ALIBABA CLOUD

Alibaba Cloud

云服务器ECS

最佳實務

Document Version: 20211224

Alibaba Cloud

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 because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should 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 this document based on the "status quo", "being defective", and "existing functions" of its products and services. 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 take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, 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 contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, 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 this document 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 directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
Danger	A danger notice 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.
Warning	A warning notice 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 restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	**Notice:** If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	**Note:** You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.配置選型

針對企業級使用者，可以通過如下流程進行配置選型：

> 說明
>
> 更多應用情境，詳情請參見 企業級配置選型。

為滿足不同客戶的需求，針對企業級的使用者，阿里雲提供了以下應用情境下的執行個體配置建議：

- **均衡效能**

  需要相對均衡的處理器與記憶體資源配比，滿足大多數情境下的應用資源需求關係。

- **高網路收發包應用**

  需要高網路收發包能力，可以根據應用情境選擇更合理的計算與記憶體的資源配比。

- **高效能運算**

  需要消耗高計算資源，GPU並行計算以及高主頻是該情境下的典型應用。

- **高效能端遊**

  使用者業務需要高處理器主頻來承載更多的使用者，需要高主頻處理器支援。

- **手遊、頁遊**

  需要消耗高計算資源，1:2的處理器與記憶體配比可以獲得最優計算資源性價比。

- **視頻轉寄**

  需要消耗高計算資源，1:2的處理器與記憶體配比可以獲得最優計算資源性價比。

- **直播彈幕**

  需要高網路收發包能力，可以根據應用情境選擇更合理的計算與記憶體的資源配比。

- **關係型資料庫**

  需要SSD雲端硬碟或更高效能的NVMe SSD本地磁碟提供高儲存IOPS且低讀寫延時，CPU與記憶體資源配比均衡（1:4）或記憶體更大（1:8）。

- **分布式緩衝**

  需要CPU與記憶體資源配比均衡（1:4）或者記憶體更大（1:8），穩定的計算效能。

- **NoSQL資料庫**

  需要SSD雲端硬碟或更高效能的NVMe SSD本地磁碟提供高儲存IOPS且低讀寫延時，CPU與記憶體資源配比均衡（1:4）或記憶體更大（1:8）。

- **Elastic Search**

  需要SSD雲端硬碟或更高效能的NVMe SSD本地磁碟提供高儲存IOPS且低讀寫延時，CPU與記憶體資源配比均衡（1:4）或記憶體更大（1:8）。

- **Hadoop**

  資料節點需要高磁碟吞吐、高網路吞吐、均衡的CPU與記憶體配比，計算節點則更關注計算效能、網路頻寬及CPU與記憶體資源配。

- **Spark**

資料節點需要高磁碟吞吐、高網路吞吐、均衡的CPU與記憶體配比，計算節點則更關注計算效能、網路頻寬及CPU與記憶體資源配。

- **Kafka**

  資料節點需要高磁碟吞吐、高網路吞吐、均衡的CPU與記憶體配比，計算節點則更關注計算效能、網路頻寬及CPU與記憶體資源配。

- **機器學習**

  需要高效能Nvidia GPU計算卡，記憶體不小於顯存的兩倍。

- **視頻編碼**

  需要高效能GPU計算卡或高效能CPU進行編解碼。

- **渲染**

  需要高效能GPU計算卡進行渲染。

2.安全

2.1. ECS安全性群組實踐（一）

本文主要介紹如何配置安全性群組的入網規則。

在雲端安全性群組提供類似虛擬防火牆功能，用於設定單個或多個 ECS 執行個體的網路存取控制，是重要的安全隔離手段。建立 ECS 執行個體時，您必須選擇一個安全性群組。您還可以添加安全性群組規則，對某個安全性群組下的所有 ECS 執行個體的出方向和入方向進行網路控制。

在配置安全性群組的入網規則之前，您應已經瞭解以下安全性群組相關的資訊：

- 安全性群組限制
- 安全性群組預設規則
- 設定安全性群組 In 方向的存取權限
- 設定安全性群組 Out 方向的存取權限

安全性群組實踐的基本建議

在開始安全性群組的實踐之前，下面有一些基本的建議：

- 最重要的規則：安全性群組應作為白名單使用。
- 開放應用出入規則時應遵循“最小授權”原則，例如，您可以選擇開放具體的連接埠（如 80 連接埠）。
- 不應使用一個安全性群組管理所有應用，因為不同的分層一定有不同的需求。
- 對於分布式應用來說，不同的應用類型應該使用不同的安全性群組，例如，您應對 Web、Service、Database、Cache 層使用不同的安全性群組，暴露不同的出入規則和許可權。
- 沒有必要為每個執行個體單獨設定一個安全性群組，控制管理成本。
- 優先考慮 VPC 網路。
- 不需要公網訪問的資源不應提供公網 IP。
- 儘可能保持單個安全性群組的規則簡潔。因為一個執行個體最多可以加入 5 個安全性群組，一個安全性群組最多可以包括 100 個安全性群組規則，所以一個執行個體可能同時應用數百條安全性群組規則。您可以彙總所有分配的安全規則以判斷是否允許流入或留出，但是，如果單個安全性群組規則很複雜，就會增加管理的複雜度。所以，應儘可能地保持單個安全性群組的規則簡潔。
- 阿里雲的控制台提供了複製安全性群組和安全性群組規則的功能。如果您想要修改線上的安全性群組和規則，您應先複製一個安全性群組，再在複製的安全性群組上進行調試，從而避免直接影響線上應用。

> **說明** 調整線上的安全性群組的出入規則是比較危險的動作。如果您無法確定，不應隨意更新安全性群組出入規則的設定。

設定安全性群組的入網規則

以下是安全性群組的入網規則的實踐建議。

不要使用 0.0.0.0/0 的入網規則

允許全部入網訪問是經常犯的錯誤。使用 0.0.0.0/0 意味著所有的連接埠都對外暴露了存取權限。這是非常不安全的。正確的做法是，先拒絕所有的連接埠對外開放。安全性群組應該是白名單訪問。例如，如果您需要暴露 Web 服務，預設情況下可以只開放 80、8080 和 443 之類的常用TCP連接埠，其它的連接埠都應關閉。

```
{ "IpProtocol" : "tcp", "FromPort" : "80", "ToPort" : "80", "SourceCidrIp" : "0.0.0.0/0", "
Policy": "accept"} ,
{ "IpProtocol" : "tcp", "FromPort" : "8080", "ToPort" : "8080", "SourceCidrIp" : "0.0.0.0/0
", "Policy": "accept"} ,
{ "IpProtocol" : "tcp", "FromPort" : "443", "ToPort" : "443", "SourceCidrIp" : "0.0.0.0/0",
"Policy": "accept"} ,
```

關閉不需要的入網規則

如果您當前使用的入規則已經包含了 0.0.0.0/0，您需要重新審視自己的應用需要對外暴露的連接埠和服務。如果確定不想讓某些連接埠直接對外提供服務，您可以加一條拒絕的規則。比如，如果您的伺服器上安裝了 MySQL 資料庫服務，預設情況下您不應該將 3306 連接埠暴露到公網，此時，您可以添加一條拒絕規則，如下所示，並將其優先順序設為100，即優先順序最低。

```
{ "IpProtocol" : "tcp", "FromPort" : "3306", "ToPort" : "3306", "SourceCidrIp" : "0.0.0.0/0
", "Policy": "drop", Priority: 100} ,
```

上面的調整會導致所有的連接埠都不能訪問 3306 連接埠，極有可能會阻止您正常的業務需求。此時，您可以通過授權另外一個安全性群組的資源進行入規則訪問。

授權另外一個安全性群組入網訪問

不同的安全性群組按照最小原則開放相應的出入規則。對於不同的應用分層應該使用不同的安全性群組，不同的安全性群組應有相應的出入規則。

例如，如果是分布式應用，您會區分不同的安全性群組，但是，不同的安全性群組可能網路不通，此時您不應該直接授權 IP 或者 CIDR 網段，而是直接授權另外一個安全性群組 ID 的所有的資源都可以直接存取。比如，您的應用對 Web、Database 分別建立了不同的安全性群組：sg-web 和 sg-database。在sg-database 中，您可以添加如下規則，授權所有的 sg-web 安全性群組的資源訪問您的 3306 連接埠。

```
{ "IpProtocol" : "tcp", "FromPort" : "3306", "ToPort" : "3306", "SourceGroupId" : "sg-web",
"Policy": "accept", Priority: 2} ,
```

授權另外一個 CIDR 可以入網訪問

傳統網路中，因為網段不太可控，建議您使用安全性群組 ID 來授信入網規則。

VPC 網路中，您可以自己通過不同的 VSwitch 設定不同的 IP 域，規劃 IP 位址。所以，在 VPC 網路中，您可以預設拒絕所有的訪問，再授信自己的專用網路的網段訪問，直接授信可以相信的 CIDR 網段。

```
{ "IpProtocol" : "icmp", "FromPort" : "-1", "ToPort" : "-1", "SourceCidrIp" : "10.0.0.0/24"
, Priority: 2} ,
{ "IpProtocol" : "tcp", "FromPort" : "0", "ToPort" : "65535", "SourceCidrIp" : "10.0.0.0/24
", Priority: 2} ,
{ "IpProtocol" : "udp", "FromPort" : "0", "ToPort" : "65535", "SourceCidrIp" : "10.0.0.0/24
", Priority: 2} ,
```

變更安全性群組規則步驟和說明

變更安全性群組規則可能會影響您的執行個體間的網路通訊。為了保證必要的網路通訊不受影響，您應先嘗試以下方法允許存取必要的執行個體，再執行安全性群組策略收緊變更。

> **說明** 執行收緊變更後，應觀察一段時間，確認業務應用無異常後再執行其它必要的變更。

- 建立一個安全性群組，將需要互連訪問的執行個體加入這個安全性群組，再執行變更操作。
- 如果授與類型為 **安全性群組訪問**，則將需要互連訪問的對端執行個體所綁定的安全性群組 ID 添加為授權對象；
- 如果授與類型為 **位址區段訪問**，則將需要互連訪問的對端執行個體內網 IP 添加為授權對象。

具體操作指引請參見 傳統網路內網執行個體互連設定方法。

2.2. ECS安全性群組實踐（二）

本文從授權和撤銷安全性群組規則、加入和移出安全性群組講解Elastic Compute Service的安全性群組最佳實務。

網路類型

阿里雲的網路類型分為傳統網路和Virtual Private Cloud，對安全性群組支援不同的設定規則：

- 如果是傳統網路，您可以設定內網入方向、內網出方向、公網入方向和公網出方向的安全性群組規則。
- 如果是Virtual Private Cloud，您可以設定內網入方向和內網出方向的安全性群組規則。

安全性群組是區分網路類型的，一台傳統網路類型的ECS執行個體只能加入傳統網路的安全性群組。一台Virtual Private Cloud類型的ECS執行個體只能加入本VPC的安全性群組。

安全性群組內網通訊的概念

本文開始之前，您應知道以下幾個安全性群組內網通訊的概念：

- 預設只有同一個安全性群組的ECS執行個體可以網路互連。即使是同一個賬戶下的ECS執行個體，如果分屬不同安全性群組，內網網路也是不通的。這個對於傳統網路和Virtual Private Cloud都適用。所以，傳統網路類型的ECS執行個體也是內網安全的。
- 如果您有兩台ECS執行個體，不在同一個安全性群組，您希望它們內網不互連，但實際上它們卻內網互連，那麼，您需要檢查您的安全性群組內網規則設定。如果內網協議存在下面的協議，建議您重新設定。
  - 允許所有連接埠。
  - 授權對象為CIDR網段（SourceCidrIp）：*0.0.0.0/0*或者*10.0.0.0/8*的規則。如果是傳統網路，上述協議會造成您的內網暴露給其它的訪問。
- 如果您想實現在不同安全性群組的資源之間的網路互連，您應使用安全性群組方式授權。對於內網訪問，您應使用源安全性群組授權，而不是CIDR網段授權。

安全規則的屬性

安全規則主要是描述不同的存取權限，包括如下屬性：

- Policy：授權策略，參數值可以是*accept*（接受）或*drop*（拒絕）。
- Priority：優先順序，根據安全性群組規則的建立時間降序排序匹配。規則優先順序可選範圍為1-100，預設值為1，即最高優先順序。數字越大，代表優先順序越低。
- NicType：網路類型。如果只指定了SourceGroupId而沒有指定SourceCidrIp，表示通過安全性群組方式授權，此時，NicType必須指定為*intranet*。
- 規則描述：
  - IpProtocol：IP協議，取值：*tcp*、*udp*、*icmp*、*gre*或*all*。all表示所有的協議。

- PortRange：IP協議相關的連接埠號碼範圍：
  - IpProtocol取值為*tcp*或*udp*時，連接埠號碼取值範圍為1~65535，格式必須是“開始端點口號/終止連接埠號碼”，如“1/200”表示連接埠號碼範圍為1~200。如果輸入值為“200/1”，介面調用將報錯。
  - IpProtocol取值為*icmp*、*gre*或*all*時，連接埠號碼範圍值為-1/-1，表示不限制連接埠。
- 如果通過安全性群組授權，應指定SourceGroupId，即源安全性群組ID。此時，根據是否跨帳號授權，您可以選擇設定源安全性群組所屬的帳號SourceGroupOwnerAccount。
- 如果通過CIDR授權，應指定SourceCidrIp，即源IP位址區段，必須使用CIDR格式。

授權一條入網請求規則

在控制台或者通過API建立一個安全性群組時，入網方向預設*deny all*，即預設情況下您拒絕所有入網請求。這並不適用於所有的情況，所以您要適度地配置您的入網規則。

比如，如果您需要開啟公網的80連接埠對外提供HTTP服務，因為是公網訪問，您希望入網儘可能多訪問，所以在IP網段上不應做限制，可以設定為*0.0.0.0/0*，具體設定可以參考以下描述，其中，括弧外為控制台參數，括弧內為OpenAPI參數，兩者相同就不做區分。

- 網卡類型（NicType）：公網（internet）。如果是Virtual Private Cloud類型的只需要填寫intranet，通過EIP實現公網訪問。
- 授權策略（Policy）：允許（accept）。
- 規則方向（NicType）：入網。
- 協議類型（IpProtocol）：TCP（tcp）。
- 連接埠範圍（PortRange）：80/80。
- 授權對象（SourceCidrIp）：0.0.0.0/0。
- 優先順序（Priority）：1。

> **說明** 上面的建議僅對公網有效。內網請求不建議使用CIDR網段，請參見傳統網路的內網安全性群組規則不要使用 CIDR 或者 IP 授權。

禁止一個入網請求規則

禁止一條規則時，您只需要配置一條拒絕策略，並設定較低的優先順序即可。這樣，當有需要時，您可以配置其它高優先順序的規則覆蓋這條規則。例如，您可以採用以下設定拒絕6379連接埠被訪問。

- 網卡類型（NicType）：內網（intranet）。
- 授權策略（Policy）：拒絕（drop）。
- 規則方向（NicType）：入網。
- 協議類型（IpProtocol）：TCP（tcp）。
- 連接埠範圍（PortRange）：6379/6379。
- 授權對象（SourceCidrIp）：0.0.0.0/0。
- 優先順序（Priority）：100。

傳統網路的內網安全性群組規則不要使用CIDR或者IP授權

對於傳統網路類型的ECS執行個體，阿里雲預設不開啟任何內網的入規則。內網的授權一定要謹慎。

> **說明** 為了安全考慮，不建議開啟任何基於CIDR網段的授權。

對於彈性計算來說，內網的IP經常變化，另外，這個IP的網段是沒有規律的，所以，建議您通過安全性群組授權對傳統網路內網的訪問。

例如，您在安全性群組sg-redis上構建了一個redis的叢集，為了只允許特定的機器（如sg-web）訪問這個redis的伺服器編組，您不需要配置任何CIDR，只需要添加一條入規則：指定相關的安全性群組ID即可。

- 網卡類型（NicType）：內網（intranet）。
- 授權策略（Policy）：允許（accept）。
- 規則方向（NicType）：入網。
- 協議類型（IpProtocol）：TCP（tcp）。
- 連接埠範圍（PortRange）：6379/6379。
- 授權對象（SourceGroupId）：sg-web。
- 優先順序（Priority）：1。

對於Virtual Private Cloud類型的執行個體，如果您已經通過多個VSwitch規劃好自己的IP範圍，您可以使用CIDR設定作為安全性群組入規則。但是，如果您的Virtual Private Cloud網段不夠清晰，建議您優先考慮使用安全性群組作為入規則。

將需要互相通訊的ECS執行個體加入同一個安全性群組

一個ECS執行個體最多可以加入5個安全性群組，而同一安全性群組內的ECS執行個體之間是網路互連的。如果您在規劃時已經有多個安全性群組，而且，直接設定多個安全規則過於複雜的話，您可以建立一個安全性群組，然後將需要內網通訊的ECS執行個體加入這個新的安全性群組。

這裡也不建議您將所有的ECS執行個體都加入一個安全性群組，這將會使得您的安全性群組規則設定變成夢魘。對於一個中大型應用來說，每個伺服器編組的角色不同，合理地規劃每個伺服器的入方向請求和出方向請求是非常有必要的。

在控制台上，您可以根據文檔加入安全性群組的描述將一台執行個體加入安全性群組。

如果您對阿里雲的OpenAPI非常熟悉，您可以參見彈性管理ECS執行個體，通過OpenAPI進行大量操作。對應的Python片段如下。

```
def join_sg(sg_id, instance_id):
    request = JoinSecurityGroupRequest()
    request.set_InstanceId(instance_id)
    request.set_SecurityGroupId(sg_id)
    response = _send_request(request)
    return response
# send open api request
def _send_request(request):
    request.set_accept_format('json')
    try:
        response_str = clt.do_action(request)
        logging.info(response_str)
        response_detail = json.loads(response_str)
        return response_detail
    except Exception as e:
        logging.error(e)
```

將ECS執行個體移除安全性群組

如果ECS執行個體加入不合適的安全性群組，將會暴露或者Block您的服務，這時您可以選擇將ECS執行個體從這個安全性群組中移除。但是在移除安全性群組之前必須保證您的ECS執行個體已經加入其它安全性群組。

> **說明** 將ECS執行個體從安全性群組移出，將會導致這台ECS執行個體和當前安全性群組內的網路不通，建議您在移出之前做好充分的測試。

對應的Python片段如下。

```
def leave_sg(sg_id, instance_id):
    request = LeaveSecurityGroupRequest()
    request.set_InstanceId(instance_id)
    request.set_SecurityGroupId(sg_id)
    response = _send_request(request)
    return response
# send open api request
def _send_request(request):
    request.set_accept_format('json')
    try:
        response_str = clt.do_action(request)
        logging.info(response_str)
        response_detail = json.loads(response_str)
        return response_detail
    except Exception as e:
        logging.error(e)
```

定義合理的安全性群組名稱和標籤

合理的安全性群組名稱和描述有助於您快速識別當前複雜的規則群組合。您可以通過修改名稱和描述來協助自己識別安全性群組。

您也可以通過為安全性群組設定標籤分組管理自己的安全性群組。您可以在控制台直接設定標籤，也可以通過API設定標籤。

刪除不需要的安全性群組

安全性群組中的安全規則類似於一條條白名單和黑名單。所以，請不要保留不需要的安全性群組，以免因為錯誤加入某台ECS執行個體而造成不必要的麻煩。

2.3. ECS安全性群組實踐（三）

在安全性群組的使用過程中，通常會將所有的雲端服務器放置在同一個安全性群組中，從而可以減少初期配置的工作量。但從長遠來看，業務系統網路的互動將變得複雜和不可控。在執行安全性群組變更時，您將無法明確添加和刪除規則的影響範圍。

合理規劃和區分不同的安全性群組將使得您的系統更加便於調整，梳理應用提供的服務並對不同應用進行分層。這裡推薦您對不同的業務規劃不同的安全性群組，並設定不同的安全性群組規則。

區分不同的安全性群組

- **公網服務的雲端服務器和內網伺服器盡量屬於不同的安全性群組**

是否對外提供公網服務，包括主動暴露某些連接埠對外訪問（例如 80、443 等），被動地提供連接埠轉寄規則（例如雲端服務器具有公網 IP、EIP、NAT 連接埠轉寄規則等），都會導致自己的應用可能被公網訪問到。

2 種情境的雲端服務器所屬的安全性群組規則要採用最嚴格的規則，建議拒絕優先，預設情況下應當關閉所有的連接埠和協議，僅僅暴露對外提供需要服務的連接埠，例如 80、443。由於僅對屬於對外公網訪問的伺服器編組，調整安全性群組規則時也比較容易控制。

對於對外提供伺服器編組的職責應該比較明晰和簡單，避免在同樣的伺服器上對外提供其它的服務。例如 MySQL、Redis 等，建議將這些服務安裝在沒有公網存取權限的雲端服務器上，然後通過安全性群組的組組授權來訪問。

如果當前有公網雲端服務器已經和其它的應用在同一個安全性群組 SG_CURRENT。您可以通過下面的方法來進行變更。

i. 梳理當前提供的公網服務暴露的連接埠和協議，例如 80、443。

ii. 新建立一個安全性群組，例如 SG_WEB， 然後添加相應的連接埠和規則。

> **說明** 授權策略：允許，協議類型：ALL， 連接埠：80/80，授權對象：0.0.0.0/0， 授權策略：允許，協議類型：ALL，連接埠：443/443，授權對象：0.0.0.0/0。

iii. 選擇安全性群組 SG_CURRENT， 然後添加一條安全性群組規則，組組授權，允許 SG_WEB 中的資源訪問SG_CURRENT。

> **說明** 授權策略：允許，協議類型：ALL，連接埠：-1/-1，授權對象：SG_WEB，優先順序：按照實際情況自訂[1-100]。

iv. 將一台需要切換安全性群組的執行個體 ECS_WEB_1 添加到新的安全性群組中。

a. 在 ECS 控制台中，選擇 **安全性群組管理**。

b. 選擇 **SG_WEB > 管理執行個體 > 添加執行個體**，選擇執行個體 ECS_WEB_1 加入到新的安全性群組 SG_WEB 中，確認 ECS_WEB_1 執行個體的流量和網路工作正常。

v. 將 ECS_WEB_1 從原來的安全性群組中移出。

a. 在 ECS 控制台中，選擇 **安全性群組管理**。

b. 選擇 **SG_WEB > 管理執行個體 > 添加執行個體**，選擇 ECS_WEB_1 ，從 SG_CURRENT 移除，測試網路連通性，確認流量和網路工作正常。

c. 如果工作不正常，將 ECS_WEB_1 仍然加回到安全性群組 SG_CURRENT 中，檢查設定的 SG_WEB 暴露的連接埠是否符合預期，然後繼續變更。

vi. 執行其它的伺服器安全性群組變更。

- **不同的應用使用不同的安全性群組**

在生產環境中，不同的作業系統大多情況下不會屬於同一個應用分組來提供負載平衡服務。提供不同的服務意味著需要暴露的連接埠和拒絕的連接埠是不同的，建議不同的作業系統盡量歸屬於不同的安全性群組。

例如，對於 Linux 作業系統，可能需要暴露 TCP（22）連接埠來實現 SSH，對 Windows 可能需要開通 TCP(3389) 遠端桌面連線。

除了不同的作業系統歸屬不同的安全性群組，即便同一個鏡像類型，提供不同的服務，如果之間不需要通過內網進行訪問的話，最好也劃歸不同的安全性群組。這樣方便解耦，並對未來的安全性群組規則進行變更，做到職責單一。

在規劃和新增應用時，除了考慮劃分不同的虛擬交換器配置子網，也應該同時合理的規劃安全性群組。使用網段+安全性群組約束自己作為服務提供者和消費者的邊界。

具體的變更流程參見上面的操作步驟。

- **生產環境和測試環境使用不同的安全性群組**

  為了更好的做系統的隔離，在實際開發過程中，您可能會構建多套的測試環境和一套線上環境。為了更合理的做網路隔離，您需要對不同的環境配置使用不同的安全性原則，避免因為測試環境的變更重新整理到了線上影響線上的穩定性。

  通過建立不同的安全性群組，限制應用的訪問域，避免生產環境和測試環境聯通。同時也可以對不同的測試環境分配不同的安全性群組，避免多套測試環境之間互相干擾，提升開發效率。

僅對需要公網訪問子網或者雲端服務器分配公網 IP

不論是傳統網路還是Virtual Private Cloud 中，合理的分配公網 IP 可以讓系統更加方便地進行公網管理，同時減少系統受攻擊的風險。在專用網路的情境下，建立虛擬交換器時，建議您盡量將需要公網訪問的服務區的 IP 區間放在固定的幾個交換器(子網 CIDR)中，方便審計和區分，避免不小心暴露公網訪問。

在分布式應用中，大多數應用都有不同的分層和分組，對於不提供公網訪問的雲端服務器盡量不提供公網 IP，如果是有多台伺服器提供公網訪問，建議您配置公網流量分發的負載平衡服務來公網服務，提升系統的可用性，避免單點。

對於不需要公網訪問的雲端服務器盡量不要分配公網 IP。專用網路中當您的雲端服務器需要訪問公網的時候，優先建議您使用 NAT Gateway，用於為 VPC 內無公網 IP 的 ECS 執行個體提供訪問互連網的代理服務，您只需要配置相應的 SNAT 規則即可為具體的 CIDR 網段或者子網提供公網訪問能力，具體配置參見SNAT。避免因為只需要訪問公網的能力而在分配了公網 IP(EIP) 之後也向公網暴露了服務。

最小原則

安全性群組應該是白名單性質的，所以需盡量開放和暴露最少的連接埠，同時儘可能少地分配公網 IP。若想訪問線上機器進行任務日誌或錯誤排查的時候直接分配公網 IP，掛載 EIP 雖然簡便，但是畢竟會將整個機器暴露在公網之上，更安全的策略是通過跳板機來管理。

使用跳板機

跳板機由於其自身的許可權巨大，除了通過工具做好審計記錄。在專用網路中，建議將跳板機分配在專有的虛擬交換器之中，對其提供相應的 EIP 或者 NAT 連接埠轉寄表。

首先建立專有的安全性群組 SG_BRIDGE，例如開放相應的連接埠，例如 Linux TCP(22) 或者 Windows RDP(3389)。為了限制安全性群組的入網規則，可以限制能登入的授權對象為企業的公網出口範圍，減少被登入和掃描的機率。

然後將作為跳板機的雲端服務器加入到該安全性群組中。為了讓該機器能訪問相應的雲端服務器，可以配置相應的組授權。例如在 SG_CURRENT 添加一條規則允許 SG_BRIDGE 訪問某些連接埠和協議。

使用跳板機 SSH 時，建議您優先使用 SSH 金鑰對 而不是密碼登入。

總之，合理的安全性群組規劃使您在擴容應用時更加遊刃有餘，同時讓您的系統更加安全。

2.4. 傳統網路內網執行個體互連設定方法

安全性群組是執行個體層級防火牆，為保障執行個體安全，設定安全性群組規則時要遵循最小授權原則，下面介紹四種安全的內網執行個體互連設定方法。

方法 1. 使用單 IP 位址授權

- 適用情境：適用於小規模執行個體間內網互連情境。

- 優點：以IP地址方式授權，安全性群組規則清晰，容易理解。
- 缺點：內網互連執行個體數量較多時，會受到安全性群組規則條數 100 條的限制，另外後期維護工作量比較大。
- 設定方法：
  i. 選擇需要互連的執行個體，進入**本執行個體安全性群組**。
  ii. 選擇需要配置安全性群組，單擊**配置規則**。
  iii. 單擊**內網入方向**，並單擊**添加安全性群組規則**。
  iv. 按以下描述添加安全性群組規則：
    - **授權策略**：允許。
    - **協議類型**：根據實際需要選擇協議類型。
    - **連接埠範圍**：根據您的實際需要設定連接埠範圍，格式為*開始端點口號/終止連接埠號碼*。
    - **授與類型**：位址區段訪問。
    - **授權對象**：輸入想要內網互連的執行個體的內網 IP 位址，格式必須是 *a.b.c.d/32*。其中，子網路遮罩必須是 */32*。

方法 2. 加入同一安全性群組

- 適用情境：如果您的應用架構比較簡單，可以為所有的執行個體選擇相同的安全性群組，綁定同一安全性群組的執行個體之間不用設定特殊規則，預設網路互連。
- 優點：安全性群組規則清晰。
- 缺點：僅適用於簡單的應用網路架構，網路架構調整時授權方法要隨之進行修改。
- 設定方法：請參見加入、移出安全性群組。

方法 3. 綁定互連安全性群組

- 適用情境：為需要互連的執行個體增加綁定一個專門用於互連的安全性群組，適用於多層應用網路架構情境。
- 優點：操作簡單，可以迅速建立執行個體間互連，可應用於複雜網路架構。
- 缺點：執行個體需綁定多個安全性群組，安全性群組規則閱讀性較差。
- 設定方法：
  i. 建立一個安全性群組並命名，例如：互連安全性群組，不需要給建立的安全性群組添加任何規則。
  ii. 將需要互連的執行個體都添加綁定建立的互連安全性群組，利用同一安全性群組的執行個體之間預設互連的特性，達到內網執行個體互連的效果。

方法 4. 安全性群組互信授權

- 適用情境：如果您的網路架構比較複雜，各執行個體上部署的應用都有不同的業務角色，您就可以選擇使用安全性群組互相授權方式。
- 優點：安全性群組規則結構清晰、閱讀性強、可跨賬戶互連。
- 缺點：安全性群組規則配置工作量較大。
- 設定方法：
  i. 選擇需要建立互信的執行個體，進入**本執行個體安全性群組**。
  ii. 選擇需要配置安全性群組，單擊**配置規則**。
  iii. 單擊**內網入方向**，並單擊**添加安全性群組規則**。

iv. 按以下描述添加安全性群組規則：

- **授權策略**：允許。
- **協議類型**：根據您的實際需要選擇協議類型。
- **連接埠範圍**：根據實際需求設定。
- **授與類型**：安全性群組訪問。
- **授權對象**：
  - 如果您選擇**本帳號授權**：按照您的組網要求，將有內網互連需求的對端執行個體的安全性群組 ID 填入**授權對象**即可。
  - 如果您選擇**跨帳號授權**：**授權對象**應填入對端執行個體的安全性群組 ID，**帳號 ID**是對端帳號 ID（可以在**帳號管理 > 安全設定**裡查到）。

建議

如果前期安全性群組授權過大，建議採用以下流程收緊授權範圍。

圖中的**刪除0.0.0.0**是指刪除原來的允許*0.0.0.0/0*位址區段的安全性群組規則。

如果安全性群組規則變更操作不當，可能會導致您的執行個體間通訊受到影響，請在修改設定前備份您要操作的安全性群組規則，以便出現互連問題時及時恢複。

安全性群組映射了執行個體在整個應用架構中的角色，推薦按照應用架構規劃防火牆規則。例如：常見的三層 Web 應用程式架構就可以規劃三個安全性群組，將部署了相應應用或資料庫的執行個體綁定對應的安全性群組：

- Web 層安全性群組：開放 80 連接埠。
- APP 層安全性群組：開放 8080 連接埠。
- DB 層安全性群組：開放 3306 連接埠。

2.5. 修改伺服器預設遠程連接埠

本文介紹如何修改 Windows 和 Linux 伺服器的預設遠程連接埠。

修改 Windows 伺服器預設遠程連接埠

本節以 Windows Server 2008 為例介紹如何修改 Windows 伺服器預設遠程連接埠。

1. 遠端連線並登入到 Windows 執行個體。
2. 運行*regedit.exe*開啟登錄編輯程式。
3. 找到如下註冊表子項：*HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\PortNumber*
4. 在彈出的對話方塊中，選擇**十進位**，在**數值資料**中輸入新的遠程連接埠號碼，在本例中即 3399。單擊**確定**。
5. （可選）如果您開啟了防火牆，需要將新的連接埠號碼添加到防火牆並設定允許串連。
6. 登入 ECS管理主控台 ，找到該執行個體，選擇**更多 > 執行個體狀態 > 重啟**。
7. 執行個體重新啟動後，在執行個體的右側單擊**管理**，進入**執行個體詳情**頁面。選擇**本執行個體安全性**

群組。

8. 在**安全性群組列表**頁面，找到相應的安全性群組，單擊**配置規則**。
9. 在**安全性群組規則**頁面，單擊**添加安全性群組規則**。根據實際的使用情境來定義安全規則，允許新配置的遠程連接埠進行串連。關於如何設定安全性群組參見添加安全性群組規則。
10. 以上步驟完成後，遠端存取伺服器，在遠程地址後面添加新遠程連接埠號碼即可串連執行個體。例如：192.168.1.2:3399。

> **說明** 調整 3389 連接埠後，使用 Mac 的遠端桌面連線客戶僅支援預設的 3389 連接埠。

修改 Linux 伺服器預設遠程連接埠

本節以 CentOS 6.8 為例介紹如何修改 Linux 伺服器預設遠程連接埠。

> **說明** 不要直接修改 22 連接埠，先添加需要的預設遠程連接埠。之所以先設定成兩個連接埠，測試成功後再關閉一個連接埠，是為了防止在修改設定檔及網路調試過程中，萬一出現新連接埠無法串連的情況下，還能通過 22 連接埠進行登入調試。

1. 遠端連線並登入到 Linux 執行個體。
2. 運行 **vim /etc/ssh/sshd_config** 命令。
3. 在鍵盤上按“I”鍵，進入編輯狀態。添加新的遠程服務連接埠，本節以 1022 連接埠為例。在*Port 22*下輸入*Port 1022*。
4. 在鍵盤上按“Esc”，輸入：**wq**退出編輯狀態。
5. 執行以下命令重啟執行個體，之後您可以通過 22 連接埠和 1022 連接埠 SSH 登入到 Linux 執行個體。

```
/etc/init.d/sshd restart
```

6. （可選）配置防火牆。使用 CentOS 7 以前的版本並開啟預設防火牆 iptables 時，應注意 iptables 預設不攔截訪問，如果您配置了 iptables 規則，需要執行**iptables -A INPUT -p tcp --dport 1022 -j ACCEPT** 配置防火牆。然後執行**service iptables restart** 重啟防火牆。

> **說明** CentOS 7 以後版本預設安裝 Firewalld。如果您已經啟用 firewalld.service，需要允許存取 TCP 1022 連接埠：運行命令 firewall-cmd --add-port=1022/tcp --permanent。返回結果為 success 即表示已經允許存取 TCP 1022 連接埠。

7. 登入 ECS管理主控台，找到該執行個體，選擇**管理**。
8. 進入**執行個體詳情**頁面。選擇**本執行個體安全性群組**。
9. 在**安全性群組列表**頁面，找到相應的安全性群組，單擊**配置規則**。
10. 在**安全性群組規則**頁面，單擊**添加安全性群組規則**。根據實際的使用情境來定義安全規則，允許新配置的遠程連接埠進行串連。關於如何設定安全性群組參見添加安全性群組規則。
11. 使用 SSH 工具串連新連接埠，來測試是否成功。登入時在 **Port** 一欄輸入新修改的連接埠號碼，在本例中即 1022。
12. 使用 1022 連接埠串連成功後，再次運行**vim /etc/ssh/sshd_config**命令，將 Port 22 刪除。
13. 運行 **/etc/init.d/sshd restart** 命令重啟執行個體，伺服器預設遠程連接埠修改完成。再次登入時使

用新連接埠號碼登入即可。

2.6. 使用Windows執行個體的日誌

日誌記錄了系統中硬體、軟體和系統問題的資訊，同時還監視著系統中發生的事件。當伺服器被入侵或者系統（應用）出現問題時，管理員可以根據日誌迅速定位問題的關鍵，再快速處理問題，從而極大地提高工作效率和伺服器的安全性。Windows系統日誌主要分為：系統日誌、應用程式記錄檔、安全日誌以及應用程式和服務日誌。本文以Windows Server 2008 R2為例，簡單地介紹四種日誌的使用和簡要分析。

進入事件檢視器

進入事件檢視器：開啟 **運行** 視窗，輸入 **eventvwr**，開啟 **事件檢視器**。

之後，您可以在 **事件檢視器** 裡查看以下四種日誌。

> **說明** 通過本文所述四種日誌的查看方法找到的所有錯誤記錄檔事件ID，您可以用於在微軟知識庫找到解決方案。

- **系統日誌**

  系統日誌包含Windows系統組件記錄的事件。例如，系統日誌中會記錄在啟動過程中載入驅動程式或其他系統組件失敗。

  系統組件所記錄的事件類型由Windows預先確定。

- **應用程式記錄檔**

  應用程式記錄檔包含由應用程式或程式記錄的事件。例如，資料庫程式可在應用程式記錄檔中記錄檔案錯誤。

  程式開發人員決定記錄哪些事件。

- **安全日誌**

  安全日誌包含諸如有效和無效的登入嘗試等事件，以及與資源使用相關的事件，如建立、開啟或刪除檔案或其他對象。

  管理員可以指定在安全日誌中記錄什麼事件。例如，如果已啟用登入審核，則安全日誌將記錄對系統的登入嘗試。

- **應用程式和服務日誌**

  應用程式和服務日誌是一種新類別的事件記錄。這些日誌儲存來自單個應用程式或組件的事件，而非可能影響整個系統的事件。

修改日誌路徑並備份日誌

日誌預設儲存在系統硬碟裡面。日誌最大值預設是20 MB，超過20 MB時會覆蓋之前的事件。您可以根據自己的需求修改。

按以下步驟修改日誌路徑並備份日誌。

1. 在 **事件檢視器** 視窗，在左側導覽列裡，單擊 **Windows 日誌**。
2. 在右邊列表中，選中一個日誌目錄，右鍵這一類日誌，如截圖所示的 **應用程式**。

3. 在 **日誌屬性** 視窗，按介面顯示修改以下資訊：
   - 日誌路徑。
   - 日誌最大大小。
   - 達到事件記錄最大大小時系統應採取的操作。

2.7. 安全性群組內網路隔離

安全性群組是一種虛擬防火牆，具備狀態檢測和包過濾功能。安全性群組由同一個地區內具有相同安全保護需求並相互信任的執行個體組成。為了滿足同安全性群組內執行個體之間網路隔離的需求，阿里雲豐富了安全性群組網路連通策略，支援安全性群組內實現網路隔離。

安全性群組內的網路隔離規則

- 安全性群組內網路隔離是網卡之間的隔離，而不是ECS執行個體之間的隔離。若執行個體上綁定了多張彈性網卡，需要在每個網卡上設定安全性群組隔離規則。
- 不會改變預設的網路連通策略。

  安全性群組內網路隔離是一種自訂的網路連通策略，對於預設安全性群組和建立的安全性群組無效。安全性群組預設的網路連通策略是：同一安全性群組內的執行個體之間私網互連，不同安全性群組的執行個體之間預設私網不通。
- 安全性群組內網路隔離的優先順序最低。

  設定了組內網路隔離的安全性群組，僅在安全性群組內沒有任何自訂規則的情況下保證安全性群組內執行個體之間網路隔離。以下情況設定了組內網路隔離但執行個體仍然互連：
  - 安全性群組內既設定了組內隔離，又設定了讓組內執行個體之間可以互相訪問的ACL。
  - 安全性群組內既設定了組內隔離，又設定了組內互連。
- 網路隔離只對當前安全性群組內的執行個體有效。

修改策略

您可以使用ModifySecurityGroupPolicy介面來修改安全性群組內的網路連通策略。

案例分析

執行個體和執行個體所屬的安全性群組的關係如下：

本樣本中，Group1、Group2、Group3分別為3個不同的安全性群組，ECS1、ECS2、ECS3分別為3個不同的ECS執行個體。ECS1和ECS2同屬安全性群組Group1和Group2，ECS2和ECS3同屬安全性群組Group3。

3個安全性群組內的網路連通原則設定如下：

安全性群組	內網連通策略	包含的執行個體
Group1	隔離	ECS1、ECS2
Group2	互連	ECS1、ECS2
Group3	互連	ECS2、ECS3

各執行個體間的網路連通情況如下：

執行個體	網路互連／隔離	原因
ECS1和ECS2	互連	ECS1、ECS2同時屬於Group1和Group2。Group1的策略是隔離，Group2的策略是互連，由於網路隔離的優先順序最低，所以ECS1和ECS2互連。
ECS2和ECS3	互連	ECS2和ECS3同時屬於Group3。Group3的策略是互連，所以ECS2和ECS3互連。
ECS1和ECS3	隔離	ECS1和ECS3分屬不同的安全性群組，不同安全性群組的執行個體之間預設網路不通。如果兩個安全性群組之間需要互相訪問，可以通過安全性群組規則授權。

2.8. 安全性群組五元組規則

安全性群組用於設定單台或多台ECS執行個體的網路存取控制，它是重要的網路安全隔離手段，用於在雲端劃分安全域。安全性群組五元組規則能精確控制源IP、源連接埠、目的IP、目的連接埠以及傳輸層協議。

背景資訊

在最初涉及安全性群組規則時，

- 安全性群組入規則只支援：源IP地址、目的連接埠、傳輸層協議。
- 安全性群組出規則只支援：目的IP地址、目的連接埠、傳輸層協議。

在多數應用情境下，該安全性群組規則簡化了設定，但存在如下弊端：

- 無法限定入規則的源連接埠範圍，預設允許存取所有源連接埠。
- 無法限定入規則的目的IP地址，預設允許存取安全性群組下的所有IP地址。
- 無法限定出規則的源連接埠範圍，預設允許存取所有源連接埠。
- 無法限定出規則的源IP地址，預設允許存取安全性群組下的所有IP地址。

五元組規則定義

五元組規則包含：源IP地址、源連接埠、目的IP地址、目的連接埠、傳輸層協議。

五元組規則完全相容原有的安全性群組規則，能更精確的控制源IP地址、源連接埠、目的IP地址、目的連接埠以及傳輸層協議。

五元組出規則樣本如下：

源IP地址： 172.16.1.0/32
源連接埠： 22
目的IP： 10.0.0.1/32
目的連接埠：不限制
傳輸層協議： TCP
授權策略： Drop

樣本中的出規則表示禁止172.16.1.0/32通過22連接埠對10.0.0.1/32發起TCP訪問。

應用情境

- 某些平台類網路產品接入第三方廠商的解決方案為使用者提供網路服務，為了防範這些產品對使用者的ECS執行個體發起非法訪問，則需要在安全性群組內設定五元組規則，更精確的控制出流量和入流量。

- 設定了組內網路隔離的安全性群組，如果您想精確控制組內若干ECS執行個體之間可以互相訪問，則需要在安全性群組內設定五元組規則。

配置五元組規則

您可以使用OpenAPI設定五元組規則。

- 增加安全性群組入規則，請參見 AuthorizeSecurityGroup。
- 增加安全性群組出規則，請參見 AuthorizeSecurityGroupEgress。
- 刪除安全性群組入規則，請參見 RevokeSecurityGroup。
- 刪除安全性群組出規則，請參見 RevokeSecurityGroupEgress。

參數說明

在授權或解除授權時，各參數的含義如下表所示。

參數	入規則中各參數含義	出規則中各參數含義
SecurityGroupId	當前入規則所屬的安全性群組ID，即目的安全性群組ID。	當前出規則所屬的安全性群組ID，即源安全性群組ID。
DestCidrIp	目的IP範圍，選擇性參數。 • 如果指定DestCidrIp，則可以更精細地控制入規則生效的目的IP範圍； • 如果不指定DestCidrIp，則入規則生效的IP範圍就是SecurityGroupId這個安全性群組下的所有IP。	目的IP，DestGroupId與DestCidrIp二者必選其一，如果二者都指定，則DestCidrIp優先順序高。
PortRange	目的連接埠範圍，必選參數	目的連接埠範圍，必選參數。
DestGroupId	不允許輸入。目的安全性群組ID一定是SecurityGroupId。	目的安全性群組ID。DestGroupId與DestCidrIp二者必選其一，如果二者都指定，則DestCidrIp優先順序高。
SourceGroupId	源安全性群組ID，SourceGroupId與SourceCidrIp二者必選其一，如果二者都指定，則SourceCidrIp優先順序高。	不允許輸入，出規則的源安全性群組ID一定是SecurityGroupId。
SourceCidrIp	源IP範圍，SourceGroupId與SourceCidrIp二者必選其一，如果二者都指定，則SourceCidrIp優先順序高。	源IP範圍，選擇性參數。 • 如果指定SourceCidrIp，則會更精細地限定出規則生效的源IP。 • 如果不指定SourceCidrIp，則生效的源IP就是SecurityGroupId這個安全性群組下的所有IP。
SourcePortRange	源連接埠範圍，選擇性參數，不填則不限制源連接埠。	源連接埠範圍，選擇性參數，不填則不限制源連接埠。

2.9. 通過API允許不同帳號下的ECS執行個體內網通訊

若您需要實現同一地區下不同帳號的ECS執行個體內網通訊，可以參考本文描述授權安全性群組間互訪。

前提條件

本文調用API的工具為阿里雲CLI，請確保您已安裝並配置了阿里雲CLI。具體操作，請參見安裝CLI和配置CLI。

背景信息

目前授權安全性群組內網通訊有以下兩種，請根據您的實際需求選擇方式。

- ECS執行個體間通訊：授權同一帳號兩台ECS執行個體間的內網通訊。
- 帳號間內網通訊：授權同一帳號同一地區下兩個安全性群組內所有的ECS執行個體的內網通訊，包括授權以後購買的同一安全性群組內的ECS執行個體。

> **說明** 帳號間內網通訊實際上是安全性群組間授權，即授權處於這兩個安全性群組內的ECS執行個體後就可以實現內網通訊。修改安全性群組配置會影響到安全性群組內所有的ECS執行個體，請根據實際需要進行操作，避免影響到ECS執行個體網路下啟動並執行業務。

安全性群組是ECS執行個體的虛擬防火牆，安全性群組本身不提供通訊能力和組網能力。授權不同安全性群組內的執行個體內網通訊後，請同時確保執行個體可以建立內網互連的能力。

- 若執行個體均是傳統網路類型，必須位於同一地區下。
- 若執行個體均是VPC類型，不同VPC間預設內網不通。建議通過公網訪問的方式通訊，或者通過Express Connect、VPN網關和雲企業網等方式提供訪問能力。詳情請參見Express Connect、VPN網關和雲企業網。
- 若執行個體網路類型不同，請設定ClassicLink允許執行個體通訊。具體操作，請參見。
- 若執行個體位於不同地區，建議通過公網訪問的方式通訊，或者通過Express Connect、VPN網關和雲企業網等方式提供訪問能力。詳情請參見Express Connect、VPN網關和雲企業網。

ECS執行個體間通訊

1. 查詢兩台ECS執行個體的內網IP地址和兩台ECS執行個體所處的安全性群組ID。

   您可以通過控制台或調用DescribeInstances介面獲得ECS執行個體所屬的安全性群組ID。假設兩台ECS執行個體的資訊如下表所示。

執行個體	IP地址	所屬安全性群組	安全性群組ID
執行個體A	10.0.0.1	sg1	sg-bp1azkttqpldxgtedXXX
執行個體B	10.0.0.2	sg2	sg-bp15ed6xe1yxeycg7XXX

2. 在sg1安全性群組中添加允許存取10.0.0.2的入方向的規則。

```
aliyun ecs AuthorizeSecurityGroup --SecurityGroupId sg-bp1azkttqpldxgtedXXX --RegionId
cn-qingdao --IpProtocol all  --PortRange=-1/-1. --SourceCidrIp 10.0.0.2 --NicType intra
net
```

3. 在sg2安全性群組中添加允許存取10.0.0.1的入方向的規則。

```
aliyun ecs AuthorizeSecurityGroup --SecurityGroupId sg-bp15ed6xe1yxeycg7XXX --RegionId
cn-qingdao --IpProtocol all  --PortRange=-1/-1. --SourceCidrIp 10.0.0.1 --NicType intra
net
```

> 說明
> - 以上命令中，地區取值為華北 1（青島）*cn-qingdao*，請您根據實際情況修改。
> - 以上命令中，調用AuthorizeSecurityGroup介面添加安全性群組入方向的允許存取規則，主要關注的參數為SecurityGroupId和SourceCidrIp。

4. 等待一分鐘後，使用ping命令測試兩台ECS執行個體之間是否內網互連。

帳號間內網通訊

1. 查詢兩個帳號的帳號名和兩個帳號下對應的安全性群組ID。

   您可以通過控制台或調用DescribeInstances介面獲得ECS執行個體所屬的安全性群組ID。假設兩個帳號的資訊如下表所示。

帳號	帳號ID	安全性群組	安全性群組ID
帳號A	a@aliyun.com	sg1	sg-bp1azkttqpldxgtedXXX
帳號B	b@aliyun.com	sg2	sg-bp15ed6xe1yxeycg7XXX

2. 在sg1安全性群組中添加允許存取sg2安全性群組入方向的規則。

```
aliyun ecs AuthorizeSecurityGroup --SecurityGroupId sg-bp1azkttqpldxgtedXXX --RegionId
cn-qingdao --IpProtocol all  --PortRange=-1/-1. --SourceGroupId sg-bp15ed6xe1yxeycg7XXX
--SourceGroupOwnerAccount b@aliyun.com --NicType intranet
```

3. 在sg2安全性群組中添加允許存取sg1安全性群組入方向的規則。

```
aliyun ecs AuthorizeSecurityGroup --SecurityGroupId sg-bp15ed6xe1yxeycg7XXX --RegionId
cn-qingdao --IpProtocol all  --PortRange=-1/-1. --SourceGroupId sg-bp1azkttqpldxgtedXXX
--SourceGroupOwnerAccount a@aliyun.com --NicType intranet
```

> 說明
> - 以上命令中，地區取值為華北 1（青島）*cn-qingdao*，請您根據實際情況修改。
> - 以上命令中，調用AuthorizeSecurityGroup介面添加安全性群組入方向的允許存取規則時，主要關注的參數為SecurityGroupId、SourceGroupId和SourceGroupOwnerAccount。

4. 等待一分鐘後，使用ping命令測試查看兩台ECS執行個體之間是否內網互連。

3.資料恢複

3.1. Linux執行個體中資料恢複

在處理磁碟相關問題時，您可能會碰到作業系統中資料盤分區丟失的情況。本文介紹了Linux系統下常見的資料盤分區丟失的問題以及對應的處理方法，同時提供了使用雲端硬碟的常見誤區以及最佳實務，避免可能的資料丟失風險。

在修複資料前，您必須先對分區丟失的資料盤建立快照，在快照建立完成後再嘗試修複。如果在修複過程中出現問題，您可以通過快照復原將資料盤還原到修複之前的狀態。

前提條件

在修複資料前，您必須先對分區丟失的資料盤建立快照，在快照建立完成後再嘗試修複。如果在修複過程中出現問題，您可以通過快照復原將資料盤還原到修複之前的狀態。

工具說明

在Linux執行個體裡，您可以選擇以下任一種工具修複磁碟分割並恢複資料：

- fdisk：Linux系統預設安裝的分區工具。
- testdisk：主要用恢複Linux系統的磁碟分割或者資料。Linux系統預設不安裝，您需要自行安裝這個軟體，比如，在CentOS系統裡，您可以運行 **yum install -y testdisk** 線上安裝。
- partprobe：Linux系統預設安裝的工具。主要用於不重啟系統時讓kernel重新讀取分區。

Linux系統下資料盤分區丟失和資料恢複處理辦法

在Linux執行個體裡，您重啟系統後，可能會出現資料盤分區丟失或者資料丟失的問題。這可能是因為您未在 */etc/fstab* 檔案裡設定自動掛載。此時，您可以先手動掛載資料盤分區。如果手動掛載時報分區表丟失，您可以通過如下三種辦法嘗試進行處理：通過fdisk恢複分區、通過testdisk恢複分區 或者 通過testdisk直接恢複資料。

- **通過fdisk恢複分區**

  對資料盤分區時，分區磁碟的起止扇區一般使用預設的值，所以可以先嘗試直接使用 fdisk 建立分區進行恢複。具體操作，請參考 Linux 格式化和掛載資料盤。

  如果上述操作無效，您可以使用 testdisk 工具嘗試修複。

- **通過 testdisk 恢複分區**

  這裡假設雲端硬碟的裝置名稱為 */dev/xvdb*。按以下步驟使用 testdisk 恢複分區：

  i. 運行 **testdisk /dev/xvdb**（根據實際情況替換裝置名稱），再選擇 **Proceed**（預設值）後按斷行符號鍵。

  ii. 選擇分區表類型進行掃描：一般選擇 *Intel*（預設）。如果您的資料盤採用GPT分區，選擇 *EFI GPT*。

  iii. 選擇 *Analyse* 後按斷行符號鍵。

  iv. 如果您沒有看到沒有任何分區資訊，選擇 *Quick Search* 後按斷行符號鍵快速搜尋。

  在返回結果中會顯示分區資訊，如下圖所示。

  v. 選中分區後，按斷行符號鍵。

vi. 選擇 *Write* 儲存分區。

> **說明** 如果不是您需要的分區，可以選擇 *Deeper Search* 繼續搜尋。

vii. 按 *Y* 鍵確認儲存分區。

viii. 運行 **partprobe /dev/xvdb**（根據實際情況替換裝置名稱）手動重新整理分區表。

ix. 重新掛載分區，查看資料盤裡的資料情況。

- **通過testdisk直接恢複資料**

  在某些情況下，您可以用testdisk掃描出磁碟分割，但是無法儲存分區，此時，您可以嘗試直接恢複檔案。具體操作步驟如下所示：

  i. 按 通過testdisk恢複分區 的第1步到第4步描述找到分區。

  ii. 按 *P* 鍵列出檔案。 返回結果如下圖。

  iii. 選中要恢複的檔案，再按 *C* 鍵。

  iv. 選擇目標目錄。本樣本中以恢複到 */home* 為例。

  如果您看到 `Copy done! 1 ok, 0 failed` 說明複製成功。如下圖所示。

  v. 切換到 */home* 目錄查看。如果您能看到檔案，說明檔案恢複成功。

常見誤區與最佳實務

資料是使用者的核心資產，很多使用者在ECS上構建網站、自建資料庫(MYSQL/MongoDB/Redis)。資料丟失會給使用者的業務帶來巨大的風險。如下是在資料安全方面的常見誤區和最佳實務。

- **常見誤區**

  阿里雲的底層儲存基於 三副本，因此有些使用者認為作業系統內資料沒有任何丟失風險。實際上這是誤解。底層儲存的三副本提供對資料磁碟的物理層保護，但是，如果系統內部使用雲端硬碟邏輯上出現問題，比如中毒、誤刪資料、檔案系統損壞等情況，還是可能出現資料丟失。此時，您需要通過快照、異地備份等相關技術最大保證資料的安全性。

- **最佳實務**

  資料盤分區恢複以及資料恢複是處理資料丟失問題最後的一道防線，但未必一定能夠恢複資料。強烈建議您參考如下最佳實務，通過對資料建立快照（自動或手動）以及各類備份方案，最大程度地保證資料的安全性。

  - **啟用自動快照**

    根據實際業務，對系統硬碟、資料盤建立自動快照。注意，在更換系統硬碟、執行個體到期後或手動釋放磁碟時，自動快照可能會被釋放。

    您可以在ECS控制台上通過 **修改磁碟屬性** 選擇 **自動快照隨磁碟釋放**。如果想保留自動快照，您可以手動去掉該選項。

    詳情請參考：ECS雲端服務器自動快照FAQ。

- **建立手動快照**

  在做下列重要或有風險的操作前，請手動為磁碟建立快照。例如：

  - 系統升級核心
  - 應用升級變更
  - 磁碟資料恢複

  在恢複磁碟時，一定要先對磁碟建立快照，快照完成後做相應的操作。

- **OSS、線下、異地備份**

  您可酌情使用OSS、線下、異地等方式備份重要資料。

3.2. Windows執行個體中資料恢複

在處理磁碟相關問題時，您可能會碰到作業系統中資料盤分區丟失的情況。本文介紹了Windows系統下常見的資料盤分區丟失的問題以及對應的處理方法，同時提供了使用雲端硬碟的常見誤區以及最佳實務，避免可能的資料丟失風險。

前提條件

在修複資料前，您必須先對丟失分區的資料盤建立快照，在快照建立完成後再嘗試修複。如果在修複過程中出現問題，您可以通過快照復原將資料盤還原到修複之前的狀態。

工具說明

在Windows執行個體裡，您可以選擇以下任一種工具恢複資料盤資料：

- 磁碟管理：Windows系統內建工具，主要用於分區格式化資料盤等。
- 資料恢複軟體：一般是商業軟體，您可以去相應的官網下載使用。主要作用是檔案系統異常恢複資料。

磁碟顯示為“外部”，無法顯示分區

在Windows系統中，您在 **磁碟管理器** 中看到磁碟顯示為 **外部**，而且不顯示分區情況，如下圖所示。

此時，按以下方式處理：

在 **外部** 磁碟處，按右鍵右邊的空白處，選擇 **匯入外部磁碟**，再單擊 **確定**。

磁碟顯示為“離線”，無法顯示分區

在Windows系統中，您在 **磁碟管理器** 中看到磁碟顯示為 **離線**，而且不顯示分區情況，如下圖所示。

此時，按以下方式處理：

在 **離線** 磁碟處，按右鍵磁碟名稱（如上圖中的 **磁碟1**）周邊的空白區，在快顯功能表中，選擇 **聯機**，再單擊 **確定**。

未分配盤符，無法顯示分區

在Windows系統中，您在 **磁碟管理器** 中能看到資料盤的資訊，但資料盤未分配盤符，如下圖所示。

此時，按以下方式處理：

按右鍵磁碟（如上圖所示的 **磁碟1**）的主要磁碟分割，在快顯功能表中，選擇 **更改磁碟機代號和路徑**，並按提示完成操作。

在磁碟管理器無法查看資料盤，報錯“枚舉儲存期間出錯”

在Windows系統中，您在 **磁碟管理器** 裡無法查看資料盤。系統日誌裡報錯“枚舉儲存期間出錯”，如下圖所示。

> **說明** 作業系統的版本不同，報錯內容也可能是“枚舉卷期間出錯”。

此時，按以下步驟處理：

1. 啟動Windows PowerShell。
2. 運行命令 **winrm quickconfig** 進行修複。當介面上詢問“執行這些更改嗎[y/n]?”時，輸入 *y* 確認執行。

修複完成後，再開啟 **磁碟管理器**，一般資料盤已經能正常顯示。

資料盤變成RAW格式

在某些特殊情況下，您可能會發現Windows下磁碟變為RAW格式。

磁碟顯示為RAW格式是因為Windows無法識別磁碟上的檔案系統。一般是因為記錄檔案系統類型或者位置的資訊丟失或者損壞，比如partition table或者boot sector。以下列出了一些比較常見的原因：

- 外接硬碟發生這種問題通常是因為沒有使用 **Safely remove hardware** 選項斷開磁碟。
- 意外斷電導致的磁碟問題。
- 硬體層故障也可能導致磁碟分割資訊丟失。
- 底層與磁碟相關的驅動或應用，例如您使用的diskprobe工具就可以直接修改磁碟的表結構。
- 電腦病毒。

您可以參考微軟官方的 Dskprobe Overview 文檔修複磁碟。

此外，Windows下有大量免費或商業的資料恢複軟體可用於找回丟失的資料。例如，您可以嘗試使用Disk Genius工具掃描，來嘗試恢複相應的檔案。

常見誤區和最佳實務

資料是使用者的核心資產，很多使用者在ECS上構建網站、自建資料庫(MYSQL/MongoDB/Redis)。如果出現資料丟失，會給使用者的業務帶來巨大的風險。如下是在資料安全方面的常見誤區和最佳實務。

- **常見誤區**

  阿里雲的底層儲存基於 三副本，因此有些使用者認為作業系統內資料沒有任何丟失風險。實際上這是誤解。底層儲存的三副本提供對資料磁碟的物理層保護，但是，如果系統內部使用雲端硬碟邏輯上出現問題，比如中毒、誤刪資料、檔案系統損壞等情況，還是可能出現資料丟失。此時，您需要通過快照、異地備份等相關技術最大保證資料的安全性。

- **最佳實務**

  資料盤分區恢複以及資料恢複是處理資料丟失問題最後的一道防線，但未必一定能夠恢複資料。強烈建議您參考如下最佳實務，通過對資料建立快照（自動或手動）以及各類備份方案，最大程度地保證資料的安全性。

- **啟用自動快照**

  根據實際業務，對系統硬碟、資料盤建立自動快照。注意，在更換系統硬碟、執行個體到期後或手動釋放磁碟時，自動快照可能會被釋放。

  您可以在ECS控制台上通過 **修改磁碟屬性** 選擇 **自動快照隨磁碟釋放**。如果想保留自動快照，您可以手動去掉該選項。

  詳情請參考：ECS雲端服務器自動快照FAQ。

- **建立手動快照**

  在做下列重要或有風險的操作前，請手動為磁碟建立快照。例如：

  - 系統升級核心
  - 應用升級變更
  - 磁碟資料恢複

  在恢複磁碟時，一定要先對磁碟建立快照，快照完成後做相應的操作。

- **OSS、線下、異地備份**

  您可酌情使用OSS、線下、異地等方式備份重要資料。

4.執行個體配置

4.1. ECS執行個體資料轉送的實現方式

在資訊化高速發展的今天，伺服器每天都會與其它單機交換大量檔案資料，檔案傳輸對大家來說是家常便飯。因此，其重要性就不言而喻了。檔案傳輸方式各有不同，選擇一款合適自己的檔案傳輸工具，在工作中能起到事半功倍的效果。節省資源、方便傳輸、提升工作效率、加密保護等等。因此，很多檔案傳輸工具應運而生，例如：NC、FTP、SCP、NFS、SAMBA、RSYNC/SERVERSYNC等等，每種方式都有自己的特點。本文將首先簡單介紹一下檔案傳輸的基本原理，然後，詳細介紹類Unix/Linux、Windows平台上熱門檔案傳輸方式，並針對它們各自的特點進行比較，讓讀者對檔案傳輸方式有比較詳盡地瞭解，從而能夠根據不同的需要選擇合適的檔案傳輸方式。

檔案傳輸原理

檔案傳輸是資訊傳輸的一種形式，它是在資料來源和資料宿之間傳送檔案資料的過程，也稱檔案資料通訊。作業系統把檔案資料提取到記憶體中做暫存，再複製到目的地，加密就是在檔案外加了一個殼，檔案本身還是一個整體，複製只是把這個整體轉移到其它地方，不需要解密，只有開啟壓縮包時才需解密。一個大檔案作為一個資料整體，是不可能瞬間從一台主機轉移到其它的主機，傳輸是一個持續的過程，但不是把檔案分割了，因此，如果在傳輸的過程中意外中斷，目標路徑中是不會有傳輸的檔案，另外，如果傳輸的是多個檔案，那麼，這些檔案是按順序分別傳輸，如果中間中斷，則正在傳輸的檔案會傳輸失敗，但是，之前已經傳完的檔案傳輸成功（如果傳輸的是檔案壓縮包，那麼，不管裡面有幾個檔案，它本身被視為一個檔案）。

通常我們看到的 NC、FTP、SCP、NFS 等等，都是可以用來傳輸檔案資料的工具，下面我們將詳細介紹主要檔案傳輸工具的特點以及用法。

NETCAT

在網路工具中有“瑞士軍刀”的美譽，它功能強大，作為網路工具的同時，它傳輸檔案的能力也不容小覷。

常用參數

參數	說明
-g <網關>	設定路由器躍程通訊網關，最多可設定8個
-G <指向器數目>	設定來源路由指向器，其數值為4的倍數
-i <延遲秒數>	設定時間間隔，以便傳送資訊及掃描通訊連接埠
-l	使用監聽模式，管控傳入的資料
-o <輸出檔案>	指定檔案名稱，把往來傳輸的資料以16進位字碼傾倒成該檔案儲存
-p <通訊連接埠>	設定本地主機使用的通訊連接埠
-r	指定本地與遠端主機的通訊連接埠
-u	使用UDP傳輸協議
-v	顯示指令執行過程
-w <逾時秒數>	設定等待連線的時間
-z	使用0輸入/輸出模式，只在掃描通訊連接埠時使用

參數	說明
-n	直接使用IP地址，而不通過網域名稱伺服器

用法舉例

1.連接埠掃描21-24(以IP192.168.2.34為例)。

```
nc -v -w 2 192.168.2.34 -z 21-24
```

返回樣本：

```
nc: connect to 192.168.2.34 port 21 (tcp) failed: Connection refused
Connection to 192.168.2.34 22 port [tcp/ssh] succeeded!
nc: connect to 192.168.2.34 port 23 (tcp) failed: Connection refused
nc: connect to 192.168.2.34 port 24 (tcp) failed: Connection refused
```

2. 從192.168.2.33拷貝檔案到192.168.2.34。

- 在192.168.2.34上：`nc-l 1234 > test.txt`
- 在192.168.2.33上：`nc192.168.2.34 < test.txt`

3.用nc命令操作memcached。

- 儲存資料：`printf "set key 0 10 6rnresultrn" |nc 192.168.2.34 11211`
- 擷取資料：`printf "get keyrn" |nc 192.168.2.34 11211`
- 刪除資料：`printf "delete keyrn" |nc 192.168.2.34 11211`
- 查看狀態：`printf "statsrn" |nc 192.168.2.34 11211`
- 類比top命令查看狀態：`watch "echo stats" |nc 192.168.2.34 11211`
- 清空緩衝：

```
printf "flush_allrn" |nc 192.168.2.34 11211        #謹慎操作，清空了緩衝就沒了
```

SCP 安全拷貝

SCP（ Secure Copy）命令的用法和 RCP 命令格式非常類似，區別就是 SCP 提供更安全保障，SCP 在需要進行驗證時會要求你輸入密碼或口令，一般推薦使用 SCP 命令，因為它比 RCP 更安全。SCP 命令使用 SSH 來傳輸資料，並使用與 SSH 相同的認證模式，提供同樣的安全保障，SSH 是目前較可靠得，為遠程登入工作階段和其他網路服務提供安全性的協議，利用 SSH 協議可以有效防止遠端管理過程中的資訊泄露問題。SCP 是基於 SSH 的應用，所以進行資料轉送的機器上必須支援 SSH 服務。

特點

SCP 類似於RCP, 它能夠保留一個特定檔案系統上的檔案屬性，能夠保留檔案屬性或者需要遞迴的拷貝子目錄。

SCP它具備更好檔案傳輸保密性。與此同時，付出的代價就是檔案傳輸時需要輸入密碼而且涉及到 SSH 的一些配置問題，這些都影響其使用的方便性，對於有特定需求的使用者，是比較合適的傳輸工具。

常用樣本

使用 SCP 命令，需要輸入密碼，如果不想每次都輸入，可以通過配置 SSH，這樣在兩台機器間拷貝檔案時不需要每次都輸入使用者名稱和密碼：

產生 RSA 類型的密鑰：

返回樣本

上述命令產生 RSA 類型的密鑰。在提示密鑰的儲存路徑和密碼時，可以直接斷行符號使用預設路徑和空密碼。這樣，產生的公用密鑰儲存/.ssh/id_rsa.pub，私人密鑰儲存在 /.ssh/id_rsa 。然後把這個金鑰組中的公用密鑰的內容複寫到要訪問的機器上的 /.ssh/authorized_keys 檔案中。這樣，下次再訪問那台機器時，就不用輸入密碼了。

在兩台Linux主機間複製檔案

命令基本格式：

```
scp [選擇性參數] file_source file_target
```

從本地複製到遠程（如下四種方式）：

```
scp local_file remote_username@remote_ip:remote_folder
scp local_file remote_username@remote_ip:remote_file
scp local_file remote_ip:remote_folder
scp local_file remote_ip:remote_file
```

> **說明** 第1,2個指定了使用者名稱，命令執行後需要再輸入密碼，第1個僅指定了遠端目錄，檔案名稱字不變，第2個指定了檔案名稱。

第3,4個沒有指定使用者名稱，命令執行後需要輸入使用者名稱和密碼，第3個僅指定了遠端目錄，檔案名稱字不變，第4個指定了檔案名稱。

從遠程複製到本地：

```
scp root@www.cumt.edu.cn:/home/root/others/music /home/space/music/i.mp3
scp -r www.cumt.edu.cn:/home/root/others/ /home/space/music/
```

> **說明** 從遠程複製到本地，只要將從本地複製到遠端命令的後2個參數調換順序即可。

Rsync

Rsync是linux/Unix檔案同步和傳送工具。用於替代rcp的一個工具，rsync可以通過rsh或ssh使用，也能以daemon模式去運行，在以daemon方式運行時rsync server會開一個873連接埠，等待用戶端去串連。串連時rsync server會檢查口令是否相符，若通過口令查核，則可以通過進行檔案傳輸，第一次連通完成時，會把整份檔案傳輸一次，以後則就只需進行增量備份。

安裝方式

> **說明** 可以使用每個發行版本內建的安裝包管理器安裝。

```
sudo apt-get  install  rsync      #在debian、ubuntu 等線上安裝方法;
slackpkg  install  rsync          #Slackware 軟體包線上安裝;
yum install rsync                 #Fedora、Redhat 等系統安裝方法;
```

源碼編譯安裝:

```
wget http://rsync.samba.org/ftp/rsync/src/rsync-3.0.9.tar.gz
tar xf rsync-3.0.9.tar.gz
cd rsync-3.0.9
./configure && make && make install
```

參數介紹:

參數	說明
-v	詳細模式輸出
-a	歸檔模式，表示以遞迴的方式傳輸檔案，並保持所有檔案屬性不變，相當於使用了組合參數-rlptgoD
-r	對子目錄以遞迴模式處理
-l	保留軟連結
-p	保持檔案許可權
-t	保持檔案時間資訊
-g	保持檔案屬組資訊
-o	保持檔案屬主資訊
-D	保持裝置檔案資訊
-H	保留硬鏈結
-S	對疏鬆檔案進行特殊處理以節省DST的空間
-z	對備份的檔案在傳輸時進行壓縮處理

rsync六種不同的工作模式

- 拷貝本地檔案，將/home/coremail目錄下的檔案拷貝到/cmbak目錄下。

  ```
  rsync -avSH /home/coremail/ /cmbak/
  ```

- 拷貝本地機器的內容到遠程機器。

  ```
  rsync -av /home/coremail/ 192.168.11.12:/home/coremail/
  ```

- 拷貝遠程機器的內容到本地機器。

  ```
  rsync -av 192.168.11.11:/home/coremail/ /home/coremail/
  ```

- 拷貝遠程rsync伺服器（daemon形式運行rsync）的檔案到本地機。

```
rsync -av root@172.16.78.192::www /databack
```

- 拷貝本地機器檔案到遠程rsync伺服器（daemon形式運行rsync）中。當DST路徑資訊包含”::”分隔字元時啟動該模式。

```
rsync -av /databack root@172.16.78.192::www
```

- 顯示遠程機的檔案清單。這類似於rsync傳輸，不過只要在命令中省略掉本地機資訊即可。

```
rsync -v rsync://192.168.11.11/data
```

rsync設定檔說明

```
cat/etc/rsyncd.conf                #內容如下
port = 873                         #連接埠號碼
uid = nobody                       #指定當模組傳輸檔案的守護進程UID
gid = nobody                       #指定當模組傳輸檔案的守護進程GID
use chroot = no                    #使用chroot到檔案系統中的目錄中
max connections = 10               #最大並發串連數
strict modes = yes                 #指定是否檢查口令檔案的許可權
pid file = /usr/local/rsyncd/rsyncd.pid       #指定PID檔案
lock file = /usr/local/rsyncd/rsyncd.lock     #指定支援max connection的鎖檔案，預設為/var/run/
rsyncd.lock
motd file = /usr/local/rsyncd/rsyncd.motd     #定義伺服器資訊的，自己寫 rsyncd.motd 檔案內容
log file = /usr/local/rsyncd/rsync.log        #rsync 伺服器的日誌
log format = %t %a %m %f %b
syslog facility = local3
timeout = 300
[conf]                                        #自訂模組
path = /usr/local/nginx/conf                  #用來指定要備份的目錄
comment = Nginx conf
ignore errors                                 #可以忽略一些IO錯誤
read only = no                                #設定no，用戶端可以上傳檔案，yes是唯讀
write only = no                               #no為用戶端可以下載，yes不能下載
hosts allow = 192.168.2.0/24                  #可以串連的IP
hosts deny = *                                #禁止串連的IP
list = false                                  #客戶請求時，使用模組列表
uid = root
gid = root
auth users = backup                           #串連使用者名稱，和linux系統使用者名稱無關係
secrets file = /etc/rsyncd.pass               #驗證密碼檔案
```

4.2. 通過讀寫分離提升資料吞吐效能

一般情況下，對資料庫的讀和寫都在同一個資料庫伺服器中操作時，業務系統效能會降低。為了提升業務系統效能，最佳化使用者體驗，可以通過讀寫分離來減輕主要資料庫的負載。本文分別從應用程式層和系統層來介紹讀寫分離的實現方法。

應用程式層實現方法

應用程式層中直接使用代碼實現，在進入Service之前，使用AOP來做出判斷，是使用寫庫還是讀庫，判斷依據可以根據方法名判斷，比如說以query、find、get等開頭的就走讀庫，其他的走寫庫。

優點：

- 多資料來源切換方便，由程式自動完成。
- 不需要引入中介軟體。
- 理論上支援任何資料庫。

缺點：

- 由程式員完成，營運參與不到。
- 不能做到動態增加資料來源。

系統層實現方法

系統層的實現方法包括以下兩種：

- 使用Distributed Relational Database Service實現讀寫分離。
- 使用中介軟體MySQL-proxy實現讀寫分離。

本教程介紹如何使用中介軟體MySQL-proxy實現讀寫分離。

MySQL proxy

MySQL Proxy是一個處於Client端和MySQL server端之間的簡單程式，它可以監測、分析或改變它們的通訊。它使用靈活，沒有限制，常見的用途包括：Server Load Balancer，故障、查詢分析，查詢過濾和修改等等。

MySQL-proxy原理

MySQL Proxy是一個中介層代理，簡單的說，MySQL Proxy就是一個串連池，負責將前台應用的串連請求轉寄給背景資料庫，並且通過使用lua指令碼，可以實現複雜的串連控制和過濾，從而實現讀寫分離和Server Load Balancer。對於應用來說，MySQL Proxy是完全透明的，應用則只需要串連到MySQL Proxy的監聽連接埠即可。當然，這樣proxy機器可能成為單點失效，但完全可以使用多個proxy機器做為冗餘，在應用伺服器的串連池配置中配置到多個proxy的串連參數即可。

優點：

- 來源程式不需要做任何改動就可以實現讀寫分離。
- 動態添加資料來源不需要重啟程式。

缺點：

- 序依賴於中介軟體，會導致切換資料庫變得困難。
- 由中介軟體做了中轉代理，效能有所下降。

操作步驟

環境說明：

- 主庫IP：121.40.18.26
- 從庫IP：101.37.36.20
- MySQL-proxy代理IP：116.62.101.76

前期準備：

- 1、建立3台ECS，並安裝mysql。
- 2、搭建主從，必須保證主從資料庫資料一致。

主環境

1. 修改mysql設定檔。

```
vim /etc/my.cnf
[mysqld]
server-id=202                    #設定伺服器唯一的id，預設是1
log-bin=mysql-bin                # 啟用二進位日誌
```

從環境

```
[mysqld]
server-id=203
```

2. 重啟主從伺服器中的MySQL服務。

```
/etc/init.d/mysqld restart
```

3. 在主伺服器上建立帳戶並授權slave。

```
mysql -uroot -p95c7586783
grant replication slave on *.* to 'syncms'@'填寫slave-IP' identified by '123456';
flush privileges;
```

4. 查看主要資料庫狀態。

```
mysql> show master status;
```

5. 配置從資料庫。

```
change master to master_host='填寫master-IP', master_user='syncms',      master_password='12
3456', master_log_file='mysql-bin.000005', master_log_pos=602;
```

6. 啟動slave同步進程並查看狀態。

```
start slave;
show slave status\G
```

7. 驗證主從同步。

```
mysql> create database testproxy;
mysql> create table testproxy.test1(ID int primary key,name char(10) not null);
mysql> insert into testproxy.test1 values(1,'one');
mysql> insert into testproxy.test1 values(2,'two');
mysql> select * from testproxy.test1;
```

從庫操作

從庫中尋找testproxy.test1表的資料，與主庫一致，主從同步成功

```
select * from testproxy.test1;
```

讀寫分離配置

1.安裝MySQL-Proxy。

```
wget https://cdn.mysql.com/archives/mysql-proxy/mysql-proxy-0.8.5-linux-glibc2.3-x86-64bit.
tar.gz
mkdir /alidata
tar xvf mysql-proxy-0.8.5-linux-glibc2.3-x86-64bit.tar.gz
mv mysql-proxy-0.8.5-linux-glibc2.3-x86-64bit/  /alidata/mysql-proxy-0.8.5
```

2.環境變數設定。

```
vim /etc/profile                        #加入以下內容
PATH=$PATH:/alidata/mysql-proxy-0.8.5/bin
export $PATH
source /etc/profile                     #使變數立即生效
mysql-proxy -V
```

3.讀寫分離設定。

```
cd /alidata/mysql-proxy-0.8.5/share/doc/mysql-proxy/
vim  rw-splitting.lua
```

MySQL Proxy會檢測用戶端串連, 當串連沒有超過min_idle_connections預設值時, 不會進行讀寫分離預設最小4個(最大8個)以上的用戶端串連才會實現讀寫分離, 現改為最小1個最大2個，便於讀寫分離的測試，生產環境中，可以根據實際情況進行調整。

調整前:

調整後:

4.將lua管理指令碼（admin.lua）複製到讀寫分離指令碼(rw-splitting.lua)所在目錄。

```
cp /alidata/mysql-proxy-0.8.5/lib/mysql-proxy/lua/admin.lua /alidata/mysql-proxy-0.8.5/shar
e/doc/mysql-proxy/
```

授權

1.主庫中操作授權，因主從同步的原因，從庫也會執行。

```
mysql -uroot -p95c7586783
grant all on *.* to 'mysql-proxy'@'填寫MySQL Proxy IP' identified by '123456';
flush privileges;
```

2.開啟MySQL-Proxy。

```
mysql-proxy --daemon --log-level=debug --log-file=/var/log/mysql-proxy.log --plugins=proxy
-b 填寫master-IP:3306 -r 填寫slave-IP:3306 --proxy-lua-script="/alidata/mysql-proxy-0.8.5/sh
are/doc/mysql-proxy/rw-splitting.lua" --plugins=admin --admin-username="admin" --admin-pass
word="admin" --admin-lua-script="/alidata/mysql-proxy-0.8.5/share/doc/mysql-proxy/admin.lua
"
```

3.啟動MySQL-Proxy之後，查看連接埠和相關進程。

```
netstat -tpln
```

```
ps -ef | grep mysql
```

測試讀寫分離

1.關閉從複製

```
stop slave;
```

2.MySQL-Proxy上操作，登入mysql-proxy後台管理。

```
mysql  -u  admin -padmin -P 4041 -h MySQL-Proxy-IP
select * from backends;                #查看狀態
```

第一次串連，會串連到主庫上。

```
mysql -umysql-proxy -p123456 -h 116.62.101.76 -P 4040
insert into testproxy.test1 values(3,'three');                #新增一條資料，由於測試需要，關閉了從
複製，因此該資料在主庫中存在，在從庫中不存在
```

多開幾個串連進行測試，當查詢testproxy.test1表的資料顯示是從庫的資料時，讀寫分離成功。

```
mysql -umysql-proxy -p123456 -h 116.62.101.76 -P 4040
select * from testproxy.test1;
```

4.3. 設定Windows作業系統慣用語言

本文使用公用鏡像中的Windows Server 2016英語版作業系統為例，從Windows更新下載語言資源套件，為一台ECS執行個體重新設定慣用語言。

背景信息

Elastic Compute Service僅提供中文版和英文版的Windows Server公用鏡像。如果您需要使用其他語言版本，如阿拉伯語、德語、俄語或日語等，可以根據本文設定ECS執行個體的慣用語言。本文為德語為示範步驟，適用於Windows Server 2012及其以上的版本作業系統。建立使用德語和德語鍵盤設定的自訂鏡像後，您可以使用該自訂鏡像根據自身需求建立任意數量的執行個體。

操作步驟

1. 串連Windows執行個體。串連方式請參見串連方式導航。
2. 開啟PowerShell模組。
3. 運行以下命令臨時禁用WSUS（Windows Server Update Services）更新源。

```
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU' -Name UseWUServer -Value 0
Restart-Service -Name wuauserv
```

4. 找到控制台，單擊Clock, Language, and Region > Language > Add a language。
5. 在Add languages對話方塊中，選擇一種語言，例如Deutsch (German) > Deutsch (Deutschland)，單擊Add。
6. 選擇語言，例如Deutsch (Deutschland)，單擊Move up更改語言優先順序。
7. 單擊所選語言右側的Options，線上檢查語言更新。
8. 等待執行個體檢查更新，大約三分鐘後更新會提示可供下載，單擊Download and install language pack。
9. 等待安裝完成。
10. 在ECS控制台重新啟動執行個體。
11. 再次串連Windows執行個體。

    顯示語言會在重啟登入後更改為德語。
12. 開啟PowerShell ISE模組，運行以下命令重新啟用WSUS。

```
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU' -Name UseWUServer -Value 1
Restart-Service -Name wuauserv
```

13. 開啟Windows Update，檢查安全更新，重新安裝配置語言設定之前已完成的所有安全更新。

後續步驟

您可以使用相同語言設定建立多台執行個體：

1. 登入 ECS管理主控台 。
2. 根據該Windows執行個體建立自訂鏡像。
3. 通過自訂鏡像建立指定數量的執行個體。

5.Block Storage

5.1. 擴容資料盤_Linux

隨著業務的增長，您的資料盤容量可能無法滿足資料存放區的需要，這時您可以使用 **磁碟擴容** 功能擴容資料盤。

> 說明
>
> - 掛載在執行個體上的資料盤，只有當執行個體處於 **運行中** (Running) 或 **已停止**(Stopped) 狀態時才可以擴容。**擴容這種資料盤需要在控制台上重啟執行個體後才能使擴容後的容量生效，而重啟執行個體會停止執行個體，中斷您的業務，所以請您謹慎操作**。
> - 建議在擴容資料盤之前手動建立快照，以備份資料。
> - 無論資料盤的狀態是 **待掛載** 還是 **使用中**，都可以執行磁碟擴容操作。
> - 訂用帳戶執行個體如果做過 續費降配 操作，當前計費周期的剩餘時間內，執行個體上的訂用帳戶雲端硬碟不支援擴容磁碟操作。
> - 如果資料盤正在建立快照，則不允許執行擴容資料盤的操作。
> - 磁碟擴容功能只能擴容資料盤，不能擴容系統硬碟或本地碟（本地 SSD 盤等）。

本文以一個高效雲端硬碟的資料盤和一個運行CentOS 7.3 64位的 ECS 執行個體為例，說明如何擴容資料盤並使擴容後的容量可用。

您可以按以下步驟完成擴容操作：

步驟 1. 在控制台上擴容資料盤的磁碟空間

步驟 2. 登入執行個體擴容檔案系統

步驟 1. 在控制台上擴容資料盤的磁碟空間

按以下步驟在控制台上擴容資料盤的磁碟空間：

1. 登入 ECS管理主控台。
2. 在左側導覽列裡，選擇 **儲存 > 雲端硬碟** 。

   > 說明　如果您需要擴容的資料盤已經掛載在某個執行個體上，您可以單擊 **執行個體**，找到相應執行個體後，進入執行個體詳情頁，並單擊 **本執行個體磁碟**。

3. 選擇地區。
4. 找到需要擴容的磁碟，並在 **操作** 列中，選擇 **更多 > 磁碟擴容** 。
5. 在 **磁碟擴容** 頁面上，設定 **擴容後容量**，在本樣本中為30 GiB。擴容後容量只能比當前容量大。
6. 待頁面上顯示費用資訊後，單擊 **確定擴容**。

   > 說明　擴容成功後，磁碟列表裡即顯示擴容後的容量。但是，如果您的資料盤已經掛載到執行個體上，只有在控制台上 重啟執行個體 後，登入執行個體才能看到新的磁碟空間容量。

在控制台上擴容資料盤的磁碟空間後，

- 如果資料盤已經掛載到執行個體上，您必須執行 步驟 2. 登入執行個體擴容檔案系統。
- 如果資料盤未掛載到執行個體上，您必須先掛載資料盤（參見 掛載雲端硬碟），再根據資料盤的實際情況執

行不同的操作：

- 如果這是一個未格式化的資料盤，您必須格式化資料盤。詳細資料，請參見 Linux 格式化和掛載資料盤。
- 如果這個資料盤之前已經格式化並分區，您必須 步驟 2. 登入執行個體擴容檔案系統。

步驟 2. 登入執行個體擴容檔案系統

在ECS控制台上完成磁碟擴容後，磁碟每個分區的檔案系統並未擴容。您需要登入執行個體擴容檔案系統。

在本樣本中，假設資料盤掛載在一台Linux執行個體上，執行個體的作業系統為CentOS 7.3 64位，未擴容前的資料盤只有一個主要磁碟分割（/dev/vdb1，ext4檔案系統），檔案系統的掛載點為 */resizetest*，檔案系統擴容完成後，資料盤仍然只有一個主要磁碟分割。

1. 使用使用者名密碼驗證串連 Linux 執行個體。
2. 運行 `umount` 命令卸載主要磁碟分割。

```
umount /dev/vdb1
```

> **說明** 使用 `df -h` 查看是否卸載成功，如果看不到 /dev/vdb1 的資訊表示卸載成功。以下為樣本輸出結果。

```
[root@iXXXXXX ~]# df -h
Filesystem Size Used Avail Use% Mounted on
/dev/vda1 40G 1.5G 36G 4% /
devtmpfs 487M 0 487M 0% /dev
tmpfs 497M 0 497M 0% /dev/shm
tmpfs 497M 312K 496M 1% /run
tmpfs 497M 0 497M 0% /sys/fs/cgroup
tmpfs 100M 0 100M 0% /run/user/0
```

3. 使用 `fdisk` 命令刪除原來的分區並建立新分區：

> **說明** 如果您使用 `parted` 工具操作分區，不能與 `fdisk` 交叉使用，否則會導致分區的起始扇區不一致。關於 `parted` 工具的使用說明可以參考這裡。

   i. 運行命令 `fdisk -l` 羅列分區資訊並記錄擴容前資料盤的最終容量、起始扇區（First sector）位置。
   ii. 運行命令 `fdisk [資料盤裝置名稱]` 進入 `fdisk` 介面。本樣本中，命令為 `fdisk /dev/vdb` 。
   iii. 輸入 `d` 並按斷行符號鍵，刪除原來的分區。

> **說明** 刪除分區不會造成資料盤內資料的丟失。

   iv. 輸入 `n` 並按斷行符號鍵，開始建立新的分區。
   v. 輸入 `p` 並按斷行符號鍵，選擇建立主要磁碟分割。因為建立的是一個單分區資料盤，所以只需要建立主要磁碟分割。

> **說明** 如果要建立4個以上的分區，您應該建立至少一個擴充分區，即選擇 `e` 。

vi. 輸入分區編號並按斷行符號鍵。因為這裡僅建立一個分區，所以輸入 *1*。

vii. 輸入第一個可用的扇區編號：為了保證資料的一致性，First sector需要與原來的分區保持一致。在本樣本中，按斷行符號鍵採用預設值。

> **說明** 如果發現First sector顯示的位置和之前記錄的不一致，說明之前可能使用 `parted` 來分區，那麼就停止當前的 `fdisk` 操作，使用 `parted` 重新操作。

viii. 輸入最後一個扇區編號：因為這裡僅建立一個分區，所以按斷行符號鍵採用預設值。

ix. 輸入 `wq` 並按斷行符號鍵，開始分區。

```
[root@iXXXXXX ~]# fdisk /dev/vdb
Welcome to fdisk (util-linux 2.23.2).
Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.
Command (m for help): d
Selected partition 1
Partition 1 is deleted
Command (m for help): n
Partition type:
p primary (0 primary, 0 extended, 4 free)
e extended
Select (default p):
Using default response p
Partition number (1-4, default 1):
First sector (2048-62914559, default 2048):
Using default value 2048
Last sector, +sectors or +size{K,M,G} (2048-62914559, default 62914559):
Using default value 62914559
Partition 1 of type Linux and of size 30 GiB is set
Command (m for help): wq
The partition table has been altered!
Calling ioctl() to re-read partition table.
Syncing disks.
```

> **說明** 如果您使用的是 `parted` 工具，進入 `parted` 介面後，輸入 `p` 羅列當前的分區情況。如果有分區，則使用 rm+ 序號來刪除老的分區表，然後使用 `unit s` 定義起始位置，單位使用扇區個數計量，最後使用 `mkpart` 命令來建立即可，如下圖所示。
>
> ▫

4. （可選）部分作業系統裡，修改分區後可能會重新自動掛載檔案系統。建議先執行 `df -h` 重新查看檔案系統空間和使用方式。如果檔案系統重新被掛載，執行 `umount [檔案系統名稱]` 再次卸載檔案系統。
5. 檢查檔案系統，並變更檔案系統大小。

```
e2fsck -f /dev/vdb1 # 檢查檔案系統
resize2fs /dev/vdb1 # 變更檔案系統大小
```

> **說明**
> - 使用 `e2fsck` 時，由於系統需要檢查並訂本文件系統元資料，所以速度較慢、耗時較長，請耐心等待。
> - 正確使用 `e2fsck` 和 `resize2fs` 指令，不會造成原有資料丟失。

以下為樣本輸出結果。

```
[root@iXXXXXX ~]# e2fsck -f /dev/vdb1
e2fsck 1.42.9 (28-Dec-2013)
Pass 1: Checking inodes, blocks, and sizes
Pass 2: Checking directory structure
Pass 3: Checking directory connectivity
Pass 4: Checking reference counts
Pass 5: Checking group summary information
/dev/vdb1: 11/1835008 files (0.0% non-contiguous), 159218/7339776 blocks
[root@iXXXXXX ~]# resize2fs /dev/vdb1
resize2fs 1.42.9 (28-Dec-2013)
Resizing the filesystem on /dev/vdb1 to 7864064 (4k) blocks.
The filesystem on /dev/vdb1 is now 7864064 blocks long.
```

6. 將擴容完成的檔案系統掛載到原來的掛載點（如本樣本中的 */resizetest*）。

```
mount /dev/vdb1 /resizetest
```

7. 查看檔案系統空間和使用方式：運行命令 `df -h`。如果出現擴容後的檔案系統資訊，說明掛載成功，可以使用擴容後的檔案系統了。

> **說明** 掛載操作完成後，不需要在控制台上重啟執行個體即可開始使用擴容後的檔案系統。

以下為樣本輸出結果。

```
[root@iXXXXXX ~]# df -h
Filesystem Size Used Avail Use% Mounted on
/dev/vda1 40G 1.5G 36G 4% /
devtmpfs 487M 0 487M 0% /dev
tmpfs 497M 0 497M 0% /dev/shm
tmpfs 497M 312K 496M 1% /run
tmpfs 497M 0 497M 0% /sys/fs/cgroup
tmpfs 100M 0 100M 0% /run/user/0
/dev/vdb1 30G 44M 28G 1% /resizetest
```

5.2. 磁碟縮容

由於目前Elastic Compute Service 不支援系統硬碟或者資料盤縮容，如果您有磁碟縮容的需求，可用通過阿里雲遷雲工具達成目的。

前提條件

在開始本教程前，請確認您已完成以下操作：

- 當磁碟掛載的是 Linux 執行個體時，您需要預先在執行個體內安裝遠端資料同步工具 rsync。
  - CentOS 執行個體：運行 `yum install rsync -y`

- CentOS 執行個體：運行 `yum install rsync -y`
- Ubuntu 執行個體：運行 `apt-get install rsync -y`
- Debian 執行個體：運行 `apt-get install rsync -y`
- 其他發行版：參考發行版官網安裝相關的文檔

- 您需要預先在控制台建立 AccessKey， 用於輸出到設定檔*user_config.json*裡。具體步驟，請參見建立AccessKey。

  > 說明 由於 AccessKey 許可權過大，為防止資料泄露，建議您建立RAM使用者子帳號，並使用RAM 使用者子帳號建立 AccessKey。具體操作，請參見建立 RAM 使用者子帳號和建立 AccessKey。

-
- 其他更多前提條件和限制條件，請參見使用遷雲工具遷移伺服器至阿里雲。

背景信息

遷雲工具的研發初衷是為了平衡阿里雲使用者的雲上及線下業務負載，但是您也可以利用其工作原理，實現Elastic Compute Service的磁碟縮容。

遷雲工具可以根據您的 ECS 執行個體重新建立一份自訂鏡像，在建立過程中通過重新指定磁碟大小，以達到縮容的目的。除了將目標對象換成了 ECS 執行個體之外，磁碟縮容和遷雲這兩種情境的工具的使用方法和使用限制完全一致。由於使用對象為虛擬化的 ECS 執行個體，還可以降低報錯機率，更加高效。

然而，這種縮容方式，會引起原有 ECS 執行個體的部分屬性發生變化，例如，執行個體ID（`InstanceId`）和 公網 IP。如果您的執行個體為Virtual Private Cloud執行個體，可以將公網IP轉換為Elastic IP Address以保留該公網 IP。因此，建議使用Elastic IP Address（EIP）或者對公網 IP 依賴程度較輕的使用者使用該方式縮容。

操作步驟

1. 使用管理員/root 帳號遠端連線到目標 ECS 執行個體。具體步驟，請參見遠端連線。
2. 單擊此處下載阿里雲遷雲工具 ZIP 壓縮包。
3. 解壓遷雲工具ZIP壓縮包，並進入對應作業系統及版本的用戶端檔案目錄找到設定檔 *user_config.json*。
4. 完成配置。詳情請參見步驟2：配置遷移源和遷移目標。

   該設定檔 Linux Shell 顯示效果如下圖所示。

   在磁碟縮容的情境中，您需要重點關注以下參數：

   - system_disk_size：該參數可以置為縮容系統硬碟的預期數值，單位為 GB，該值不能小於系統硬碟實際使用空間大小。
   - data_disks：該參數可以置為縮容資料盤的預期數值，單位為 GB，該值不能小於資料盤實際使用空間大小。

   > 說明
   > - 當 Linux 執行個體內建資料盤時，即使您不考慮縮容資料盤，也需要配置參數*data_disks*。
   > - 當 Windows 執行個體內建資料盤時，如果沒有縮容資料盤的需求，可以不配置參數*data_disks*。

5. 執行用戶端主程式*go2aliyun_client.exe*。

- Windows 執行個體：右擊*go2aliyun_client.exe*，選擇**以管理員身份運行**。
- Linux 執行個體：
  a. 運行 `chmod +x go2aliyun_client` 賦予用戶端可執行許可權。
  b. 運行 `./ go2aliyun_client` 運行用戶端。

6. 等待運行結果。
   - 當出現 `Goto Aliyun Finished!` 提示時，前往ECS 控制台鏡像詳情頁查看經過縮容後的自訂鏡像。如果自訂鏡像已產生，您可以釋放原執行個體，然後使用產生的自訂鏡像建立ECS執行個體，建立完成後，磁碟縮容工作已完成。如何建立，請參見建立 ECS 執行個體。
   - 當出現 `Goto Aliyun Not Finished!` 提示時，檢查同一目錄下*Logs*檔案夾下的記錄檔排查故障，詳情請參見排查故障。

     修複問題後，重新運行遷雲工具即可恢複縮容工作，遷雲工具會從上一次執行的進度中繼續遷雲，無需重頭開始。

相關文檔

- 遷雲工具
- 使用遷雲工具遷移伺服器至阿里雲

6.監控

6.1. 使用CloudMonitor監控ECS執行個體

合理的監控設定能極大減輕雲上業務的營運成本和壓力。設定合理的監控可以讓您即時瞭解系統業務的運行情況，並能協助您提前發現問題，避免可能會出現的業務故障。同時，警示機制能讓您在故障發生後第一時間發現問題，縮短故障處理時間，以便儘快恢複業務。

本文中以一個網站為樣本，介紹如何配置使用CloudMonitor。本樣本中，使用了ECS、RDS、OSS和負載平衡。

前提條件

在開始設定CloudMonitor前，您需要完成以下操作：

- 檢查ECS監控外掛程式運行情況，確保監控資訊能夠正常採集。如果安裝失敗需要手動安裝，請參考CloudMonitor外掛程式安裝指南。
- 提前 添加警示連絡人和聯絡組，建議設定至少2人以上的連絡人，互為主備，以便及時響應監控警示。監控選項的設定，具體可參考 雲端服務資源使用概覽和警示概覽。
- 利用CloudMonitor的Dashboard功能，給您業務系統的雲資源設定一個全域監控總覽，可隨時檢查整個業務系統資源的健康狀態。

  為了更好地監控大屏展示效果，這裡將ECS的CPU、記憶體、磁碟的使用率單獨分組展示；將RDS的四項指標分兩組展示。

設定警示閾值和警示規則

建議您根據實際業務情況設定各項監控指標的警示閾值。閾值太低會頻繁觸發警示，影響監控服務體驗。閾值太高，在觸發閾值後沒有足夠的預留時間來響應和處理警示。

以CPU使用率為例，因為需要給伺服器預留部分處理效能保障伺服器正常運行，所以建議您將CPU警示閾值設定為70%，連續三次超過閾值後開始警示。

如果您還需要設定其他資源的警示規則，單擊 **添加警示規則**，繼續設定記憶體或磁碟的警示規則和警示通知人。樣本：

設定RDS監控

建議將RDS的CPU使用率警示閾值設定為70%，連續三次超過閾值後開始警示。您可以根據實際情況設定硬碟使用率、IOPS使用率、串連數等其他 監控項。

設定負載平衡監控

為了更好使用負載平衡的CloudMonitor服務，您需要先開啟負載平衡的健全狀態檢查，將負載平衡頻寬值的70%作為警示閾值，如下圖所示。

設定進程監控

對於常見的web應用，設定 進程監控，不僅可以即時監控應用進程的運行情況，還有助於排查處理故障，下圖是Java進程的相關監控樣本。具體操作請參考 添加進程監控。

佈建網站監控

在雲端服務器外層的監控服務，網站監控主要用於類比真實使用者訪問情況，即時測試業務可用性，有助於排查處理故障。

如果以上監控選項不能滿足您的實際業務監控需求，您可以使用 自訂監控。

7.藉助於執行個體RAM角色訪問其他雲產品

以往部署在 ECS 執行個體中的應用程式如果需要訪問阿里雲其他雲產品，您通常需要藉助AccessKeyID 和 AccessKeySecret（下文簡稱 AK）來實現。AK 是您訪問阿里雲 API 的密鑰，具有相應帳號的完整許可權。為了方便應用程式對 AK 的管理，您通常需要將 AK 儲存在應用程式的設定檔中或以其他方式儲存在 ECS 執行個體中，這在一定程度上增加了 AK 管理的複雜性，並且降低了 AK 的保密性。甚至，如果您需要實現多地區一致性部署，AK 會隨著鏡像以及使用鏡像建立的執行個體擴散出去。這種情況下，當您需要更換 AK 時，您就需要逐台更新和重新部署執行個體和鏡像。

現在藉助於 ECS 執行個體 RAM 角色，您可以將RAM角色和 ECS 執行個體關聯起來，執行個體內部的應用程式可以通過 STS 臨時憑證訪問其他雲產品。其中 STS 臨時憑證由系統自動產生和更新，應用程式可以使用指定的執行個體中繼資料URL 擷取 STS 臨時憑證，無需特別管理。同時藉助於 RAM，通過對角色和授權策略的管理，您可以達到不同執行個體對不同雲產品或相同雲產品具有各自存取權限的目的。

本文以部署在 ECS 執行個體上的 Python 訪問 OSS 為例，詳細介紹了如何藉助 ECS 執行個體 RAM 角色，使執行個體內部的應用程式可以使用 STS 臨時憑證訪問其他雲產品。

> **說明** 為了方便您隨本文範例快速入門，文檔裡所有操作均在OpenAPI Explorer完成。OpenAPI Explorer 通過已登入使用者資訊擷取當前帳號臨時 AK，對當前帳號發起線上資源操作，請謹慎操作。建立執行個體操作會產生費用。操作完成後請及時釋放執行個體。

操作步驟

為了使 ECS 藉助執行個體 RAM 角色，實現內部 Python 可以使用 STS 臨時憑證訪問 OSS，您需要完成以下步驟：

步驟 1. 建立 RAM 角色並配置授權策略

步驟 2. 指定 RAM 角色建立並設定 ECS 執行個體

步驟 3. 在執行個體內部訪問執行個體中繼資料 URL 擷取 STS 臨時憑證

步驟 4. 基於臨時憑證，使用 Python SDK 訪問 OSS

步驟 1. 建立 RAM 角色並配置授權策略

按以下步驟建立 RAM 角色並配置授權策略。

1. 建立 RAM 角色。找到 OpenAPI Explorer RAM 產品下 CreateRole API。其中：
   - RoleName：設定角色的名稱。根據自己的需要填寫，本樣本中為 *EcsRamRoleTest*。
   - AssumeRolePolicyDocument： 填寫如下內容，表示該角色為一個服務角色，受信雲端服務（本樣本中為 ECS）可以扮演該角色。

```
{
"Statement": [
{
"Action": "sts:AssumeRole",
"Effect": "Allow",
"Principal": {
  "Service": [
    "ecs.aliyuncs.com"
  ]
}
}
],
"Version": "1"
}
```

2. 建立授權策略。找到 OpenAPI Explorer RAM 產品下的 CreatePolicy API。其中：
   - PolicyName：設定授權策略的名稱。本樣本中為 *EcsRamRolePolicyTest*。
   - PolicyDocument：輸入授權策略內容。本樣本中填寫如下內容，表示該角色具有 OSS 唯讀許可權。

```
{
"Statement": [
{
"Action": [
  "oss:Get*",
  "oss:List*"
],
"Effect": "Allow",
"Resource": "*"
}
],
"Version": "1"
}
```

3. 為角色附加授權。找到 OpenAPI Explorer RAM 產品下 AttachPolicyToRole API。其中：
   - PolicyType：填寫 *Custom*。
   - PolicyName：填寫第 2 步建立的策略名稱，如本樣本中的 *EcsRamRolePolicyTest*。
   - RoleName：填寫第 1 步建立的角色名稱，如本樣本中的 *EcsRamRoleTest*。

步驟 2. 為 ECS 執行個體指定 RAM 角色

您可以通過以下任一種方式為 ECS 執行個體指定 RAM 角色：

- 將執行個體 RAM 角色附加到一個已有的 VPC 類型ECS執行個體上
- 指定 RAM 角色建立並設定 ECS 執行個體

將執行個體 RAM 角色附加到一個已有的 VPC 類型ECS執行個體上

您可以使用 ECS 的 AttachInstanceRamRole API 附加執行個體 RAM 角色到已有的 VPC 類型 ECS 執行個體授權訪問，設定資訊如下：

- RegionId：為執行個體所在的地區 ID。

- RamRoleName：RAM 角色的名稱。本樣本中為 *EcsRamRoleTest*。
- InstanceIds：需要附加執行個體 RAM 角色的 VPC 類型 ECS 執行個體 ID。本樣本中為 ["i-bXXXXXXXX"]。

指定 RAM 角色建立並設定 ECS 執行個體

按以下步驟指定 RAM 角色建立並設定 ECS 執行個體。

1. 建立執行個體。找到 OpenAPI Explorer ECS 產品下的 CreateInstance API，根據實際情況填寫請求參數。必須填寫的參數包括：
   - RegionId：執行個體所在地區。本樣本中為 *cn-hangzhou*。
   - ImageId：執行個體的鏡像。本樣本中為 *centos_7_03_64_40G_alibase_20170503.vhd*。
   - InstanceType：執行個體的規格。本樣本中為 *ecs.xn4.small*。
   - VSwitchId：執行個體所在的 VPC 虛擬交換器。因為 ECS 執行個體 RAM 角色目前只支援 VPC 類型 ECS 執行個體，所以 VSwitchId 是必需的。
   - RamRoleName：RAM 角色的名稱。本樣本中為 *EcsRamRoleTest*。

   如果您希望授權子帳號建立指定 RAM 角色的 ECS 執行個體，那麼子帳號除了擁有建立 ECS 執行個體的許可權之外，還需要增加 PassRole 許可權。所以，您需要建立一個如下所示的自訂授權策略並綁定到子帳號上。如果是建立 ECS 執行個體，[ECS RAM Action] 可以是 `ecs:CreateInstance`，您也可以根據實際情況添加更多的許可權。如果您需要為子帳號授予所有 ECS 操作許可權，[ECS RAM Action] 應該替換為 `ecs:*`。

   ```
   {
   "Statement": [
   {
   "Action": "[ECS RAM Action]",
   "Resource": "*",
   "Effect": "Allow"
   },
   {
   "Action": "ram:PassRole",
   "Resource": "*",
   "Effect": "Allow"
   ],
   "Version": "1"
   }
   ```

2. 設定密碼並啟動執行個體。
3. 使用 API 或在控制台設定 ECS 執行個體能訪問公網。

步驟 3. 在執行個體內部訪問執行個體中繼資料 URL 擷取 STS 臨時憑證

按以下步驟擷取執行個體的 STS 臨時憑證。

> **說明** STS 臨時憑證失效前半小時會產生新的 STS 臨時憑證，在這半小時內，新舊 STS 臨時憑證均可使用。

1. 遠端連線執行個體。
2. 訪問 `http://100.100.100.200/latest/meta-data/ram/security-credentials/EcsRamRoleTest` 擷取 STS 臨時憑證。路徑最後一部分是 RAM 角色名稱，您應替換為自己的建立的 RAM 角色名稱。

> **說明** 本樣本中使用 `curl` 命令訪問上述 URL。如果您使用的是 Windows ECS 執行個體，請參見執行個體中繼資料。

樣本輸出結果如下。

```
[root@local ~]# curl http://100.100.100.200/latest/meta-data/ram/security-credentials/EcsRamRoleTest
{
"AccessKeyId" : "STS.J8XXXXXXXXX4",
"AccessKeySecret" : "9PjfXXXXXXXXBf2XAW",
"Expiration" : "2017-06-09T09:17:19Z",
"SecurityToken" : "CAIXXXXXXXXXXwmBkleCTkyI+",
"LastUpdated" : "2017-06-09T03:17:18Z",
"Code" : "Success"
}cess"
}
```

步驟 4. 基於臨時憑證，使用 Python SDK 訪問 OSS

本樣本中，我們基於 STS 臨時憑證使用 Python SDK 列舉執行個體所在地區的某個 OSS 儲存空間（Bucket）裡的 10 個檔案。

前提條件

您已經遠端連線到 ECS 執行個體。

您的 ECS 執行個體已經安裝了 Python。如果您用的是 Linux ECS 執行個體，必須安裝 pip。

您在執行個體所在的地區已經建立了儲存空間（Bucket），並已經擷取 Bucket 的名稱和 Endpoint。本樣本中，Bucket 名稱為 `ramroletest`，Endpoint 為 `oss-cn-hangzhou.aliyuncs.com`。

操作步驟

按以下步驟使用 Python SDK 訪問 OSS。

1. 運行命令 `pip install oss2`，安裝 OSS Python SDK。
2. 執行下述命令進行測試，其中：
   - `oss2.StsAuth` 中的 3 個參數分別對應於上述 URL 返回的 AccessKeyId、AccessKeySecret 和 SecurityToken。
   - `oss2.Bucket` 中後 2 個參數是 Bucket 的名稱和 Endpoint。

```
import oss2
from itertools import islice
auth = oss2.StsAuth(<AccessKeyId>, <AccessKeySecret>, <SecurityToken>)
bucket = oss2.Bucket(auth, <您的 Endpoint>, <您的 Bucket 名稱>)
for b in islice(oss2.ObjectIterator(bucket), 10):
  print(b.key).key)
```

樣本輸出結果如下。

```
[root@local ~]# python
Python 2.7.5 (default, Nov  6 2016, 00:28:07)
[GCC 4.8.5 20150623 (Red Hat 4.8.5-11)] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import oss2
>>> from itertools import islice
>>> auth = oss2.StsAuth("STS.J8XXXXXXXXX4", "9PjfXXXXXXXXXBf2XAW", "CAIXXXXXXXXXXXwmBk
leCTkyI+")
>>> bucket = oss2.Bucket(auth, "oss-cn-hangzhou.aliyuncs.com", "ramroletest")
>>> for b in islice(oss2.ObjectIterator(bucket), 10):
...     print(b.key)
...
ramroletest.txt
test.shh
```

8.災備方案

保障企業業務穩定、IT系統功能正常、資料安全十分重要，可以同時保障資料備份與系統、應用容災的災備解決方案應勢而生，且發展迅速。ECS可使用快照、鏡像進行備份。

災備設計

- **快照備份**

  阿里雲ECS可使用快照進行系統硬碟、資料盤的備份。目前，阿里雲提供快照2.0服務，提供了更高的快照額度、更靈活的自動任務策略，並進一步降低了對業務I/O的影響。快照備份實行增量原理，第一次備份為全量備份，後續為增量備份。增量快照具有快速建立以及儲存容量小的優點。備份所需時間與待備份的增量資料體積有關。

  > **說明** 快照建立遵循增量原理，為了提高您的備份速度，建議您在建立完畢新快照後，再刪除最新的曆史快照。

  例如，快照1、快照2和快照3分別是磁碟的第一份、第二份和第三份快照。檔案系統對磁碟的資料進行分塊檢查，當建立快照時，只有變化了的資料區塊，才會被複製到快照中。阿里雲ECS的快照備份可配置為手動備份，也可配置為自動備份。配置為自動備份後可以指定磁碟自動建立快照的時間（24個整點）、重複日期（周一到周日）和保留時間（可自訂，範圍是1-65536天，或選擇持續保留）。

- **快照復原**

  當系統出現問題，需要將一塊磁碟的資料復原到之前的某一時刻，可以通過快照復原實現，前提是該磁碟已經建立了快照。注意：

  - 復原磁碟是無法復原操作，一旦復原完成，原有的資料將無法恢複，請謹慎操作。
  - 復原磁碟後，從所使用的快照的建立日期到目前時間這段時間內的資料都會丟失。

- **鏡像備份**

  鏡像檔案相當於副本檔案，該副本檔案包含了一塊或多塊磁碟中的所有資料，對於ECS而言，這些磁碟可以是單個系統硬碟，也可以是系統硬碟加資料盤的組合。使用鏡像備份時，均是全量備份，且只能手動觸發。

- **鏡像恢複**

  阿里雲ECS支援使用快照建立自訂鏡像，將快照的作業系統、資料環境資訊完整的包含在鏡像中。然後使用自訂鏡像建立多台具有相同作業系統和資料環境資訊的執行個體。ECS的快照與鏡像配置請參考快照與鏡像。

  > **說明** 建立的自訂鏡像不能跨地區使用。

技術指標

RTO和RPO：與資料量大小有關，通常而言是小時層級。

應用情境

- **備份恢複**

阿里雲ECS可通過快照與鏡像對系統硬碟、資料盤進行備份。如果儲存在磁碟上的資料本身就是錯誤的資料，比如由於應用錯誤導致的資料錯誤，或者駭客利用應用漏洞進行惡意讀寫，此時就可以使用快照服務將磁碟上的資料恢複到期望的狀態。另外ECS可通過鏡像重新初始化磁碟或使用自訂鏡像新購ECS執行個體。

- **容災應用**

  ECS可以從架構上實現容災情境下的應用。例如，在應用前端購買SLB產品，後端相同應用部署至少兩台ECS伺服器，或者是使用阿里雲的彈性伸縮技術，根據自訂ECS自身資源的使用規則進行彈性擴容。這樣即便其中一台ECS伺服器故障或者資源利用超負荷，也不會使服務對外終止，從而實現容災情境下的應用。下圖以同城兩可用性區域機房部署ECS叢集為例，所有通訊均在阿里雲千兆內網中完成，響應快速並減少了公網流量費用：

  - Server Load Balancer：裝置側通過多可用性區域層級SLB做首層流量接入，使用者流量被分發至兩個及以上的可用性區域機房，機房內均部署ECS叢集。
  - ECS叢集：可用性區域機房部署的ECS節點是對等的，單節點故障不影響資料層應用和伺服器管控功能。發生故障後系統會自動熱遷移，另外的ECS節點可以持續提供業務訪問，防止可能的單點故障或者熱遷移失敗導致的業務訪問中斷。熱遷移失敗後通過系統事件獲知故障資訊，您可以及時部署新節點。
  - 資料層：在地區層級部署Object Storage Service，不同可用性區域機房的ECS節點可以直接讀取檔案資訊。若是資料庫應用，使用多可用性區域ApsaraDB for RDS服務做承載，主節點支援多可用性區域讀寫，與應用程式層流量來源無衝突關係。同時，備節點支援多可用性區域讀能力，防止主節點故障時，ECS無法讀取資料。