Alibaba Cloud
云服务器 ECS

安全

檔案版本：20191107

目錄

1 安全性群組

1.1 安全性群組

安全性群組是一個邏輯上的分組，這個分組是由同一個地域（Region）內具有相同安全保護需求並相互信任的執行個體組成。每個執行個體至少屬於一個安全性群組，在建立的時候就需要指定。同一安全性群組內的執行個體之間預設私網網路互通，不同安全性群組的執行個體之間預設私網不通。可以授權兩個安全性群組之間互訪。

安全性群組是一種虛擬防火牆，具備狀態檢測包過濾功能。安全性群組用於設定單台或多台雲伺服器的網路存取控制，它是重要的網路安全隔離手段，用於在雲端劃分安全域。

安全性群組限制

- 每個使用者在每個地域最少可建立100個安全性群組，並可以根據使用者會員等級的提高而增加。如需提高上限，可以提交工單
- 一個執行個體中的每個彈性網卡都預設最多可以加入5個安全性群組。如需提高上限，可以提交工單，增加到10個或者16個安全性群組。
- 安全性群組的網路類型分為經典網路和專有網路。
  - 經典網路類型的執行個體可以加入同一地域（Region）下經典網路類型的安全性群組。

    單個經典網路類型的安全性群組內的執行個體個數不能超過1000。如果您有超過1000個執行個體需要內網互訪，可以將他們分配到多個安全性群組內，並通過互相授權的方式允許互訪。
  - 專有網路類型的執行個體可以加入同一專有網路（VPC）下的安全性群組。

    單個VPC類型的安全性群組內的私網IP個數不能超過2000（主網卡和輔助網卡共用此配額）。如果您有超過2000個私網IP需要內網互訪，可以將這些私網IP的執行個體分配到多個安全性群組內，並通過互相授權的方式允許互訪。
- 安全性群組是有狀態的。如果資料包在Outbound方向是被允許的，那麼對應的此串連在Inbound方向也是允許的。

更多資訊，請參見安全性群組 *FAQ*。

安全性群組規則

安全性群組規則可以允許或者禁止與安全性群組相關聯的Elastic Compute Service執行個體的公網和內網的入出方向的訪問。

您可以隨時授權和取消安全性群組規則。您的變更安全性群組規則會自動應用於與安全性群組相關聯的ECS執行個體上。

在設定安全性群組規則的時候，安全性群組的規則務必簡潔。如果您給一個執行個體分配多個安全性群組，則該執行個體可能會應用多達數百條規則。訪問該執行個體時，可能會出現網路不通的問題。

安全性群組規則限制

- 每個安全性群組最多有100條安全性群組規則，即每個安全性群組的入方向規則與出方向規則的總數不能超過100。
- 一個執行個體中的每個彈性網卡最多可以設定500條安全性群組規則。

1.2 應用案例

本文介紹了幾個常見的安全性群組應用案例，同時包括Virtual Private Cloud和傳統網路 的安全性群組設定說明。

> 說明:
>
> - 建立安全性群組和添加安全性群組規則的詳細操作，請參見 建立安全性群組 和 添加安全性群組規則。
> - 常用連接埠，請參見 *ECS* 執行個體常用連接埠介紹。
> - 常用連接埠的安全性群組規則配置，請參見 *#unique_7*。

- 案例 1：實現內網互連

  情境舉例：傳統網路裡，如果需要在同一個地區內不同帳號或不同安全性群組的ECS執行個體之間拷貝資源，您可以通過安全性群組設定實現兩台ECS執行個體內網互連後再拷貝。

- 案例 2：屏蔽、攔截、阻斷特定*IP*地址對執行個體或執行個體特定連接埠的訪問

  情境舉例：如果您的ECS執行個體因為異常的IP地址登入引發安全問題或者造成記憶體溢出、頻寬跑滿、CPU跑滿等問題，您可以通過安全性群組設定攔截這些異常IP地址。

- 案例 3：只允許特定*IP*地址遠程登入到執行個體

  情境舉例：如果您的ECS執行個體被肉雞，您可以修改遠程登入連接埠號碼，並設定只允許特定的IP地址遠程登入到您的ECS執行個體。

- 案例 4：只允許執行個體訪問外部特定*IP*地址

  情境舉例：如果您的ECS執行個體被肉雞，對外惡意掃描或發包，您可以通過安全性群組設定您的ECS執行個體只能訪問外部特定IP或連接埠。

- **案例 5：允許遠端連線執行個體**

  情境舉例：您可以通過公網或內網遠端連線到執行個體上，管理執行個體。

- **案例 6：允許公網通過HTTP、HTTPS等服務訪問執行個體**

  情境舉例：您在執行個體上架設了一個網站，希望您的使用者能通過HTTP或HTTPS服務訪問到您的網站。

案例 1：實現內網互連

使用安全性群組實現相同地區不同帳號下或不同安全性群組內ECS執行個體間的內網互連。有兩種情況：

- **情境 1：執行個體屬於同一個地區、同一個帳號**
- **情境 2：執行個體屬於同一個地區、不同帳號**

> **說明:**
>
> **對於VPC網路類型的ECS執行個體，如果它們在同一個VPC網路內，可以通過安全性群組規則實現內網互連。如果ECS執行個體不在同一個VPC內（無論是否屬於同一個帳號或在同一個地區裡），您可以使用*Express Connect*實現*VPC*互連。**

情境 1：同一地區、同一帳號

- **VPC：處於同一個VPC內的ECS執行個體，在執行個體所在安全性群組中分別添加一條安全性群組規則，授權另一個安全性群組內的執行個體訪問本安全性群組內的執行個體，實現內網互連。安全性群組規則如下表所示。**

網卡類型	規則方向	授權策略	協議類型	連接埠範圍	優先順序	授與類型	授權對象
不需要設定	入方向	允許	設定適用的協議類型	設定連接埠範圍	1	安全性群組訪問（本帳號授權）	選擇允許訪問的執行個體所在的安全性群組ID

- **傳統網路：在執行個體所在安全性群組中分別添加一條安全性群組規則，授權另一個安全性群組內的執行個體訪問本安全性群組內的執行個體，實現內網互連。安全性群組規則如下表所示。**

網路類型	網卡類型	規則方向	授權策略	協議類型	連接埠範圍	優先順序	授與類型	授權對象

傳統網路	內網	入方向	允許	設定適用的協議類型	設定連接埠範圍	1	安全性群組訪問（本帳號授權）	選擇允許訪問的執行個體所在的安全性群組ID

同一地區、同一帳號的2個執行個體，如果在同一個安全性群組內，預設內網互連，不需要設定。

如果在不同的安全性群組內，預設內網不通，此時，根據網路類型做不同的設定：

情境 2：同一地區、不同帳號

這部分的描述僅適用於傳統網路類型的ECS執行個體。

同一個地區內、不同帳號下，傳統網路執行個體可以通過安全性群組授權實現內網互連。比如：

- UserA在華東1有一台傳統網路的ECS執行個體InstanceA（內網IP：A.A.A.A），InstanceA所屬的安全性群組為GroupA。
- UserB在華東1有一台傳統網路的ECS執行個體InstanceB（內網IP：B.B.B.B），InstanceB所屬的安全性群組為GroupB。
- 在GroupA中添加安全性群組規則，授權InstanceB內網訪問InstanceA，如下表所示。

網卡類型	規則方向	授權策略	協議類型	連接埠範圍	授與類型	授權對象	優先順序
內網	入方向	允許	選擇適用的協議類型	設定連接埠範圍	安全性群組訪問（跨帳號授權）	GroupB的ID，並在 帳號 ID 裡填寫UserB的ID	1

- 在GroupB中添加安全性群組規則，授權InstanceA內網訪問InstanceB，如下表所示。

網卡類型	規則方向	授權策略	協議類型	連接埠範圍	授與類型	授權對象	優先順序
內網	入方向	允許	選擇適用的協議類型	設定連接埠範圍	安全性群組訪問（跨帳號授權）	GroupA的ID，並在 帳號 ID 裡填寫UserA的ID	1

说明:

出於安全性考慮，傳統網路的內網入方向規則，授與類型優先選擇 安全性群組訪問；如果選擇位址區段訪問，則僅支援單IP授權，授權對象的格式只能是a.b.c.d/32，其中IP地址應根據您的實際需求設定，僅支援IPv4，子網路遮罩必須是/32。

案例 2：屏蔽、攔截、阻斷特定IP地址對執行個體或執行個體特定連接埠的訪問

如果需要使用安全性群組屏蔽、攔截、阻止特定IP地址對您的ECS執行個體的訪問，或者屏蔽特定IP地址訪問ECS執行個體的特定連接埠（如本例中的TCP 22連接埠），您可以參考以下樣本設定安全性群組規則：

- **如果要拒絕特定公網IP位址區段對ECS所有連接埠的訪問，添加如下表所示的安全性群組規則：**

網路類型	網卡類型	規則方向	授權策略	協議類型	連接埠範圍	授與類型	授權對象	優先順序
VPC	不需要設定	入方向	拒絕	全部	-1/-1	位址區段訪問	待屏蔽的IP位址區段，採用CIDR格式，如a.b.c.d/27。	1
傳統網路	公網							

- **如果要拒絕特定IP位址區段對ECS特定連接埠（如TCP 22連接埠）的訪問，添加如下安全性群組規則：**

網路類型	網卡類型	規則方向	授權策略	協議類型	連接埠範圍	授與類型	授權對象	優先順序
VPC	不需要設定	入方向	拒絕	SSH(22)	22/22	位址區段訪問	待屏蔽的IP位址區段，採用CIDR格式，如a.b.c.d/27。	1
傳統網路	公網							

案例 3：只允許特定IP地址遠程登入到執行個體

如果您只想讓某些特定IP地址遠程登入到執行個體，可以參考以下樣本的步驟在執行個體所在安全性群組裡添加以下2條規則（以Linux執行個體為例，設定只讓特定IP地址訪問TCP 22連接埠）：

1. **允許特定IP地址訪問TCP 22連接埠，優先順序為1，優先順序最高，最先執行。安全性群組規則如下表所示。**

網路類型	網卡類型	規則方向	授權策略	協議類型	連接埠範圍	授與類型	授權對象	優先順序

VPC	不需要配置	入方向	允許	SSH(22)	22/22	位址區段訪問	允許遠端連線的IP地址，如1.2.3.4。	1
傳統網路	公網							

2. 拒絕其他IP地址訪問TCP 22連接埠，優先順序為2，低於優先順序為1的規則。安全性群組規則如下表所示。

網路類型	網卡類型	規則方向	授權策略	協議類型	連接埠範圍	授與類型	授權對象	優先順序
VPC	不需要配置	入方向	拒絕	SSH(22)	22/22	位址區段訪問	0.0.0.0/0	2
傳統網路	公網							

完成設定後：

- 使用IP地址為 1.2.3.4 的機器遠端連線Linux執行個體時，串連成功。
- 其他IP地址的機器遠端連線Linux執行個體時，串連失敗。

案例 4：只允許執行個體訪問外部特定IP地址

如果您只想讓執行個體訪問特定的IP地址，參考以下樣本的步驟在執行個體所在安全性群組中添加安全性群組規則：

1. 禁止執行個體以任何協議訪問所有公網IP地址，優先順序應低於允許訪問的規則（如本例中設定優先權為2）。安全性群組規則如下表所示。

網路類型	網卡類型	規則方向	授權策略	協議類型	連接埠範圍	授與類型	授權對象	優先順序
VPC	不需要配置	出方向	拒絕	全部	-1/-1	位址區段訪問	0.0.0.0/0	2
傳統網路	公網							

2. 允許執行個體訪問特定公網IP地址，優先順序應高於拒絕訪問的安全性群組規則的優先順序（如本例中設定為1）

網路類型	網卡類型	規則方向	授權策略	協議類型	連接埠範圍	授與類型	授權對象	優先順序

VPC	不需要配置	出方向	允許	選擇適用的協議類型	設定連接埠範圍	位址區段訪問	允許執行個體訪問的特定公網IP地址，如1.2.3.4。	1
傳統網路	公網							

添加了安全性群組規則後，在串連執行個體，執行 `ping`、`telnet` 等測試。如果執行個體只能訪問允許訪問的IP地址，說明安全性群組規則已經生效。

案例 5：允許遠端連線執行個體

允許遠端連線ECS執行個體分為兩種情況：

- 情境 1：允許公網遠端連線指定執行個體
- 情境 2：允許內網其他帳號下的某台ECS執行個體或所有ECS執行個體遠端連線指定執行個體

情境 1：允許公網遠端連線執行個體

如果要允許公網遠端連線執行個體，參考以下樣本添加安全性群組規則。

- VPC：添加如下所示安全性群組規則。

網路類型	網卡類型	規則方向	授權策略	協議類型	連接埠範圍	授與類型	授權對象	優先順序
VPC	不需要設定	入方向	允許	Windows：RDP(3389)	3389/3389	位址區段訪問	如果允許任意公網IP地址串連執行個體，填寫0.0.0.0/0。如果只允許特定IP地址遠端連線執行個體，參見案例 3：只允許特定IP地址遠程登入到執行個體。	1
				Linux：SSH(22)	22/22			
				自訂TCP	自訂			

- 傳統網路：添加如下表所示安全性群組規則。

網路類型	網卡類型	規則方向	授權策略	協議類型	連接埠範圍	授與類型	授權對象	優先順序
傳統網路	公網	入方向	允許	Windows：RDP(3389)	3389/3389	位址區段訪問	如果允許任意公網IP地址串連執行個體，填寫0.0.0.0/0。如果只允許特定公網IP地址串連執行個體，參見 案例 3：只允許特定 IP 地址遠程登入到執行個體。	1
				Linux：SSH(22)	22/22			
				自訂TCP	自訂			

自訂遠端連線連接埠的詳細操作，請參見 伺服器預設遠程連接埠修改。

情境 2：允許內網其他帳號下某個安全性群組內的ECS執行個體遠端連線您的執行個體

如果您的帳號與同地區其他帳號內網互連，而且您想允許內網其他帳號下某個安全性群組內的ECS執行個體遠端連線執行個體，按以下樣本添加安全性群組規則。

- 允許內網其他帳號某個執行個體內網IP地址串連您的執行個體
  - VPC：先保證2個帳號的執行個體 *#unique_8*，再添加如下表所示的安全性群組規則。

網路類型	網卡類型	規則方向	授權策略	協議類型	連接埠範圍	授與類型	授權對象	優先順序
VPC	不需要設定	入方向	允許	Windows：RDP(3389)	3389/3389	位址區段訪問	對方執行個體的私人IP地址	1
				Linux：SSH(22)	22/22			

				自訂 TCP	自訂			

- 傳統網路：應添加如下表所示的安全性群組規則。

網路類型	網卡類型	規則方向	授權策略	協議類型	連接埠範圍	授與類型	授權對象	優先順序
傳統網路	內網	入方向	允許	Windows：RDP(3389)	3389/3389	位址區段訪問	對方執行個體的內網IP地址，出於安全性考慮，僅支援單IP授權，例如：a.b.c.d/32。	1
				Linux：SSH(22)	22/22			
				自訂 TCP	自訂			

· 允許內網其他帳號某個安全性群組裡的所有ECS執行個體串連您的執行個體

- VPC類型的執行個體，先保證2個帳號的執行個體 *#unique_8*，再添加如下表所示的安全性群組規則。

網路類型	網卡類型	規則方向	授權策略	協議類型	連接埠範圍	授與類型	授權對象	優先順序
VPC	不需要設定	入方向	允許	Windows：RDP(3389)	3389/3389	安全性群組訪問（跨帳號授權）	對方ECS執行個體所屬的安全性群組ID，並填寫對方帳號ID	1
				Linux：SSH(22)	22/22			
				自訂 TCP	自訂			

- 傳統網路執行個體，添加如下表所示的安全性群組規則。

網路類型	網卡類型	規則方向	授權策略	協議類型	連接埠範圍	授與類型	授權對象	優先順序

傳統網路	內網	入方向	允許	Windows：RDP(3389)	3389/3389	安全性群組訪問（跨帳號授權）	對方ECS執行個體所屬的安全性群組ID，並填寫對方帳號ID	1
				Linux：SSH(22)	22/22			
				自訂TCP	自訂			

案例 6：允許公網通過HTTP、HTTPS等服務訪問執行個體

如果您在執行個體上架設了一個網站，希望您的使用者能通過HTTP或HTTPS服務訪問到您的網站，您需要在執行個體所在安全性群組中添加以下安全性群組規則。

- VPC：假設允許公網上所有IP地址訪問您的網站，添加如下表所示的安全性群組規則。

網路類型	網卡類型	規則方向	授權策略	協議類型	連接埠範圍	授與類型	授權對象	優先順序
VPC	不需要配置	入方向	允許	HTTP(80)	80/80	位址區段訪問	0.0.0.0/0	1
				HTTPS(443)	443/443			
				自訂TCP	自訂，如8080/8080			

- 傳統網路：假設允許公網上所有IP地址訪問您的網站，添加如下表所示的安全性群組規則。

網路類型	網卡類型	規則方向	授權策略	協議類型	連接埠範圍	授與類型	授權對象	優先順序
傳統網路	公網	入方向	允許	HTTP(80)	80/80	位址區段訪問	0.0.0.0/0	1
				HTTPS(443)	443/443			
				自訂TCP	自訂，如8080/8080			

说明:

- 如果您無法通過`http://公網 IP`位址訪問您的執行個體，請參見檢查*TCP 80*連接埠是否正常工作。

1.3 ECS 執行個體常用連接埠介紹

以下為 ECS 執行個體常用連接埠列表：

連接埠	服務	說明
21	FTP	FTP 服務所開放的連接埠，用於上傳、下載檔案。
22	SSH	SSH 連接埠，用於通過命令列模式 *#unique_9*。
23	Telnet	Telnet 連接埠，用於 Telnet 遠程登入 ECS 執行個體。
25	SMTP	SMTP 服務所開放的連接埠，用於發送郵件。 基於安全考慮，ECS 執行個體 25 連接埠預設受限，如需解鎖，請參閱 *TCP 25* **連接埠控制台解鎖申請**。
80	HTTP	用於 HTTP 服務提供訪問功能，例如，IIS、Apache、Nginx 等服務。 您可以參閱 **檢查** *TCP 80* **連接埠是否正常工作** 排查 80 連接埠故障。
110	POP3	用於 POP3 協議，POP3 是電子郵件收發的協議。
143	IMAP	用於 IMAP（Internet Message Access Protocol）協議，IMAP 是用於電子郵件的接收的協議。
443	HTTPS	用於 HTTPS 服務提供訪問功能。HTTPS 是一種能提供加密和通過安全連接埠傳輸的一種協議。
1433	SQL Server	SQL Server 的 TCP 通訊埠，用於供 SQL Server 對外提供服務。

1434	SQL Server	SQL Server 的 UDP 連接埠，用於返回 SQL Server 使用了哪個 TCP/IP 連接埠。
1521	Oracle	Oracle 通訊連接埠，ECS 執行個體上部署了 Oracle SQL 需要允許存取的連接埠。
3306	MySQL	MySQL 資料庫對外提供服務的連接埠。
3389	Windows Server Remote Desktop Services	Windows Server Remote Desktop Services（遠端桌面服務）連接埠，可以通過這個連接埠 *#unique_10*。
8080	代理連接埠	同 80 連接埠一樣，8080 連接埠常用於 WWW 代理服務，實現網頁瀏覽。如果您使用了 8080 連接埠，訪問網站或使用Proxy 伺服器時，需要在 IP 位址後面加上 `:8080`。安裝 Apache Tomcat 服務後，預設服務連接埠為 8080。
137、138、139	NetBIOS 協議	· 137、138 為 UDP 連接埠，通過網路位置傳輸檔案時使用的連接埠。 · 139 通過這個連接埠進入的串連試圖獲得 NetBIOS/SMB 服務。 NetBIOS 協議常被用於 Windows 檔案、印表機共用和 Samba。

無法訪問某些連接埠

現象：ECS 執行個體監聽了對應連接埠，但這個連接埠在部分地區無法訪問，而其它連接埠訪問正常的情況。

分析：部分電訊廠商判斷連接埠 135、139、444、445、5800、5900 等為高危連接埠，預設被屏蔽。

解決：建議您修改敏感連接埠為其它非高危連接埠承載業務。

參考連結

- 更多關於 Windows 執行個體服務連接埠說明，請參閱微軟文檔 *Windows* 伺服器系統的服務概述和網路連接埠要求。
- 如何通過安全性群組允許存取服務連接埠，請參閱 添加安全性群組規則。

1.4 建立安全性群組

一台ECS執行個體必須至少屬於一個安全性群組。更多資訊，請參見 安全性群組。

如果您未建立安全性群組即開始建立ECS執行個體，可以選擇使用我們自動為您建立的安全性群組。詳細資料，請參見 *#unique_11*。

您也可以根據業務需要建立一個安全性群組，並將執行個體移入安全性群組。本文描述如何建立安全性群組。

前提條件

如果您要建立VPC型別安全組，必須先 *#unique_12*。

> **說明:**
> VPC裡的安全性群組，可以跨交換器，但是不能跨VPC。

操作步驟

1. 登入 *ECS*管理主控台。
2. 在左側導覽列中，選擇 網路和安全 > 安全性群組。
3. 選擇地區。
4. 單擊 建立安全性群組。
5. 在彈出的 建立安全性群組 對話方塊中，完成以下配置：
   - 模板：根據安全性群組中執行個體上需要部署的服務，選擇合適的模板，簡化安全性群組規則配置，如下表所示。

情境	模板	說明
安全性群組中的Linux執行個體上需要部署Web服務	Web Server Linux	預設允許存取TCP 80、TCP 443、TCP 22和ICMP協議入方向訪問
安全性群組中的Windows執行個體上需要部署Web服務	Web Server Windows	預設允許存取TCP 80、TCP 443、TCP 3389和ICMP協議入方向訪問

沒有特殊的需求	自訂	安全性群組建立成功後，根據需要的服務 添加安全性群組規則

- 安全性群組名稱：按頁面提示要求設定安全性群組名稱。
- 描述：簡短地描述安全性群組，方便後期管理。
- 網路類型：
  - 如果為VPC型別安全組，選擇 專用網路，並選擇已經建立的專用網路。
  - 如果為傳統網路型別安全組，選擇 傳統網路。

6. 單擊 確定。

對於您自己建立的安全性群組，在沒有添加任何安全性群組規則之前，私網和公網預設規則均為：出方向允許所有訪問，入方向拒絕所有訪問。

後續操作

建立好安全性群組後，您必須 添加安全性群組規則。

您也可以根據業務需要，加入、移出安全性群組。

相關API

#unique_14

1.5 添加安全性群組規則

您可以添加安全性群組規則，允許或禁止安全性群組內的ECS執行個體對公網或私網的訪問：

- VPC網路：只需要設定出方向或入方向的規則，不區分內網和公網。Virtual Private Cloud執行個體的公網訪問通過私網網卡映射完成，所以，您在執行個體內部看不到公網網卡，在安全性群組裡也只能設定內網規則。您設定的安全性群組規則同時對內網和公網生效。
- 傳統網路：需要分別設定公網或內網的出方向或入方向規則。

安全性群組規則的變更會自動應用到安全性群組內的ECS執行個體上。

前提條件

您已經建立了一個安全性群組，具體操作，請參見 建立安全性群組。

您已經知道自己的執行個體需要允許或禁止哪些公網或內網的訪問。

操作步驟

1. 登入 *Elastic Compute Service*管理主控台。

2. 在左側導覽列中，選擇 網路和安全 > 安全性群組。
3. 選擇地區。
4. 找到要配置授權規則的安全性群組，在 操作 列中，單擊 配置規則。
5. 在 安全性群組規則 頁面上，單擊 添加安全性群組規則。

> 说明:
> - 如果您不需要設定ICMP、GRE協議規則，或者您想使用下表中列出的協議的預設連接埠，單擊 快速建立規則。
> - 每個安全性群組的入方向規則與出方向規則的總數不能超過100條。

協議	SSH	telnet	HTTP	HTTPS	MS SQL
連接埠	22	23	80	443	1433
協議	Oracle	MySQL	RDP	PostgreSQL	Redis
連接埠	1521	3306	3389	5432	6379

> 说明:
> 各個參數配置說明，請參見第6步描述。

6. 在彈出的對話方塊中，設定以下參數：
   - 網卡類型：
     - 如果是VPC類型的安全性群組，不需要選擇這個參數。需要注意以下資訊：
       - 如果您的執行個體能訪問公網，可以設定公網和內網的訪問規則。
       - 如果您的執行個體不能訪問公網，只能設定內網的訪問規則。
     - 如果是傳統網路的安全性群組，選擇 公網 或 內網。
   - 規則方向：
     - 出方向：是指ECS執行個體訪問內網中其他ECS執行個體或者公網上的資源。
     - 入方向：是指內網中的其他ECS執行個體或公網上的資源訪問ECS執行個體。
   - 授權策略：選擇 允許 或 拒絕。

> 说明:

這裡的 拒絕 策略是直接丟棄資料包，不給任何回應資訊。如果2個安全性群組規則其他都相同只有授權策略不同，則 拒絕 授權生效，接受 授權不生效。

- 協議類型 和 連接埠範圍：連接埠範圍的設定受協議類型影響。下表是協議類型與連接埠範圍的關係。

協議類型	連接埠範圍	應用情境
全部	顯示為-1/-1，表示不限制連接埠。不能設定。	可用於完全互相信任的應用情境。
全部ICMP	顯示為-1/-1，表示不限制連接埠。不能設定。	使用 `ping` 程式檢測執行個體之間的通訊狀況。
全部GRE	顯示為-1/-1，表示不限制連接埠。不能設定。	用於VPN服務。
自訂TCP 自訂UDP	自訂連接埠範圍，有效連接埠值是1 ~ 65535，連接埠範圍的合法格式是開始連接埠/結束連接埠。即使是一個連接埠，也需要採用合法格式設定連接埠範圍，比如：80/80表示連接埠80。	可用於允許或拒絕一個或幾個連續的連接埠。
SSH	顯示為22/22。 串連ECS執行個體後您能修改連接埠號碼，具體操作，請參見 伺服器預設遠程連接埠修改。	用於SSH遠端連線到Linux執行個體。
TELNET	顯示為23/23。	用於Telnet遠程登入執行個體。
HTTP	顯示為80/80。	執行個體作為網站或Web應用伺服器。
HTTPS	顯示為443/443。	執行個體作為支援HTTPS協議的網站或Web應用伺服器。
MS SQL	顯示為1433/1433。	執行個體作為MS SQL伺服器。
Oracle	顯示為1521/1521。	執行個體作為Oracle SQL伺服器。
MySQL	顯示為3306/3306。	執行個體作為MySQL伺服器。

RDP	顯示為3389/3389。 串連ECS執行個體後您能修改連接埠號碼，具體操作，請參見 伺服器預設遠程連接埠修改。	執行個體是Windows執行個體，需要遠端桌面連線執行個體。
PostgreSQL	顯示為5432/5432。	執行個體作為PostgreSQL伺服器。
Redis	顯示為6379/6379。	執行個體作為Redis伺服器。

说明:

公網出方向的STMP連接埠25預設受限，無法通過安全性群組規則開啟，但是您可以 申請解鎖連接埠25。其他常用連接埠資訊，請參見 *ECS* 執行個體常用連接埠介紹。

- 授與類型 和 授權對象：授權對象的設定受授與類型影響，以下是兩者之間的關係。

授與類型	授權對象
位址區段訪問	填寫單一IP地址或者CIDR網段格式，如：12.1.1.1或13.1.1.1/25。僅支援IPv4。如果填寫0.0.0.0/0表示允許或拒絕所有IP地址的訪問，設定時請務必謹慎。
安全性群組訪問	只對內網有效。授權本帳號或其他帳號下某個安全性群組中的執行個體訪問本安全性群組中的執行個體，實現內網互連。 - 本帳號授權：選擇同一帳號下的其他安全性群組ID。如果是VPC網路的安全性群組，必須為同一個VPC的安全性群組。 - 跨帳號授權：填寫目標安全性群組ID，以及對方帳號ID。在 帳號管理 > 安全設定 裡查看帳號ID。 因為安全性群組訪問只對內網有效，所以，對VPC網路執行個體，安全性群組訪問的規則僅適用於內網訪問，不適用於公網訪問。公網訪問只能通過 位址區段訪問 授權。

说明:

出於安全性考慮，傳統網路的內網入方向規則，授與類型優先選擇 安全性群組訪問。如果選擇 位址區段訪問，則只能授權單個IP地址，授權對象的格式只能是 a.b.c.d/32，僅支援IPv4，子網路遮罩必須是 /32。

- 優先順序：1 ~ 100，數值越小，優先順序越高。更多優先順序資訊，參見 *ECS*安全性群組規則優先順序說明。

7. 單擊 確定，即成功地為指定安全性群組添加了一條安全性群組規則。

安全性群組規則一般是立即生效，但是也可能有稍許延遲。

查看安全性群組規則是否生效

假設您在執行個體裡安裝了Web服務，並在一個安全性群組裡添加了一條安全性群組規則：公網入方向，允許所有IP地址訪問執行個體的TCP 80連接埠。

Linux執行個體

如果是安全性群組中的一台Linux執行個體，按以下步驟查看安全性群組規則是否生效。

1. *#unique_9*。
2. 運行以下命令查看TCP 80是否被監聽。

```
netstat -an | grep 80
```

如果返回以下結果，說明TCP 80連接埠已開通。

```
tcp        0      0 0.0.0.0:80                  0.0.0.0:*
        LISTEN
```

3. 在瀏覽器地址欄裡輸入 `http://執行個體公網IP地址`。如果訪問成功，說明規則已經生效。

Windows執行個體

如果是安全性群組中的一台Windows執行個體，按以下步驟查看安全性群組規則是否生效。

1. *#unique_10*。
2. 運行 命令提示字元，輸入以下命令查看TCP 80是否被監聽。

```
netstat -aon | findstr :80
```

如果返回以下結果，說明TCP 80連接埠已開通。

```
TCP    0.0.0.0:80           0.0.0.0:0              LISTENING
1172
```

3. 在瀏覽器地址欄裡輸入 `http://執行個體公網IP地址`。如果訪問成功，說明規則已經生效。

ECS安全性群組規則優先順序說明

安全性群組規則的優先順序可以設為1 ~ 100的任一個數值，數值越小，優先順序越高。

ECS執行個體可以加入不同的安全性群組。無論是同一個安全性群組內或不同安全性群組之間，如果安全性群組規則互相矛盾，即協議類型、連接埠範圍、授與類型、授權對象都相同，最終生效的安全性群組規則如下：

- 如果 優先順序 相同，則 拒絕 授權規則生效，接受 授權規則不生效。
- 如果 優先順序 不同，則優先順序高的規則生效，與 授權策略 的設定無關。

相關文檔

- 安全性群組*FAQ*
- 安全性群組
- *#unique_11*
- *ECS*安全性群組中規則的優先順序執行匹配順序說明

1.6 加入、移出安全性群組

加入安全性群組

在控制台中，您可以將執行個體加入一個安全性群組。一個 ECS 執行個體最多可以加入 5 個安全性群組。

1. 登入 *ECS*管理主控台。
2. 單擊左側導覽列中的 執行個體。
3. 單擊頁面頂部的地區。
4. 選擇需要執行個體，單擊執行個體的名稱，或右側的 管理，會跳轉到執行個體詳情頁。
5. 單擊 本執行個體安全性群組。
6. 單擊 加入安全性群組。在彈出對話方塊，選中需要的安全性群組。
7. 單擊 確定。

加入安全性群組後，安全性群組的規則自動對執行個體進行生效，不需要更新。

移出安全性群組

當一個執行個體加入 2 個以上安全性群組時，根據業務需要，您可以將執行個體移出某個安全性群組。

 说明:

- 一個執行個體至少需要加入 1 個安全性群組，所以執行個體只加入 1 個安全性群組時，您不能將它移出安全性群組。
- 將 ECS 執行個體從安全性群組移出，將會導致這個 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。

1. 登入 *ECS*管理主控台。
2. 單擊左側導覽列中的 執行個體。
3. 單擊頁面頂部的地區。
4. 選擇需要執行個體，單擊執行個體的名稱，或右側的 管理，會跳轉到執行個體詳情頁。
5. 單擊 本執行個體安全性群組。您可以看到該執行個體所在安全性群組的列表。
6. 選中想要移除的安全性群組，單擊右側的 移出。
7. 在彈出的提示框中，單擊 確定。

關於安全性群組的使用情境，請參考應用案例。

2 金鑰組

2.1 SSH 金鑰對

SSH 金鑰對，常簡稱為金鑰組，是區別於使用者名加密碼遠程登入 Linux 執行個體的認證方式。SSH 金鑰對通過密碼編譯演算法生成一對密鑰，預設採用 RSA 2048 位的加密方式。一個對外界公開，稱為 公開金鑰，另一個您自己保留，稱為 私密金鑰，私密金鑰使用未加密的 PEM（Privacy-enhanced Electronic Mail） 編碼的 `PKCS#8` 格式。

功能優勢

相較於使用者名和密碼認證方式，SSH 金鑰對有以下優勢：

安全性

SSH 金鑰對登入認證更為安全可靠：

- **金鑰組安全強度遠高於常規使用者口令，可以杜絕暴力破解威脅。**
- **不可能通過公開金鑰推匯出私密金鑰。**

便捷性

- **如果您將公開金鑰配置在 Linux 執行個體中，那麼，在本地或者另外一台執行個體中，您可以使用私密金鑰通過 SSH 命令或相關工具登入目標執行個體，而不需要輸入密碼。**
- **便於遠程登入大量 Linux 執行個體，方便管理。如果您需要批量維護多台 Linux 執行個體，推薦使用這種方式登入。**

使用限制

使用 SSH 金鑰對有如下限制：

- **僅支援 Linux 執行個體。如果使用 SSH 金鑰對登入 Linux 執行個體，預設禁用密碼登入，以提高安全性。**
- **目前，ECS 只支援建立 2048 位的 RSA 金鑰組。**
  - **ECS 會保存金鑰組的公開金鑰部分。**
  - **金鑰組建立成功後，您需要妥善保管私密金鑰。**
- **一個雲帳號在一個地域最多可以擁有 500 個金鑰組。**
- **一台 Linux 執行個體只能綁定一個 SSH 金鑰對。如果您的執行個體已綁定金鑰組，綁定新的金鑰組會替換原來的金鑰組。**

- 基於資料安全考慮，在執行個體狀態為 運行中 （Running） 綁定或者解綁金鑰組時，您需要重啟執行個體使操作生效。
- 已停售的執行個體規格 無法使用 SSH 金鑰對。

生成方式

SSH 金鑰對的生成方式包括：

- 由 *ECS* 生成，預設採用 RSA 2048 位的加密方式。

  

  说明:

  如果您的金鑰組由 ECS 生成，那麼在首次生成金鑰組時，請務必下載並妥善保存私密金鑰。當該金鑰組綁定某台執行個體時，如果沒有私密金鑰，您將無法登入執行個體。
- 由您採用 SSH 金鑰對產生器生成後再匯入 ECS，匯入的金鑰組必須支援下列任一種加密方式：
  - rsa
  - dsa
  - ssh-rsa
  - ssh-dss
  - ecdsa
  - ssh-rsa-cert-v00@openssh.com
  - ssh-dss-cert-v00@openssh.com
  - ssh-rsa-cert-v01@openssh.com
  - ssh-dss-cert-v01@openssh.com
  - ecdsa-sha2-nistp256-cert-v01@openssh.com
  - ecdsa-sha2-nistp384-cert-v01@openssh.com
  - ecdsa-sha2-nistp521-cert-v01@openssh.com

相關操作

- 如果您沒有 SSH 金鑰對，可以 *#unique_17*。
- 如果您使用其它工具生成了金鑰組，可以 *#unique_18*。
- 如果您不再需要某個金鑰組，可以 *#unique_19*。
- 如果您想使用或者禁用 SSH 金鑰對訪問已經建立好的執行個體，可以 *#unique_20*。
- 您可以在 建立執行個體 時指定 SSH 金鑰對。
- 您可以 *#unique_22*。

3 存取控制RAM

如果您購買了多台Elastic Compute Service 執行個體，您的組織裡有多個使用者需要使用這些執行個體。如果這些使用者共用使用您的雲帳號密鑰，那麼存在以下問題：

- 您的密鑰由多人共用，泄密風險高；
- 您無法限制使用者的存取權限，容易出現誤操作導致安全風險。

存取控制 RAM (Resource Access Management) 是阿里雲提供的資源存取控制服務。通過 RAM，您可以集中管理您的使用者（比如員工、系統或應用程式），以及控制使用者可以訪問您名下哪些資源的許可權。

存取控制 RAM 將協助您系統管理使用者對資源的存取權限控制。例如，為了加強網路安全控制，您可以給某個群組附加一個授權策略，該策略規定：如果使用者的原始 IP 地址不是來自商業網路，則拒絕此類使用者請求訪問您名下的 ECS 資源。

您可以給不同群組設定不同許可權，例如：

- SysAdmins：該群組需要建立和管理 ECS 鏡像、執行個體、快照、安全性群組等許可權。您給 SysAdmins 組附加了一個授權策略，該策略授予群組成員執行所有 ECS 操作的許可權。
- Developers：該群組只需要使用執行個體的許可權。您可以給 Developers 組附加一個授權策略，該策略授予群組成員調用 DescribeInstances、StartInstance、StopInstance、CreateInstance 和 DeleteInstance 的許可權。
- 如果某開發人員的工作職責發生轉變，成為一名系統管理人員，您可以方便的將其從 Developpers 群組移到 SysAdmins 群組。

更多關於存取控制 RAM的介紹，請參考 *RAM* 的產品文檔。

4 執行個體RAM角色

4.1 什麼是執行個體 RAM 角色

ECS 執行個體 RAM（Resource Access Management） 角色（以下簡稱 執行個體 RAM 角色）是 RAM 角色的一種，它讓 ECS 執行個體扮演具有某些許可權的角色，從而賦予執行個體一定的存取權限。

執行個體 RAM 角色允許您將一個 *#unique_27* 關聯到 ECS 執行個體，在執行個體內部基於 STS（Security Token Service）臨時憑證（臨時憑證將周期性更新）訪問其他雲產品的 API。這樣，一方面可以保證 AccessKey 安全，另一方面也可以藉助 RAM 實現許可權的精細化控制和管理。

設計背景

一般情況下，ECS 執行個體的應用程式是通過 使用者帳號 或者 *#unique_28* 的 AccessKey（AccessKeyId + AccessKeySecret）訪問阿里雲各產品的 API。

為了滿足調用需求，需要直接把 AccessKey 固化在執行個體中，如寫在設定檔中。但是這種方式存在許可權過大、泄露資訊和難以維護等問題。因此，我們設計了執行個體 RAM 角色解決這些問題。

功能優勢

使用執行個體 RAM 角色，您可以：

- **藉助執行個體 RAM 角色，將 *#unique_27* 和 ECS 執行個體關聯起來。**
- **安全地在 ECS 執行個體中使用 STS 臨時憑證訪問阿里雲的其他雲端服務，如 OSS、ECS、RDS 等。**
- **為不同的執行個體賦予包含不同授權策略的角色，使它們對不同的雲資源具有不同的存取權限，實現更精細粒度的許可權控制。**
- **無需自行在執行個體中儲存 AccessKey，通過修改角色的授權即可變更許可權，快捷地維護 ECS 執行個體所擁有的存取權限。**

費用詳情

Elastic Compute Service 不對執行個體 RAM 角色收取額外的費用。

使用限制

使用執行個體 RAM 角色存在如下限制：

- 只有Virtual Private Cloud 網路類型的執行個體才能使用執行個體角色。
- 一個 ECS 執行個體一次只能授予一個執行個體 RAM 角色。

使用執行個體 RAM 角色

目前有兩種使用 RAM 角色的方式：

- 通過控制台使用執行個體 *RAM* 角色
- 通過 *API* 使用執行個體 *RAM* 角色

參考連結

- 您可以參閱文檔 *#unique_31* 查看支援 STS 臨時憑證的雲端服務。
- 您可以參閱文檔 藉助執行個體 *RAM* 角色訪問其它雲產品 *API* 查看如何訪問其他雲產品的 API 。

4.2 通過控制台使用執行個體 RAM 角色

使用限制

使用執行個體 RAM 角色存在如下限制：

- 只有Virtual Private Cloud 網路類型的 ECS 執行個體才能使用執行個體 RAM 角色。
- 一個 ECS 執行個體一次只能授予一個執行個體 RAM 角色。
- 當您給 ECS 執行個體授予了執行個體 RAM 角色後，並希望在 ECS 執行個體內部部署的應用程式中訪問雲產品的 API 時，您需要通過 *#unique_32* 擷取執行個體 RAM 角色的臨時授權 Token。參閱 *6.* （可選）擷取臨時授權 *Token*。
- 如果您是通過 RAM 使用者子帳號使用執行個體 RAM 角色，您需要通過雲帳號 *7.* （可選）授權 *RAM* 使用者使用執行個體 *RAM* 角色。

前提條件

您已經開通 RAM 服務，參閱 RAM 文檔 *#unique_33* 開通 RAM 服務。

1. 建立執行個體 RAM 角色

1. 登入 *RAM* 控制台。
2. 在瀏覽窗格中，單擊 角色管理。
3. 在角色管理頁面，單擊 建立角色。

4. 在彈窗中：

   a. 角色類型 選擇 服務角色。

   b. 類型資訊 選擇 ECS 雲端服務器。

   c. 輸入角色名稱及備忘，如 EcsRamRoleDocumentTesting。

   d. 單擊 確認 完成建立。

2. 授權執行個體 RAM 角色

1. 登入 *RAM* 控制台。
2. 在瀏覽窗格中，單擊 策略管理。
3. 在 策略管理 頁面，單擊 建立授權策略。
4. 在彈窗中：

   a. 權限原則模板 選擇 空白模板。

   b. 輸入 授權策略名稱 及 策略內容，如 EcsRamRoleDocumentTestingPolicy。

   > 说明:
   > 關於如何編寫策略內容，您可以參閱 RAM 文檔 *#unique_34*。

   c. 單擊 建立授權策略 完成授權。
5. 在瀏覽窗格中，單擊 角色管理。
6. 在 角色管理 頁面，選擇建立好的角色，如 EcsRamRoleDocumentTesting，單擊 授權。
7. 輸入建立的 授權策略名稱，如 EcsRamRoleDocumentTestingPolicy。
8. 單擊符號 > 選中策略名，單擊 確認。

3. 授予執行個體 RAM 角色

1. 登入 *ECS*管理主控台。
2. 在瀏覽窗格中，單擊 執行個體。
3. 選擇地區。
4. 找到要操作的 ECS 執行個體，選擇 更多 > 授予/收回 RAM 角色。
5. 在彈窗中，選擇建立好的執行個體 RAM 角色，如 EcsRamRoleDocumentTesting，單擊 確定 完成授予。

4. （可選）收回執行個體 RAM 角色

   1. 登入 *ECS*管理主控台。
   2. 在瀏覽窗格中，單擊 執行個體。
   3. 選擇地區。
   4. 選擇一個已經授予 RAM 角色的 ECS 執行個體，選擇 更多 > 授予/收回 RAM 角色。
   5. 操作類型 選擇 收回，單擊 確定 即可收回執行個體 RAM 角色。

5. （可選）更換執行個體 RAM 角色

   1. 登入 *ECS*管理主控台。
   2. 在瀏覽窗格中，單擊 執行個體。
   3. 選擇地區。
   4. 選擇一個已經授予 RAM 角色的 ECS 執行個體，選擇 更多 > 授予/收回 RAM 角色。
   5. 操作類型 選擇 授予，在已有 RAM 角色 中選擇其他執行個體 RAM 角色，單擊 確定 即可更換當前 RAM 角色。

6. （可選）擷取臨時授權 Token

   您可以獲得執行個體 RAM 角色的臨時授權 Token，該臨時授權 Token 可以執行執行個體 RAM 角色的許可權和資源，並且該臨時授權 Token 會自動周期性地更新。樣本：

   1. 遠端連線並登入到 ECS 執行個體。
   2. 檢索名為 EcsRamRoleDocumentTesting 的執行個體 RAM 角色的臨時授權 Token：
      - Linux 執行個體： 執行命令 `curl http://100.100.100.200/latest/meta-data/Ram/security-credentials/EcsRamRoleDocumentTesting`。
      - Windows 執行個體：參閱 *#unique_32*。
   3. 獲得臨時授權 Token。返回樣本如下：

```
{
"AccessKeyId" : "XXXXXXXXX",
"AccessKeySecret" : "XXXXXXXXX",
"Expiration" : "2017-11-01T05:20:01Z",
"SecurityToken" : "XXXXXXXXX",
"LastUpdated" : "2017-10-31T23:20:01Z",
"Code" : "Success"
```

```
}
```

7. （可選）授權 RAM 使用者使用執行個體 RAM 角色

> **说明:**
> **當您授權 RAM 使用者使用執行個體 RAM 角色時，您必須授權 RAM 使用者對該執行個體 RAM 角色的 PassRole 許可權。其中，PassRole 決定該 RAM 使用者能否直接執行角色策略賦予的許可權。**

登入 RAM 控制台，參閱 *#unique_35* 完成授權，授權策略如下所示：

```
{
"Version": "2016-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": [
"ecs: [ECS RAM Action]",
"ecs: CreateInstance",
"ecs: AttachInstanceRamRole",
"ecs: DetachInstanceRAMRole"
],
"Resource": "*"
},
{
"Effect": "Allow",
"Action": "ram:PassRole",
"Resource": "*"
}
]
}
```

其中，`[ECS RAM Action]` 表示可授權 RAM 使用者的許可權，請參閱 *#unique_36*。

參考連結

- **您也可以通過 *API* 使用執行個體 *RAM* 角色。**
- **您也許想藉助執行個體 *RAM* 角色訪問其它雲產品 *API*。**

4.3 通過 API 使用執行個體 RAM 角色

使用限制

使用執行個體 RAM 角色存在如下限制：

- **只有Virtual Private Cloud 網路類型的 ECS 執行個體才能使用執行個體 RAM 角色。**
- **一個 ECS 執行個體一次只能授予一個執行個體 RAM 角色。**

- 當您給 ECS 執行個體授予了執行個體 RAM 角色後，並希望在 ECS 執行個體內部部署的應用程式中訪問雲產品的 API 時，您需要通過 *#unique_32* 擷取執行個體 RAM 角色的臨時授權 Token。參閱 *5.* （可選）擷取臨時授權 *Token*。
- 如果您是通過 RAM 使用者子帳號使用執行個體 RAM 角色，您需要通過雲帳號 *6.* （可選）授權 *RAM* 使用者使用執行個體 *RAM* 角色。

前提條件

您已經開通 RAM 服務，參閱 RAM 文檔 *#unique_33* 開通 RAM 服務。

1. 建立執行個體 RAM 角色

1. 調用介面 *#unique_37* 建立執行個體 RAM 角色。
2. 設定 RoleName 參數，如將其值置為 EcsRamRoleDocumentTesting。
3. 按如下原則設定 AssumeRolePolicyDocument：

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

2. 授權執行個體 RAM 角色

1. 調用介面 *#unique_38* 建立授權策略。
2. 設定 RoleName 參數，如將其值置為 EcsRamRoleDocumentTestingPolicy。
3. 按如下原則設定 PolicyDocument：

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

```
}
```

4. **調用介面** *#unique_39* **授權角色策略。**
5. **設定** `PolicyType` **參數為 Custom。**
6. **設定** `PolicyName` **參數，如 EcsRamRoleDocumentTestingPolicy。**
7. **設定** `RoleName` **參數，如 EcsRamRoleDocumentTesting。**

3. 授予執行個體 RAM 角色

1. **調用介面** *#unique_40* **為執行個體授予 RAM 角色。**
2. **設定** `RegionId` **及** `InstanceIds` **參數指定一個 ECS 執行個體。**
3. **設定** `RamRoleName` **參數，如 EcsRamRoleDocumentTesting。**

4. （可選）收回執行個體 RAM 角色

1. **調用介面** *#unique_41* **收回執行個體 RAM 角色。**
2. **設定** `RegionId` **及** `InstanceIds` **參數指定一個 ECS 執行個體。**
3. **設定** `RamRoleName` **參數，如 EcsRamRoleDocumentTesting。**

5. （可選）擷取臨時授權 Token

您可以獲得執行個體 RAM 角色的臨時授權 Token，該臨時授權 Token 可以執行執行個體 RAM 角色的許可權和資源，並且該臨時授權 Token 會自動周期性地更新。樣本：

1. **檢索名為 EcsRamRoleDocumentTesting 的執行個體 RAM 角色的臨時授權 Token：**
   - **Linux 執行個體： 執行命令** `curl http://100.100.100.200/latest/meta-data/Ram/security-credentials/EcsRamRoleDocumentTesting`。
   - **Windows 執行個體：參閱文檔** *#unique_32*。
2. **獲得臨時授權 Token。返回樣本如下：**

```
{
"AccessKeyId" : "XXXXXXXXX",
"AccessKeySecret" : "XXXXXXXXX",
"Expiration" : "2017-11-01T05:20:01Z",
"SecurityToken" : "XXXXXXXXX",
"LastUpdated" : "2017-10-31T23:20:01Z",
"Code" : "Success"
}
```

6. （可選）授權 RAM 使用者使用執行個體 RAM 角色

说明:

當您授權 RAM 使用者使用執行個體 RAM 角色時，您必須授權 RAM 使用者對該執行個體 RAM 角色的 PassRole 許可權。其中，PassRole 決定該 RAM 使用者能否直接執行角色策略賦予的許可權。

登入 RAM 控制台，參閱文檔 *#unique_35* 完成授權，如下所示：

```
{
"Version": "2016-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": [
"ecs: [ECS RAM Action]",
"ecs: CreateInstance",
"ecs: AttachInstanceRamRole",
"ecs: DetachInstanceRAMRole"
],
"Resource": "*"
},
{
"Effect": "Allow",
"Action": "ram:PassRole",
"Resource": "*"
}
]
}
```

其中，[ECS RAM Action] 表示可授權 RAM 使用者的許可權，請參閱 *#unique_36*。

參考連結

- **您也可以 通過控制台使用執行個體 *RAM* 角色。**
- **您也許想 藉助執行個體 *RAM* 角色訪問其它雲產品 *API*。**
- **執行個體 RAM 角色相關的 API 介面包括：**
  - **建立 RAM 角色：*#unique_37***
  - **查詢 RAM 角色列表：*#unique_42***
  - **建立 RAM 角色策略：*#unique_38***
  - **授權 RAM 角色策略：*#unique_39***
  - **授予執行個體 RAM 角色：*#unique_40***
  - **收回執行個體 RAM 角色：*#unique_41***
  - **查詢執行個體 RAM 角色：*#unique_43***

5 DDoS基礎防護

功能可以有效防止Elastic Compute Service執行個體受到惡意攻擊，從而保證ECS系統的穩定，即當流入ECS執行個體的流量超出執行個體規格對應的限制時，雲盾就會幫助ECS執行個體限流，避免ECS系統出現問題。

阿里雲雲盾預設為ECS執行個體免費提供最大5 Gbit/s惡意流量攻擊，不同執行個體規格的免費防護流量不同，您可以登入雲盾DDoS防護管理主控台查看實際防護閾值，詳情請參見 雲盾DDoS基礎防護黑洞閾值。

DDoS基礎防護工作原理

啟用DDoS基礎防護後，雲盾會即時監控進入ECS執行個體的流量。當監測到超大流量或者包括DDoS攻擊在內的異常流量時，在不影響正常業務的前提下，雲盾會將可疑流量從原始網路路徑中重新導向到淨化產品上，識別並剝離惡意流量，並將還原的合法流量回注到原始網路中轉寄給目標ECS執行個體。這一過程，就是 流量清洗。更詳細的資訊，請參見 DDoS基礎防護服務-產品架構。

> 说明:
> 啟用了DDoS基礎防護的ECS執行個體，當來自互連網的流量大於5 Gbit/s時，為保護整個叢集的安全，阿里雲會讓相應ECS執行個體進入黑洞，丟棄進入該執行個體的所有流量，屏蔽公網對它的所有訪問。詳細資料，請參見 DDoS防護指南 -阿里雲黑洞策略。

流量清洗的觸發條件包括：

- 流量模型的特徵。當流量符合攻擊流量特徵時，就會觸發清洗。
- 流量大小。DDoS攻擊一般流量都非常大，通常都以Gbit/s為單位，因此，當進入ECS執行個體的流量達到設定的閾值時，無論是否為正常業務流量，雲盾都會啟動流量清洗。

流量清洗的方法包括：過濾攻擊報文、限制流量速度、限制資料包速度等。

所以，在使用DDoS基礎防護時，您需要設定以下閾值：

- BPS清洗閾值：當入方向流量超過BPS清洗閾值時，會觸發流量清洗。
- PPS清洗閾值：當入方向資料包數超過PPS清洗閾值時，會觸發流量清洗。

Elastic Compute Service的清洗閾值

Elastic Compute Service的清洗閾值由執行個體規格決定。下表列出了目前 在售 和 已停售 的部分執行個體規格的清洗閾值。

執行個體規格	最大BPS清洗閾值（Mbit/s）	最大PPS清洗閾值（PPS）
ecs.g5.16xlarge	20000	4000000
ecs.g5.22xlarge	30000	4500000
ecs.g5.2xlarge	2500	800000
ecs.g5.4xlarge	5000	1000000
ecs.g5.6xlarge	7500	1500000
ecs.g5.8xlarge	10000	2000000
ecs.g5.large	1000	300000
ecs.g5.xlarge	1500	500000
ecs.sn2ne.14xlarge	10000	4500000
ecs.sn2ne.2xlarge	2000	1000000
ecs.sn2ne.4xlarge	3000	1600000
ecs.sn2ne.8xlarge	6000	2500000
ecs.sn2ne.large	1000	300000
ecs.sn2ne.xlarge	1500	500000
ecs.c5.16xlarge	20000	4000000
ecs.c5.2xlarge	2500	800000
ecs.c5.4xlarge	5000	1000000
ecs.c5.6xlarge	7500	1500000
ecs.c5.8xlarge	10000	2000000
ecs.c5.large	1000	300000
ecs.c5.xlarge	1500	500000
ecs.sn1ne.2xlarge	2000	1000000
ecs.sn1ne.4xlarge	3000	1600000
ecs.sn1ne.8xlarge	6000	2500000
ecs.sn1ne.large	1000	300000
ecs.sn1ne.xlarge	1500	500000
ecs.r5.16xlarge	20000	4000000
ecs.r5.22xlarge	30000	4500000
ecs.r5.2xlarge	2500	800000
ecs.r5.4xlarge	5000	1000000

執行個體規格	最大BPS清洗閾值（Mbit/s）	最大PPS清洗閾值（PPS）
ecs.r5.6xlarge	7500	1500000
ecs.r5.8xlarge	10000	2000000
ecs.r5.large	1000	300000
ecs.r5.xlarge	1500	500000
ecs.re4.20xlarge	15000	2000000
ecs.re4.40xlarge	30000	4000000
ecs.se1ne.14xlarge	10000	4500000
ecs.se1ne.2xlarge	2000	1000000
ecs.se1ne.4xlarge	3000	1600000
ecs.se1ne.8xlarge	6000	2500000
ecs.se1ne.large	1000	300000
ecs.se1ne.xlarge	1500	500000
ecs.se1.14xlarge	10000	1200000
ecs.se1.2xlarge	1500	400000
ecs.se1.4xlarge	3000	500000
ecs.se1.8xlarge	6000	800000
ecs.se1.large	500	100000
ecs.d1ne.2xlarge	6000	1000000
ecs.d1ne.4xlarge	12000	1600000
ecs.d1ne.6xlarge	16000	2000000
ecs.d1ne.8xlarge	20000	2500000
ecs.d1ne.14xlarge	35000	4500000
ecs.d1.2xlarge	3000	300000
ecs.d1.4xlarge	6000	600000
ecs.d1.6xlarge	8000	800000
ecs.d1.8xlarge	10000	1000000
ecs.d1-c8d3.8xlarge	10000	1000000
ecs.d1.14xlarge	17000	1800000
ecs.d1-c14d3.14xlarge	17000	1400000
ecs.i2.xlarge	1000	500000

執行個體規格	最大BPS清洗閾值（Mbit/s）	最大PPS清洗閾值（PPS）
ecs.i2.2xlarge	2000	1000000
ecs.i2.4xlarge	3000	1500000
ecs.i2.8xlarge	6000	2000000
ecs.i2.16xlarge	10000	4000000
ecs.i1.xlarge	800	200000
ecs.i1.2xlarge	1500	400000
ecs.i1.4xlarge	3000	500000
ecs.i1-c10d1.8xlarge	6000	800000
ecs.i1-c5d1.4xlarge	3000	400000
ecs.i1.14xlarge	10000	1200000
ecs.hfc5.large	1000	300000
ecs.hfc5.xlarge	1500	500000
ecs.hfc5.2xlarge	2000	1000000
ecs.hfc5.4xlarge	3000	1600000
ecs.hfc5.6xlarge	4500	2000000
ecs.hfc5.8xlarge	6000	2500000
ecs.hfg5.large	1000	300000
ecs.hfg5.xlarge	1500	500000
ecs.hfg5.2xlarge	2000	1000000
ecs.hfg5.4xlarge	3000	1600000
ecs.hfg5.6xlarge	4500	2000000
ecs.hfg5.8xlarge	6000	2500000
ecs.hfg5.14xlarge	10000	4000000
ecs.c4.2xlarge	3000	400000
ecs.c4.4xlarge	6000	800000
ecs.c4.xlarge	1500	200000
ecs.ce4.xlarge	1500	200000
ecs.cm4.4xlarge	6000	800000
ecs.cm4.6xlarge	10000	1200000
ecs.cm4.xlarge	1500	200000

執行個體規格	最大BPS清洗閾值（Mbit/s）	最大PPS清洗閾值（PPS）
ecs.gn5-c28g1.14xlarge	10000	4500000
ecs.gn5-c4g1.xlarge	3000	300000
ecs.gn5-c4g1.2xlarge	5000	1000000
ecs.gn5-c8g1.2xlarge	3000	400000
ecs.gn5-c8g1.4xlarge	5000	1000000
ecs.gn5-c28g1.7xlarge	5000	2250000
ecs.gn5-c8g1.8xlarge	10000	2000000
ecs.gn5-c8g1.14xlarge	25000	4000000
ecs.gn5i-c2g1.large	1000	100000
ecs.gn5i-c4g1.xlarge	1500	200000
ecs.gn5i-c8g1.2xlarge	2000	400000
ecs.gn5i-c16g1.4xlarge	3000	800000
ecs.gn5i-c28g1.14xlarge	10000	2000000
ecs.gn4-c4g1.xlarge	3000	300000
ecs.gn4-c8g1.2xlarge	3000	400000
ecs.gn4-c4g1.2xlarge	5000	500000
ecs.gn4-c8g1.4xlarge	5000	500000
ecs.gn4.8xlarge	6000	800000
ecs.gn4.14xlarge	10000	1200000
ecs.ga1.xlarge	1000	200000
ecs.ga1.2xlarge	1500	300000
ecs.ga1.4xlarge	3000	500000
ecs.ga1.8xlarge	6000	800000
ecs.ga1.14xlarge	10000	1200000
ecs.f1-c28f1.7xlarge	5000	2000000
ecs.f1-c8f1.2xlarge	2000	800000
ecs.f2-c28f1.14xlarge	10000	2000000
ecs.f2-c28f1.7xlarge	5000	1000000
ecs.f2-c8f1.2xlarge	2000	400000
ecs.f2-c8f1.4xlarge	5000	1000000

執行個體規格	最大BPS清洗閾值（Mbit/s）	最大PPS清洗閾值（PPS）
ecs.t5-c1m1.2xlarge	1200	400000
ecs.t5-c1m1.large	500	100000
ecs.t5-c1m1.xlarge	800	200000
ecs.t5-c1m1.4xlarge	1200	600000
ecs.t5-c1m2.2xlarge	1200	400000
ecs.t5-c1m2.large	500	100000
ecs.t5-c1m2.xlarge	800	200000
ecs.t5-c1m2.4xlarge	1200	600000
ecs.t5-c1m4.2xlarge	1200	400000
ecs.t5-c1m4.large	500	100000
ecs.t5-c1m4.xlarge	800	200000
ecs.t5-lc1m1.small	200	60000
ecs.t5-lc1m2.large	400	100000
ecs.t5-lc1m2.small	200	60000
ecs.t5-lc1m4.large	400	100000
ecs.t5-lc2m1.nano	100	40000
ecs.ebmg4.8xlarge	10000	4500000
ecs.ebmg5.24xlarge	10000	4500000
ecs.sccg5.24xlarge	10000	4500000
ecs.xn4.small	500	50000
ecs.mn4.small	500	50000
ecs.mn4.large	500	100000
ecs.mn4.xlarge	800	150000
ecs.mn4.2xlarge	1200	300000
ecs.mn4.4xlarge	2500	400000
ecs.n4.small	500	50000
ecs.n4.large	500	100000
ecs.n4.xlarge	800	150000
ecs.n4.2xlarge	1200	300000
ecs.n4.4xlarge	2500	400000

執行個體規格	最大BPS清洗閾值（Mbit/s）	最大PPS清洗閾值（PPS）
ecs.n4.8xlarge	5000	500000
ecs.e4.small	500	50000
ecs.sn1.medium	500	100000
ecs.sn1.large	800	200000
ecs.sn1.xlarge	1500	400000
ecs.sn1.3xlarge	3000	500000
ecs.sn1.7xlarge	6000	800000
ecs.sn2.medium	500	100000
ecs.sn2.large	800	200000
ecs.sn2.xlarge	1500	400000
ecs.sn2.3xlarge	3000	500000
ecs.sn2.7xlarge	6000	800000
ecs.sn2.13xlarge	10000	120000

相關操作

Elastic Compute Service預設開啟DDoS基礎防護。ECS執行個體建立後，您可以執行以下操作：

- 設定清洗閾值：ECS執行個體建立後，預設按執行個體規格對應的最大閾值執行DDoS基礎防護。但是，部分執行個體規格的最大清洗閾值（BPS）可能過大，無法起到應有的防護作用，所以，您需要根據實際情況調整清洗閾值，具體操作，請參見 *DDoS*基礎防護使用者指南-*DDoS*基礎防護設定。
- （不推薦）取消流量清洗：當進入ECS執行個體的流量達到清洗閾值時，無論是否為正常業務流量，雲盾都會啟動流量清洗，此時，可能會導致正常業務不可用或受影響。為了保證正常業務，您可以手動取消流量清洗。具體操作，請參見 *DDoS*基礎防護使用者指南-如何取消流量清洗。

> **警告：**
> 取消流量清洗後，當流入ECS執行個體的流量超過5 Gbit/s時，您的ECS執行個體會被打進黑洞。請謹慎操作。