# Alibaba Cloud
# Elastic Compute Service

## Best Practices

Issue: 20181008

# 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. |  **Note:** 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]`* |
| {} or {a\|b} | It indicates that it is a required value, and only one item can be selected. | `swich` *`{stand \| slave}`* |

# Contents

# 1 Security

## 1.1 Modify the default remote access port

This section describes how to modify the remote port of a Linux instance running CentOS 6.8.

**Modify the default remote port of a Windows instance**

1. *Connect to the Windows instance*.
2. Run *regedit.exe* to open Registry Editor.
3. On the left-side navigation pane of the Registry Editor, find *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\PortNumber*.
4. In the dialog box, select **Decimal as Base**, and then type a number in the **Value data** field as the new remote port number, which is 3399 in this example. Click **OK**.
5. (Optional) If you have enabled firewall, open the new port on the firewall.
6. Log on to the *ECS console*, find the instance, and then select **More** > **Restart**.
7. After the instance is restarted, click the **Manage** of the instance to enter the **Instance Details** page. Click **Security Groups**.
8. On the **Security Groups** page, click **Add Rules**.
9. On the **Security Group Rules** page, click **Add Security Group Rule**. Add a new security group rule to allow access to the new remote port. For more information about adding security group rules, see *Add security group rules*.
10. Connect to the instance by accessing the IP address ending with the new port number. For example, 192.168.1.2:3399 in this example.

> **Note:**
> Only the default port 3389 can be used for access by Mac remote desktop users.

### Modify the default remote port of a Linux instance

This section describes how to modify the remote port of a Linux instance running CentOS 6.8.

> **Note:**
> Do not modify the 22 port directly, first add the new default remote port. Set two ports first and delete one after the test succeeds. It ensures that you can use port 22 to debug any problems if you cannot connect the instance via the new port.

1. *Connect to the Linux instance*.
2. Run **`vim /etc/ssh/sshd_config`**.
3. Press the "I" key on the keyboard to enter the Edit mode. Add new remote service port (for example, Port 1022). Enter *`Port 1022`* under *`Port 22`*.
4. Press "ESC" and enter **`: wq`** to exit the editing.
5. Restart the instance by executing the following command. You can then log on to the Linux instance via 22 port and 1022 port.

   ```
   /etc/init.d/ssh restart
   ```

6. (Optional) Configure the firewall. When you use Linux versions earlier than CentOS 7 and has enabled firewall iptables, note that iptables do not intercept access by default. If you configured iptables rules, run **`iptables -A INPUT -p tcp --dport 1022 -j ACCEPT`** to configure the firewall. Then perform **`service iptables restart`** to restart the firewall.

   > **Note:**
   > Firewalld is installed by default on CentOS 7 and later versions. If you have enabled firewalld.service, open TCP port 1022 by running the command firewall-cmd --add-port=1022/tcp --permanent. If success is returned, TCP port 1022 is opened.

7. Log on to the *ECS console*, find the instance, and then select **Manage**.
8. Enter the **Instance Details** page. Click **Security Groups**.
9. On the **Security Groups** page, click **Add Rules**.
10. On the **Security Group Rules** page, click **Add Security Group Rule**. Add a new security group rule to allow access to the new remote port. For more information about adding security group rules, see *Add security group rules*.

11. Use the SSH tool to connect to the new port to test if the default remote port is modified successfully. Enter the new port number in **Port** when logging on to the instance, which is 1022 in this example.

12. Once you successfully connect the instance via port 1022, run **`vim /etc/ssh/sshd_config`** again to remove port 22.
13. Run **`/etc/init.d/sshd`** to restart the instance and the default remote port is successfully modified. Connect to the instance by accessing the IP address ending with the new port number.

## 1.2 Use logs in Windows instances

Logs are records of hardware and software in the system, and system error information. They can also be used to monitor system events. When a server intrusion or system (application) error occurs, administrators can quickly locate the problems by using logs and solve the problems quickly, which improves work efficiency and server security substantially. Windows logs can be mainly divided into four categories: system logs, application logs, security logs, and applications and services logs. In this example, we use Windows Server 2008 R2 to introduce the use and analysis of the four categories of logs.

**Open the Event Viewer**

Follow these steps to open Event Viewer: Open the **Run** window, type **`eventvwr`**, and then click OK to open the **Event Viewer**.

Then, you can view the following four categories of logs in **Event Viewer**.

> **Note:**
> You can find the solutions to any error event ID that you can find in these logs in Microsoft knowledge base.

- **System Logs**

  System logs include events recorded by Windows system components. For example, system logs record failures that occur when loading drivers or other system components during startup.

  The types of events recorded by system components are predetermined by Windows.

- **Application logs**

Application logs include events recorded by applications or programs. For example, a database application can record file errors in application logs.

The types of events recorded are determined by developers.

- **Security logs**

  Security logs include events such as valid and invalid logon attempts, and resource usage related events such as creation, opening, or deletion of files or other objects.

  Administrators can specify the types of events recorded in security logs. For example, if logon has been set to be audited, logon attempts are recorded in security logs.

- **Application and service logs**

  Application and service logs are a new type of event logs. These logs store events from a single application or component, rather than events that may affect the global system.

**Modify log path and back up logs**

Logs are stored on the system disk by default. The maximum log size is 20 MB by default, and the earliest events are overwritten when 20 MB is exceeded. You can modify the maximum log size according to your needs.

Follow these steps to modify the log path and back up logs:

1. In the left-side navigation pane of **Event Viewer**, click **Windows Logs**.
2. Right click a log name, such as **Application** and click Properties.
3. In the **Log Properties** dialog box, you can modify the following settings:
   - Log path
   - Maximum log size
   - Operations executed when maximum event log size is reached

# 2 Data recovery

## 2.1 Data restoration in Linux instances

When solving problems related to disks, you may frequently encounter the loss of data disk partitions. This article describes common data partition loss problems and corresponding solutions in Linux, and provides common mistakes and best practices for cloud disks to avoid possible risks of data loss.

Before restoring data, you must create snapshots for data disks that lose partitions. If problems occur during the restoration process, you can roll back data disks to the status before restoration.

**Prerequisites**

Before restoring data, you must create snapshots for data disks that lose partitions. If problems occur during the restoration process, you can roll back data disks to the status before restoration.

**Introduction to disk management tools**

You can select one of the following tools to fix the disk partition and restore the data in a Linux instance:

- fdisk : The default partitioning tool installed in Linux instances.
- testdisk : It is primarily used to restore disk partitions or data in the Linux system. The tool is not installed by default in Linux. You must install it on your own. For example, in a CentOS system, you can run the **`yum install -y testdisk`** command to install it online.
- partprobe : This is the default tool installed in the Linux system. It is primarily used to enable the kernel to re-read the partition without restarting the system.

**Handle data disk partition loss and data restoration in Linux**

After you restart a Linux instance, you may encounter data disk partition loss or data loss issues. This may be because you have not set the partitions to be mounted automatically on startup of the instance in the *`etc/fstab`* file. In this case, you can manually mount the data disk partition first. If the system prompts partition table loss when you manually mount the data disk, you can try to solve the problem through the following three methods: *Restore partitions by using fdisk*, *Restore partitions by using testdisk*, or *Restore data by using testdisk*.

- **Restore partitions by using fdisk**

Default values usually apply to the starting and ending sectors of the partition when you partition a data disk. You can then directly use fdisk to restore the partition. For more information about this tool, see *Linux Format and mount a data disk*.

If the preceding operations do not help, you can try testdisk for the restoration.

- **Restore partitions by using testdisk**

  Here we suppose the cloud disk device is named `/dev/xvdb`. Follow these steps to restore the partitions by using testdisk:

  1. Run **`testdisk /dev/xvdb`** (replace the device name as appropriate), and then select **`Proceed`** (default value) and press the Enter key.
  2. Select the partition table type for scanning: *`Intel`* by default. If your data disk uses the GPT format, select *`EFI GPT`*.
  3. Select *`Analyse`* and then press the Enter key.
  4. If you cannot see any partition, select *`Quick Search`* and then press the Enter key for a quick search.

     The partition information is displayed in the returned result, as shown in the following figure.

  5. Select the partition and press the Enter key.
  6. Select *`Write`* to save the partition.

     **Note:**
     Select *`Deeper Search`* to continue searching if the expected partition is not listed.

  7. Press the Y key to save the partition.
  8. Run **`partprobe /dev/xvdb`** (replace the device name as appropriate) to refresh the partition table manually.

9. Mount the partition again and view the data in the data disk.

- **Restore data by using testdisk**

  In some cases, you can use testdisk to scan and locate the disk partition, but you cannot save the partition. In this case, you can try to restore files directly. Follow these steps:

  1. Find the partition following Step 1 to Step 4 described in *Restore partitions by using teskdisk*.
  2. List files by pressing the `P` key. The returned result is shown in the following figure.

  3. Select the files to restore, and press the `C` key.
  4. Select a directory. In this example, the file is restored and copied to the */home* directory.

     If you see `Copy done! 1 ok, 0 failed`, it indicates that copy was successful, as shown in the following figure.

  5. Switch to the */home* directory to view details. If you can see files, it indicates that files have been restored successfully.

## Common mistakes and best practices

Data is users' core asset. Many users establish websites and databases (MYSQL/MongoDB/ Redis) on ECS. Huge risks to the users' services may occur when data is lost. Common mistakes and best practices are summarized as follows.

- **Common mistakes**

  The bottom layer of Alibaba Cloud block-level storage is based on *triplicate technology*. Therefore, some users consider that no risk of data loss in the operating system exists. It is actually a misunderstanding. The three copies of data stored in the bottom layer provide physical layer protection for data disks. However, if problems occur to the cloud disk logic in the system, such as viruses, accidental data deletion, and file system damage, the data may still be lost. To guarantee data security, you have to use technologies such as Snapshot and backup.

- **Best practices**

Data disk partition restoration and data restoration are the final solutions for solving data loss problems, but it is never guaranteed. We strongly recommend that you follow the best practices to perform auto or manual snapshot on data and run different backup schemes to maximize your data security.

— **Enable automatic snapshots**

Automatic snapshots are enabled for the system disk and data disk based on actual service conditions. Note that automatic snapshot may be released when the system disk is changed , the instance is expired, or the disk is manually released.

You log on to the ECS console to **change the attributes of the disks** to enable **snapshot release with the disk**. Disable snapshot release with the disk if you want to retain the snapshots.

For more information, see *FAQ about automatic snapshots*.

— **Create manual snapshots**

Create snapshots manually before any important or risky operations such as:

- Upgrade the kernel
- Upgrade or change of applications
- Restoration of disk data

You must create snapshots for disks before restoring them. After the snapshots are completed, you can perform other operations.

— **OSS, offline, or offsite backup**

You can back up important data by means of OSS, offline, or offsite backup based on actual conditions.

## 2.2 Data restoration in Windows instances

When solving problems related to disks, you may frequently encounter the loss of data disk partitions. This article describes common data partition loss problems and corresponding solutions in Windows, and provides common mistakes and best practices for cloud disks to avoid possible risks of data loss.

**Prerequisites**

Before restoring data, you must create snapshots for data disks that lose partitions. If problems occur during the restoration process, you can roll back data disks to the status before restoration.

### Introduction to disk management tools

In Windows instances, you can select either of the following tools for restoring data disk data:

- Disk Management: A tool provided by Windows for partitioning and formatting the disk.
- Data restoration software: Generally, they are commercial software, and can be downloaded from the providers' official websites. They are mainly used for restoring data in an abnormal file system.

### Status of the disk is Foreign and no partitions are displayed

In the **Disk Management** of Windows, the disk is in the **Foreign** status and displays no partitions.

Solution:

Right click the **Foreign** disk, select **Import Foreign Disks**, and then click **OK**.

### Status of the disk is Offline and no partitions are displayed

In the **Disk Management** of Windows, the disk is in the **Offline** status and displays no partitions.

Solution:

Right click the **Offline** disk (for example, **Disk 1**), select **Online**, and then click **OK**.

### No drive letter assigned

In the **Disk Management** of Windows, you can view data disk information, but no drive letter is allocated to the data disk.

Solution:

Right click primary partition of the disk (for example, **Disk 1**), click **Change drive letter and paths**, and then complete operations by prompt.

### Error occurred during storage enumeration

In the **Disk Management** of Windows, you cannot view data disks. An error occurred during storage enumeration is reported in the system log.

**Note:**

Some versions may report Error occurred during enumeration of volumes. They are the same.

Solution:

1. Start Windows PowerShell.
2. Run **`winrm quickconfig`** for restoring. When “Make these changes [y/n]?” is displayed on the interface, you must type *y* to run the command.

After the restoration, you can have the data disks in the **Disk Management**.

### Data disk is in RAW format

In some special circumstances, the disk in Windows is in RAW format.

If the file system of a disk is unrecognizable to Windows, it is displayed as a RAW disk. This usually occurs when the partition table or boot sector that records the type or location of the file system is lost or damaged. Common causes are listed as follows:

- **Safely remove hardware** is not used when disconnecting the external disk.
- Disk problems caused by power outages or unexpected shutdown.
- Hardware layer failure may also cause information loss of the disk partition.
- Bottom layer drivers or disk-related applications. For example, DiskProbe can be used to directly modify the disk table structure.
- Computer viruses.

For more information about how to fix these problems, see *Dskprobe Overview* document.

Moreover, Windows also contains a large variety of free or commercial data restoration software to restore lost data. For example, you can try to use Disk Genius to scan and restore expected documents.

### Common mistakes and best practices

Data is users’ core asset. Many users establish websites and databases (MYSQL/MongoDB/Redis) on ECS. Huge risks to the users’ services may occur when data is lost. Common mistakes and best practices are summarized as follows.

- **Common mistakes**

  The bottom layer of Alibaba Cloud block-level storage is based on *triplicate technology*. Therefore, some users consider that no risk of data loss in the operating system exists. It is actually a misunderstanding. The three copies of data stored in the bottom layer provide physical layer protection for data disks. However, if problems occur to the cloud disk logic in the system, such as viruses, accidental data deletion, and file system damage, the data may still be lost. To guarantee data security, you have to use technologies such as Snapshot and backup.

- **Best practices**

  Data disk partition restoration and data restoration are the final solutions for solving data loss problems, but it is never guaranteed. We strongly recommend that you follow the best practices to perform auto or manual snapshot on data and run different backup schemes to maximize your data security.

  — **Enable automatic snapshots**

    Automatic snapshots are enabled for the system disk and data disk based on actual service conditions. Note that automatic snapshot may be released when the system disk is changed , the instance is expired, or the disk is manually released.

    You log on to the ECS console to **change the attributes of the disks** to **enable snapshot release with the disk**. Disable snapshot release with the disk if you want to retain the snapshots.

    For more information, see *FAQ about automatic snapshots*.

  — **Create manual snapshots**

    Create snapshots manually before any important or risky operations such as:

    - Upgrade the kernel
    - Upgrade or change of applications
    - Restoration of disk data

    You must create snapshots for disks before restoring them. After the snapshots are completed, you can perform other operations.

  — **OSS, offline, or offsite backup**

    You can back up important data by means of OSS, offline, or offsite backup based on actual conditions.