Alibaba Cloud Threat Detection

Overview of Console

Issue: 20190906

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]*

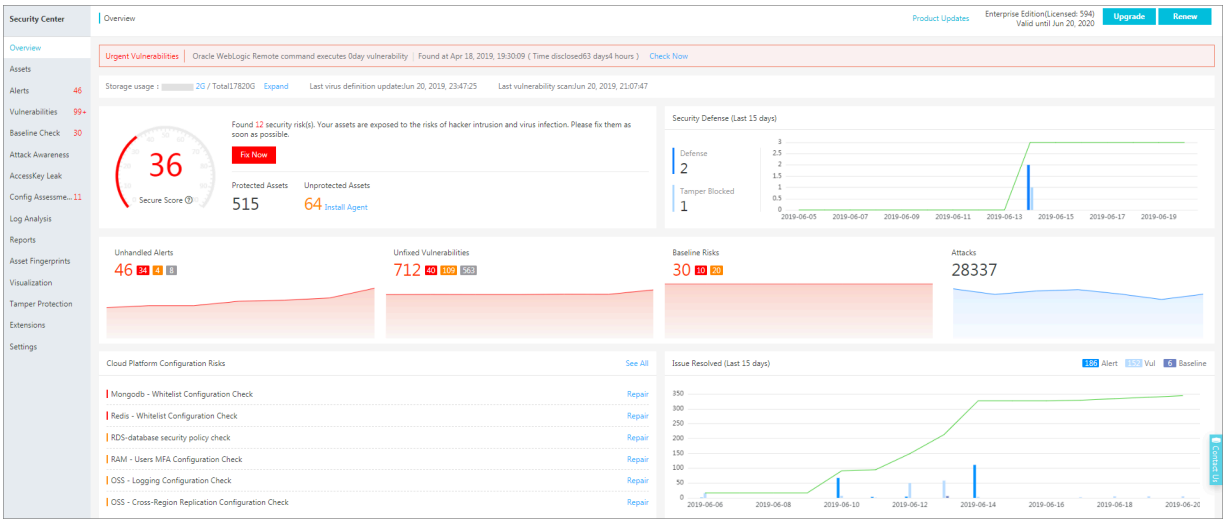
Style	Description	Example
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich {stand | slave}`

Contents

1 Overview

As the security operation center of Alibaba Cloud, the Overview page of the Security Center console displays the threats to, and the safety score of all your assets, and all the Alibaba Cloud Security services you have bought. You can upgrade Security Center, renew your Security Center service, scale up your assets, and modify the notification method.

On the Overview page, you can view important security information of your assets and execute related operations.



The Overview page includes the following modules:

- Upgrade、Renew: Click Upgrade/Renewon the top right of the Overview page, you can upgrade to your Security Center to the Enterprise Edition, scale up your assets, or renew your Security Center service.

- Secure score: Safety score displays your assest's security score evaluated by Security Center, and the number of protected and unprotected assets. For specific score descriptions, see Safety score table.

  Click Fix Now to expand the Security Risk page. You can refer to the corresponding help documentation or directly address the risk immediately, based on the prompts on the page.

  Security Risk Handling contains all the security risks and threats that you need to address as quickly as possible, including the following categories:

  - Unhandled alerts
  - Unfixed vulnerability
  - Baseline risks
  - Cloud platform configuration risks
  - Other risks or threats such as attack events

- Asset status: View the number of assets for which you have installed and not installed the Agent plug-in, that is, assets that are already within the scope of Security Center and the number of assets that have not been protected by Security Center. And View the total number of risk assets present; view the number of servers, websites, and cloud products that are at risk.

  To add unprotected assets under the protection of Security Center, click the number under Unprotected Assets and on the displayed Install/Uninstall Security Center Agent page, install the Security Center agent. For more information, see Install Security Center agent.
- Threat Statistics: Threat statistics includes the number of unhandled alerts, unfixed vulnerabilities, baseline risks and attacks.
- Cloud Platform Configuration Risks: This module displays the detected baseline risks of your cloud products.
- Issues Resolved: This module displays the number of events, vulnerabilities, and vulnerable baseline configurations handled during the week in the form of column charts.

Upgrade to the Enterprise Edition, scale up assets, and renew your Security Center service

Security Center provides a Basic Edition, Advanced and an Enterprise Edition. You can view information on your specific edition in the upper-right corner of the Overview page. For more information on the differences in features of the Basic Edition and the Enterprise Edition, see Features.

- Basic Edition: The edition of Security Center is shown in the upper-right corner of the page. An Upgrade button is also displayed. If you upgrade your Security Center Basic Edition to the Advanced or Enterprise Edition, you are able to use such advanced functions as baseline checks, asset fingerprints, malicious processes (malware checking), and log analysis (needs to be purchased additionally).
- Advanced/Enterprise Edition: The expiration date of your Security Center service, and the size of your assets (the number of servers) are displayed in the upper-right corner of the page. A Renew button is also displayed.

> Note:
> If your current number of servers exceeds the number that you specified when purchasing Security Center, an Asset Scaling button is displayed in the upper-right corner of the page. To guarantee the availability of all features, we recommend that you scale up your assets.

Safety score table

Safety score	Description
95–100	Your assets are fully secured.
85–94	There are some security risks to your assets. We recommend that you strengthen the security of your servers and your system as soon as possible.
70–84	There are many security risks in your assets detected by Security Center. We highly recommend that you strengthen the security and protection of your system as soon as possible.
69 and lower	Your assets are exposed to security risks and may be easily compromised. We recommend that you immediately strengthen the security and protection of your system.

Table 1-1: Impacts to safety score table

Impact	Strengthening suggestion
Lack of a security operation center	Establish an in-depth defense system. If you have any queries, submit a ticket for technical support.
Unfixed vulnerabilities	Fix the vulnerabilities. For more information, see #unique_5.
Unhandled security events	Handle the security events in a timely manner.
Lack of host protection	Enable the enterprise edition of Server Guard.
The protection status is offline (the Security Center agent is not installed or offline).	Install the Security Center agent.
Web-CMS vulnerabilities	Fix the Web-CMS vulnerabilities.
System software vulnerabilities	Fix the software vulnerabilities.
Risks detected by baseline checks	Fix the vulnerabilities of baseline.
Unexpected logons	Check and handle the unexpected logons.
Webshell threats	Check and handle the webshell files.
Host exceptions	Handle the host exception events.

Threat statistics

The Overview page displays the statistics of the threats that Security Center detects in all your assets, and the corresponding trend diagrams, including:

- Events: Number of unhandled security events.
- Times of attacks: Number of attacks today.
- Vulnerabilities: Number of unhandled vulnerabilities.
- Baseline check: Number of vulnerable baseline configurations.