Alibaba Cloud Threat Detection

Best Practices

Issue: 20190327

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 due to product version upgrades , adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall 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 the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults " and "as available" basis. 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 bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, 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 content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, 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 the Alibaba Cloud website, product programs, or content 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 contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information 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.
	This warning information 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 restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus , page names, and other UI elements.	Click OK.
`Courier font`	It is used for commands.	Run the `cd / d C :/ windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *[-all|-t]*

Style	Description	Example
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich {stand | slave}`

Contents

1 How to use Alibaba Cloud security products to build a safe website

This article describes how to build a safe website with Alibaba Cloud security products DDoS Protection, Web Application Firewall (WAF) and Thread Detection Service.

DDoS Protection

DDoS Protection is a service that features a set of high-defensive IPs, and acts as a protective barrier for the origin. It safeguards network servers under high volume DDoS attacks. There are two DDoS Protection editions in Alibaba Cloud, they are *Anti-DDoS Pro* and *Anti-DDoS Premium*.

Web Application Firewall (WAF)

Alibaba Cloud WAF helps you to defend against common web attacks such as SQL injections, Cross-site scripting (XSS), web shell, Trojan, and unauthorized access, and to filter out massive HTTP flood requests. It protects your web resources from being exposed and guarantees your website security and availability.

Thread Detection Service

Thread Detection Service (TDS) is a security service with security event detection, vulnerability scanning, and configuration baseline check.

Limitations of use DDoS Protection and Web Application Firewall in China

According to Measures for the Administration of Internet Information Services and Registration Administration Measures for Non-Commercial Internet Information Services, China mandates a filing system for non-commercial Internet information services and a licensing system for commercial Internet information services. Anyone that has not obtained an ICP registration is prohibited from operating Internet information services. Specifically, all websites that provide services to Mainland China must first obtain the ICP registration. If your website is hosted on an instance deployed within Mainland China or uses Security Products like DDoS Protection, Web Application Firewall (WAF) within Mainland China, you can apply for ICP registration through the *Alibaba Cloud ICP Filing system*. For more information, see *ICP Registration*.

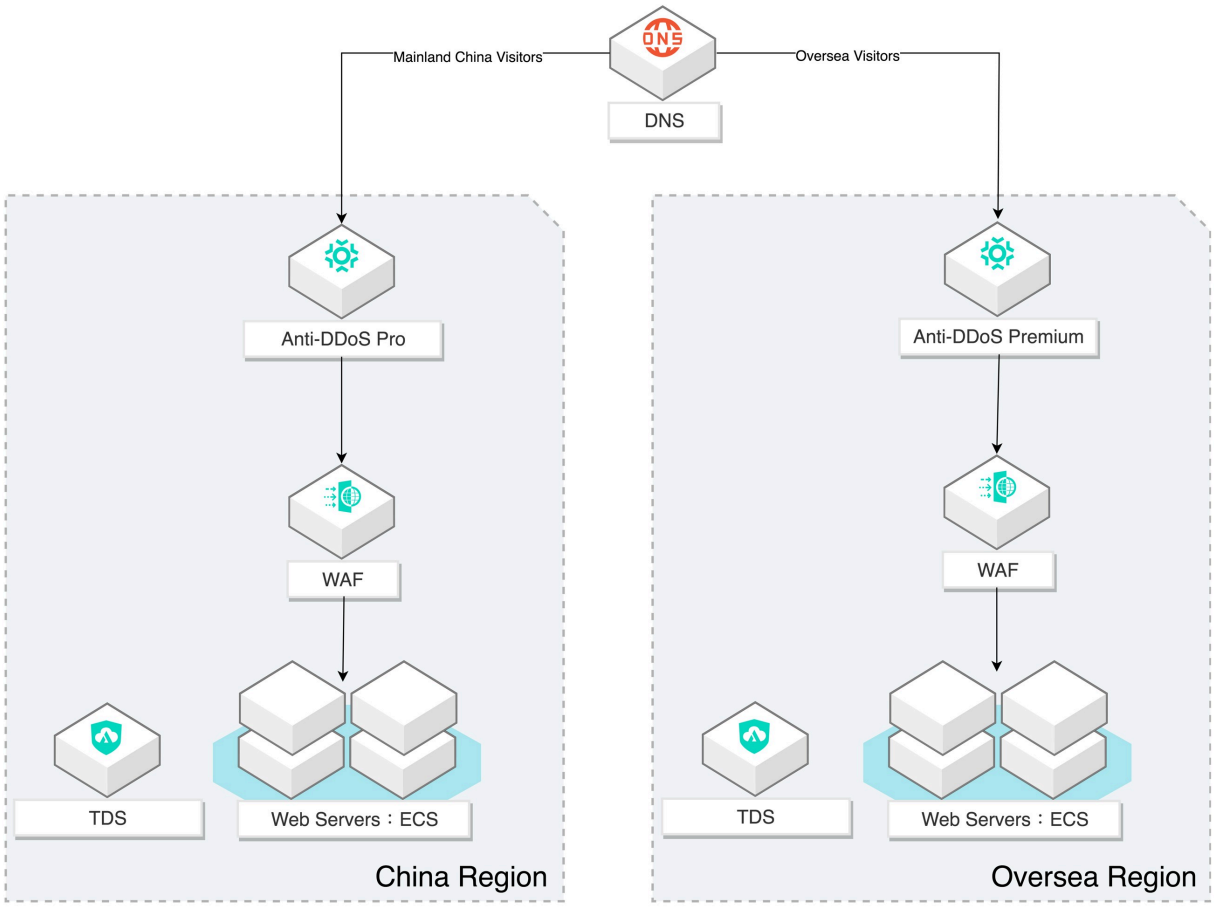
Prerequisites

Before you begin, make sure of the following:

- You have Alibaba Cloud Account If not, *sign up with Alibaba Cloud* and *add a payment method*.
- If you want to purchase any security products in Mainland China, *register by using your real name* and at least one domain completed ICP filing.

Overview

The following figure illustrates the best practice to build up a safe website:



In order to improve user experience in Mainland China. Alibaba Cloud recommend you to duplicate your website resources in China Region to guarantee performance is not impacted by GFW. You can also use Alibaba Cloud DNS to ensure all DNS queries are rapidly responded to by the server in closest geographic proximity. For more information, see *Alibaba Cloud DNS*.

Procedure

1. Enable and configure Web Application Firewall (WAF).

2. Apply protection configuration in Web Application Firewall (WAF).

Protection Function	Recommended Setting	Description
Web Application Protection	· Status: Enable · Mode: Protection · Mode of protection policy: Normal	When you find that many requests are intercepted by mistake under the normal mode, we recommend that you use the Loose mode. When you require stricter protection against path traversal, SQL injection, and command running attacks, we recommend that you use the Strict mode.
Malicious IP Penalty	Status: Enable	The IP address would be blocked for 6 minutes if there are 2 threats from that IP found in 1 minute.
HTTP Flood Protection	· Status: Enable · Mode: Normal · Custom Rules: Enable · Recommended Rules setting:When a single source IP address accesses [URL] for more than [XX] times within [XX] seconds, block this IP address for [XX] hour. The block frequency depends on your actual business situation.	When you find many HTTP flood attacks are not blocked in the Normal mode, you can switch to the Emergency mode. In Emergency mode, WAF imposes strong blocking rules against HTTP flood attacks, but it may also cause many false positives.

Protection Function	Recommended Setting	Description
HTTP ACL Policy	· Status: Enable · Matching Field: IP · Logical Operator: Does not have · Matching content: [IP subnet] · Action:Block	If your website is not serve public. You can configure IP HTTP fields in HTTP ACL Policy to whitelist certain of IP addresses . You can also combine three conditions at most to fit different business scenarios such as anti-leech and allow specify User-Agent.
New intelligent protection engine	Status: Enable	The intelligent protection engine mainly protects against SQL injection and other web attack methods , not HTTP flood attacks. If you have high web attack protection requirements , we recommend that you enable the new intelligent protection engine function .

Protection Function	Recommended Setting	Description
Sensitive information leak prevention	· Status: Enable · Matching Condition: Response Code includes [4XX] · Matching Action: Block · Matching Condition :Sensitive Info includes [ID Cards, Credit Cards, Telephone No.] · Matching Action: Sensitive Information filtering	You can set rules to block of specific HTTP request status codes to avoid leaking sensitive server information. For example, you can set the following protection rule to block HTTP 404 status codes. For specified webpage URLs that may display mobile phone numbers, ID card numbers , and other sensitive information, configure the relevant rules to filter this information or provide warnings. For example, you can set the following protection rule to filter ID card numbers on the webpage.

3. Configure security group to protect source website servers.
4. Enable and configure DDoS Protection.
5. Enable TDS and install the Agent.
6. Configure TDS Baseline check and vulnerability scanning.

Below are listed of supported check items and recommended setting:

Category	Check items	Recommended Setting
Database	· Memcached Security Baseline · Redis Security Baseline · MongoDB Baseline	If you are running NoSQL services in ECS. Select the according database security baseline checking.

Category	Check items	Recommended Setting
System	· CentOS Linux 7 Security Baseline · CentOS Linux 6 Security Baseline · Windows 2008 R2 Security Baseline · Windows 2012 R2 Security Baseline	Depends on the operating system you are running. Select the according system security baseline checking.
Weak Password	· PostgreSQL Weak Password · Linux Weak Password · FTP Anonymous Logon Configurations · SQL Server Weak Password · MySQL Weak Password · Windows Account Weak Password · FTP Weak Password	Depends on the operating system you are running. Select Linux Weak Password or Windows Account Weak Password. If you are running additional services in ECS. Select the according weak password baseline checking.
Middleware Baseline	· Apache Tomcat 7 Security Baseline	Currently Alibaba Cloud Cloud Security Center only support Tomcat 7 security baseline checking. If you are running Tomcat 7 in ECS. Select Apache Tomcat 7 Security Baseline checking.