*.
  2. Choose Identities > Users > Create User.
  3. Select Console Password Logon and Programmatic Access and enter the required User Account Information.
  4. Click OK to save the generated account, password, AccessKeyID, and AccessKeySecret.
  5. Select the required user account, click Add Permissions to grant the read/write permission (AliyunOSSFullAccess) and migration permission

(AliyunMGWFullAccess) for the RAM user. The Add Permissions dialog is shown in the following figure.



6. Choose OK > Finished.
7. In the left-side navigation pane, select Overview, click the link in the RAM user logon section, and enter the username and password of the newly created RAM user to log on to the console.



Appendix: How to use NFS

Before using NFS, you need to start the NFS service and enable access to the port of the NFS service in the firewall.

- Assume that you need to share the */ data* folder as the source data address. Proceed as follows:

  1. Enable the NFS file system.

     ```
     [ root @ test  ~]#  yum   install  - y   nfs - utils
     ```

  2. Share the */ data* folder. In the */ etc / exports* file, add /data *(rw,no_root_squash).

     ```
     [ root @ test  ~]#  vi  / etc / exports

     # If   the   port   number   of   mountd   is   greater   than
      1024 ,  you   need   to   add   the   insecure   parameter .
     #/ data  * ( rw , no_root_sq  uash , insecure ),
     / data  *( rw , no_root_sq  uash )
     ```

  3. Start the NFS service.

     ```
     [ root @ localhost  ~]# systemctl   start   nginx . service
     ```

  4. View the status of the NFS service. The following status indicates that the service is running.

     ```
     [ root @ localhost  ~]# systemctl   status   nginx . service
     â—  nfs - server . service  -  NFS   server   and   services
      Loaded :  loaded  (/ usr / lib / systemd / system / nfs - server
      . service ;  disabled ;  vendor   preset :  disabled )
      Active :  active  ( exited )  since   Thu   2018 - 12 - 06   15 :
      47 : 03   CST ;  58s   ago
      Process :  10641   ExecStartP  ost =/ bin / sh  - c   if
      systemctl  - q   is - active   gssproxy ;  then   systemctl
        restart   gssproxy  ;  fi  ( code = exited ,  status = 0 /
      SUCCESS )
      Process :  10623   ExecStart =/ usr / sbin / rpc . nfsd  $
      RPCNFSDARG  S  ( code = exited ,  status = 0 / SUCCESS )
      Process :  10621   ExecStartP  re =/ usr / sbin / exportfs  - r
      ( code = exited ,  status = 0 / SUCCESS )
      Main   PID :  10623  ( code = exited ,  status = 0 / SUCCESS )
      CGroup : / system . slice / nfs - server . service


      Dec   06   15 : 47 : 03   test   systemd [ 1 ]:  Starting   NFS
      server   and   s ...
      Dec   06   15 : 47 : 03   test   systemd [ 1 ]:  Started   NFS
      server   and   se ...
     ```

```
 Hint :  Some   lines   were   ellipsized ,  use  - l   to   show
   in   full .
```

5. Enable the service to run at startup.

```
[ root @ localhost  ~]#  systemctl   enable   nginx . service
```

6. View the status of the rpcbind service. The following status indicates that the service is running.

```
[ root @ test  ~]#  systemctl   status   rpcbind . service
â—  rpcbind . service  -  RPC   bind   service
 Loaded :  loaded  (/ usr / lib / systemd / system / rpcbind .
 service ;  enabled ;  vendor   preset :  enabled )
 Active :  active  ( running )  since   Thu   2018 - 12 - 06   15
 : 47 : 03   CST ;  7min   ago
 Main   PID :  10598  ( rpcbind )
 CGroup : / system . slice / rpcbind . service
â””â”€ 10598  / sbin / rpcbind  - w


 Dec   06   15 : 47 : 03   test   systemd [ 1 ]:  Starting   RPC
 bind   service ...
 Dec   06   15 : 47 : 03   test   systemd [ 1 ]:  Started   RPC
 bind   service .
 Hint :  Some   lines   were   ellipsized ,  use  - l   to   show
   in   full .
```

- Firewalld is used by default for ECS instances that run CentOS 7. You can use the `systemctl status firewalld` command to check whether firewalld is enabled. If you are using iptables, use the related iptables commands to enable access to the ports (that are required by NFS) based on the following firewalld settings. Configure firewalld as follows:

1. View the list of enabled ports that are required for NFS.

```
[ root @ test  ~]#  rpcinfo  - p   localhost
    program   vers   proto     port    service
     100000      4     tcp      111    portmapper
     100000      3     tcp      111    portmapper
     100000      2     tcp      111    portmapper
     100000      4     udp      111    portmapper
     100000      3     udp      111    portmapper
     100000      2     udp      111    portmapper
     100024      1     udp    50382    status
     100024      1     tcp    59133    status
     100005      1     udp    20048    mountd
     100005      1     tcp    20048    mountd
     100005      2     udp    20048    mountd
     100005      2     tcp    20048    mountd
     100005      3     udp    20048    mountd
     100005      3     tcp    20048    mountd
     100003      3     tcp     2049    nfs
     100003      4     tcp     2049    nfs
     100227      3     tcp     2049    nfs_acl
     100003      3     udp     2049    nfs
     100003      4     udp     2049    nfs
     100227      3     udp     2049    nfs_acl
```

```
    100021      1     udp    37473    nlockmgr
    100021      3     udp    37473    nlockmgr
    100021      4     udp    37473    nlockmgr
    100021      1     tcp    37688    nlockmgr
    100021      3     tcp    37688    nlockmgr
    100021      4     tcp    37688    nlockmgr
```

2. Add the following firewall rules to enable the corresponding ports of the `portmapper`, `mountd`, and `nfs` services. These ports include port 111, port 20048, and port 2049 for the TCP and UDP protocols respectively.

   Note:
   As the `mountd` service uses a random port number, you must use one of the following methods to retrieve the port number of the `mountd` service and then configure firewalld.

   - Use the `rpcinfo -p localhost` command to view the port number used by the `mountd` service.
   - Open the */etc/sysconfig/nfs* file, replace xxx with a port number in the `MOUNTD_PORT=xxx` expression to specify a fixed port number for the `mountd` service.

3. Add the following firewall rules:

```
[root@test ~]# firewall-cmd --zone=public --add-
port=111/tcp --permanent
success
[root@test ~]# firewall-cmd --zone=public --add-
port=20048/tcp --permanent
success
[root@test ~]# firewall-cmd --zone=public --add-
port=2049/tcp --permanent
success
[root@test ~]# firewall-cmd --zone=public --add-
port=111/udp --permanent
success
[root@test ~]# firewall-cmd --zone=public --add-
port=20048/udp --permanent
success
[root@test ~]# firewall-cmd --zone=public --add-
port=2049/udp --permanent
success
```

4. Update firewall rules.

```
[root@test ~]# firewall-cmd --reload
success
```

3 Create a migration job

This section describes the operations and considerations for data migration.

Precautions

When creating a migration job, you need to note the following issues:

- A migration job occupies the network resources of the source data address and the destination data address. To ensure business continuity, we recommend that you specify a speed limit for a migration task or perform the migration task during an off-peak period.
- Before a migration task is performed, files at both the source data address and the destination data address are checked. If files at the source data address have the same names as those at the destination data address and have a later update time than those at the destination data address, the files at the destination data address are overwritten during a migration task. If the content for two files is different, you must change the name of one of the files and back up these files.

Step 1: Create a source data address

1. Log on to the *Data Migration Service console*.
2. Choose Data Online Migration > Data Address, and then click Create Data Address.
3. In the Create Data Address dialog box, set the required options and click OK. The options are described as follows:

Option	Required	Description
Data type	Yes	Select NAS.
Data Region	Yes	Select a region where an ECS instance is located.
Data Name	Yes	Enter 3 to 63 characters. Special characters, except for hyphens (-) and underscores (_), are not supported.
NAS Type	Yes	Select Others.
VPC	Yes	Select a VPC where the instance is located.
Switches	Yes	Select a VSwitch that the VPC uses.

Option	Required	Description
NAS Address	Yes	Enter the private IP address of the ECS instance.
Sub Folder	Yes	Enter the path of the shared folder where data to be migrated is located.
Connection Method	Yes	Select the type of protocol used to share access to files.
Connection Password	Optional	Select whether a password is required to access the shared folder. · No Password: You can access the shared folder without a username and password. · Use Password: Enter the required username and password. You must use the username and password to access the shared folder. Note: When a Windows operating system is running on the instance, you must enter the username and password. For a Linux operating system, you can select one of the preceding options.

Note:
For more information about the status of a data address after you create it, see *Data address status*.

4. You are required to apply for whitelist permissions because this feature is in the beta testing phase. Click Application.
5. Enter the required information and submit the beta testing application for migration. After the application has been approved, you will receive an SMS notification.

Step 2: Create a destination data address

1. Select Data Online Migration > Data Address and click Create Data Address.

2. In the Create Data Adress dialog box, set the required options and click OK. The options are described as follows:

Option	Required	Description
Data Type	Yes	Select OSS.
Data Region	Yes	Select a region where the destination data address is located.
Data Name	Yes	Enter 3 to 63 characters. Special characters, except for hyphens (-) and underscores (_), are not supported.
OSS Endpoint	Yes	Select an endpoint based on the region where data is located. For more information, see *Endpoints*.
AccessKeyId and AccessKeySecret	Yes	Enter an AccessKey that is used to migrate data. For more information, see *Create an AccessKey*.
OSS Bucket	Yes	Select a bucket to store migration data.
OSS Prefix	No	An OSS prefix cannot start with a forward slash (/) and must end with a forward slash (/). For example: `data / to / oss /`. If you want to store data to the root directory of a bucket, you can leave the OSS Prefix field blank.

Step 3: Create a migration job

1. Select Data Online Migration > Migration Jobs and click Create Job.
2. In the Create Job dialog box, read the Terms of Migration Service, select I understand the above terms and conditions, and activate Data Migration Service, and then click Next.
3. In the Create Job dialog box, set the required options and click Next.

   The options are described as follows:

Option	Required	Description
Job Name	Yes	Enter 3 to 63 characters including lowercase letters, numbers, and hyphens (-). A job name cannot start or end with a hyphen (-).

Option	Required	Description
Source Data Address	Yes	Select the created source data address.
Destination Data Address	Yes	Select the created destination data address.  Notice: If the region where the source data address is located is different from the region where the destination data address is located, you can *open a ticket* to apply for the permission of creating a cross-region migration job. You must ensure that your business is legitimate, data transit conforms to local rules and regulations, and that the data does not include illegal information.

Option	Required	Description
Migration Type	Yes	Before you start a migration job, the migration service compares files of the source data address with those of the destination data address. When the names of files at the destination data address are the same as those at the source data address and the files at the destination data address have the latest update time, these files are disregarded during migration. However, the other files are migrated. · Full: You can specify the Start Time Point of File. Files whose last modified time is later than the specified start time are migrated. After all of the files are migrated, a migration job is closed. When you perform a full migration job again, the migration service only migrates files that have been changed after the last full migration job. · Incremental: You must specify the Migration Interval and Migration Times to perform an incremental migration job. You must specify the Start Point Time of File. Files whose last modified time is later than the specified start time are migrated for the first time. After the first migration job is complete, an incremental migration job is performed based on the Migration Interval. At the source data address, files that are created or modified between the time when the last migration job started and before the time when this migration starts will be migrated to the destination data address. Assume that you specify N for the Migration Times. A full migration is performed once. In the future, an incremental migration will be performed (N - 1) times. For example, you set the Migration Interval to 1 and Migration Times to 5. Additionally, you set the Start Time Point of File to 03/05/2019 08:00:00

Option	Required	Description
Start Time Point of File	Yes (only for Full and Incremental)	· All: All files are migrated. · Assign: Files that are created or modified after the specified time are migrated. For example, when you set the Start Time Point of File to 11/01/2018 08:00:00, only files that are created or modified after 11/01/2018 08:00:00 are migrated. Files that are created or modified before the specified time will be skipped.
Migration Interval	Yes (only for Incremental migration)	The default value is 1 Hour and the maximum value is 24 Hours.
Migration Times	Yes (only for Incremental migration)	The default value is 1 time and the maximum value is 30 times.
Start Time Point of File	Yes (only for Sync)	· All: All files are synchronized. · Assign: Files that are created or modified after the specified time are synchronized. For example, when you set the Start Time Point of File to 11/01/2018 08:00:00, only files that are created or modified after 11/01/2018 08:00:00 are synchronized. Files that are created or modified before the specified time will be skipped.
Start Time of Job	Yes (only for Sync)	· Immediately: A synchronization immediately runs after a migration job is complete. · Schedule: You can set the scheduled time and synchronize data at the specified time.
Job Period	Yes (only for Sync)	The time interval between two synchronizations. A synchronization runs whenever a job period ends. Valid units: hour, day, and week.

Option	Required	Description
The next synchronization runs until the last synchronization ends.	Yes (only for Sync)	Don't trigger a new task if another task is running. Assume that you set the Job Period to 1 Hour and you forgot to select this option. The next synchronization runs regardless of whether the last synchronized is completed within one hour. This option is selected by default.

4. Click Next to enter the Performance tab.

   · When you select Full or Incremental, enter the Data Size and the File Count.

   > Note:
   > To ensure a successful migration, you must accurately estimate the amount of data to be migrated. For more information, see *Estimate the amount of data to be migrated*.

   · When you select Sync, enter theSubtask File Count and Subtask File Size.

   - Subtask File Count: You can separate a migration job into multiple subtasks based on the number of files that you specify. You can run a maximum of 20 subtasks at a time. Set the appropriate number of files for each subtask to reduce the time of a migration job. The default value is 1000. Assume that you need to migrate 10,000 files. When you set the Subtask File Count to 500, the migration job is separated into 20 subtasks that run at the same time. When you set the Subtask File Count to 100, the migration job is separated into 100 subtasks. Each time 20 subtasks run and the remaining subtasks wait to run.
   - Subtask File Size: You can separate a migration job into multiple subtasks based on the number of files that you specify. You can run a maximum of 20 subtasks at a time. Set the appropriate size of files for each subtask to reduce the time of a migration job. The default value is 1 GB. Assume that you need to migrate a total size of 40 GB files. When you set the Subtask File Size to 2 GB, the migration job is separated to 20 subtasks that run at the same time. When you set the Subtask File Size to 1 GB, the migration job is separated to 40 subtasks. Each time 20 subtasks run and the remaining subtasks wait for running.

   > Note:

A subtask is generated when either the specified Subtask File Count or Subtask File Size is met. When the number of files reaches the specified Subtask File Count but the file size does not reach the specified Subtask File Size, a subtask is generated based on the number of files. When the file size reaches the specified Subtask File Size but the number of files does not reach the specified Subtask File Count, a subtask is generated based on the file size. Assume that you set the Subtask File Count to 1000 and Subtask File Size to 1 GB. When the number of files reaches 1000 but the file size does not reach 1 GB, a subtask is generated based on the number of files. When the file size reaches 1 GB but the number of files does not reach 1000, a subtask is generated based on the file size.

5. This step is optional. On the Performance tab, navigate to the Flow Control area and set the Time Range and the Max Flow, and then click Add.

    Note:
   To ensure business continuity, we recommend that you set the Time Range and the Max Flow based on the fluctuation of visits.

6. Click Create. Wait for a while until a migration job is completed.

View the status of a data address

After you create the data address of an ECS instance, one of the following states is displayed:

- Normal: A data address is properly created.
- Creating: It takes time to create the first data address of an ECS instance (about three minutes). Wait for a while. If the status of a data address is in the Creating state for a long time, you can click Refresh in the upper-right corner to update the state.
- Invalid: An error occurred while creating a data address. You can verify that the configuration information is correct and Data Migration Service is allowed to access the shared files of an ECS instance. If this issue persists, you can contact the *Technical support center*.

4 Manage migration jobs

This section describes several subsequent operations after you create a migration job.

Subsequent operations change based on the migration type. You can manage migration jobs with different types as follows.

Manage full migration and incremental migration jobs

- View the status of a migration job

  After you create a migration job, one of the following states can occur:

  - Migrating: indicates that data is migrating. Wait.
  - Create Failed: indicates that you failed to create a migration job. You can view the cause of the failure and recreate a migration job.
  - Completed: indicates that a migration job is complete. You can view a migration report.
  - Failed: indicates that a migration job fails. You can view a migration report and migrate the failed files.

- Modify flow control settings

  During a migration job, you can modify flow control settings at any time based on your needs.

  1. In the *Data Migration Service console*, choose Data Online Migration > Migration Jobs. On the Migration Jobs page, locate a migration job and click Manage next to the job.
  2. Click Stop and ensure that the job is stopped.
  3. On the Flow Control Time Schedule chart, click Reset.
     - To add a flow control setting, select the appropriate Time Range and Max Flow, and click Add.
     - To delete a flow control setting, click  next to a specific flow control setting.
     - To modify a flow control setting, you must first delete the previous setting and add another flow control setting.
  4. Click OK, and click Start to restart the job.

- View a migration report

  1. On the Migration Jobs page, locate a job and click Manage next to the job.
  2. Click Generate Migration Report. After a report is generated, click Export to export the report.

     In a migration report, the following file names appear in the File list section:

     - The name of a file ends with `_total_lis t`. This file includes the list of all migration files.
     - The name of a file ends with `_completed _list`. This file includes the list of migrated files.
     - The name of a file ends with `_error_lis t`. This file includes the list of files that failed to migrate.
  3. At the destination data address, locate the automatically generated *aliyun_mgw _import_re port /* file folder. The preceding files are included in the folder. You can download and view the detailed list of files. We recommend that you use the *ossbrowser* tool to view these files.

     The file formats for the files are as follows:

     - The name of a file that includes the list of all migration files includes the source data address, file name, file size (measured in bytes), and last modified time. The format of a source data address is `nas ://< the name of a mount point >:/< prefix >/< objectName >`. For example, `nas :// 0a28888892 - afr82 . cn - hangzhou . nas . aliyuncs . com :/ myprefix / testfile . txt`.
     - The name of a file that includes the list of successfully migrated files includes the file name, file size (measured in bytes), checksum (CRC64), and migration completion time.
     - The name of a file that includes the list of files failed to migrate includes the file name, migration start time, migration end time, and error description.

- Retry after a migration failure

  If a migration job failed, you can view the generated file whose name ends with _error_list to find the causes of failure and troubleshoot the issue. On the Migration Jobs page, locate the failed job, clickManage next to the job, and clickRetry to

migrate failed files. For more information about FAQs for migration failures, see *Common causes of a migration failure and solutions*.

Manage synchronization jobs

- View the status of a synchronization job

  After you create a synchronization job, one of the following states can occur:

  - Migrating: the synchronization task is in progress.
  - Stopped: Click Manage next to a synchronization job to enter the Migration Report page. After you clickStop, the job status changes to Stopped.
  - Create Failed: indicates that you failed to create a synchronization job. You can view the causes of failure and recreate a synchronization job.

- Manage a synchronization job

  - View the details of a synchronization job: On the Migration Jobs page, click Manage next to a synchronization job to view the job details, such as Basic, Schedule, and Flow Control Time schedule.
  - Stop or start a synchronization job: On the Migration Report page, you can stop or start the synchronization job at any time.
  - View the history of a job: On the Migration Jobs page, locate a job and click Check History next to the job to view the job history.

    ■ After a synchronization job is complete, one of the following states for a task is displayed:

    ■ Scanning: indicates that a synchronization job is scanning the files of the source data address. The number of scanned files is displayed in the File Count column.

    ■ Scan Finished: indicates that a scan is complete. The total number and size of files are display in the File Count and File Size columns, respectively.

    ■ Success: indicate that a synchronization job is complete. The number of synchronized files is displayed. You can click  next to Completed to download the list of completed files.

    ■ Failed: An error may occur when you run a synchronization job. Click Retry to resynchronize failed files. You can click  next to Failed to

download the list of failed files. Based on the list, you can view the details of failed files, such as deleted or lost source files.

More information

For more information, see the following sections:

- *Migrate data between Alibaba Cloud Object Storage Service (OSS) buckets*
- *Migrate data from HTTP/HTTPS sources to OSS*
- *Migrate data from Tencent Cloud Object Service (COS) to OSS*
- *Migrate data from Amazon Simple Storage Service (Amazon S3) to OSS*
- *Migrate data from Azure Blob to OSS*
- *Migrate data from Qiniu Cloud-Object Storage (KODO) to OSS*
- *Migrate data from Baidu Object Storage (BOS) to OSS*
- *Migrate data from Kingsoft Standard Storage Service (KS3) to OSS*
- *Migrate data from UPYUN Storage Service (USS) to OSS*
- *Migrate data from Google Cloud Storage to OSS*
- *Migrate data between NAS file systems*
- *Migrate data from NAS to OSS*