Alibaba Cloud Server Load Balancer

健康檢查

檔案版本：20190802

法律聲明

阿里雲提醒您在閱讀或使用本文檔之前仔細閱讀、充分理解本法律聲明各條款的內容。如果您閱讀或使用本文檔，您的閱讀或使用行為將被視為對本聲明全部內容的認可。

1. 您應當通過阿里雲網站或阿里雲提供的其他授權通道下載、擷取本文檔，且僅能用於自身的合法合規的商務活動。本文檔的內容視為阿里雲的保密資訊，您應當嚴格遵守保密義務；未經阿里雲事先書面同意，您不得向任何第三方披露本手冊內容或提供給任何第三方使用。
2. 未經阿里雲事先書面許可，任何單位、公司或個人不得擅自摘抄、翻譯、複製本文檔內容的部分或全部，不得以任何方式或途徑進行傳播和宣傳。
3. 由於產品版本升級、調整或其他原因，本文檔內容有可能變更。阿里雲保留在沒有任何通知或者提示下對本文檔的內容進行修改的權利，並在阿里雲授權通道中不時發布更新後的使用者文檔。您應當即時關注使用者文檔的版本變更並通過阿里雲授權渠道下載、擷取最新版的使用者文檔。
4. 本文檔僅作為使用者使用阿里雲產品及服務的參考性指引，阿里雲以產品及服務的”現狀“、“有缺陷”和“當前功能”的狀態提供本文檔。阿里雲在現有技術的基礎上盡最大努力提供相應的介紹及操作指引，但阿里雲在此明確聲明對本文檔內容的準確性、完整性、適用性、可靠性等不作任何明示或暗示的保證。任何單位、公司或個人因為下載、使用或信賴本文檔而發生任何差錯或經濟損失的，阿里雲不承擔任何法律責任。在任何情況下，阿里雲均不對任何間接性、後果性、懲戒性、偶然性、特殊性或刑罰性的損害，包括使用者使用或信賴本文檔而遭受的利潤損失，承擔責任（即使阿里雲已被告知該等損失的可能性）。
5. 阿里雲網站上所有內容，包括但不限於著作、產品、圖片、檔案、資訊、資料、網站架構、網站畫面的安排、網頁設計，均由阿里雲和/或其關係企業依法擁有其智慧財產權，包括但不限於商標權、專利權、著作權、商業秘密等。非經阿里雲和/或其關係企業書面同意，任何人不得擅自使用、修改、複製、公開傳播、改變、散布、發行或公開發表阿里雲網站、產品程式或內容。此外，未經阿里雲事先書面同意，任何人不得為了任何營銷、廣告、促銷或其他目的使用、公布或複製阿里雲的名稱（包括但不限於單獨為或以組合形式包含”阿里雲”、Aliyun”、“萬網”等阿里雲和/或其關係企業品牌，上述品牌的附屬標誌及圖案或任何類似公司名稱、商號、商標、產品或服務名稱、網域名稱、圖案標示、標誌、標識或通過特定描述使第三方能夠識別阿里雲和/或其關係企業）。
6. 如若發現本文檔存在任何錯誤，請與阿里雲取得直接聯絡。

通用約定

格式	說明	範例
	該類警示資訊將導致系統重大變更甚至故障，或者導致人身傷害等結果。	 **禁止:** 重設操作將丟失使用者配置資料。
	該類警示資訊可能導致系統重大變更甚至故障，或者導致人身傷害等結果。	 **警告:** 重啟操作將導致業務中斷，恢複業務所需時間約10分鐘。
	用於補充說明、最佳實務、竅門等，不是使用者必須瞭解的內容。	 **说明:** 您也可以通過按Ctrl + A選中全部檔案。
>	多級菜單遞進。	設定 > 網路 > 設定網路類型
粗體	表示按鍵、菜單、頁面名稱等UI元素。	單擊 確定。
`courier 字型`	命令。	執行 `cd / d C :/ windows` 命令，進入Windows系統檔案夾。
*## *	表示參數、變數。	`bae log list --instanceid` *Instance_ID*
[]或者[a|b]	表示可選項，至多選擇一個。	`ipconfig` *[-all|-t]*
{}或者{a|b}	表示必選項，至多選擇一個。	`swich` *{stand | slave}*

目錄

1 健康檢查介紹

負載平衡通過健康檢查來判斷後端伺服器（ECS執行個體）的業務可用性。健康檢查機制提高了前端業務整體可用性，避免了後端ECS異常對總體服務的影響。

開啟健康檢查功能後，當後端某台ECS健康檢查出現異常時，負載平衡會自動將新的請求分發到其它健康檢查正常的ECS上；而當該ECS恢複正常運行時，負載平衡會將其自動回復到負載平衡服務中。

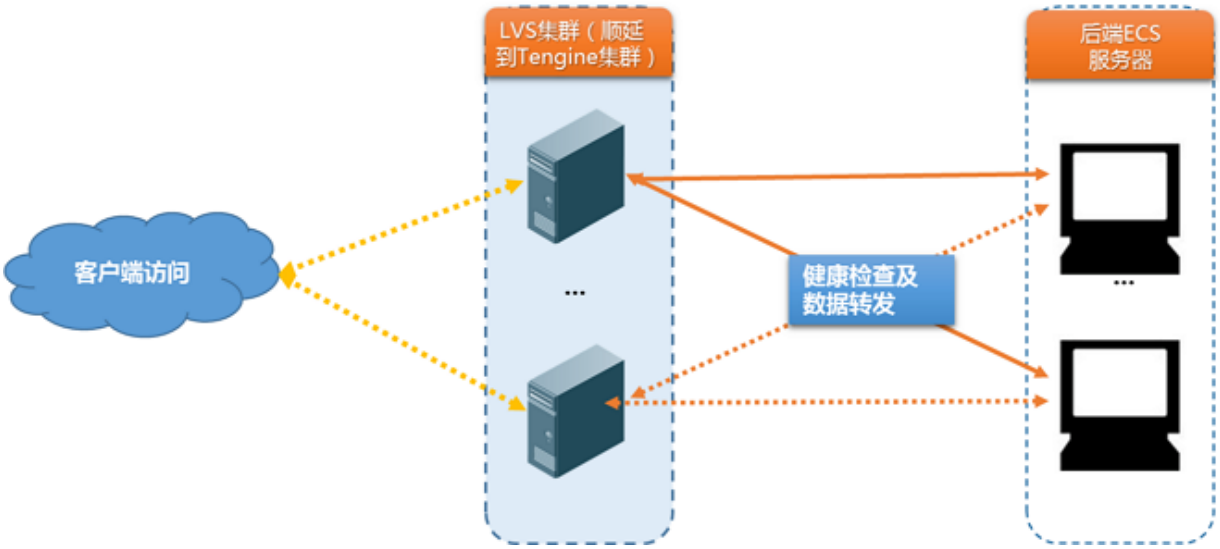
如果您的業務對負載敏感性高，高頻率的健康檢查探測可能會對正常業務訪問造成影響。您可以結合業務情況，通過降低健康檢查頻率、增大健康檢查間隔、七層檢查修改為四層檢查等方式，來降低對業務的影響。但為了保障業務的持續可用，不建議關閉健康檢查。

健康檢查過程

負載平衡採用叢集部署。LVS叢集或Tengine叢集內的相關節點伺服器同時承載了資料轉寄和健康檢查職責。

LVS叢集內不同伺服器分別獨立、並行地根據負載平衡策略進行資料轉寄和健康檢查操作。如果某一台LVS節點伺服器對後端某一台ECS健康檢查失敗，則該LVS節點伺服器將不會再將新的用戶端請求分發給相應的異常ECS。LVS叢集內所有伺服器同步進行該操作。

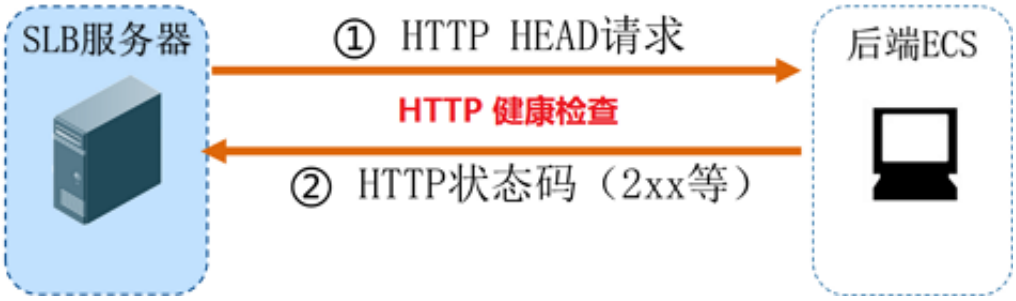
如下圖所示，負載平衡健康檢查使用的地址段是100.64.0.0/10，後端伺服器務必不能屏蔽該地址段。您無需在ECS安全性群組中額外針對該地址段配置放行策略，但如有配置iptables等安全性原則，請務必放行（100.64.0.0/10 是阿里雲保留地址，其他使用者無法分配到該網段內，不會存在安全風險）。



HTTP/HTTPS監聽健康檢查機制

針對七層（HTTP或HTTPS協議）監聽，健康檢查通過HTTP HEAD探測來獲取狀態資訊，如下圖所示。

對於HTTPS監聽，證書在負載平衡系統中進行管理。負載平衡與後端ECS之間的資料互動（包括健康檢查資料和業務互動資料），不再通過HTTPS進行傳輸，以提高系統效能。

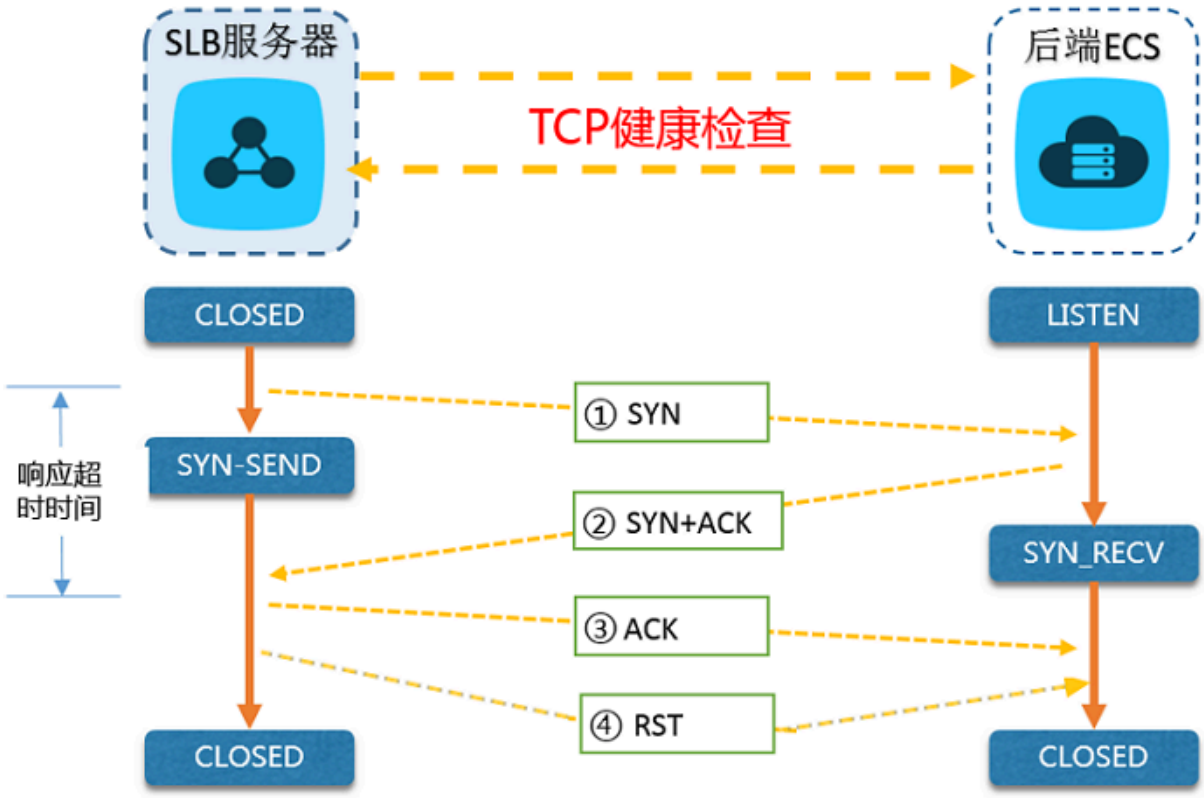


七層監聽的檢查機制如下：

1. Tengine節點伺服器根據監聽的健康檢查配置，向後端ECS的內網IP+【健康檢查通信埠】+【檢查路徑】發送HTTP HEAD請求（包含設定的【網域名稱】）。
2. 後端ECS收到請求後，根據相應服務的運行情況，返回HTTP狀態碼。
3. 如果在【響應逾時時間】之內，Tengine節點伺服器沒有收到後端ECS返回的資訊，則認為服務無響應，判定健康檢查失敗。
4. 如果在【響應逾時時間】之內，Tengine節點伺服器成功接收到後端ECS返回的資訊，則將該返回資訊與配置的狀態碼進行比對。如果匹配則判定健康檢查成功，反之則判定健康檢查失敗。

TCP監聽健康檢查機制

針對四層TCP監聽，為了提高健康檢查效率，健康檢查通過定製的TCP探測來獲取狀態資訊，如下圖所示。



TCP監聽的檢查機制如下：

1. LVS節點伺服器根據監聽的健康檢查配置，向後端ECS的內網IP+【健康檢查通信埠】發送TCP SYN資料包。
2. 後端ECS收到請求後，如果相應通信埠正在正常監聽，則會返回SYN+ACK資料包。
3. 如果在【響應逾時時間】之內，LVS節點伺服器沒有收到後端ECS返回的資料包，則認為服務無響應，判定健康檢查失敗；並向後端ECS發送RST資料包中斷TCP串連。
4. 如果在【響應逾時時間】之內，LVS節點伺服器成功收到後端ECS返回的資料包，則認為服務正常運行，判定健康檢查成功，而後向後端ECS發送RST資料包中斷TCP串連。

说明:

正常的TCP三向交握，LVS節點伺服器在收到後端ECS返回的SYN+ACK資料包後，會進一步發送ACK資料包，隨後立即發送RST資料包中斷TCP串連。

該實現機制可能會導致後端ECS認為相關TCP串連出現異常（非正常退出），並在業務軟體如Java串連池等日誌中拋出相應的錯誤資訊，如 `Connection reset by peer` 。

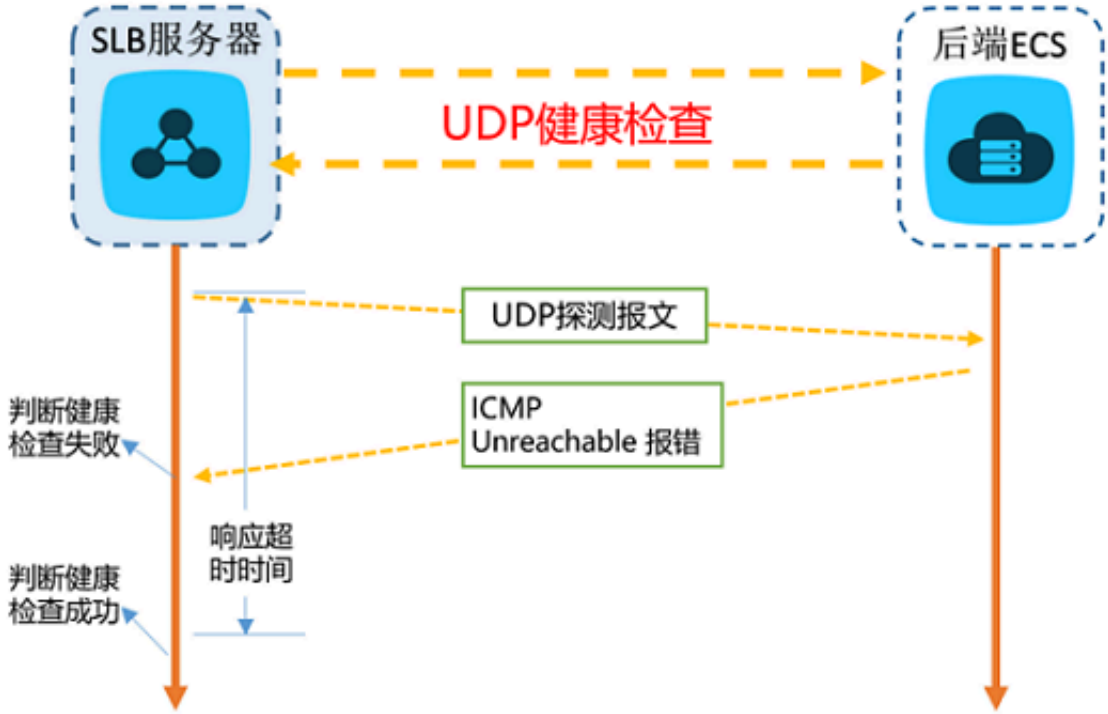
解決方案：

- TCP監聽採用HTTP方式進行健康檢查。

- 在後端ECS配置了獲取用戶端真實IP後，忽略來自前述負載平衡服務地址段相關訪問導致的串連錯誤。

UDP監聽健康檢查

針對四層UDP監聽，健康檢查通過UDP報文探測來獲取狀態資訊，如下圖所示。



UDP監聽的檢查機制如下：

1. LVS節點伺服器根據監聽的健康檢查配置，向後端ECS的內網IP+【健康檢查通信埠】發送UDP報文。
2. 如果後端ECS相應通信埠未正常監聽，則系統會返回類似返回 `port XX unreachable` 的ICMP報錯資訊；反之不做任何處理。
3. 如果在【響應逾時時間】之內，LVS節點伺服器收到了後端ECS返回的上述錯誤資訊，則認為服務異常，判定健康檢查失敗。
4. 如果在【響應逾時時間】之內，LVS節點伺服器沒有收到後端ECS返回的任何資訊，則認為服務正常，判定健康檢查成功。

說明：
當前UDP協議服務健康檢查可能存在服務真實狀態與健康檢查不一致的問題：

如果後端ECS是Linux伺服器，在大並發場景下，由於Linux的防ICMP攻擊保護機制，會限制伺服器發送ICMP的速度。此時，即便服務已經出現異常，但由於無法向前端返回 `port XX unreachabl e` 報錯資訊，會導致負載平衡由於沒收到ICMP應答進而判定健康檢查成功，最終導致服務真實狀態與健康檢查不一致。

解決方案：

負載平衡通過發送您指定的字元串到後端伺服器，必須得到指定應答後才認為檢查成功。但該實現機制需要用戶端程式配合應答。

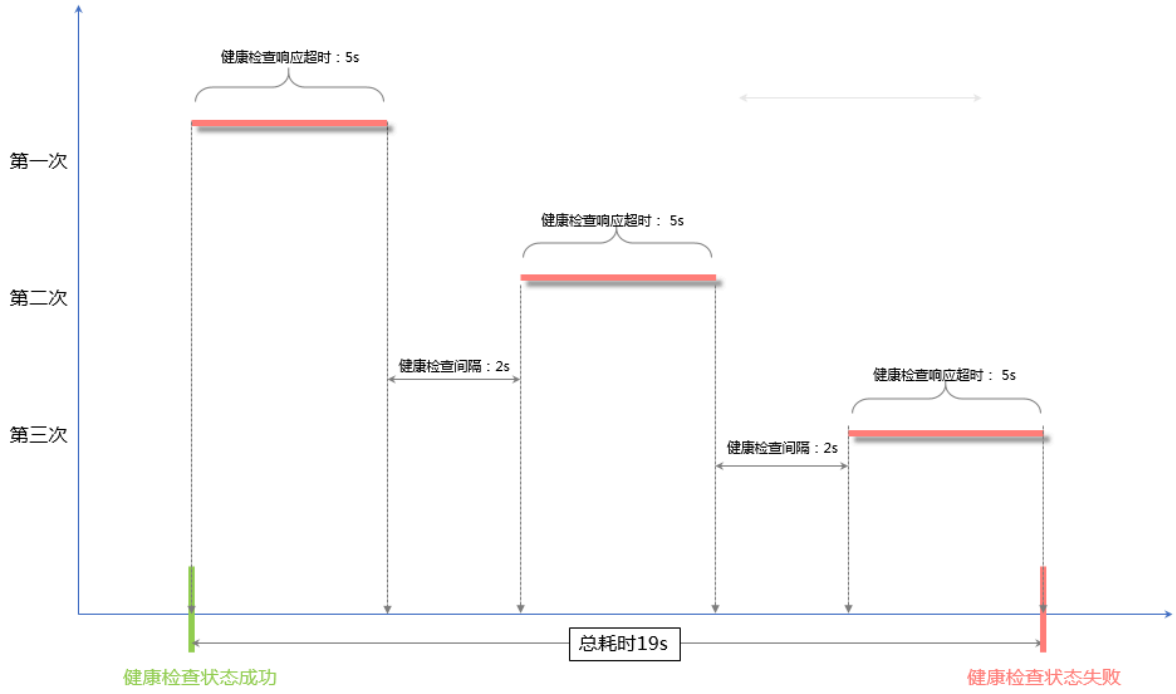
健康檢查時間窗

健康檢查機制的引入，有效提高了商務服務的可用性。但是，為了避免頻繁的健康檢查失敗引起的切換對系統可用性的衝擊，健康檢查只有在健康檢查時間窗內連續多次檢查成功或失敗後，才會進行狀態切換。健康檢查時間窗由以下三個因素決定：

- 健康檢查間隔 (每隔多久進行一次健康檢查)
- 響應逾時時間 (等待伺服器返回健康檢查的時間)
- 檢查閾值 (健康檢查連續成功或失敗的次數)

健康檢查時間窗的計算方法如下：

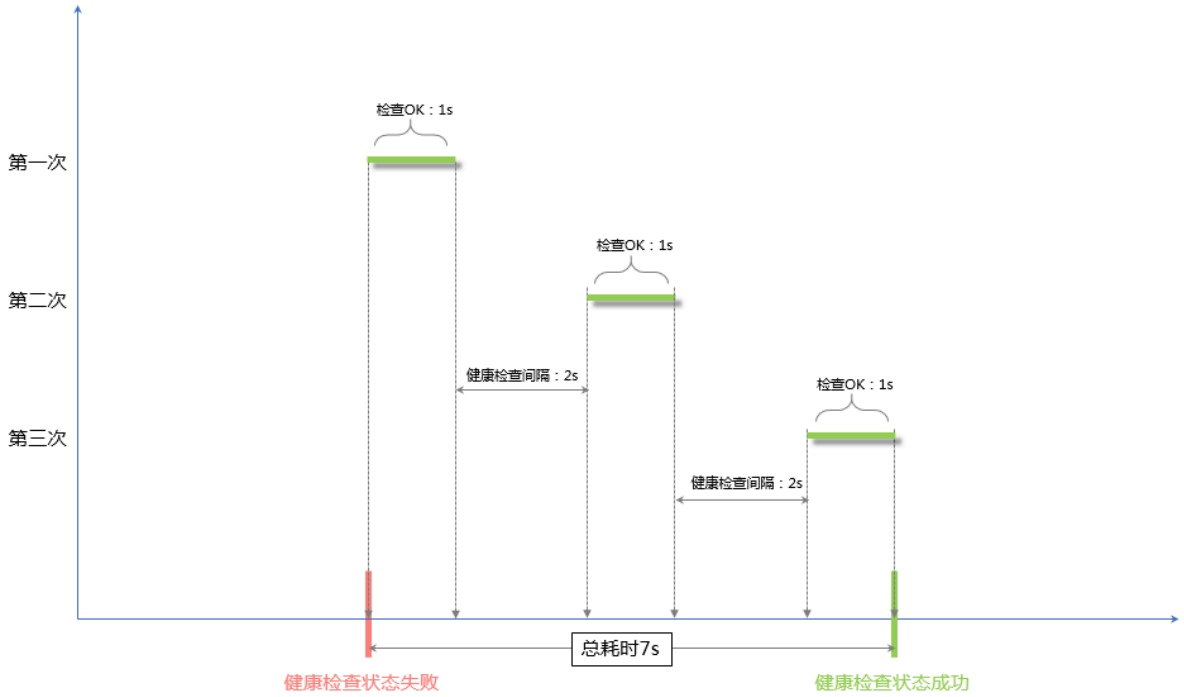
- 健康檢查失敗時間窗=響應逾時時間×不健康閾值+檢查間隔×(不健康閾值-1)



- 健康檢查成功時間窗= (健康檢查成功回應時間x健康閾值)+檢查間隔x(健康閾值-1)

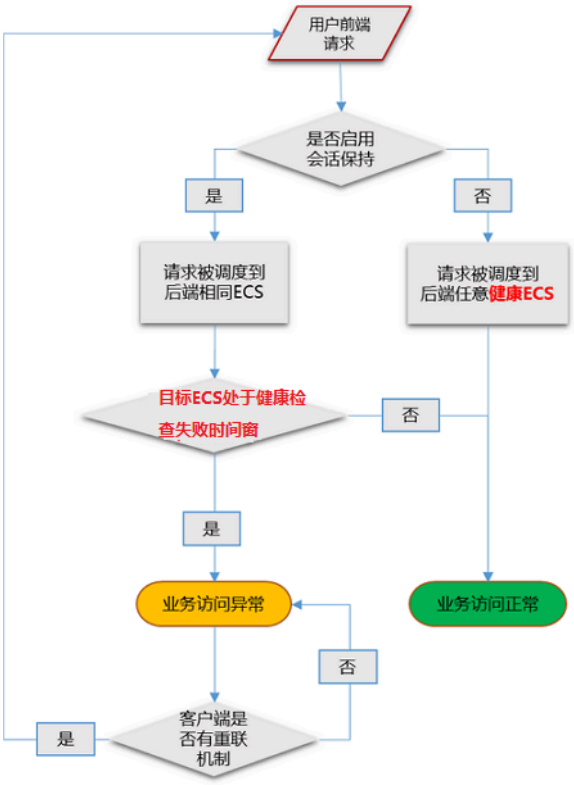
说明：

健康檢查成功回應時間是一次健康檢查請求從發出到響應的時間。當採用TCP方式健康檢查時，由於僅探測通信埠是否存活，因此該時間非常短，幾乎可以忽略不計。當採用HTTP方式健康檢查時，該時間取決於應用伺服器的效能和負載，但通常都在秒級以內。



健康檢查狀態對請求轉寄的影響如下：

- 如果目標ECS的健康檢查失敗，新的請求不會再分發到相應ECS上，所以對前端訪問沒有影響。
- 如果目標ECS的健康檢查成功，新的請求會分發到該ECS上，前端訪問正常。
- 如果目標ECS存在異常，正處於健康檢查失敗時間窗，而健康檢查還未達到檢查失敗判定次數（預設為三次），則相應請求還是會被分發到該ECS，進而導致前端訪問請求失敗。


用户前端
请求
是否启用
会话保持
是
否
请求被调度到
后端相同ECS
请求被调度到
后端任意健康ECS
目标ECS处于健康检
查失败时间窗
否
是
业务访问异常
业务访问正常
否
客户端是
否有重联
机制
是

2 配置健康檢查

您可以在添加監聽時配置健康檢查。通常，使用預設的健康檢查配置即可。

配置健康檢查

您可以通過控制台或API配置監聽的健康檢查。更多詳細資料，參見健康檢查介紹和健康檢查常見問題。

完成以下操作，配置健康檢查：

1. 登入負載平衡管理主控台。
2. 選擇地域，查看該地域的所有Server Load Balancer執行個體。
3. 單擊Server Load Balancer執行個體的ID。
4. 在執行個體詳情頁面，單擊監聽。
5. 單擊添加監聽或目標監聽的配置選項。
6. 在健康檢查頁面，配置健康檢查。

   在配置健康檢查時，建議您使用預設值。

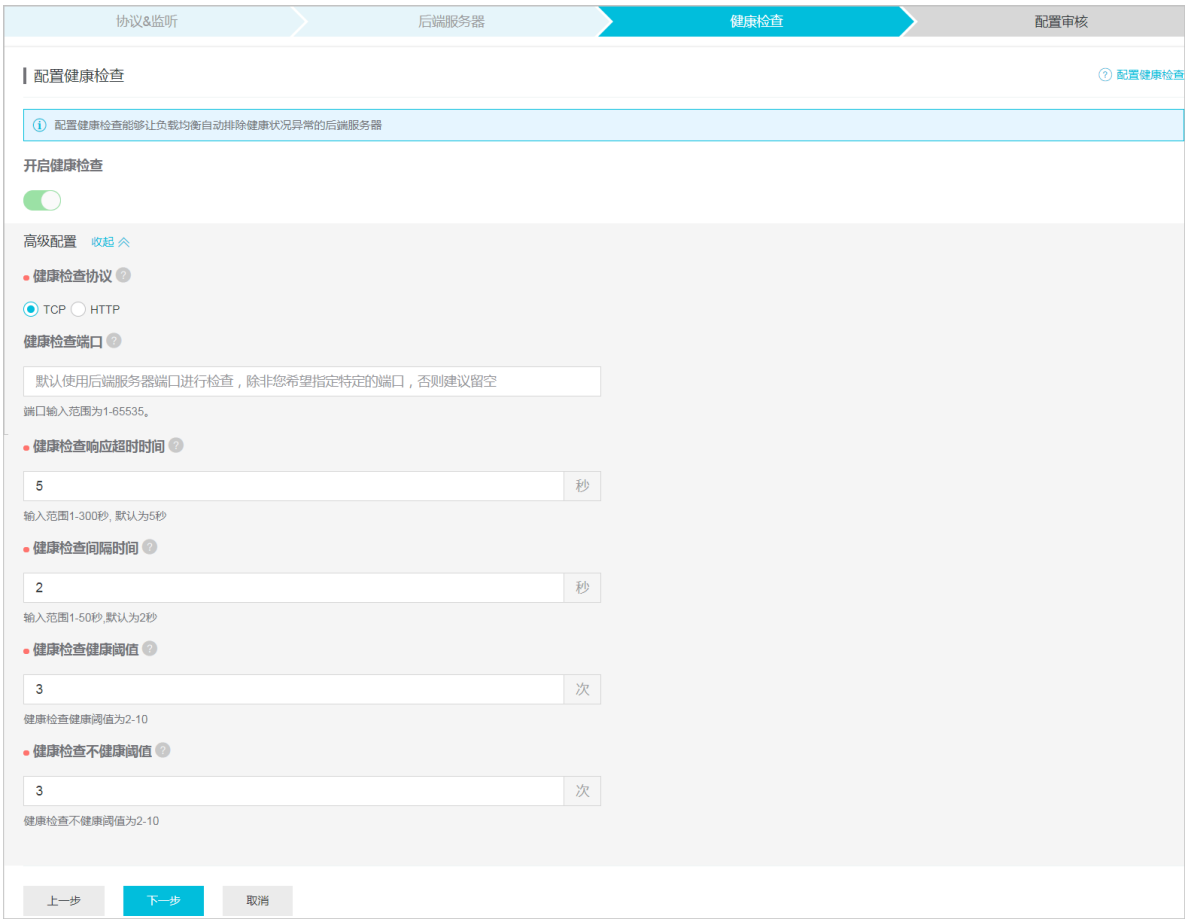
   表 2-1: 健康檢查配置說明

健康檢查配置	說明
健康檢查模式	監聽為TCP協議時，健康檢查方式可選TCP或HTTP模式。 · TCP模式的健康檢查是基於網路層探測。 · HTTP模式的健康檢查是通過發送head請求。

健康檢查配置	說明
網域名稱和檢查路徑 （僅限HTTP方式的健康檢查）	HTTP健康檢查預設由負載平衡系統通過後端ECS內網IP地址向該伺服器應用配置的預設首頁發起http head請求。 如果您用來進行健康檢查的頁面並不是應用伺服器的預設首頁，需要指定具體的檢查路徑。 因為有些應用伺服器會對請求中的host欄位做校驗，即要求要求標頭中必須存在host欄位。如果在健康檢查中配置了網域名稱，則SLB會將網域名稱配置到host欄位中去，反之，如果沒有佈建網域名，SLB則不會在請求中附帶host欄位，因此健康檢查請求就會被伺服器拒絕，可能導致健康檢查失敗。綜上原因，如果您的應用伺服器需要校驗請求的host欄位校，那麼則需要配置相關的網域名稱，確保健康檢查正常工作。
正常狀態碼 （僅限HTTP方式的健康檢查）	選擇健康檢查正常的HTTP狀態碼。 預設值為http_2xx和http_3xx。
檢查通信埠	健康檢查服務訪問後端時的探測通信埠。 預設值為配置監聽時指定的後端通信埠。 說明: 如果該監聽配置了虛擬伺服器組或主備伺服器組，且組內的ECS執行個體的通信埠都不相同，此時不需要配置檢查通信埠。負載平衡系統會使用各自ECS的後端通信埠進行健康檢查。
響應逾時時間	接收來自健全狀態檢查的響應需要等待的時間。如果後端ECS在指定的時間內沒有正確響應，則判定為健康檢查失敗。 範圍是1-300秒，UDP監聽的預設值為10秒，HTTP/HTTPS/TCP監聽的預設值為5秒。

健康檢查配置	說明
健康檢查間隔	進行健康檢查的時間間隔。 LVS叢集內所有節點，都會獨立、並行地遵循該屬性對後端ECS進行健康檢查。由於各LVS節點的檢查時間並不同步，所以，如果從後端某一ECS上進行單獨統計，會發現來自負載平衡的健康檢查請求在時間上並不會遵循上述時間間隔。 範圍是1-50秒，UDP監聽的預設值為5秒，HTTP/HTTPS/TCP監聽的預設值為2秒。
不健康閾值	同一LVS節點伺服器針對同一ECS伺服器，從成功到失敗的連續健康檢查失敗次數。 可選值2-10，預設為3次。
健康閾值	同一LVS節點伺服器針對同一ECS伺服器，從失敗到成功的連續健康檢查成功次數。 可選值 2-10，預設為3次。

健康檢查配置	說明
健康檢查請求和健康檢查返回結果	為UDP監聽配置健康檢查時，您可以在健康檢查請求中輸入請求的內容（比如youraccountID），在健康檢查返回結果中輸入預期的返回結果（比如slb123）。 同時在後端伺服器的應用邏輯中加入相應的健康檢查應答邏輯，如收到youraccountID的請求時，回應slb123。 此時，當負載平衡收到後端伺服器發來的正確響應時，則認為健康檢查成功，否則認為健康檢查失敗。此方式能最大程度確保健康檢查的可靠性。



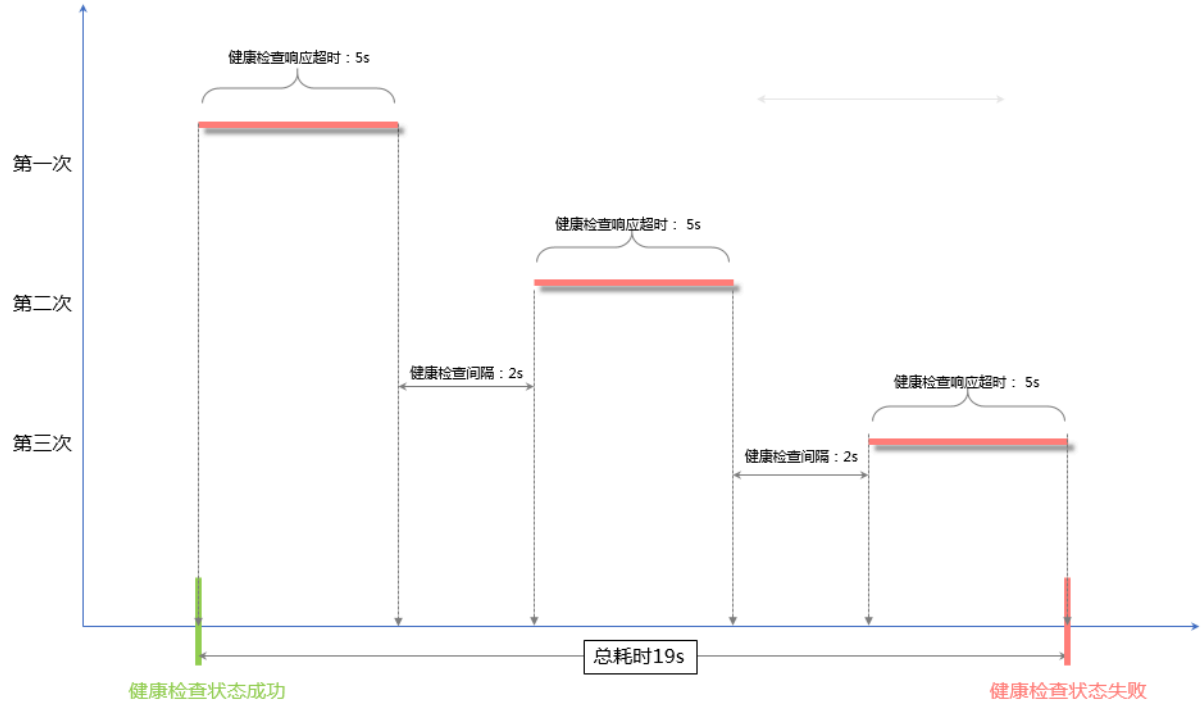
健康檢查響應逾時和健康檢查間隔樣本

以如下健康檢查配置為例：

- 響應逾時時間：5秒
- 健康檢查間隔：2秒
- 健康閾值：3次
- 不健康閾值：3次

健康檢查失敗時間窗=響應逾時時間×不健康閾值+檢查間隔×(不健康閾值-1)，即5×3+2×（3-1）=19s。

從健康狀態到不健康狀態的檢查過程如下圖所示：

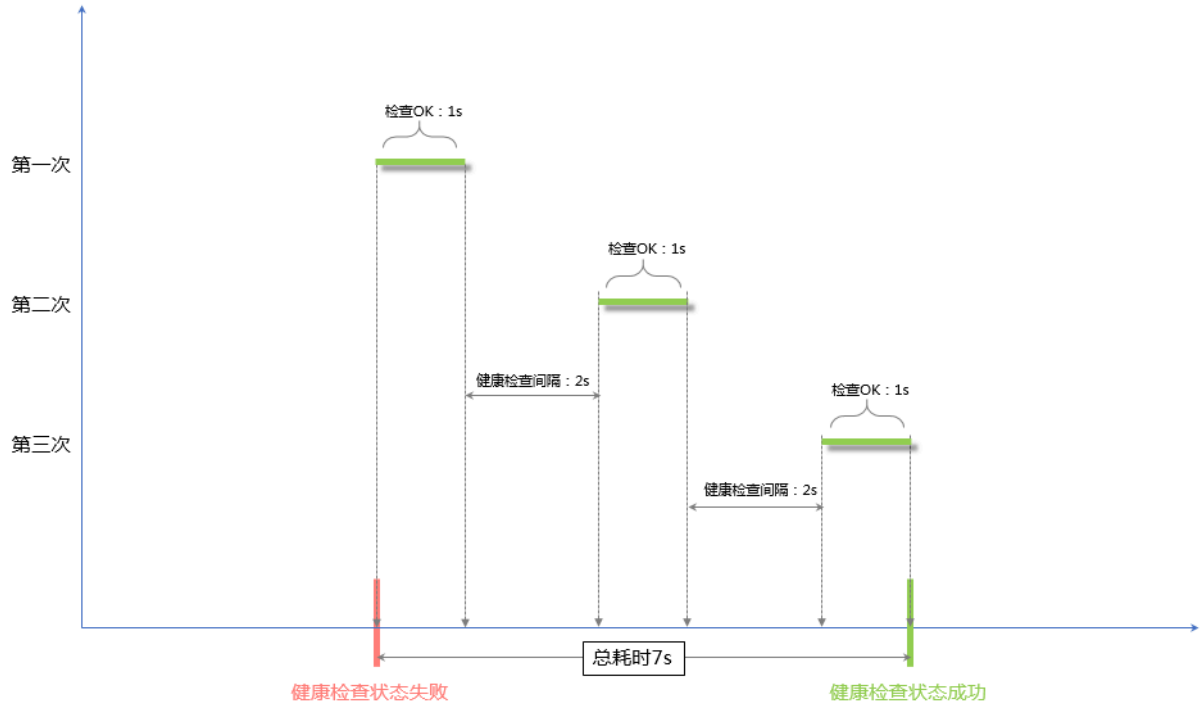


健康檢查成功時間窗= (健康檢查成功回應時間×健康閾值)+檢查間隔×(健康閾值-1)，即（1×3）+2×（3-1）=7s。

说明:

健康檢查成功回應時間是一次健康檢查請求從發出到響應的時間。當採用TCP方式健康檢查時，由於僅探測通信埠是否存活，因此該時間非常短，幾乎可以忽略不計。當採用HTTP方式健康檢查時，該時間取決於應用伺服器的效能和負載，但通常都在秒級以內。

從不健康狀態到健康的狀態檢查過程如下圖所示（假設伺服器響應健康檢查請求需要耗時1s）：



HTTP健康檢查中網域名稱的設定

當使用HTTP方式進行健康檢查時，可以設定健康檢查的網域名稱，但並非強制選項。因為有些應用伺服器會對請求中的host欄位做校驗，即要求要求標頭中必須存在host欄位。如果在健康檢查中配置了網域名稱，則SLB會將網域名稱配置到host欄位中去，反之，如果沒有佈建網域名，SLB則不會在請求中附帶host欄位，因此健康檢查請求就會被伺服器拒絕，可能導致健康檢查失敗。綜上原因，如果您的應用伺服器需要校驗請求的host欄位校，那麼則需要配置相關的網域名稱，確保健康檢查正常工作。

3 關閉健全狀態檢查

您可以關閉健全狀態檢查功能，但關閉健全狀態檢查後，當後端某個ECS健全狀態檢查出現異常時，負載平衡還是會把請求轉寄到該異常的ECS上，造成部分業務不可訪問。所以建議一般情況下不要關閉健全狀態檢查。

背景信息

说明:

只有HTTP和HTTPS監聽支援關閉健全狀態檢查。UDP和TCP監聽無法關閉健全狀態檢查。

操作步驟

1. 登入負載平衡管理主控台。
2. 在執行個體管理頁面，單擊負載平衡執行個體的ID。
3. 在監聽頁簽下，單擊監聽操作列的配置。
4. 在配置監聽對話方塊，單擊下一步至健全狀態檢查。
5. 關閉健全狀態檢查開關，單擊下一步，單擊提交，然後單擊確定。