

Alibaba Cloud

Anti-DDoS Announcements & Updates

Document Version: 20211206

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 .
<code>Courier font</code>	Courier font is used for commands	Run the <code>cd /d C:/window</code> command to enter the Windows system folder.
<i>Italic</i>	Italic formatting is used for parameters and variables.	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] or [a b]	This format is used for an optional value, where only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	This format is used for a required value, where only one item can be selected.	<code>switch {active stand}</code>

Table of Contents

1. Release notes	06
2. System upgrades	19
2.1. [System upgrade] Anti-DDoS Premium is upgraded on July ...	19
2.2. [System upgrade] Anti-DDoS Premium is upgraded on June...	19
2.3. [System upgrade] Anti-DDoS Pro is upgraded on June 4, 2...	19
2.4. [System upgrade] Anti-DDoS Premium is upgraded on May...	20
2.5. [System upgrade] Anti-DDoS Premium is upgraded in April...	20
2.6. [System upgrade] Anti-DDoS Premium is upgraded on April...	20
2.7. [System upgrade] Anti-DDoS Premium is upgraded on April...	21
2.8. [System upgrade] Anti-DDoS Premium is upgraded on Febr...	21
2.9. [System upgrade] Anti-DDoS Pro is upgraded on January 1...	21
2.10. [System upgrade] Anti-DDoS Pro of the previous version i...	22
2.11. [System upgrade] Anti-DDoS Pro no longer provides traffic...	22
2.12. [System upgrade] Anti-DDoS Pro of the previous version i...	23
2.13. [System upgrade] Anti-DDoS Premium is upgraded on Dec...	23
2.14. [System upgrade] Anti-DDoS Premium and GameShield ar...	23
2.15. [System upgrade] Anti-DDoS Pro is upgraded on Decembe...	24
2.16. [System upgrade] Anti-DDoS Pro of the previous version i...	24
2.17. [System upgrade] Anti-DDoS Pro is upgraded on Decembe...	25
2.18. [System upgrade] Anti-DDoS Premium is upgraded on Dec...	25
2.19. [System upgrade] Anti-DDoS Pro of the previous version i...	25
2.20. [System upgrade] Anti-DDoS Premium is upgraded on De...	26
2.21. [System upgrade] Anti-DDoS Premium is upgraded on No...	26
2.22. [System upgrade] Anti-DDoS Premium is upgraded on No...	26
2.23. [System upgrade] Anti-DDoS Premium is upgraded on No...	27
2.24. [System upgrade] Anti-DDoS Premium is upgraded on Oc...	27

2.25. [System upgrade] Anti-DDoS Premium is upgraded on Ma...	27
3.Updates	29
3.1. [Update] The protection bandwidth of Anti-DDoS Pro of th...	29
3.2. [Update] The protection bandwidth of Anti-DDoS Pro of t...	29
4.Product notices	30
4.1. [Notice] APIs in the previous version of Anti-DDoS Pro are...	30
4.2. [Notice] Anti-DDoS Pro of the previous version is discontin...	30
4.3. [Notice] The Security Reports feature in the previous versi...	30
4.4. [Notice] Anti-DDoS Pro of the previous version is discontin...	31

1. Release notes


This topic describes the release notes for Anti-DDoS Pro, Anti-DDoS Premium, and Anti-DDoS Origin and provides links to the relevant references.

2021

Release date	Applicable service	Feature	Description	References
2021-10-18	Anti-DDoS Pro	Investigation	Operation logs within the previous 180 days instead of 30 days can be queried. You can use the logs to track and analyze important operations.	View operations logs
2021-09-30	Anti-DDoS Pro and Anti-DDoS Premium	Provisioning	Ports in the range from port 80 to port 65535 can be added. This extends protection for services over different ports.	Add a website
2021-09-30	Anti-DDoS Pro and Anti-DDoS Premium	Provisioning	<p>Online Certificate Status Protocol (OCSP) can be enabled when you add a domain name to Anti-DDoS Pro or Anti-DDoS Premium.</p> <p>If you enable OCSP for an HTTPS service that is added to Anti-DDoS Pro or Anti-DDoS Premium, Anti-DDoS Pro or Anti-DDoS Premium runs OCSP queries and caches the query results. When a client initiates a Transport Layer Security (TLS) handshake with the origin server, Anti-DDoS Pro or Anti-DDoS Premium returns the OCSP details and the certificate chain to the client. This prevents the blocking issues that are caused by OCSP queries from the client and makes access to the HTTPS service more efficient.</p>	Add a website

Release date	Applicable service	Feature	Description	References
2021-09-17	Anti-DDoS Pro and Anti-DDoS Premium	Investigation	<p>The details about connection flood attacks can be queried on the Attack Analysis tab.</p> <p>You can query the details about connection flood attacks to obtain the trend of attack traffic and the details about traffic scrubbing. You can also view the rankings of the source IP addresses from which attacks are initiated and the distribution of source regions from which attacks originate. Then, you can optimize mitigation policies and track and analyze the attacks based on the details.</p>	View information on the Attack Analysis page
2021-08-20	Anti-DDoS Pro and Anti-DDoS Premium	Provisioning	<p>Descriptions can be configured for the added forwarding rules. This allows O&M personnel to locate the required services in an efficient manner when they manage protection policies. This makes O&M operations more efficient.</p>	Create a forwarding rule
2021-08-20	Anti-DDoS Pro and Anti-DDoS Premium	Provisioning	<p>The origin redundancy feature is supported.</p> <p>The origin redundancy feature allows you to configure primary and secondary origin servers. If an origin server is unavailable, you can switch to the other origin server with a few clicks. This way, the disaster recovery capabilities are improved when Anti-DDoS Pro or Anti-DDoS Premium forwards traffic to origin servers. This also ensures service availability.</p>	Modify the back-to-origin settings for a port
2021-08-18	Anti-DDoS Pro and Anti-DDoS Premium	Investigation	<p>Attack analysis reports can be exported.</p> <p>You can export the details about a DDoS attack event to your computer in the PNG or PDF format. This way, you can report and store the details about the attack event.</p>	View information on the Attack Analysis page

Release date	Applicable service	Feature	Description	References
2021-07-28	Anti-DDoS Pro and Anti-DDoS Premium	Investigation	<p>The details about web resource exhaustion attacks can be queried on the Attack Analysis tab.</p> <p>You can get an idea of the scrubbing capabilities of Anti-DDoS Pro or Anti-DDoS Premium, accurately evaluate the impacts of attacks on your services, and promptly adjust protection policies based on the details about the web resource exhaustion attacks.</p>	View information on the Attack Analysis page
2021-07-10	Anti-DDoS Pro and Anti-DDoS Premium	Investigation	Log collection can be enabled or disabled for multiple domain names on the Log Analysis page at a time.	Quick start
2021-07-07	Anti-DDoS Pro and Anti-DDoS Premium	Sec-Traffic Manager	<p>Switch to DDoS is supported for the interaction rules of Sec-Traffic Manager.</p> <p>After you create an interaction rule, service traffic is automatically switched to your Anti-DDoS Pro or Anti-DDoS Premium instance for scrubbing only when blackhole filtering is triggered. You can also manually switch service traffic to your instance for scrubbing before blackhole filtering is triggered based on the protection requirements of your services. This reduces the adverse impacts caused by blackhole filtering and traffic switchover.</p>	Create a cloud service interaction rule Create a tiered protection rule Create a CDN or DCDN interaction rule Create a network acceleration rule
2021-06-01	Anti-DDoS Pro	Assets	<p>IPv6 addresses are supported for Anti-DDoS Pro instances.</p> <p>You can apply for an IPv6 address for an Anti-DDoS Pro instance. This way, IPv4 traffic and IPv6 traffic can be forwarded to the same origin server that uses IPv4 addresses or to the respective origin servers that use IPv4 and IPv6 addresses.</p>	Purchase an Anti-DDoS Pro or Anti-DDoS Premium instance

Release date	Applicable service	Feature	Description	References
2021-05-24	Anti-DDoS Pro and Anti-DDoS Premium	Investigation	<p>In addition to blackhole filtering events and traffic scrubbing events that are detected in Anti-DDoS Pro or Anti-DDoS Premium, the events of flood attacks at Layer 4 and the events of HTTP flood attacks at Layer 7 can also be monitored by CloudMonitor. This feature provides comprehensive information about the security events that are detected in Anti-DDoS Pro or Anti-DDoS Premium.</p> <p>You can configure alert rules for events that are detected in Anti-DDoS Pro or Anti-DDoS Premium. This way, if an attack event is detected, CloudMonitor can send alert notifications in a timely manner.</p>	Monitor attack events that occur on Anti-DDoS Pro or Anti-DDoS Premium
2021-05-15	Anti-DDoS Pro and Anti-DDoS Premium	Provisioning	The features that are used to add domain names and ports are supported by Terraform. For more information, see Terraform . You can use Terraform to manage configurations in a centralized manner. This makes O&M more efficient.	Terraform documentation
2021-04-30	Anti-DDoS Premium	Provisioning	<p>The access configurations of multiple domain names can be modified at a time in Anti-DDoS Premium.</p> <div>  Note Anti-DDoS Pro supports this feature before Anti-DDoS Premium does. </div>	Edit a website configuration
2021-04-27	Anti-DDoS Premium	Investigation	<p>Attack analysis reports can be queried in Anti-DDoS Premium. This way, you can obtain information, such as the attack trend charts, analysis results of attack sources, and geographical distribution of attack sources.</p> <div>  Note Anti-DDoS Pro supports this feature before Anti-DDoS Premium does. </div>	View information on the Attack Analysis page

Release date	Applicable service	Feature	Description	References
2021-04-22	Anti-DDoS Pro and Anti-DDoS Premium	Mitigation Settings	<p>The mitigation settings for UDP reflection attacks can be configured on the Protection for Infrastructure tab.</p> <p>You can configure filtering policies based on the source ports of UDP traffic. You can enable one-click filtering for the source ports of common UDP reflection attacks. You can also customize filtering policies for the source ports of new types of UDP reflection attacks. This allows you to respond to UDP reflection attacks at the earliest opportunity and ensure the availability of UDP services.</p>	Use the feature of UDP Reflection Attacks Protection
2021-04-15	Anti-DDoS Pro and Anti-DDoS Premium	Investigation	<p>The entry point to the Cloud monitor alerts page is added to the Investigation module in the left-side navigation pane.</p> <p>On the Cloud monitor alerts page, you can view the types of alerts supported by Anti-DDoS Pro and Anti-DDoS Premium. You can also click the required button to go to the CloudMonitor console and enable alerting for Anti-DDoS Pro and Anti-DDoS Premium.</p>	Create threshold-triggered alert rules in the CloudMonitor console
2021-03-31	Anti-DDoS Premium	Sec-Traffic Manager	<p>Network acceleration policies are optimized for Anti-DDoS Premium.</p> <p>The waiting time that is required for automatic switchback during network acceleration is reduced from 30 minutes to 10 minutes.</p>	Create a network acceleration rule
2021-03-26	Anti-DDoS Pro and Anti-DDoS Premium	Website Config	<p>Custom combinations of cipher suites are supported in Transport Layer Security (TLS) policies.</p> <p>After you add the domain name of a website to your Anti-DDoS Pro or Anti-DDoS Premium instance, you can specify the cipher suite based on your business requirements.</p>	Customize a TLS policy

Release date	Applicable service	Feature	Description	References
2021-03-26	Anti-DDoS Pro and Anti-DDoS Premium	Website Config	<p>Multiple domain names are supported to forward back-to-origin requests.</p> <p>When you add a website to your Anti-DDoS Pro or Anti-DDoS Premium instance, you can specify more than one domain name that is mapped to your origin servers to forward back-to-origin requests. If you specify more than one IP address or domain name, Anti-DDoS Pro and Anti-DDoS Premium use IP hash load balancing to forward website traffic to the origin servers.</p> <p>You can specify multiple domain names to forward back-to-origin requests in distributed business scenarios. This way, you can use Anti-DDoS Pro or Anti-DDoS Premium together with your network, and the workload on a single origin server is reduced. This improves service stability and disaster recovery.</p>	Add a website
2021-03-26	Anti-DDoS Pro and Anti-DDoS Premium	Website Config	<p>Remarks can be specified for a website.</p> <p>After you add the domain name of a website to your Anti-DDoS Pro or Anti-DDoS Premium instance, you can specify remarks for the website. If you add multiple websites to your Anti-DDoS Pro or Anti-DDoS Premium instance, you can identify services based on the remarks. This makes O&M more efficient.</p>	Add a website
2021-03-26	Anti-DDoS Pro and Anti-DDoS Premium	Website Config	<p>Custom header fields and field values are supported to label requests.</p> <p>When you add the domain name of a website to your Anti-DDoS Pro or Anti-DDoS Premium instance, you can specify a custom header field and the value of the field for the domain name. When the instance processes the requests of this domain name, the instance adds the custom header field to these requests. This allows you to collect statistics on and analyze the back-to-origin data. For example, you can accurately count the actual source ports of the requests.</p>	Mark back-to-origin requests

Release date	Applicable service	Feature	Description	References
2021-03-26	Anti-DDoS Pro and Anti-DDoS Premium	Static Page Caching	Manual cache refreshing is supported for static page caching. If you create custom rules for static page caching and the source content of the cached page changes, you can forcibly refresh the page cache in Anti-DDoS Pro or Anti-DDoS Premium to synchronize the latest content in time.	Configure static page caching

2020

Release date	Applicable service	Feature	Description	References
--------------	--------------------	---------	-------------	------------

Release date	Applicable service	Feature	Description	References
2020-12-15	Anti-DDoS Pro and Anti-DDoS Premium	Website Config	<p>The configurations of Enable HTTPS Routing and Enable HTTP are provided.</p> <p>When you add the domain name of a website to your Anti-DDoS Pro or Anti-DDoS Premium instance, you can configure the Enable HTTPS Routing or Enable HTTP setting for the website. If you turn on Enable HTTPS Routing, all HTTP requests from clients to the instance are redirected to HTTPS requests, which enhances service security. If you turn on Enable HTTP, HTTPS requests to the instance are redirected to HTTP requests and then the HTTP requests are forwarded to the origin servers. This reduces the workload required to process HTTPS requests on the origin servers. These features allow the instance to authenticate inbound requests and help reduce the workload on downstream links and hosts.</p>	Add a website

Release date	Applicable service	Feature	Description	References
2020-11-05	Anti-DDoS Pro and Anti-DDoS Premium	Alert Rules	Multiple domain name metrics, such as queries per second (QPS) and abnormal status codes, are supported by alert rules. You can use these metrics to monitor the websites that are protected by your Anti-DDoS Pro or Anti-DDoS Premium instance and identify exceptions at the earliest opportunity.	Configure an alert rule for Anti-DDoS Pro or Anti-DDoS Premium
2020-10-27	Anti-DDoS Pro and Anti-DDoS Premium	Mitigation Settings > Custom Policies	Custom policies are supported. You can customize policies based on the IP address of your Anti-DDoS Pro or Anti-DDoS Premium instance and apply these custom policies to the instance.	Create custom mitigation policies for specific scenarios
2020-09-24	Anti-DDoS Pro	Attack Analysis	Attack Analysis is supported only for Anti-DDoS Pro. The entry point to the Attack Analysis page is added to the left-side navigation pane of the Anti-DDoS Pro console. The Attack Analysis page displays the details about attack events to provide a clear view of the process and details about protection against DDoS attacks. The details include an attack trend chart, attack source analysis, and protection flowchart.	View information on the Attack Analysis page
2020-09-08	Anti-DDoS Premium	Security Overview	Traffic information about Secure Mainland China Acceleration (Sec-MCA) is provided on the Security Overview page. On the Security Overview page, you can query the inbound, outbound, and attack traffic of Sec-MCA. This way, you can understand the traffic, attack mitigation effects, and the deduction of protection quotas for Sec-MCA.	Check the security overview

Release date	Applicable service	Feature	Description	References
2020-07-09	Anti-DDoS Pro and Anti-DDoS Premium	Mitigation Settings	<p>Major changes:</p> <ul style="list-style-type: none"> The Blocking Time option is provided for you to set the duration for IP addresses to be retained in a blacklist when you configure a Blacklist and Whitelist (Instance IP) policy for your Anti-DDoS Pro instance. In the Anti-DDoS Premium console, the Blacklist and Whitelist (Instance IP) settings are provided on the Protection for Infrastructure tab, and the Intelligent protection settings are provided on the Protection for Non-website Services tab. 	<p>Configure the IP address blacklist and whitelist for an Anti-DDoS Pro or Anti-DDoS Premium instance</p> <p>Configure intelligent protection</p>
2020-06-22	Anti-DDoS Premium	Sec-Traffic Manager > Sec-MCA	The Sec-MCA feature in Anti-DDoS Premium provides protection at both Layer 4 and Layer 7. This feature accelerates network access for your services outside mainland China and protects your assets against DDoS attacks.	Configure Anti-DDoS Premium Sec-MCA
2020-05-19	Anti-DDoS Pro and Anti-DDoS Premium	Sec-Traffic Manager > CDN/DCDN Interaction	<p>Anti-DDoS Pro and Anti-DDoS Premium can work with Dynamic Route for CDN (DCDN) to scrub malicious traffic and accelerate content delivery:</p> <ul style="list-style-type: none"> If no attacks are detected, DCDN accelerates traffic of your workloads. If attacks are detected, traffic of your workloads is automatically redirected to Anti-DDoS Pro or Anti-DDoS Premium for scrubbing. This ensures service availability. After the attacks stop, traffic of your workloads is automatically redirected to DCDN. 	Create a CDN or DCDN interaction rule
2020-04-30	Anti-DDoS Pro and Anti-DDoS Premium	Sec-Traffic Manager > CDN Interaction	If attacks are detected, CDN-accelerated domain names that integrate with Anti-DDoS Pro or Anti-DDoS Premium are added to a sandbox. The traffic of the domain names is redirected to Anti-DDoS Pro or Anti-DDoS Premium for scrubbing. This ensures service availability.	Overview

Release date	Applicable service	Feature	Description	References
2020-04-22	Anti-DDoS Pro and Anti-DDoS Premium	Sec-Traffic Manager > General	You can set the waiting time that is required for traffic switchback in general scheduling rules. Before the waiting time elapses, you can also manually switch traffic from Anti-DDoS Pro or Anti-DDoS Premium back to cloud resources.	Overview
2020-04-01	Anti-DDoS Pro and Anti-DDoS Premium	New API operations	New API operations are provided for you to manage and integrate Anti-DDoS Pro and Anti-DDoS Premium instances.	List of operations by function
2020-03-03	Anti-DDoS Premium	Anti-DDoS Premium interacting with CloudMonitor	Anti-DDoS Premium allows you to view basic O&M data in CloudMonitor. You can customize alert rules for Anti-DDoS Premium in the CloudMonitor console based on your business requirements.	Configure an alert rule for Anti-DDoS Pro or Anti-DDoS Premium Monitor attack events that occur on Anti-DDoS Pro or Anti-DDoS Premium
2020-02-18	Anti-DDoS Pro and Anti-DDoS Premium	Integrated console and region selection	The consoles of Anti-DDoS Pro and Anti-DDoS Premium are integrated. <ul style="list-style-type: none"> In the console, you can select Mainland China for Anti-DDoS Pro or Outside Mainland China for Anti-DDoS Premium. You can access Anti-DDoS Pro and Anti-DDoS Premium in the same console. The Anti-DDoS Premium console is updated to provide a graphical user interface that is similar to that of the Anti-DDoS Pro console. 	Differences between the features of Anti-DDoS Pro and Anti-DDoS Premium

2019

Release date	Applicable service	Feature	Description	References
--------------	--------------------	---------	-------------	------------

Release date	Applicable service	Feature	Description	References
2019-12-18	Anti-DDoS Origin	Console	<p>A new version of the console is available.</p> <ul style="list-style-type: none">• In the left-side navigation pane, Anti-DDoS Basic is changed to Anti-DDoS Services.• In the left-side navigation pane, the Basic Protection > Instances page is changed to the Assets page. On the Assets page, the content of DDoS Attack Protection Information is updated.• In the left-side navigation pane, the Protection Package > Security Report, Protection Package > Protection Packages, Protection Package > Traffic Packages, and Protection Package > Operation Logs pages are changed to the Anti-DDoS Origin > Manage Instances page.• In the left-side navigation pane, the following entry points are added:<ul style="list-style-type: none">◦ Anti-DDoS Services > Anti-DDoS Pro: directs you to the Anti-DDoS Pro console.◦ Anti-DDoS Services > Anti-DDoS Premium: directs you to the Anti-DDoS Premium console.◦ Industry-specific > Game Shield: directs you to the GameShield console.◦ How to Choose: directs you to a topic named Select an Anti-DDoS service based on the protection scenario.	Assets

Release date	Applicable service	Feature	Description	References
2019-12-18	Anti-DDoS Origin	Assets	<p>The Basic Protection > Instances page is changed to the Assets page.</p> <p>The Assets page displays the protection status of activated assets within your Alibaba Cloud account. The page provides a quick overview of security risks for your assets from DDoS attacks. On the page, you can also increase the protection capacity for a specific asset. Supported assets include Elastic Compute Service (ECS) instances, Server Load Balancer (SLB) instances, and elastic IP addresses (EIPs).</p>	Assets
2019-12-18	Anti-DDoS Origin	Elastic protection	<p>The preset protection threshold is changed to the elastic protection threshold. The console no longer shows a score in the Security Credibility field.</p> <p>In elastic protection mode, Anti-DDoS Origin allows you to assign an extra protection capacity for your assets based on the original basic protection capacity that is provided free of charge. The extra protection capacity assigned for an asset changes based on several factors. The factors include the number of resources that an anti-DDoS cluster consumes, available resources, historical attacks that your assets encounter, and security credits of your account.</p>	Security Credibility

2. System upgrades

2.1. [System upgrade] Anti-DDoS Premium is upgraded on July 7, 2020

Applicable services: Anti-DDoS Premium

Time: (UTC+8) 06:00:00 to 07:00:00 on July 7, 2020

Description: The network of data centers where Anti-DDoS Premium is deployed is upgraded.

Impact: During the upgrade, connections to some IP addresses need to be reestablished. This breaks the TCP-based connections two to three times. Transient disconnection errors have little impact on services that use short-lived connections and persistent connections that can be automatically reestablished. Make sure that your services support automatic reconnection to ensure fault tolerance.

Customer service: We apologize for any inconvenience caused. If you require any further assistance, we recommend that you contact [customer service](#).

2.2. [System upgrade] Anti-DDoS Premium is upgraded on June 25, 2020

Applicable services: Anti-DDoS Premium

Time: (UTC+8) 00:00:00 to 06:00:00 on June 25, 2020

Description: Scrubbing nodes in the UK are added to the traffic scrubbing centers.

Impact: After the upgrade, the following back-to-origin Classless Inter-Domain Routing (CIDR) blocks are added to Anti-DDoS Premium:

- 170.33.88.0/24
- 170.33.92.0/24
- 170.33.93.0/24
- 170.33.90.0/24

If you use Anti-DDoS Premium and have configured access control policies on your origin server, update the whitelist of your origin server to allow the preceding back-to-origin CIDR blocks. This prevents the back-to-origin IP addresses of Anti-DDoS Premium from being blocked. For more information, see [Allow back-to-origin IP addresses to access the origin server](#).

Customer service: We apologize for any inconvenience caused. If you require any further assistance, we recommend that you contact [customer service](#).

2.3. [System upgrade] Anti-DDoS Pro is upgraded on June 4, 2020

Applicable services: Anti-DDoS Pro

Time: (UTC+8) 00:00:00 on June 4, 2020

Description: Anti-DDoS Pro is upgraded.

Impact: Based on national regulations of China, Anti-DDoS Pro no longer protects services that use ports 80, 8080, 443, and 8443 from 00:00:00 on June 4, 2020.

Customer service: We apologize for any inconvenience caused. If you require any further assistance, we recommend that you contact [customer service](#).

2.4. [System upgrade] Anti-DDoS Premium is upgraded on May 7, 2020

Applicable services: Anti-DDoS Premium

Time: (UTC+8) 01:00:00 to 05:00:00 on May 7, 2020

Description: The network of data centers where Anti-DDoS Premium is deployed is upgraded.

Impact: During the upgrade, connections to some IP addresses need to be reestablished. This breaks the TCP-based connections two to three times. Transient disconnection errors have little impact on services that use short-lived connections and persistent connections that can be automatically reestablished. Make sure that your services support automatic reconnection to ensure fault tolerance.

Customer service: We apologize for any inconvenience caused. If you require any further assistance, we recommend that you contact [customer service](#).

2.5. [System upgrade] Anti-DDoS Premium is upgraded in April and May 2020

Applicable services: Anti-DDoS Premium

Time:

- (UTC+8) 14:00:00 to 18:00:00 on April 28, 2020
- (UTC+8) 00:00:00 to 04:00:00 on April 30, 2020
- (UTC+8) 09:00:00 to 12:00:00 on May 7, 2020
- (UTC+8) 15:00:00 to 19:00:00 on May 12, 2020
- (UTC+8) 00:00:00 to 04:00:00 on May 15, 2020
- (UTC+8) 00:00:00 to 04:00:00 on May 19, 2020

Description: The network of data centers where Anti-DDoS Premium is deployed is upgraded.

Impact: During the upgrade, connections to some IP addresses need to be reestablished. This breaks the TCP-based connections two to three times. Transient disconnection errors have little impact on services that use short-lived connections and persistent connections that can be automatically reestablished. Make sure that your services support automatic reconnection to ensure fault tolerance.

Customer service: We apologize for any inconvenience caused. If you require any further assistance, we recommend that you contact [customer service](#).

2.6. [System upgrade] Anti-DDoS Premium is upgraded on April 23, 2020

Applicable services: Anti-DDoS Premium

Time: (UTC+8) 23:00:00 on April 23, 2020 to 03:00:00 on April 24, 2020

Description: The network of data centers where Anti-DDoS Premium is deployed is upgraded.

Impact: During the upgrade, connections to some IP addresses need to be reestablished. This breaks the TCP-based connections two to three times. Transient disconnection errors have little impact on services that use short-lived connections and persistent connections that can be automatically reestablished. Make sure that your services support automatic reconnection to ensure fault tolerance.

Customer service: We apologize for any inconvenience caused. If you require any further assistance, we recommend that you contact [customer service](#).

2.7. [System upgrade] Anti-DDoS Premium is upgraded on April 22, 2020

Applicable services: Anti-DDoS Premium

Time: (UTC+8) 00:00:00 to 06:00:00 on April 22, 2020

Description: The network of data centers where Anti-DDoS Premium Mainland China Acceleration (MCA) is deployed is upgraded.

Impact: During the upgrade, connections to some IP addresses need to be reestablished. This breaks the TCP-based connections two to three times. Transient disconnection errors have little impact on services that use short-lived connections and persistent connections that can be automatically reestablished. Make sure that your services support automatic reconnection to ensure fault tolerance.

Customer service: We apologize for any inconvenience caused. If you require any further assistance, we recommend that you contact [customer service](#).

2.8. [System upgrade] Anti-DDoS Premium is upgraded on February 28, 2020

Applicable services: Anti-DDoS Premium

Time: (UTC+8) 00:00:00 to 06:00:00 on February 28, 2020

Description: The network of data centers in Japan where Anti-DDoS Premium is deployed is upgraded.

Impact: During the upgrade, connections to some IP addresses need to be reestablished. This breaks the TCP-based connections two to four times. Transient disconnection errors have little impact on services that use short-lived connections and persistent connections that can be automatically reestablished. Make sure that your services support automatic reconnection to ensure fault tolerance.

Customer service: We apologize for any inconvenience caused. If you require any further assistance, we recommend that you contact [customer service](#).

2.9. [System upgrade] Anti-DDoS Pro is upgraded on January 14 and 16, 2020

Applicable services: Anti-DDoS Pro

Time: (UTC+8) 00:00:00 to 06:00:00 on January 14 and 16, 2020

Description: The software of data centers where Anti-DDoS Pro is deployed is upgraded.

Impact: During the upgrade, connections to some IP addresses need to be reestablished. This breaks the TCP-based connections five times. Transient disconnection errors have little impact on services that use short-lived connections and persistent connections that can be automatically reestablished. Make sure that your services support automatic reconnection to ensure fault tolerance.

Customer service: We apologize for any inconvenience caused. If you require any further assistance, we recommend that you contact [customer service](#).

2.10. [System upgrade] Anti-DDoS Pro of the previous version is upgraded on January 7 and 9, 2020

Applicable services: Anti-DDoS Pro of the previous version

Time: (UTC+8) 01:00:00 to 07:00:00 on January 7 and 9, 2020

Description: The software of data centers of China Telecom in Wuhan where Anti-DDoS Pro is deployed is upgraded.

Impact: During the upgrade, connections to some IP addresses need to be reestablished. This breaks the TCP-based connections two to four times. Transient disconnection errors have little impact on services that use short-lived connections and persistent connections that can be automatically reestablished. Make sure that your services support automatic reconnection to ensure fault tolerance.

Customer service: We apologize for any inconvenience caused. If you require any further assistance, we recommend that you contact [customer service](#).

2.11. [System upgrade] Anti-DDoS Pro no longer provides traffic forwarding services for instances that have expired for more than seven days from January 6, 2020

Applicable services: Anti-DDoS Pro and Anti-DDoS Premium

Time: (UTC+8) 00:00:00 on January 6, 2020

Description: Anti-DDoS Pro of the previous version no longer provides traffic forwarding services for instances that have expired for more than seven days.

Impact: Anti-DDoS Pro of the previous version no longer provides traffic forwarding services for instances that have expired for more than seven days from 00:00:00 on January 6, 2020. If you use Anti-DDoS Pro of the previous version, pay attention to the expiration status of your instance. Renew your instance in a timely manner or configure auto-renewal for your instance to avoid impact on your services.

Customer service: We apologize for any inconvenience caused. If you require any further assistance, we recommend that you contact [customer service](#).

2.12. [System upgrade] Anti-DDoS Pro of the previous version is upgraded on December 24, 2019

Applicable services: Anti-DDoS Pro of the previous version

Time: (UTC+8) 02:00:00 to 08:00:00 on December 24, 2019

Description: The software of data centers of China Telecom in Wuhan where Anti-DDoS Pro is deployed is upgraded.

Impact: During the upgrade, connections to some IP addresses need to be reestablished. This breaks the TCP-based connections two to four times. Transient disconnection errors have little impact on services that use short-lived connections and persistent connections that can be automatically reestablished. Make sure that your services support automatic reconnection to ensure fault tolerance.

Customer service: We apologize for any inconvenience caused. If you require any further assistance, we recommend that you contact [customer service](#).

2.13. [System upgrade] Anti-DDoS Premium is upgraded on December 25 and 31, 2019

Applicable services: Anti-DDoS Premium

Time: (UTC+8) 00:00:00 to 04:00:00 on December 25 and 31, 2019

Description: The network of data centers in Hong Kong (China) and Malaysia where Anti-DDoS Premium is deployed is upgraded.

Impact: During the upgrade, connections to some IP addresses need to be reestablished. This breaks the TCP-based connections two to four times. Transient disconnection errors have little impact on services that use short-lived connections and persistent connections that can be automatically reestablished. Make sure that your services support automatic reconnection to ensure fault tolerance.

Customer service: We apologize for any inconvenience caused. If you require any further assistance, we recommend that you contact [customer service](#).

2.14. [System upgrade] Anti-DDoS Premium and GameShield are upgraded on December 19, 2019

Applicable services: Anti-DDoS Premium and GameShield

Time: (UTC+8) 10:00:00 to 12:00:00 on December 19, 2019

Description: The software of data centers in Singapore where Anti-DDoS Premium and GameShield are deployed is upgraded.

Impact: During the upgrade, connections to some IP addresses need to be reestablished. This breaks the TCP-based connections one to three times. Transient disconnection errors have little impact on services that use short-lived connections and persistent connections that can be automatically reestablished. Make sure that your services support automatic reconnection to ensure fault tolerance.

Customer service: We apologize for any inconvenience caused. If you require any further assistance, we recommend that you contact [customer service](#).

2.15. [System upgrade] Anti-DDoS Pro is upgraded on December 15, 2019

Applicable services: Anti-DDoS Pro

Time: (UTC+8) 06:00:00 to 09:00:00 on December 15, 2019

Description: The software of data centers where Anti-DDoS Pro is deployed is upgraded.

Impact: After the upgrade, the following back-to-origin CIDR blocks are added to Anti-DDoS Pro:

```
47.113.25.0/24
```

If you use Anti-DDoS Pro and have configured access control policies on your origin server, update the whitelist of your origin server to allow the preceding back-to-origin CIDR blocks. This prevents the back-to-origin IP addresses of Anti-DDoS Pro from being blocked during geo-disaster recovery.

During the upgrade, your services are not affected. In some cases, the origin server is configured with strong security verification policies and the IP addresses need to be authenticated again. This breaks the TCP-based connections two to four times. Transient disconnection errors have little impact on services that use short-lived connections and persistent connections that can be automatically reestablished. Make sure that your services support automatic reconnection to ensure fault tolerance.

Customer service: We apologize for any inconvenience caused. If you require any further assistance, we recommend that you contact [customer service](#).

2.16. [System upgrade] Anti-DDoS Pro of the previous version is upgraded on December 27, 2019

Applicable services: Anti-DDoS Pro of the previous version

Time: (UTC+8) 00:00:00 to 06:00:00 on December 27, 2019

Description: Anti-DDoS Pro instances of the previous version that are deployed in a data center of China Unicom in North China is upgraded.

Impact: During the upgrade, your services are not affected. In some cases, the origin server is configured with strong security verification policies and the IP addresses need to be authenticated again. This breaks the TCP-based connections eight times. Transient disconnection errors have little impact on services that use short-lived connections and persistent connections that can be automatically reestablished. Make sure that your services support automatic reconnection to ensure fault tolerance.

Customer service: We apologize for any inconvenience caused. If you require any further assistance, we recommend that you contact [customer service](#).

2.17. [System upgrade] Anti-DDoS Pro is upgraded on December 18, 2019

Applicable services: Anti-DDoS Pro

Time: (UTC+8) 00:00:00 to 06:00:00 on December 18, 2019

Description: The software of data centers where Anti-DDoS Pro is deployed is upgraded.

Impact: During the upgrade, your services are not affected. In some cases, the origin server is configured with strong security verification policies and the IP addresses need to be authenticated again. This breaks the TCP-based connections four to six times. Transient disconnection errors have little impact on services that use short-lived connections and persistent connections that can be automatically reestablished. Make sure that your services support automatic reconnection to ensure fault tolerance.

Customer service: We apologize for any inconvenience caused. If you require any further assistance, we recommend that you contact [customer service](#).

2.18. [System upgrade] Anti-DDoS Premium is upgraded on December 5 and 6, 2019

Applicable services: Anti-DDoS Premium

Time: (UTC+8) 17:00:00 to 21:30:00 on December 5 and 6, 2019

Description: The network of data centers in the eastern United States where Anti-DDoS Premium is deployed is upgraded.

Impact: During the upgrade, connections to some IP addresses need to be reestablished. This breaks the TCP-based connections two to four times. Transient disconnection errors have little impact on services that use short-lived connections and persistent connections that can be automatically reestablished. Make sure that your services support automatic reconnection to ensure fault tolerance.

Customer service: We apologize for any inconvenience caused. If you require any further assistance, we recommend that you contact [customer service](#).

2.19. [System upgrade] Anti-DDoS Pro of the previous version is upgraded on December 6, 2019

Applicable services: Anti-DDoS Pro of the previous version

Time: (UTC+8) 01:00:00 to 07:00:00 on December 6, 2019

Description: The software of data centers of China Telecom in Wuhan where Anti-DDoS Pro is deployed is upgraded.

Impact: During the upgrade, connections to some IP addresses need to be reestablished. This breaks the TCP-based connections two to four times. Transient disconnection errors have little impact on services that use short-lived connections and persistent connections that can be automatically reestablished. Make sure that your services support automatic reconnection to ensure fault tolerance.

Customer service: We apologize for any inconvenience caused. If you require any further assistance, we recommend that you contact [customer service](#).

2.20. [System upgrade] Anti-DDoS Premium is upgraded on December 17, 2019

Applicable services: Anti-DDoS Premium

Time: (UTC+8) 00:00:00 to 04:00:00 on December 17, 2019

Description: The network of data centers in Singapore where Anti-DDoS Premium is deployed is upgraded.

Impact: During the upgrade, connections to some IP addresses need to be reestablished. This breaks the TCP-based connections one to two times. Transient disconnection errors have little impact on services that use short-lived connections and persistent connections that can be automatically reestablished. Make sure that your services support automatic reconnection to ensure fault tolerance.

Customer service: We apologize for any inconvenience caused. If you require any further assistance, we recommend that you contact [customer service](#).

2.21. [System upgrade] Anti-DDoS Premium is upgraded on November 28, 2019

Applicable services: Anti-DDoS Premium

Time: (UTC+8) 10:00:00 to 14:00:00 on November 28, 2019

Description: The network of data centers in Germany where Anti-DDoS Premium is deployed is upgraded.

Impact: During the upgrade, connections to some IP addresses need to be reestablished. This breaks the TCP-based connections one to two times. Transient disconnection errors have little impact on services that use short-lived connections and persistent connections that can be automatically reestablished. Make sure that your services support automatic reconnection to ensure fault tolerance.

Customer service: We apologize for any inconvenience caused. If you require any further assistance, we recommend that you contact [customer service](#).

2.22. [System upgrade] Anti-DDoS Premium is upgraded on November 21, 2019

Applicable services: Anti-DDoS Premium

Time: (UTC+8) 15:00:00 to 19:00:00 on November 21, 2019

Description: The network of data centers in the eastern United States where Anti-DDoS Premium is deployed is upgraded.

Impact : During the upgrade, connections to some IP addresses need to be reestablished. This breaks the TCP-based connections one to two times. Transient disconnection errors have little impact on services that use short-lived connections and persistent connections that can be automatically reestablished. Make sure that your services support automatic reconnection to ensure fault tolerance.

Customer service: We apologize for any inconvenience caused. If you require any further assistance, we recommend that you contact [customer service](#).

2.23. [System upgrade] Anti-DDoS Premium is upgraded on November 14, 2019

Applicable services: Anti-DDoS Premium

Time: (UTC+8) 12:00:00 to 18:00:00 on November 14, 2019

Description: The network of data centers in the western United States where Anti-DDoS Premium is deployed is upgraded.

Impact : During the upgrade, your services are not affected. In some cases, the origin server is configured with strong security verification policies and the IP addresses need to be authenticated again. This breaks the TCP-based connections one to two times. Transient disconnection errors have little impact on services that use short-lived connections and persistent connections that can be automatically reestablished. Make sure that your services support automatic reconnection to ensure fault tolerance.

Customer service: We apologize for any inconvenience caused. If you require any further assistance, we recommend that you contact [customer service](#).

2.24. [System upgrade] Anti-DDoS Premium is upgraded on October 25, 2019

Applicable services: Anti-DDoS Premium

Time: (UTC+8) 00:00:00 to 04:00:00 on October 25, 2019

Description: The network of data centers in Japan where Anti-DDoS Premium is deployed is upgraded.

Impact : During the upgrade, your services are not affected. In some cases, the origin server is configured with strong security verification policies and the IP addresses need to be authenticated again. This breaks the TCP-based connections one to two times. Transient disconnection errors have little impact on services that use short-lived connections and persistent connections that can be automatically reestablished. Make sure that your services support automatic reconnection to ensure fault tolerance.

Customer service: We apologize for any inconvenience caused. If you require any further assistance, we recommend that you contact [customer service](#).

2.25. [System upgrade] Anti-DDoS Premium is upgraded on May 15, 2020

Applicable services: Anti-DDoS Premium

Time: (UTC+8) 01:00:00 to 05:00:00 on May 15, 2020

Description: The network of data centers where Anti-DDoS Premium is deployed is upgraded.

Impact: During the upgrade, connections to some IP addresses need to be reestablished. This breaks the TCP-based connections two to three times. Transient disconnection errors have little impact on services that use short-lived connections and persistent connections that can be automatically reestablished. Make sure that your services support automatic reconnection to ensure fault tolerance.

Customer service: We apologize for any inconvenience caused. If you require any further assistance, we recommend that you contact [customer service](#).

3. Updates

3.1. [Update] The protection bandwidth of Anti-DDoS Pro of the previous version is adjusted on June 30, 2020

Applicable services: Anti-DDoS Pro of the previous version

Time: (UTC+8) 23:00:00 to 24:00:00 on June 30, 2020

Description: After the protection bandwidth of Anti-DDoS Pro of the previous version is adjusted, the maximum protection bandwidth will be 300 Gbit/s. Anti-DDoS Pro of the previous version no longer provides the basic protection bandwidth and burstable protection bandwidth that is greater than 300 Gbit/s.

Impact: During the adjustment, your services are not affected. If you use Anti-DDoS Pro of the previous version and need a protection bandwidth that is greater than 300 Gbit/s, you can request technical support to migrate your services to Anti-DDoS Pro free of charge. Anti-DDoS Pro provides a protection bandwidth that is greater than 300 Gbit/s. For more information, see [What are Anti-DDoS Pro and Anti-DDoS Premium](#).

Customer service: We apologize for any inconvenience caused. If you require any further assistance, we recommend that you contact [customer service](#).

3.2. [Update] The protection bandwidth of Anti-DDoS Pro of the previous version is adjusted on December 26, 2019

Applicable services: Anti-DDoS Pro of the previous version

Time: (UTC+8) 19:00:00 to 20:00:00 on December 26, 2019

Description: After the protection bandwidth of Anti-DDoS Pro of the previous version is adjusted, the maximum protection bandwidth that is provided is 300 Gbit/s. Anti-DDoS Pro of the previous version no longer provides the basic protection bandwidth and burstable protection bandwidth that is greater than 300 Gbit/s.

Impact: During the adjustment, your services are not affected. If you use Anti-DDoS Pro of the previous version and need a protection bandwidth that is greater than 300 Gbit/s, you can request technical support to migrate your services to Anti-DDoS Pro of the latest version free of charge. Anti-DDoS Pro of the latest version provides a protection bandwidth that is greater than 300 Gbit/s. For more information, see [What are Anti-DDoS Pro and Anti-DDoS Premium](#).

Customer service: We apologize for any inconvenience caused. If you require any further assistance, we recommend that you contact [customer service](#).

4.Product notices

4.1. [Notice] APIs in the previous version of Anti-DDoS Pro are deprecated at 00:00:00 (UTC+8) on June 30, 2020

Applicable services: Anti-DDoS Pro of the previous version

Time: (UTC+8) 00:00:00 on June 30, 2020

Description: API users of Anti-DDoS Pro of the latest version and Anti-DDoS Premium are affected.

Impact: If you use Anti-DDoS Pro APIs of the previous version, start to use the APIs of the latest version instead at your earliest convenience. For more information, see [List of operations by function](#).

4.2. [Notice] Anti-DDoS Pro of the previous version is discontinued from the market

Applicable services: Anti-DDoS Pro of the previous version

Time:

- After (UTC+8) 00:00:00 on June 1, 2020, you cannot renew your Anti-DDoS Pro instances of the previous version.
- After (UTC+8) 00:00:00 on September 1, 2020, you cannot use your Anti-DDoS Pro instances of the previous version to forward your business traffic.

Description: Anti-DDoS Pro of the previous version stops renewal and business traffic forwarding services after the scheduled time. The following scrubbing lines are affected: China Telecom + China Unicom, China Telecom + China Unicom + old BGP, old BGP, and scrubbing lines that are deployed in on-premises data centers outside mainland China.

Impact: You cannot renew your Anti-DDoS Pro instances of the previous version and use the instances to forward your business traffic.

- If you use an Anti-DDoS Pro instance of the previous version, submit a [ticket](#) to obtain technical support and migrate your services to an Anti-DDoS Pro instance of the latest version or an Anti-DDoS Premium instance. Anti-DDoS Pro instances of the latest version or Anti-DDoS Premium instances can provide better network performance, protection, and disaster recovery. The migration causes no business losses and is free of charge.
- If you use Anti-DDoS Pro of the latest version or Anti-DDoS Premium, ignore this notice.

4.3. [Notice] The Security Reports feature in the previous version of Anti-DDoS Pro is deprecated on April 29, 2020

Applicable services: Anti-DDoS Pro of the previous version

Time: (UTC+8) 00:00:00 on April 29, 2020

Description: The Security Reports feature in the previous version of Anti-DDoS Pro is deprecated.

Impact: After the Security Reports feature in the previous version of Anti-DDoS Pro is deprecated, you can query data of your services only on the Overview page. The Overview page allows you to query data of your services from more dimensions.

4.4. [Notice] Anti-DDoS Pro of the previous version is discontinued from the market

Applicable services: Anti-DDoS Pro of the previous version

Time: (UTC+8) 00:00:00 on September 30, 2020

Description: Anti-DDoS Pro of the previous version is discontinued from the market after the scheduled time. The following scrubbing lines are affected: China Telecom + China Unicom, China Telecom + China Unicom + old BGP, old BGP, and scrubbing lines that are deployed in on-premises data centers outside mainland China.

Impact: Anti-DDoS Pro of the previous version stops providing services.

- If you use an Anti-DDoS Pro instance of the previous version, **contact your customer service** to migrate your services to an Anti-DDoS Pro instance of the latest version. Instances of the latest version provide better network performance, protection, and disaster recovery. The migration causes no business losses and is free of charge.
- If you use Anti-DDoS Pro of the latest version, ignore this notice.