目录

目录 1
实例概述 3
实例网络类型 3
协议版本 3
创建应用型负载均衡 3
前提条件 3
创建实例 3
管理应用型负载均衡 3
查询应用型负载均衡实例 3
关闭、开启应用型负载均衡实例 4
删除应用型负载均衡实例 4
绑定弹性ip 4
解绑弹性ip 4
修改功能版本 4
添加http监听器 4
前提条件 4
创建监听器 4
添加https监听器 4
前提条件 5
创建监听器 5
个性化配置 5
个性化配置项及参数 5
配置示例 6
转发策略 6
转发条件的域名配置规则 6
转发条件的路径配置规则 6
重定向配置 7
使用场景 7
使用限制 7
配置重定向 7
重定向配置举例 7
前提条件 7
步骤一：配置HTTPS监听的转发策略 7
步骤二：配置HTTP重定向HTTPS 7
创建和管理服务器组 8
创建服务器组 8
访问控制 8
访问控制 8
新建ACL 8
监听器配置acl 8
tls安全策略说明 9
健康检查 9
创建健康检查 9
监控指标说明 10
负载均衡实例维度 10
7层监听器（HTTP/HTTPS）维度 11
证书管理 11
前提条件 11
添加证书 11
更换证书 11

实例概述

应用型负载均衡ALB实例接收来自客户端的请求，并按照监听规则将请求分发至后端服务器。使用ALB服务，您需要创建一个ALB实例，在实例中添加监听和后端服务器。

实例网络类型

公网类型ALB

公网类型的ALB实例负责处理来自公网的访问请求，通过弹性公网IP提供公网能力，将来自互联网的访问请求按照监听规则转发至后端服务器。

内网类型ALB 仅北京机房支持

协议版本

ALB实例的协议版本支持IPv4、IPv6版本

创建应用型负载均衡

前提条件

您已经创建了虚拟私有网络VPC 请确认您已经申请应用型负载均衡使用权限

创建实例

1. 登录应用型负载均衡控制台。
2. 在**实例**页面，单击新建**负载均衡**。
3. 在**应用型负载均衡**购买页面，完成以下配置，单击**下一步**。

配置	说明
数据中心	选择实例所属的地域。
功能版本	支持标准版和高阶版。 标准版：单实例限制10w qps。 高阶版：单实例限制100w qps。
网络类型	选择实例网络类型，系统会根据您的选择分配私网或公网服务地址。 公网类型：公网ALB通过弹性公网IP提供公网能力，选择公网将会收取弹性公网IP的实例费、带宽或流量费用。 私网类型：私网ALB实例会分配一个私网IP，支持云上VPC内的资源访问ALB。
所属虚拟私有网络	选择实例所属的VPC。
负载均衡版本	选择实例的协议版本。 IPv4：表示ALB实例仅支持客户端使用IPv4地址访问。 IPv6：表示ALB实例支持客户端使用IPv6地址访问。目前仅支持转发至IPv4的后端服务。
实例名称	输入自定义实例名称。

4. 可选择绑定弹性IP或不绑定弹性IP，单击**下一步** 。
5. 配置确认无误，单击**购买** 。

管理应用型负载均衡

查询应用型负载均衡实例

1. 登录应用型负载均衡ALB控制台。
2. 在**实例**页面，单击目标实例ID。
3. 单击**实例详情**页签，查看实例详细信息。

- 实例状态包含：active创建成功、error创建错误，building创建中，deleting删除中。building、deleting状态时不允许进行任何操作。

关闭、开启应用型负载均衡实例

1. 登录应用型负载均衡ALB控制台。
2. 在**实例**页面，单击目标实例ID。
3. 单击**实例详情**页签，单击**关闭/开启** 。关闭负载均衡后，负载均衡不可继续使用。

删除应用型负载均衡实例

1. 登录应用型负载均衡ALB控制台。
2. 在**实例**页面，找到目标实例，单击**删除** 。
   - 请先删除负载均衡下所有监听器，再删除负载均衡实例。

绑定弹性ip

前提条件
您已经创建弹性ip实例。具体操作，请参见创建弹性ip。

1. 登录应用型负载均衡ALB控制台。
2. 在**实例**页面，找到目标实例，单击操作列**绑定** 。
3. 选择目标eip，单击**确定**。

解绑弹性ip

1. 登录弹性IP控制台。
2. 在**实例**页面，找到目标实例，单击操作列解绑。

修改功能版本

1. 登录应用型负载均衡ALB控制台。
2. 在**实例**页面，找到目标实例，单击操作列**修改** 。
3. 选择高阶版，单机**购买**。 标准版QPS限制为10w ，高阶版QPS限制为100w

添加http监听器

您可以在负载均衡实例上添加一个 HTTP 监听器转发来自客户端的 HTTP 协议请求。

前提条件

您已经创建ALB实例。具体操作，请参见创建应用型负载均衡。

创建监听器

1. 登录应用型负载均衡控制台。
2. 进入监听器页面，单击新建**监听器**。
3. 在配置监听器界面，完成以下配置，然后单击**确定**。

监听配置	说明
前端协议	选择监听器的协议类型。
后端协议	后端协议是指ALB与后端服务之间的协议，支持HTTP1.0和支持HTTP1.1。
端口	输入用来接收请求并向后端服务器进行请求转发的监听端口，端口范围为1~65535。在同一个负载均衡实例内，监听端口不可重复。22、111、179、65001-65535为系统保留，不允许使用。
转发方式	轮询：依据负载云服务器的权重，请求轮流发送。 最小连接数：优先将请求发给拥有最小连接数的后端服务。
会话保持	使来自同一客户端的请求被转发到同一台后端服务器上。ALB开启会话保持后，需要选择Cookie的处理方式 - 植入Cookie：客户端第一次访问时，ALB会在返回请求中植入Cookie（即在HTTP/HTTPS响应报文中插入SERVERID），下次客户端携带此Cookie访问，负载均衡服务会将请求定向转发给之前记录到的后端服务器上。 - 重写Cookie：当ALB发现用户自定义了Cookie，将会对原来的Cookie进行重写，下次客户端携带新的Cookie访问，ALB会将请求定向转发给之前记录的后端服务器。
访问控制	可以选择关联一个负载均衡ACL策略。
健康检查	请参见健康检查文档。
个性化配置	请参见个性化配置文档。

添加https监听器

HTTPS协议适用于需要加密传输的应用。您可以创建使用加密连接的HTTPS监听转发来自HTTPS协议的请求。

前提条件

您已经创建ALB实例。具体操作，请参见创建应用型负载均衡。

创建监听器

1. 登录应用型负载均衡控制台。
2. 进入监听器页面，单击新建**监听器**。
3. 在配置监听器界面，完成以下配置，然后单击确定。

监听配置	说明
前端协议	选择监听器的协议类型。
证书	用来证明服务器的身份。您可在负载均衡证书页面上传服务器证书，ALB获取该证书并使用。
TLS安全策略	TLS安全策略包含HTTPS可选的TLS协议版本和配套的加密算法套件，更多信息，请参见TLS安全策略说明。
启用HTTP/2	前向协议，选择是否开启HTTP/2。
后端协议	后端协议是指ALB与后端服务之间的协议，支持HTTP1.0和支持HTTP1.1。
端口	输入用来接收请求并向后端服务器进行请求转发的监听端口，端口范围为1~65535。 在同一个负载均衡实例内，监听端口不可重复。22、111、179、65001-65535为系统保留，不允许使用。
转发方式	轮询：依据负载云服务器的权重，请求轮流发送。 最小连接数：优先将请求发给拥有最小连接数的后端服务。
会话保持	使来自同一客户端的请求被转发到同一台后端服务器上。ALB开启会话保持后，需要选择Cookie的处理方式，有植入Cookie和重写Cookie两种处理方式。 - 植入Cookie：客户端第一次访问时，ALB会在返回请求中植入Cookie（即在HTTP/HTTPS响应报文中插入SERVERID），下次客户端携带此Cookie访问，负载均衡服务会将请求定向转发给之前记录到的后端服务器上。 - 重写Cookie：当ALB发现用户自定义了Cookie，将会对原来的Cookie进行重写，下次客户端携带新的Cookie访问，ALB会将请求定向转发给之前记录的后端服务器。
访问控制	可以选择关联一个负载均衡ACL策略。
健康检查	请参见健康检查文档。
个性化配置	请参见个性化配置文档。

个性化配置

个性化配置项及参数

配置字段	类型	是否可缺省	默认值	参数范围	说明
client_header_timeout	Integer	是	600s	[30-600]单位s	获取到 Client 请求头部的超时时间, 超时返回408。
client_header_buffer_size	Integer	是	1k	[1-256]单位k	存放 Client 请求头部的默认 Buffer 大小。
client_body_timeout	Integer	是	600s	[30-600]单位s	获取 Client 请求 Body 的超时时间，不是获取整个 Body 的持续时间，而是指空闲一段时间没有传输数据的超时时间，超时返回408。
client_max_body_size	Integer	是	51200M	[1-51200]单位M	- 默认配置范围为1M-256M，直接配置即可。- 最大支持10240M，即10G。当 client_max_body_size 的配置范围大于256M时，必须设置 proxy_request_buffering 的值为 off。
keepalive_timeout	Integer	是	300s	[0-900]单位s	Client-Server 长连接保持时间，设置为0则禁用长连接
proxy_connect_timeout	Integer	是	5s	[4-120]单位s	upstream 后端连接超时时间。nginx建议不超过75
proxy_read_timeout	Integer	是	60s	[1-3600]单位s	读取 upstream 后端响应超时时间。

proxy_send_timeout	Integer	是	60s	[30-3600]单位s	向 upstream 后端发送请求的超时时间。
proxy_request_buffering	String	是	off	on，off	- on 表示缓存客户端请求体：CLB 会缓存请求，全部接收完成后再分块转发给后端 CVM。- off 表示不缓存客户端请求体：CLB 收到请求后，立即转发给后端 CVM，此时会导致后端 CVM 有一定性能压力。
ssl_early_data	String	是	off	on；off	只有选择tls1.3才可以选择on
x_forwarded_for	String	是	true	true；false	通过x_forwarded_for头字段获取客户端IP
x_forwarded_proto	String	是	true	true；false	通过x_forwarded_proto字段获取负载均衡实例的监听协议
x_forwarded_port	String	是	true	true；false	通过x_forwarded_port字段获取负载均衡实例的监听端口
x_forwarded_client_port	String	是	false	true；false	通过x_forwarded_client_port字段获取访问负载均衡实例的客户端端口
x_forwarded_slb_id	String	是	false	true；false	通过x_forwarded_slb_id字段获取负载均衡实例ID
max_fails	Integer	是	1f	[0-10000]单位f	响应请求的失败次数（值为0时表示关闭代答）
fail_timeout	Integer	是	10s	[0-10000]单位s	响应请求的失败时间

配置示例

1. 登录负载均衡控制台，在在配置监听器界面，打开个性化配置开关。
2. 输入配置项和参数，需以;结尾，配置完成后，点击确定即可创建监听器。

注意：

- 所有未在个性化配置代码配置中配置的配置项将全部置为默认值。如：第一次配置时将proxy_connect_timeout设置为10s，第二次配置时将本行配置删除，点击确认编辑监听器后会重新置为默认值5s。
- 若想将 proxy_request_buffering 设置成为 on，必须先设置client_max_body_size小于256M，若没有此配置项创建监听器会报错。
- 若打开开关后未填写任何配置项，下次进入页面，开关会置为关闭状态。
- 配置项填写错误或参数值错误会实时标红，请按照文档检查配置。
- 若同一行结尾填写多个;会自动处理为一个;，不影响使用。

转发策略

您可以定义ALB实例的监听转发规则，将客户端请求按照指定规则转发到一个或多个服务器组中的一个或多个后端服务器，以及将后端响应结果按照指定规则转发给客户端。

转发条件的域名配置规则

域名配置规则支持精准匹配、通配符匹配和正则表达式。

配置规则	说明	举例
精准匹配	请求的域名和设定的域名需完全一致。	www.a.com
通配符匹配	请求的域名和设定的域名除通配符外需完全一致。	*.a.com

转发条件的路径配置规则

路径配置规则支持精准匹配、通配符匹配和正则表达式。	配置规则	说明	举例
精准匹配	请求的路径和设定路径需完全一致。	=/a	
前缀匹配	请求的路径匹配已设定路径开头的URL。匹配完如果还有正则匹配，则会继续匹配正则	/a	
通配符匹配	请求的路径和设定的路径除通配符外需完全一致。	/a/*	
正则匹配	请求路径和设定的路径根据正则表达式匹配。 ~ 开头表示区分大小写的正则匹配 ~* 开头表示不区分大小写的正则匹配	~^/a/(.*) ~*^/a/(.*)	

默认规则匹配	通用匹配，如果没有其它匹配,会匹配到此路径	/

重定向配置

ALB负载均衡支持重定向功能，该功能支持用户在ALB实例的HTTP/HTTPS监听器的转发策略上配置重定向。

使用场景

- 当企业要求强制HTTPS加密协议访问时，可将之前的HTTP请求重定向至HTTPS请求；
- Web业务需要临时下线或长期下线等，需将原有页面重定向到新页面，否则会让用户请求失败，返回404/503等错误；

使用限制

- 若监听上已有转发策略配置了重定向，则不允许作为重定向的目的监听器；

配置重定向

1. 登录应用型负载均衡控制台。
2. 进入监听器页面，单击需要重定向的HTTP/HTTPS监听器右侧操作列新建转发策略按钮，弹出新建转发策略对话框。
3. 配置以下参数：
    1. 域名：目前仅支持添加一个域名；
    2. 路径：目前仅支持添加一条路径：
    3. 动作：选择动作为重定向；
    4. 重定向状态码：选择重定向的方式
        - 301：当用户请求的网址资源永远的迁移到了新的网址，可以使用301，使得用户访问旧网址时直接替换成重定向网址。
        - 302：临时重定向，当用户请求的网址资源临时改变了位置，可以使用临时重定向，但是302只能实现GET到GET的重定向，非GET请求可能会重定向为GET请求。
        - 307：临时重定向，当用户请求的网址资源临时改变了位置，可以使用临时重定向，307可以保持请求方法不变，如POST请求仍旧重定向为POST请求。
    5. 目标监听器：选择需要重定向的目标监听器；请确保目标监听器中存在与请求路径一致的转发策略或存在路径为/的转发策略；
4. 单击确定按钮，完成配置。

重定向配置举例

下面以http重定向到https监听为例介绍如何使用重定向功能,如请求http://example.com/test，都将重定向请求到https://example.com/test;

前提条件

- 已创建ALB实例
- 已创建HTTP监听
- 已创建HTTPS监听

步骤一：配置HTTPS监听的转发策略

1. 单击HTTPS监听器右侧操作列新建转发策略按钮，弹出新建转发策略对话框。
2. 配置以下参数：
    1. 路径设置为“/test”;
    2. 动作设置为转发;
    3. 服务器组：选择处理后端请求的服务器组;
3. 单击确定按钮，完成配置。

步骤二：配置HTTP重定向HTTPS

4. 单击HTTPS监听器右侧操作列新建转发策略按钮，弹出新建转发策略对话框。
5. 配置以下参数：
    1. 域名设置为example.com;
    2. 路径设置为“/test”;
    3. 动作设置为重定向;

4. 状态码可选301；
5. 目标监听器为上一步骤配置的https监听；

6. 单击确定按钮，完成配置。

创建和管理服务器组

您可以通过创建服务器组的方式，请求路由到一个或多个后端服务器。在创建每个监听的转发规则时，指定服务器组和转发条件。满足转发规则的转发条件时，流量会被转发到相应的服务器组。

创建服务器组

1. 登录应用型负载均衡ALB控制台。
2. 在左侧导航栏，选择应用型负载均衡ALB > 服务器组。
3. 在服务器组页面，单击新建服务器组。
4. 在创建服务器组对话框，完成以下配置，然后单击创建。

配置	说明
服务器组名称	输入自定义服务器组名称。
虚拟私有网络	从VPC下拉列表中选择一个VPC，该服务器属于所选VPC。
服务器组类型	选择一种服务器组类型 服务器： 云上资源，虚拟机或裸金属类型 边界网关：云下资源，专线或kis类型
开启后端长连接	选择是否开启后端长连接，默认为短链接。 长连接：当开启后端长连接后，ALB到后端服务器之间会维持一定数量的TCP长连接，当新请求到达时，如果有空闲的TCP长连接，ALB优先使用TCP长连接转发请求到后端服务器，从而减少TCP握手建连次数，减轻后端服务器压力。 自适应：自适应client的connection header，判断后向为长连接或者短连接
选择VPC	筛选功能，ALB支持挂载其他VPC后端服务器，帮助客户迅速筛选到目标VPC

5. 添加后端服务器
   - 后端服务为服务器类型时，选择目标服务器，填写端口、权重，点击添加，即完成添加服务器动作。
   - 后端服务为边界网关时，需手动填写对端ip、端口、权重，点击添加，即完成添加服务器动作。

访问控制

访问控制

通过设置入方向的允许或拒绝规则，对客户端请求精确控制，管理请求转发。
可以针对不同的监听设置访问白名单或黑名单：

- **白名单**：允许特定IP或IP段访问负载均衡。仅转发来自所选访问控制策略组中设置的IP地址或地址段的请求，白名单适用于只允许特定IP访问的场景。
- **黑名单**：禁止特定IP访问负载均衡。不会转发来自所选访问控制策略组中设置的IP地址或地址段，黑名单适用于只限制某些特定IP访问的场景。

新建ACL

1. 登录负载均衡控制台。
2. 在左侧导航栏，选择**访问控制**。
3. 在**访问控制**页面，单击新建ACL。
4. 在**创建访问控制策略组**对话框，完成以下配置，然后单击**确定**。

配置	说明
优先级	取值范围为1~999，数值越小，代表优先级越高。
协议	匹配流量的协议类型，支持IP。
行为	允许或拒绝。
源IP	流量的源 IP 或源网段，支持 IP 或 CIDR。为什么端口没意义。

监听器配置acl

1. 进入监听器页面，选中目标监听器，点击**配置ACL**。

2. 在关联访问控制列可以选择想要关联的访问控制，点击**确定**。

tls安全策略说明

TLS安全策略包含HTTPS可选的TLS协议版本和配套的加密算法套件。TLS协议版本越高，HTTPS通信的安全性越高，但是相较于低版本TLS协议，高版本TLS协议对浏览器的兼容性较差。

安全策略	支持的TLS版本	支持的加密算法套件
TlsCipherPolicy1.0	TLSv1.0、TLSv1.1、TLSv1.2	**TLSv1.0和v1.1支持：** - ECDHE-RSA-AES128-CBC-SHA - ECDHE-RSA-AES256-CBC-SHA - RSA-AES128-CBC-SHA - RSA-AES256-CBC-SHA - RSA-3DES-EDE-CBC-SHA - ECDHE-ECDSA-AES256-SHA - ECDHE-ECDSA-AES256-GCM-SHA384 - ECDHE-ECDSA-AES128-SHA - ECDHE-ECDSA-AES128-GCM-SHA256 **TLSv1.2支持：** - ECDHE-RSA--AES128-CBC-SHA - ECDHE-RSA-AES256-CBC-SHA - RSA-AES128-CBC-SHA - RSA-AES256-CBC-SHA - RSA-3DES-EDE-CBC-SHA - ECDHE-RSA-AES128-GCM-SHA256 - ECDHE-RSA-AES256-GCM-SHA384 - ECDHE RSA-AES128-CBC-SHA256 - ECDHE-RSA-AES-256-CBC-SHA384 - RSA-AES128-GCM-SHA256 - RSA-AES256-GCM-SHA384 - RSA-AES128-CBC-SHA256 - RSA-AES256-CBC-SHA256 - ECDHE-ECDSA-AES256-SHA - ECDHE-ECDSA-AES256-GCM-SHA384 - ECDHE-ECDSA-AES128-SHA - ECDHE-ECDSA-AES128-GCM-SHA256 **TLSv1.3支持：** - AES-256-GCM-SHA384 - CHACHA20-POLY1305-SHA256 - AES-128-GCM-SHA256
TlsCipherPolicy1.1	TLSv1.1、TLSv1.2	
TlsCipherPolicy1.2	TLSv1.2	
TlsCipherPolicy1.2-strict	TLSv1.2-strict	TLSv1.2-strict - ECDHE-RSA-AES128-GCM-SHA256 - ECDHE-RSA-AES256-GCM-SHA384 - ECDHE-RSA-AES128-SHA256 - ECDHE-RSA-AES128-SHA - ECDHE-ECDSA-AES256-SHA - ECDHE-ECDSA-AES256-GCM-SHA384 - ECDHE-ECDSA-AES128-SHA - ECDHE-ECDSA-AES128-GCM-SHA256
TlsCipherPolicy1.2-most-strict-with1.3	TLSv1.0、TLSv1.1、TLSv1.2、TLSv1.3	

健康检查

您可以配置健康检查来检查服务器组的运行状况，从而判断服务器的业务可用性。本文为您介绍如何创建、编辑和删除健康检查。

创建健康检查

方式一：创建监听器界面配置健康检查

1. 登录应用型负载均衡ALB控制台。
2. 进入监听器页面，单击新建**监听器**。点击开启健康检查，完成以下参数的配置，然后单击**创建**。

健康检查配置	说明

协议	选择健康检查协议类型，目前仅支持默认协议HTTP。 **HTTP**：通过发送HEAD请求模拟浏览器的访问行为来检查服务器应用是否健康。
健康检查方法	选择一种健康检查方法，目前仅支持默认HEAD方法。 **HEAD**：HTTP监听健康检查默认采用HEAD方法。请确保您的后端服务器支持HEAD请求。如果您的后端应用服务器不支持HEAD方法或HEAD方法被禁用，则可能会出现健康检查失败，此时可以使用GET方法来进行健康检查。
健康检查HTTP协议版本	继承监听器选择的后端协议版本
健康检查路径路径	输入健康检查页面的URL，建议对静态页面进行检查。 HTTP健康检查默认由负载均衡系统使用后端ECS内网IP地址向该服务器应用配置的缺省首页发起HTTP Head请求。如果您用来进行健康检查的页面并不是应用服务器的缺省首页，需要指定具体的检查路径。
健康检查域名	输入健康检查的域名。 默认使用后端服务器的内网IP地址作为健康检查的域名。如果您需要指定一个域名，请输入域名。
响应超时时间	接收健康检查的响应需要等待的时间。如果后端ECS在指定的时间内没有正确响应，则判定为健康检查失败。取值范围：1~3600秒，默认值为4秒。
健康检查间隔	输入进行健康检查的时间间隔。取值范围：1~1000秒，默认值为5秒。
健康阈值	健康检查连续成功多少次后，将后端服务器的健康检查状态由失败判定为成功的次数。取值范围：1~10，默认为6次。
不健康阈值	健康检查连续失败多少次后，将后端服务器的健康检查状态由成功判定为失败的次数。取值范围：1~10，默认为4次。

监控指标说明

本文为您介绍应用型负载均衡ALB的监控项。

目前公网负载均衡实例和私网负载均衡实例支持如下两个维度监控项（如无特殊说明，采样周期均为30s）：

- 负载均衡实例维度
- 监听器维度

您可以在控制台>负载均衡或者云监控查看ALB的相关指标，负载均衡不同维度的具体监控指标如下：

负载均衡实例维度

监控指标(Metric)	指标名称	指标含义	单位
slb.bps.in	入网带宽	客户端访问负载均衡的入网带宽。	bps
slb.bps.out	出网带宽	负载均衡响应客户端请求的出网带宽。	bps
slb.pps.in	每秒流入包数	负载均衡每秒接收到的数据包的个数。	个
slb.pps.out	每秒流出包数	负载均衡每秒发出的数据包的个数。	个
slb.cps	每秒新建连接数	从客户端到负载均衡每秒的新建连接数。	个
slb.activeconn	活跃连接数	在采样周期内的某一时刻，从客户端到负载均衡的活跃连接数。	个
slb.inactiveconn	不活跃连接数	在采样周期内的某一时刻，从客户端到负载均衡的不活跃连接数。	个
slb.concurrentconn	并发连接数	在采样周期内的某一时刻，从客户端到负载均衡的并发连接数。	个
slb.drop.bps.in	丢弃入流量	客户端访问负载均衡时丢弃的带宽。	bps
slb.drop.bps.out	丢弃出流量	负载均衡响应客户端请求丢弃的带宽。	bps
slb.drop.bps.acl	ACL丢弃流量	负载均衡匹配ACL源IP丢弃的带宽。	bps
slb.drop.pps.in	丢弃流入数据包	客户端访问负载均衡时丢弃的数据包。	pps
slb.drop.pps.out	丢弃流出数据包	负载均衡响应客户端请求丢弃的数据包。	pps
slb.drop.pps.acl	ACL丢弃数据包	负载均衡匹配ACL源IP丢弃的数据包。	pps
slb.req_rate	7层协议QPS	统计负载均衡当前7层查询速率，负载均衡每秒接受到的请求数。	qps
slb.rs_init	健康检查未完成的rs数量	健康检查未完成的rs数量	个
slb.rs_disable	健康检查未开启的rs数量	健康检查未开启的rs数量（该指标目前只支持四层负载均衡）	个
slb.rs_up	健康检查状态为健康的rs数量	健康检查未完成的rs数量	个
slb.rs_down	健康检查状态为不健康的rs数量	健康检查未开启的rs数量	个

7层监听器（HTTP/HTTPS）维度

监控指标(Metric)	指标名称	指标含义	单位
listener.bps.in	入网带宽	监听器入网带宽，采样周期内平均值	bps
listener.bps.out	出网带宽	监听器出网带宽，采样周期内平均值	bps
listener.pps.in	每秒流入包数	监听器每秒流入包数，采样周期内包总数平均值	个
listener.pps.out	每秒流出包数	监听器每秒流出包数，采样周期内包总数平均值	个
listener.cps	每秒新建连接数	监听器每秒新建连接数，采样周期内新建连接数平均值	个
listener.activeconn	当前活跃连接数	在采样周期内的某一时刻，从客户端到监听器上的活跃连接数。	个
listener.inactiveconn	当前未活跃连接数	在采样周期内的某一时刻，从客户端到监听器上的未活跃连接数。	个
listener.concurrentconn	并发连接数	在采样周期内的某一时刻，从客户端到监听器上的并发连接数。	个
listener.httpcode.2xx	监听器返回的2XX的状态码数量	采样周期内监听器返回的2XX的状态码数量。	个
listener.httpcode.3xx	监听器返回的3XX的状态码数量	采样周期内监听器返回的3XX的状态码数量。	个
listener.httpcode.4xx	监听器返回的4XX的状态码数量	采样周期内监听器返回的4XX的状态码数量。	个
listener.httpcode.5xx	监听器返回的5XX的状态码数量	采样周期内监听器返回的5XX的状态码数量。	个
listener.httpcode.backend.2xx	真实服务器返回的2XX的状态码数量	采样周期内真实服务器返回的2XX的状态码数量。	个
listener.httpcode.backend.4xx	真实服务器返回的4XX的状态码数量	采样周期内真实服务器返回的4XX的状态码数量。	个
listener.httpcode.backend.5xx	真实服务器返回的5XX的状态码数量	采样周期内真实服务器返回的5XX的状态码数量。	个
listener.latency	HTTP/HTTPS请求到后端的延时	从监听器将请求转发给后端服务器开始，到监听器收到后端服务器返回响应的头部header为止的延时。	ms
listener.requestcount	7层监听QPS	监听器每秒接受到的请求数。	qps

证书管理

证书主要分为默认证书和扩展证书，每一个HTTPS监听器都有一个扩展证书界面，包含了监听器的扩展证书，监听器的默认证书不会展示在扩展证书页面。您可以在扩展证书界面通过添加扩展证书增加监听关联的证书，添加到扩展证书的证书，不能域名完全相同，有匹配的规则的证书,不能从扩展证书中移出。

- 默认证书：创建HTTPS监听器时必选一个默认证书，可以在修改监听器页面对默认证书进行修改。
- 扩展证书：当后端服务器绑定多个证书时，可通过SNI功能上传多个扩展证书实现同一个HTTPS监听器根据多个域名自动选择证书来完成HTTPS认证和访问后端服务。

系统默认支持SNI功能，上传扩展证书后，客户端在发起SSL握手请求时就提交请求的域名信息，负载均衡收到SSL请求后，会根据域名去查找证书，如果找到域名对应的证书，则返回该证书；如果没有找到域名对应的证书，则返回默认证书。

前提条件

您已在证书中心购买或上传服务器证书。

添加证书

1. 登录应用型负载均衡ALB控制台。
2. 在监听器页面，找到目标HTTPS实例，单击实例ID。
3. 单击**扩展证书**页签，进入扩展证书页面
4. 单击添加扩展证书，上传对应证书，单击"确定"。 说明：一个负载均衡的监听器最多支持100个SNI证书

更换证书

支持两种更换证书的方式 一、全量更新证书关联的全部监听器证书。平滑更换，不会影响业务。

1. 登录负载均衡证书控制台。
2. 点击**更新**。

二、仅更新部分监听器的证书。平滑更换，不会影响业务。

1. 登录应用型负载均衡ALB控制台。
2. 在监听器页面，找到目标HTTPS实例，单击实例ID。
3. 单击**扩展证书**页签，进入扩展证书页面。
4. 点击**更换**。